Security leaders seek to protect enterprise endpoints from attacks and breaches, and to offer efficient and secure remote access. As EDR matures and reaches wide adoption, XDR, UES and SASE emerge to offer ways to integrate stand-alone security solutions.

Table of Contents

Analysis..................................................................................................................................................2
What You Need to Know.................................................................................................................. 2
The Hype Cycle................................................................................................................................ 3
The Priority Matrix.............................................................................................................................4
Off the Hype Cycle........................................................................................................................... 5
On the Rise...................................................................................................................................... 6
Unified Endpoint Security............................................................................................................6
Extended Detection and Response.............................................................................................8
Business Email Compromise Protection....................................................................................9
At the Peak.....................................................................................................................................11
BYOPC Security..........................................................................................................................11
Secure Access Service Edge (SASE)........................................................................................ 13
Sliding Into the Trough.................................................................................................................... 15
In-App Protection..........................................................................................................................15
Browser Isolation..........................................................................................................................16
Device Endpoint Security for Frontline Workers..........................................................................19
Virtual Mobile Infrastructure.........................................................................................................20
Desktop as a Service......................................................................................................................21
Unified Endpoint Management....................................................................................................23
Mobile Threat Defense..................................................................................................................25
Zero Trust Network Access..........................................................................................................27
Climbing the Slope..........................................................................................................................29
Data Sanitization........................................................................................................................................... 29
Secure Instant Communications.................................................................................................................. 30
Endpoint Detection and Response.............................................................................................................. 32
Secure Web Gateways................................................................................................................................. 34
Cloud Access Security Brokers.................................................................................................................... 35
Secure Enterprise Data Communications..................................................................................................... 37
Entering the Plateau..................................................................................................................................... 38
Endpoint Protection Platforms.................................................................................................................... 38
Appendixes................................................................................................................................................ 41
Hype Cycle Phases, Benefit Ratings and Maturity Levels................................................................................. 42
Gartner Recommended Reading.................................................................................................................. 43

List of Tables

Table 1. Hype Cycle Phases.......................................................................................................................... 42
Table 2. Benefit Ratings............................................................................................................................... 42
Table 3. Maturity Levels.................................................................................................................................. 43

List of Figures

Figure 1. Hype Cycle for Endpoint Security, 2020......................................................................................... 4
Figure 2. Priority Matrix for Endpoint Security, 2020...................................................................................... 5
Figure 3. Hype Cycle for Endpoint Security, 2019............................................................................................. 41

Analysis

What You Need to Know

Endpoint security innovators have been focusing on better and more automated hunting, detection and remediation of threats, with endpoint detection and response (EDR) and extended detection and response (XDR) being in the spotlight. The abrupt surge in remote work has made secure remote access a priority, bringing back to the forefront BYOPC and VPNs for the short term, and emphasizing on SASE and ZTNA for the long term. Security leaders are asked to protect endpoints from attacks, while also allowing access from any device to any application over any network, with minimal impact on user experience. We illustrate the most relevant innovations in the endpoint security space, for security leaders to adopt and put in place to address these challenges.
The Hype Cycle

The Hype Cycle for Endpoint Security tracks the innovations that aid security leaders in protecting their enterprise endpoints from attacks and breaches. The technologies and practices in this space are being shaped by two trends: the continued growth of endpoint attacks and the sudden surge in remote working.

The growth of ransomware, fileless and phishing attacks has urged technology providers to innovate. To counter advanced attacks, it becomes crucial to correlate data from the endpoint and elsewhere when threat hunting; XDR has, therefore, entered the Hype Cycle for the first time. At the same time, the more mature EDR is growing in adoption and, while EPP is reaching its full maturity, the more recent concept of UES — which combines elements of EDR, EPP and MTD — is entering the Hype Cycle. Business email compromise (BEC) protection entered the Hype Cycle this year to counter phishing attacks. In addition, SWG, even though a network-based technology, is central to prevent attacks on endpoints and increasingly adopted by organizations, especially in its cloud-based implementation.

The recent global crisis has caused, among other things, a sharp increase in remote work. Technologies and practices that enable remote work that were reaching their full maturity — such as secure enterprise data communications (VPNs), CASB, BYOPC, UEM and DaaS — have come back into prominence and are experiencing a drastic increase in adoption by organizations as tactical solutions. A significant portion of that remote work will continue in the long term and will need a strategic solution.\(^1\) ZTNA, and its evolution into SASE, facilitates access from any device to any application over any network, and both ZTNA and SASE are gaining in adoption as they mature.
The Priority Matrix

A new wave has appeared in the Hype Cycle. Most of the innovations that are heading toward the Peak of Inflated Expectations involve security for multiple channels or multiple systems. For example, UES involves securing workstations, as well as smartphones and tablets, with a single product. Similarly, XDR’s scope goes beyond the endpoint, to combine information from multiple sources, such as the network, to detect threats. This technology trend is met with interest as 25% of end-user organizations participating in a Gartner survey in early 2020 were found to be currently pursuing a vendor consolidation strategy.²

At the peak this year, SASE allows any endpoint to access any application over any network in a protected manner. This is the one transformational innovation in the Hype Cycle for Endpoint Security, and security leaders should start putting in place a strategy that would make their investments in ZTNA and CASB converge along with SD-WAN into a SASE long-term outcome.

Some more mature technologies retreated along the curve as innovation tries to cope with new threats and provide detection techniques. This was the case for EDR and the more mature EPP, and
for in-app protection, which this past year had to cope with threats such as ransomware and web skimming, respectively.

Figure 2. Priority Matrix for Endpoint Security, 2020

### Priority Matrix for Endpoint Security, 2020

<table>
<thead>
<tr>
<th>benefit</th>
<th>years to mainstream adoption</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>less than two years</td>
</tr>
<tr>
<td>transformational</td>
<td></td>
</tr>
<tr>
<td>moderate</td>
<td>Endpoint Protection Platforms</td>
</tr>
<tr>
<td>low</td>
<td></td>
</tr>
</tbody>
</table>

Source: Gartner
ID: 49032

Off the Hype Cycle

Ten innovations were either removed or replaced in the Hype Cycle, either because they evolved to become features of broader technologies or have developed into tools that address more than security:

- Protected browsers have largely become a UEM feature.
- DLP for mobile devices is not something we see implemented as it is replaced by containment, provided by UEM or offered as integrated DLP from CASB suites.
Managed detection and response, while still very relevant in the security space, has become a feature of EDR solutions, and the newer XDR ones, for endpoint security.

The techniques used by user and entity behavior analytics have been embedded into a number of other innovations, such as EDR.

While crucial in the long term, useful approaches for IoT security remain network-oriented, largely limited by the poor state of legacy IoT devices.

Content collaboration platforms are still relevant for data leakage protection. However, the focus is on creating and maintaining a collaboration environment, and we did not include them in this iteration of the Hype Cycle.

Some security mechanisms are embedded into the various systems used transparently. In the case of trusted environments, mechanisms such as TEE on Android and secure enclaves on iOS are today commonly used by applications on these devices. Mobile identity and user authentication are two other examples.

With the newfound focus on remote work, BYOD has been replaced by BYOPC.

On the Rise

Unified Endpoint Security

**Analysis By:** Rob Smith

**Definition:** Similar to the convergence Gartner saw on endpoint management to a single unified endpoint management system, Gartner sees the evolution of endpoint security toward unified endpoint security. This innovation combines the main features of endpoint protection platform (EPP), endpoint detection and response (EDR), and mobile threat defense (MTD) into one solution. This solution has single console with threat analysis across all endpoint devices offering the ability to detect previously undiscoverable threats through cross-data analysis.

**Position and Adoption Speed Justification:** Vendors are embracing the initial unified endpoint security (UES) concept offering bundles of all components of endpoint security as a single license, single console interface, and in a few cases offering cross-platform analysis. The need for UES is being driven by IT demand for a single console for all security events. This has been accelerated by the recent COVID-19 crisis which has forced the need for IT to support whatever device the user has available. Like the unified endpoint management (UEM) market before it, UES will take a few years to mature and gain acceptance.

Successful vendors in UES will be those that can demonstrate significant productivity gains from the integration of security and operations and those that can rapidly process large amounts of data to detect previously unknown threats.

**User Advice:** Recent surveys show that the majority of IT organizations are considering security vendor consolidation. Too often though, combined systems don’t provide an overall best-of-breed solution but instead best-of-breed in some functionality. UES has the potential to be a single best-
of-breed solution for all of endpoint security provided the unified product’s cross-device data analytics is strong. This will require a vendor who understands both traditional client and mobile security to build a single threat detection framework regardless of the device type.

Organizations should evaluate UES adoption with two main goals in mind. On the one side to extend the detection and response beyond the traditional laptop and desktop endpoints, to mobile devices. In that sense the concept of UES is a subset of the concept of XDR, limited to endpoints. On the other, to obtain a single endpoint security management component from where to conduct security management for all enterprise endpoints.

One area for rapid UES adoption is in conjunction with a zero trust network access (ZTNA) system. As ZTNA increases in popularity, UES becomes a critical component in the continuous authentication process providing device security and telemetry data to improve the integrity of the connection.

Gartner has seen MTD deployed primarily to government, military, and other highly regulated organizations, but the technology is spreading to other verticals and companies as the need for mobile device security has increased dramatically. As part of a UES solution, MTD now offers the ability to deliver real-time user telemetry data such as if the user is on a public Wi-Fi or if the user’s PC and mobile are in the same location. This adds greater value to the overall security posture of the user.

Gartner also sees demand for UES to closely integrate with UEM to provide a single console for device management and security. This has the added benefit that as a security event occurs, policy can automatically be adjusted across all devices.

**Business Impact:** As the need to support any managed or unmanaged device from anywhere at any time becomes standard, the challenge to secure the device and obtain device integrity information increases. UES has the potential to integrate endpoint management and endpoint security to provide a lower total cost of ownership and better operations productivity. It also provides better security outcomes by reducing the complexity for IT to secure devices, improves visibility across all device types, and offers the potential to detect previously unknown threats — all from within a single console. This has an immediate benefit of lower support costs due to less consoles to manage and monitor. It also has the benefit of reducing risks of successful attacks by acting as a single integrated point for security improving detection and stopping attacks such as ransomware from spreading to other devices.

**Benefit Rating:** High

**Market Penetration:** 1% to 5% of target audience

**Maturity:** Emerging

**Sample Vendors:** BlackBerry; Broadcom (Symantec); Cybereason; Kaspersky; McAfee; Microsoft; Sophos; Tanium

**Recommended Reading:** “Magic Quadrant for Endpoint Protection Platforms”
"Market Guide for Endpoint Detection and Response Solutions"

"Market Guide for Mobile Threat Defense"

"Market Guide for Zero Trust Network Access"

Extended Detection and Response

**Analysis By:** Peter Firstbrook

**Definition:** Extended detection and response (XDR) is a vendor-specific, threat detection and incident response tool that unifies multiple security products into a security operations system. Primary functions include centralization and normalization of data in a repository for analysis and query, improved protection and detection sensitivity resulting from simplified configuration and security product coordination. The incident response capability can change the state of individual security products as part of the recovery process.

**Position and Adoption Speed Justification:** XDRs are similar in function to security information and event management (SIEM) and security orchestration, automation and response (SOAR) tools. However, XDRs are differentiated by the level of integration of vendor-specific products at deployment, and the focus on threat detection and incident response. Emerging XDR tools are primarily marketed by security solution providers that have a portfolio of infrastructure protection products, such as:

- Endpoint detection and response (EDR)
- Cloud access security broker (CASB)
- Secure email gateway (SEG)
- Secure Web Gateway (SWG)
- Firewalls
- Intrusion detection system (IDS)
- Identity infrastructure

More advanced XDRs are focusing up the stack by integrating with identity, data protection and application access. XDR products are still in the development phase, and numerous risks can derail this approach. Only a small list of vendors can truly offer an XDR and committing to an XDR could lead to overreliance on a single vendor. The large vendors that are capable of providing an XDR product often execute much slower than the best-of-breed startups in addressing new threats.

**User Advice:** XDR products will appeal to pragmatic security and risk management (SRM) leaders with limited resources who are seeking to reduce the total cost and complexity of their security infrastructures and improving their proactive hardening and incident response capabilities. Prospective buyers should work with stakeholders to determine whether an XDR strategy is right for your organization, based on staffing and productivity levels, level of federation of IT, risk tolerance, and security budget.
Develop an internal architecture and purchasing policy that is in line with your XDR strategy, including when and why exceptions might be permissible. Ensure that future security purchases and planned technology retirements are aligned with a long-term XDR architecture strategy. Focus product evaluations on the relevance and quality of integrated security tools, the productivity gain of the security operations center and improvements in detection fidelity.

**Business Impact:** XDR vendors can deliver a unified portfolio of critical security functions. They can provide more-accurate detection and prevention capability and lower total cost of ownership (TCO), driven by higher-security operations productivity and lower acquisition costs, as well as faster time to value, than most security solutions stacks.

**Benefit Rating:** High

**Market Penetration:** Less than 1% of target audience

**Maturity:** Emerging

**Sample Vendors:** Cisco; FireEye; Fortinet; McAfee; Microsoft; Palo Alto Networks; Sophos; Symantec; Trend Micro

**Recommended Reading:** “Innovation Insight for Extended Detection and Response”

“Use Central Log Management for Security Operations Use Cases”

“SOAR: Assessing Readiness Through Use-Case Analysis”

“Magic Quadrant for Security Information and Event Management”

**Business Email Compromise Protection**

**Analysis By:** Mark Harris

**Definition:** Business email compromise (BEC) protection detects and filters malicious emails that fraudulently impersonate business associates to misdirect funds or data.

BEC messages typically do not include malicious links or attachments making them very difficult to identify. Attackers are often well-informed by publicly available information (i.e., LinkedIn) to increase their effectiveness. State-of-the-art techniques to detecting BEC include natural language and social graph analysis that can detect deviations from historical communication patterns.

**Position and Adoption Speed Justification:** BEC attacks are often well-crafted to impersonate business associates, do not include links or attachments, and often exploit compromised email accounts, making them very difficult to identify.

Techniques for detecting BEC include:

- Natural language analysis (NLA) and natural language understanding (NLU) to identify requests for transfer of payments
Relationship analysis using machine learning trained on historical communication patterns between individuals

Sender verification technologies such as DMARC to verify the source of the email

Vendors often use a combination of these techniques to improve accuracy and some have even gone as far as trying to recognize the typing patterns of individuals to detect intruders.

Achieving accurate results can be challenging so often are limited to warning the user, which can lead to “warning” fatigue where a user simply ignores the notification. Although machine learning and NLU are relatively mature techniques, their application to email security and in particular BEC has only appeared over the past couple of years. Adoption rates are low at present and as the technology matures expect this to be part of a complete email security solution rather than a stand-alone supplemental product.

**User Advice:** Security and risk management leaders should review existing email security solutions to ensure that BEC and internal email protection is included. Either upgrade existing email security solutions to include specific BEC protection or supplement existing controls with a cloud email security supplement that specifically targets BEC. In addition, other controls are needed including user education, multifactor authentication and improved operating procedures including authenticating email requests for financial or data transactions and using payment portals.

**Business Impact:** BEC attacks continue to pose a significant risk to all industries and segments. These attacks are often relatively low-tech and highly targeted at valuable individuals such as the CEO. According to the FBI, there was $1.8 billion dollar losses in BEC attacks in 2019, in the U.S.

The damage caused by these attacks reaches well-beyond financial losses. Fraudulent invoices are the most common method of BEC attacks. In such an attack, the recipient receives what appears to be a legitimate invoice from an organization. Fraudulent invoices accounted for 39% of such attacks in 2018, posing an internal risk to organizations and a reputation risk. If a supplier or customer falls for a BEC attack that purports to come from a known organization, it can harm the established trust in the existing relationship as well.

**Benefit Rating:** High

**Market Penetration:** 1% to 5% of target audience

**Maturity:** Emerging

**Sample Vendors:** Abnormal Security; Armorblox; Mimecast; Proofpoint

**Recommended Reading:** “Cool Vendors in Cloud Office Security”

“Protecting Against Business Email Compromise Phishing”

“Market Guide for Email Security”
BYOPC Security

**Analysis By:** Rob Smith; Stephen Kleynhans

**Definition:** Bring your own PC (BYOPC) is an endpoint deployment strategy that allows employees to use a personally selected and purchased client device to execute enterprise applications and access company services and data. It typically spans PCs, Macs, and Chromebooks. BYOPC poses serious potential security threats due to unmanaged, unpatched, and infected user equipment.

**Position and Adoption Speed Justification:** Adoption of BYOPC is strong due to the COVID-19 pandemic as organizations simply had no other alternative. Long-term adoption will vary based on hardware availability and IT’s desire to provide and manage PCs to work-from-home users. Regardless of the number of BYOPC devices, security risks remain high for BYOPC forcing immediate adoption of new tools to secure access to data and applications from these devices. Gartner expects adoption to increase as IT perfects additional technologies such as cloud apps, virtualized apps, and DaaS. For those organizations that do not embrace cloud, adoption will decrease as hardware supply returns.

**User Advice:** Prior to the COVID-19 crisis, there was little interest in BYOPC. However, due to an urgent need to enable working from home for employees and a lack of available hardware, it has become widely adopted in a short timespan posing new and significant security risks. Expect the need to support BYOPC to be dependent upon a long-term work-from-home strategy. Also expect to support security tools needed for a BYOPC environment.

It is important to note that Gartner always recommends providing the user with a device that is managed and secure over using a BYOPC. But due to global circumstances, BYOPC has become a necessary strategy that requires specific security practices to be in place.

Best security practices for BYOPC include:

- Assume that any BYOPC device has malware or ransomware and should never be trusted. This is a high priority.
- Enabling multifactor authentication (MFA) for all access to any corporate resource regardless if virtual or not and if cloud or on-premises. This is a high priority.
- Contain all cloud application data. Do not allow local storage or upload of local data from any BYOPC device as this could infect the cloud system. This is a high priority.
- Consider using a cloud access security broker (CASB) or a zero trust network access (ZTNA) solution for any access to cloud applications. This is a medium priority.
- For long-term employee usage, enable desktop as a service (DaaS) to replicate an employee’s desktop without the need to manage the BYOPC. This is a medium priority.
- Virtualize access to any traditional on-premises application. This is a high priority.

- Supporting a BYOPC is a difficult challenge. This is why Gartner recommends DaaS, virtualized apps, or cloud services instead so the BYOPC is essentially a dumb terminal. This is a high priority.

- Under no circumstances should normal remote VPN access be allowed from a BYOPC as it poses a serious risk of a ransomware infection. This is a high priority.

- Define a policy for BYOPC that stipulates minimum standards expected of users (including but not limited to: a supported and patched OS from Microsoft/Apple/Google/others, a supported and updated anti-malware solution, completion of cybersecurity awareness). This is a medium priority.

- Understand the risks from other household members potentially using the same device and potentially the same local account. This is a medium priority.

Following the above suggestions will significantly reduce the security risk of enabling BYOPC.

**Business Impact:** BYOPC vastly increases the number of workers that have access to enterprise data and applications without the need for an additional investment in corporate hardware or dedicated office space. However, it poses serious security risks as these devices are often infected with malware or ransomware and fall victim to phishing attacks. As such, IT must be prepared to limit and control access to any BYOPC device. This means offsetting the PC hardware investment with critical security technologies such as MFA, CASB, ZTNA, VDI, and DaaS. Without investment in these technologies, IT faces a much higher potential cost in the form of ransomware. Also, it is critical that IT work with HR, legal, and workers councils to develop a proper work-from-home policy. The policy is critical in order to limit any exposure due to the new work-from-home reality.

**Benefit Rating:** Transformational

**Market Penetration:** 5% to 20% of target audience

**Maturity:** Adolescent

**Sample Vendors:** Cisco Systems; Citrix; Google; Microsoft Azure; Okta; VMware

**Recommended Reading:** “Solving the Challenges of Modern Remote Access”


“Physical, Virtual and Cloud Desktops: Is a Hybrid Approach Inevitable?”

“Market Guide for Zero Trust Network Access”

“Magic Quadrant for Cloud Access Security Brokers”

“Toolkit: Remote Work Policies”
Secure Access Service Edge (SASE)

**Analysis By:** Joe Skorupa; Neil MacDonald

**Definition:** Secure access service edge (SASE, pronounced “sassy”) delivers multiple capabilities such as SD-WAN, SWG, CASB, NGFW and zero trust network access (ZTNA).

SASE supports branch office and remote worker access. SASE is delivered as a service, and based upon the identity of the device/entity, combined with real-time context and security/compliance policies. Identities can be associated with people, devices, IoT or edge computing locations.

**Position and Adoption Speed Justification:** SASE is driven by enterprise digital business transformation: the adoption of cloud-based services by distributed and mobile workforces; edge computing and business continuity plans that must include flexible, anywhere, anytime, secure remote access. While the term originated in 2019, the architecture has been deployed by early adopters as early as 2017. By 2024, at least 40% of enterprises will have explicit strategies to adopt SASE, up from less than 1% at year-end 2018.

By 2023, 20% of enterprises will have adopted SWG, CASB, ZTNA and branch FWaaS capabilities from the same vendor, up from less than 5% in 2019. However, today most implementations involve two vendors (SD-WAN + Network Security), although single vendor solutions are appearing. Dual-vendor deployments that have deep cross-vendor integration are highly functional and largely eliminate the need to deploy anything more than a L4 stateful firewall in the branch office. This will drive a new wave of consolidation as vendors struggle to invest to compete in this highly disruptive, rapidly evolving landscape.

SASE is in the early stages of market development but is being actively marketed and developed by the vendor community. Although the term is relatively new, the architectural approach (cloud if you can, on-premises if you must) has been deployed for at least two years. The inversion of networking and network security patterns as users, devices and services leave the traditional enterprise perimeter will transform the competitive landscape for network and network security as a service over the next decade, although the winners and losers will be apparent by 2022. True SASE services are cloud-native — dynamically scalable, globally accessible, typically microservices-based and multitenant. The breadth of services required to fulfill the broad use cases means very few vendors will offer a complete solution in 2020, although many already deliver a broad set of capabilities. Multiple incumbent networking and network security vendors are developing new or enhancing existing cloud-delivery-based capabilities.

**User Advice:** There have been more than a dozen SASE announcements over the past 12 months by vendors seeking to stake out their position in this extremely competitive market. There will be a great deal of slideware and marketecture, especially from incumbents that are ill-prepared for the cloud-based delivery as a service model and the investments required for distributed PoPs. This is a case where software architecture and implementation matters.

When evaluating SASE offering, be sure to:
- Involve your CISO and lead network architect when evaluating offerings and roadmaps from incumbent and emerging vendors as SASE cuts across traditional technology boundaries.
- Leverage a WAN refresh, firewall refresh, VPN refresh or SD-WAN deployment to drive the redesign of your network and network security architectures.
- Strive for not more than two vendors to deliver all core services.
- Use cost-cutting initiatives in 2020 from MPLS offload to fund branch office and workforce transformation via adoption of SASE.
- Understand what capabilities you require in terms of networking and security, including latency, throughput, geographic coverage and endpoint types.
- Combine branch office and secure remote access in a single implementation, even if the transition will occur over an extended period.
- Avoid vendors that propose to deliver the broad set of services by linking a large number of products via virtual machine service chaining.
- Prioritize use cases where SASE drives measurable business value. Mobile workforce, contractor access and edge computing applications that are latency sensitive are three likely opportunities.

Some buyers will implement a well-integrated dual vendor best-of-breed strategy while others will select a single vendor approach. Expect resistance from team members that are wedded to appliance-based deployments.

**Business Impact:** SASE will enable I&O and security teams to deliver the rich set of secure networking and security services in a consistent and integrated manner to support the needs of digital business transformation, edge computing and workforce mobility. This will enable new digital business use cases (such as digital ecosystem and mobile workforce enablement) with increased ease of use, while at the same time reducing costs and complexity via vendor consolidation and dedicated circuit offload.

COVID-19 has highlighted the need for business continuity plans that include flexible, anywhere, anytime, secure remote access, at scale, even from untrusted devices. SASE’s cloud-delivered set of services, including zero trust network access, is driving rapid adoption of SASE.

**Benefit Rating:** Transformational

**Market Penetration:** 1% to 5% of target audience

**Maturity:** Emerging

**Sample Vendors:** Akamai; Cato Networks; Cisco; Citrix; iboss; Netskope; Open Systems; Palo Alto Networks; VMware; Zscaler

**Recommended Reading:** “The Future of Network Security Is in the Cloud”

“Magic Quadrant for Cloud Access Security Brokers”
In-app Protection

**Analysis By:** Dionisio Zumerle

**Definition:** In-app protection refers to protection capabilities that are implemented within the application (instead of the network or the operating system) to prevent and detect a variety of attacks such as malicious data exfiltration, intrusion, script injection, tampering and reverse engineering.

**Position and Adoption Speed Justification:** In-app protection is well-suited for applications that have their software logic distributed on various untrusted environments. This is increasingly the case with single-page and progressive web applications, as well as with software running on connected and mobile devices.

In-app protection encompasses a variety of passive and active defenses. It initially revolved around application shielding, a technology space that provides hardening protection such as code obfuscation and white-box cryptography.

Increasingly end-user requirements have made vendors focus on anti-tampering protections such as application monitoring, runtime application protection, anti-malware and anti-bot.

Hardening techniques are mature but have to be adapted to new devices and operating systems, such as the mobile ones. Anti-tampering techniques are newer and their maturity is low. Additionally, in-app protection techniques must keep the pace of newer and advanced attacks and, therefore, are in constant evolution themselves. With the newly found focus on protecting modern web applications, the maturity of the innovation recently decreased.

Adoption is growing as developers are becoming more aware of the availability of these solutions and attacks become more prominent.

**User Advice:** Organizations should use in-app protection for mobile applications, web applications with client-side JavaScript and software on IoT devices. The candidate application must distribute the software logic onto untrusted environments, and access either transactional or sensitive data. Banking, retail, e-commerce, insurance and healthcare providers are examples of organizations that should adopt in-app protection. Special consideration should be placed onto consumer-facing applications.
There are various ways to implement in-app protection and can be categorized as in-code, in-workload, in-browser and postcoding. Depending on the implementation, in-app protection may or may not require substantial changes to the source code, and may or may not require recompilation. Solutions that intervene on the binary are quicker to implement but will prove to be more platform-bound and more impacted by significant platform changes.

While available from stand-alone in-app protection providers, many WAAP providers are adding in-app protection in their portfolio, either through acquisition or partnership, making it easier for organizations to adopt this technology.

**Business Impact:** In-app protection should be used to instill self-defending mechanisms into an application. By monitoring the application workload, in-app protection provides insight into the interactions of distributed application components, improving detection capabilities compared to solely relying on WAF and perimeter protections.

In-app protection can also be used to improve user experience. For example, by hardening the application, an online retailer can minimize the number of step-up authentication requests made to its customers.

The application shielding techniques of in-app protection, such as code obfuscation, can serve as a dissuasive measure as it makes it harder for attackers to attack an application.

**Benefit Rating:** High

**Market Penetration:** 5% to 20% of target audience

**Maturity:** Adolescent

**Sample Vendors:** Arxan; Build38; F5; Guardsquare; Imperva; Intertrust; Jscrambler; OneSpan; PerimeterX; Promon

**Recommended Reading:** “Teach Your Applications the Art of Self-Defense”
“Market Guide for In-App Protection”
“Protecting Web Applications and APIs From Exploits and Abuse”
“Building Security Into Mobile Apps Using Checklists, SDKs, App Wrapping and App Hardening”

**Browser Isolation**

**Analysis By:** Neil MacDonald

**Definition:** Browser isolation is the strong separation of the browsing process from the end-user system to protect the system, its network and its resources from attacks that are carried out via the browser or to protect a sensitive application from a potentially compromised browser. Browser isolation is achieved using two main approaches: (1) remote browser isolation and (2) local browser
isolation. At this time, the more mature of the two, with a larger number of vendor alternatives, is remote browser isolation.

**Position and Adoption Speed Justification:** Most organizations use URL filtering in the form of secure web gateways (SWGs) to protect their users and devices from the evils of the internet; and organizations have been slow to adopt browser isolation technologies. However, as demonstrated by the recent surge in ransomware, attacks still get through. Rather than allowing potentially hostile content in from the web, browser isolation strategies keep the session isolated (much like a suspicious package being opened by a remote-controlled robot).

There are two primary approaches:

- Remote browser isolation is conceptually like VDI; every browser session is remotely presented from a browser server and treated as if it might have been compromised. And, ideally, every session is reset back to a known good state from immutable templates when completed. With remote browser isolation, all webpages are rendered remotely, and an image or document object model of the website is sent to the user’s local browser. Unlike VDI, nearly all remote browser solutions use Linux and containers to increase hardware densities and reduce licensing costs. Some vendors offer on-premises deployment options, while others are entirely cloud-based. Remote browser isolation capabilities are available from many point solution vendors and are also available as separately charged features from some larger security platform offerings such as secure email and web gateways; and, indeed, multiple acquisitions have already occurred. For example, Zscaler recently acquired Appsfolute and McAfee acquired Light Point security. Further, we see RBI being a critical capability in the future delivery of a secure access service edge (SASE), supporting integration with SWG, CASB and ZTNA services. RBI also is used in the reverse direction when unmanaged devices are accessing sensitive data and applications. By controlling the browser used to access the application and data, this gives information security a critical control point when dealing with unmanaged and potentially compromised devices to add capabilities like sensitive data monitoring and protection from bot-based attacks.

- In contrast, local browser isolation attempts to isolate the browsing process from the rest of the end user’s desktop using software-based isolation techniques such as running a separate VM, or using underlying hardware-based isolation. Microsoft released local browser isolation capabilities with Windows Defender Application Guard with Windows 10. There are a very small number of vendors that provide local browser isolation using this model and they are forced to offer compatibility with Microsoft’s approach.

**User Advice:**

- Evaluate and pilot a browser isolation solution for specific high-risk users, such as finance, or use cases such as rendering email-based URLs, particularly if your organization is risk-averse.

- Pressure your SWG, CASB and/or SEG vendor to provide remote browser isolation as an optional defense-in-depth protection option.
Start with a limited number of users and by selectively isolating a limited number of URLs, then expand the use cases.

Focus on higher-risk individuals that are more likely to be targeted, such as in the executive office, research and development, or finance (for example, payment processing). Alternatively, focus on uncategorized URLs (which are inherently more risky) or those URLs with low reputation scores to isolate.

Favor remote browser solutions that don’t require a local agent or application to be installed, and instead use HTML5 to deliver remote sessions to the user’s local modern browser for access. Evaluate different vendor approaches for rendering based on performance and bandwidth.

Evaluate different vendor approaches for rendering based on performance, latency and bandwidth requirements.

Design and implement a capability for content movement from the public internet into enterprise systems, but only after intensive scanning using multilayered threat detection techniques.

Sign one- to two-year contracts only, because the market is in flux with downward pricing pressure.

**Business Impact:** Most attacks are delivered via the public internet either through web browsing or emailed links that trick the user into visiting malicious sites. Simply removing (or more strongly, isolating) the browser from the end user’s desktop significantly improves enterprise security posture. Through 2022, organizations that isolate high-risk internet browsing and access to URLs in email will experience a 70% reduction in attacks that compromise end-user systems. Notably, remote browser isolation can thwart ransomware attacks, blocking their ability to encrypt the users’ files on their devices or in enterprise file shares, neither of which are directly accessible from the remote browser session.

**Benefit Rating:** High

**Market Penetration:** 5% to 20% of target audience

**Maturity:** Adolescent

**Sample Vendors:** Authentic8; Cyberinc; Ericom Software; Garrison; Hysolate; McAfee; Menlo Security; Proofpoint; Symantec; Zscaler

**Recommended Reading:** “Innovation Insight for Remote Browser Isolation”

“Magic Quadrant for Secure Web Gateways”

“Quick Answer: Cost Effectively Scaling Secure Access While Preparing for a Remote Workforce”

“The Future of Network Security Is in the Cloud”
Device Endpoint Security for Frontline Workers

**Analysis By:** Patrick Hevesi

**Definition:** Device endpoint security for frontline workers includes a set of technologies that provide protection for purpose-built devices and their users. Depending on the industry and use cases of the frontline worker, devices may need to be physically secured to permanent stations, tracked and checked out for use during a shift, or possibly used by multiple users in a particular area.

**Position and Adoption Speed Justification:** Many frontline workers have fully managed, purpose-built, locked-down, ruggedized mobile devices tailored to their job. These devices come at a premium and can cause challenges for keeping the devices up to date and patched to maintain their security. This has led to some organizations and vendors to explore personal devices with protection around the mobile applications, but this provides less control than a fully managed device and can open up the organization to data leakage or other malicious attacks. More companies have also begun to enable frontline workers with access to cloud SaaS applications, which exposes organizations and workers to additional cloud security risks.

**User Advice:** For company-owned and managed devices where more specialized devices are required:

- Evaluate and deploy specialized devices for purpose-built frontline worker use cases.
- Fully manage and lock down the devices with UEM/MAM, and ensure that mobile OS security settings, updates and patches are applied.
- Ensure physical security for mobile devices, including cables for kiosks, geofencing/geolocation for on-the-move devices, and check-in and check-out processes for multiuse devices.

For personally owned or consumer-grade devices, where LOB and other corporate collaboration apps are allowed to run:

- Use UEM tools to apply mobile application management (MAM) policies to add layers or encryption, MFA and time-based lockout on frontline worker apps.
- Look to mobile threat defense vendors for device-based risk attestation integrated with the applications managed by MAM.

For custom-built frontline worker apps:

- Ensure LOB applications are engineered with secure design principles and custom-built multiuser authentication.
- Employ MAST and MARS for assessing mobile apps for risks, such as for the purpose of mobile app catalog vetting in EMM.
- Use app shielding, app wrapping and in-app MTD (or more generally, “in-app protection”) for protecting your IP within binaries, and also protecting apps in runtime on a given device.
If cloud-based applications are used, we recommend using CASBs for threat and data protection, as well as adaptive access control for frontline users and devices when they consume external SaaS services.

**Business Impact:** Frontline mobile devices will, in many cases, be off-premises and possibly handled by customers, contractors, temporary staff and employees. Frontline scenarios often involve access to sensitive and critical systems, such as industrial controls, which raises the risk profiles and the related precautions.

IT security will have to deploy a combination of multiple solutions to mitigate all the possible use cases and security risks. As some of the solutions are built for traditional mobile management scenarios and not frontline workers, custom development work may be required to meet the security requirements.

**Benefit Rating:** Moderate

**Market Penetration:** 5% to 20% of target audience

**Maturity:** Early mainstream

**Sample Vendors:** CommuniTake; Imprivata (GroundControl); Lookout; Microsoft; Samsung; SOTI; Symantec; Veracode; Zebra; Zimperium

**Recommended Reading:** “Protecting Web Apps and APIs from Exploits and Abuse”

“Market Guide for Mobile Threat Defense”

“Mobile OSs and Device Security: A Comparison of Platforms”

“Advance and Improve Your Mobile Security Strategy”

**Virtual Mobile Infrastructure**

**Analysis By:** Dionisio Zumerle

**Definition:** Virtual mobile infrastructure (VMI) provides remote access to a mobile workspace that hosts enterprise apps and data. The workspace can be accessed via a local app on iOS and Android devices. The virtual environment itself is based on a remote instance of Android.

**Position and Adoption Speed Justification:** VMI solutions provide secure access to enterprise information and minimize data loss risks as they do not store data on the mobile device. A user can quickly log in and log out from an account without leaving data on the device, and the tailored VMI experience takes away user experience issues that are present with virtualized Windows environments run on mobile form factors. Where VMI runs over an iOS device, it provides the flexibility of Android, combined with the consistency of the iOS devices.

VMI takes a mature virtualization technology and adapts it to the less mature iOS and Android mobile operating systems. The technological maturity of this implementation is increasing, but there are some limitations. The most obvious one is that VMI provides limited to no offline functionality.
and most solutions require a reliable high-speed connection to operate. Also, VMI solutions cannot use Google Play services. While VMI accesses some sensors such as microphone and camera, it is limited and not ideal for applications that need real-time usage of the local device sensors, such as extended reality and immersive computing applications.

**User Advice:** While VMI’s limitations make it unsuitable for most mainstream mobility scenarios, it can simplify access to enterprise apps and data, and reduce data leakage in specific use cases. VMI can be an option in shared-device scenarios for high-security environments, especially ones with good connectivity. With the sharp increase in remote working, VMI can provide a quick solution for organizations that need to provide access to users on their mobile devices, including BYOD ones, as the VMI environment is separate from any personal usage of the tablet or smartphone.

**Business Impact:** VMI is well-suited for use cases and industries where enterprises must trade off user experience in favor of increased data security. VMI can be used by frontline workers in regulated industries such as energy and gas, or in high-security manufacturing, especially where devices must be shared because of shifts or other reasons. VMI can be used by nurses sharing tablets in hospitals, or by students sharing tablets in schools. We do not foresee mainstream adoption for B2E and highly mobile use cases.

**Benefit Rating:** Low

**Market Penetration:** Less than 1% of target audience

**Maturity:** Adolescent

**Sample Vendors:** Avast; Hypori; Nubo; Raytheon; Sierraware; Trend Micro

**Desktop as a Service**

**Analysis By:** Nathan Hill; Stuart Downes, Michael Silver

**Definition:** Desktop as a service (DaaS) is a service offering that provides users with an on-demand, virtualized desktop experience delivered from a remotely hosted location. It includes provisioning, patching and maintenance of the management plane and resources to host workloads.

**Position and Adoption Speed Justification:** Organizations have long been interested in adopting virtual desktop infrastructure (VDI), but complexity and capital investment have made VDI implementations difficult. Relying on a service provider to take on the risk of platform build-out and to provide high-volume computing services is an attractive alternative for organizations that want to deliver applications on a device-neutral basis.

DaaS vendors originate from a software, cloud or hosting backgrounds. Some own the complete platform (such as Amazon WorkSpaces and Microsoft Windows Virtual Desktop), while others leverage hyperscale platforms, especially from Amazon and Microsoft, to bring a service-brokered offering to market.
The adoption of cloud office and SaaS increases the viability of a DaaS solution as an organization’s data and services become increasingly externalized, especially when supporting highly geographically dispersed workers. This, coupled with the entry of Microsoft into the market, has injected a significant amount of hype back into DaaS. Microsoft isn’t the only DaaS choice, but it heavily influences digital workplace I&O leaders’ thinking, due to Microsoft’s control points in the ecosystem. DaaS is moving toward the Trough of Disillusionment partly because of greater understanding of its long-term cost implications, but also as knowledge of all strengths and weaknesses become more widely understood.

COVID-19 has highlighted the value and business continuity strength of DaaS in its ability to rapidly enable remote work where on-premises options have stalled due to issues with data center access and infrastructure supply chains. COVID-19 is likely to accelerate adoption of DaaS, and may perpetuate as a delivery architecture even when employees return to the office.

**User Advice:** Enterprises should consider DaaS for use cases related to transient access requirements, business continuity needs or accelerating business goals. The typically high total cost of ownership (TCO) makes it hard to justify DaaS, but COVID-19 has highlighted it as a very strong solution for remote working and work-from-home scenarios. Organizations should not hesitate to conduct a proof of concept (POC) to gain a better understanding of how this service can benefit their organization.

Use DaaS for:

- Short-term employees, such as seasonal workers, where user volumes spike, or for workspace provisioning to third parties and contractors. The per-user/per-month common billing approach makes this ideal to avoid asset-loss risk and to reduce the provisioning lead time associated with notebooks.
- Merger and acquisition (M&A). As with short-term employees, VDI can help with M&As, but the lead time for infrastructure procurement and underutilized capacity may make DaaS a better fit to accelerate the M&A process, even if only temporarily.
- Remote workers. DaaS can extend the workspace to remote users, especially with hyperscale solutions that have deep global penetration, and may be preferable to expanding an existing data center or colocation footprint.
- Business continuity. DaaS can be used as a workspace recovery solution and has proven a successful solution during COVID-19, enabling organizations to securely extend work from home.

Graphics-enabled DaaS extends the service to designer use cases. However, the cost differential compared with on-premises VDI and the performance sensitivity can be even greater here. Organizations must test functionality and performance thoroughly. Look to combine DaaS with other services provided from the same cloud provider to improve network connectivity to the cloud (such as SLA-backed, dedicated links) to optimize performance.

For smaller organizations that are aggressively migrating to cloud services and have fewer legacy integration challenges, the adoption of DaaS as a complete workforce solution is likely to be more
viable. Typically, these organizations do not want to invest capital expenditure (capex) in data center infrastructures and operating expenditure (opex) in associated administration staff, if this distracts them from their core business goals.

**Business Impact:** DaaS has suffered from the challenges associated with the technologies that power it, namely server-based computing (SBC) and VDI. Cost, complexity and connectivity have all been inhibitors. However, with more organizations looking to deliver user-centric services across different devices and locations with an ever-increasing consumption of cloud services (SaaS, storage and productivity tools), DaaS is considered a strategic solution. The benefits of the “pay-per-use” utility of the DaaS opex model have gained mind share, as has the entry of Microsoft into the market. However, the service needs to be able to deliver a complete workspace solution for it to be viable as a primary business platform. Growth in adoption through the COVID-19 pandemic is helping to accelerate maturity in the service, but hype still remains.

Many DaaS vendors are expanding their service portfolio beyond simple OS hosting to deliver a complete workspace management life cycle solution. However, organizations that are totally reliant on browser-agnostic web applications will question the need for a Windows OS-based workspace intermediary.

**Benefit Rating:** High

**Market Penetration:** 5% to 20% of target audience

**Maturity:** Early mainstream

**Sample Vendors:** Amazon; Citrix; Dizo; Dizzion; Evolve IP; Microsoft; Nutanix; Tehama; VMware; Workspot

**Recommended Reading:**
- “Market Guide for Desktop as a Service”
- “Forecast Analysis: Desktop as a Service, Worldwide”
- “Microsoft’s WVD Will Accelerate Virtual Desktop Maturity but May Not Lower Total Cost of Ownership Enough”
- “Physical, Virtual and Cloud Desktops: Is a Hybrid Approach Inevitable?”
- “How to Keep End Users Connected to the Digital Workplace During Disruptions”

**Unified Endpoint Management**

**Analysis By:** Dan Wilson; Chris Silva

**Definition:** UEM is a set of offerings that comprise management of mobile devices (MDM) and personal computers via traditional client management technology (CMT) or modern OS management. This is through a single console that combines the application of data protection, device configuration and usage policies. UEM tools use analytics and telemetry from users, apps
and devices to inform policy and related actions; and integrate with Unified Endpoint Security (UES) tools to enhance policy management and enable frictionless authentication.

**Position and Adoption Speed Justification:** Gartner has long described the evolution to UEM as a journey through three waves:

1. Using separate tools for PCs and mobile devices (traditional management)
2. Using the same management product, but different processes, for PCs and mobile devices
3. True convergence — PCs and mobile devices are managed through the mobile device management (MDM) APIs provided by the OS, whether it’s Apple iOS or macOS, Google Android, or Microsoft Windows.

Now we are seeing UEM expand beyond the management of PCs and mobile devices to offer deeper insights through endpoint analytics and deeper integration with identity and access management and unified endpoint security tools. In addition to the base UEM capabilities, many vendors are expanding their offering to differentiate. While Gartner is seeing some clients embrace UEM tools and modern OS management, most organizations are still seeing UEM as a roadmap item to be addressed in the next few years. In preparation for UEM, organizations must do three things:

- Modernize application stacks, removing dependencies of critical apps on a specific platform or a specific browser/runtime environment.
- Consolidate mobile and endpoint management teams to eliminate political barriers to UEM adoption.
- Upskill staff to understand how to address the critical functions of CMT with UEM techniques.

Hype is moving toward the trough. Interest in UEM remains strong and use-case-driven, yet many organizations revealed the significant processes and technology changes that are required for modernizing management.

**User Advice:** Clients should stop procuring and consider not renewing licenses for disparate MDM, EMM and CMT tools. They should review existing entitlements to determine the most cost-effective and best fit UEM solution to adopt to replace those tools in the next year. They should investigate the potential to embrace modern OS management using the UEM products in the next two years.

**Business Impact:** Taking full advantage of UEM disrupts long-standing traditional processes, tools and organizational designs. It will require a new approach, consolidated organization and significant process reengineering, but has several benefits:

- Simplifies management of continuous OS updates.
- Enables management of devices regardless of their connection (on LAN, VPN, or internet connected).
- Support a wider range of devices and operating systems.
- Enables internet-based patching, policy, configuration management.
- Reduces the total cost of ownership (TCO) of managing endpoint devices by simplifying device management and support processes.
- Supports tool portfolio rationalization and reduction efforts.
- Establishes a baseline for integrated Unified Endpoint Security tools to provide continuous, contextual authentication and controls.

**Benefit Rating:** High

**Market Penetration:** 20% to 50% of target audience

**Maturity:** Early mainstream

**Sample Vendors:** BlackBerry; Citrix; IBM; Ivanti; ManageEngine; Matrix42; Microsoft; MobileIron; Sophos; VMware

**Recommended Reading:**
- “How to Keep End Users Connected to the Digital Workplace During Disruptions”
- “Essential Considerations When Choosing Separate PC and Mobile Management Tools”
- “Adopt Continuous Endpoint Engineering and Modern Management to Ensure Digital Workplace Success”
- “Prepare for Unified Endpoint Management to Displace MDM and CMT”
- “Magic Quadrant for Unified Endpoint Management Tools”
- “Solution Criteria for Unified Endpoint Management Systems”

**Mobile Threat Defense**

**Analysis By:** Dionisio Zumerle

**Definition:** Mobile threat defense (MTD) solutions protect organizations from threats on iOS and Android mobile devices. MTD solutions provide prevention, detection and remediation at the device, network and application levels.

**Position and Adoption Speed Justification:** Enterprises adopt MTD solutions to counter mobile threats. Most often they integrate MTD with their UEM, to increase their security capabilities. However, organizations increasingly use MTD on unmanaged devices, such as in BYOD scenarios. The main use cases that drive adoption are mobile phishing, mobile endpoint detection and response (EDR), app vetting and device vulnerability management.

MTD solutions have reached a level of maturity that makes them suitable for wide enterprise adoption. After a period of intense innovation, MTD innovation has slowed down. In addition to innovation to counter the evolving mobile malware, innovation also focuses on improving the MTD user experience on the device, for example, when providing phishing protection.
MTD adoption has been slower than what the mobile security hype purported, as the industry awaited highly visible or publicized mobile breaches that did not occur. Still, regulated industries and enterprises with high-security requirements have adopted MTD solutions. In their attempt to build a unified endpoint security (UES) offering, endpoint protection platform (EPP) vendors have acquired smaller MTD vendors, others partner with stand-alone MTD vendors, while recently some EPP vendors have been introducing their own MTD homegrown solutions. The availability of MTD through EPP vendors has made adoption easier for enterprises.

**User Advice:** In addition to a basic security baseline that the average UEM can provide, organizations should perform application vetting and device vulnerability management. Where the current tools do not suffice to do so, enterprises should adopt MTD solutions to improve endpoint security hygiene. Device vulnerability management complexity is particularly accentuated where enterprises operate large fleets of Android devices and these organizations should prioritize the adoption of MTD.

Enterprises that have chosen an unmanaged approach should look into MTD to protect their infrastructure from threats from unmanaged mobile devices. For example, certain MTD tools integrate with Microsoft Outlook, Microsoft Office 365 suite, as well as other popular enterprise suites and managed enterprise apps to provide ZTNA functionality on unmanaged devices.

Increasingly mobile devices are involved in advanced attacks, sometimes as part of a broader attack. For example, mobile phishing attacks can obtain account credentials that an attacker can reuse against an enterprise API, or on a corporate laptop. Because of the current lack of visibility on mobile devices, most organizations never identify these portions of the attack. MTD solutions, stand-alone or as part of a broader EDR or UES deployment, can improve detection of attacks against enterprises.

**Business Impact:** Because mobile security issues have rarely led to spectacular breaches, enterprises adopting MTD sometimes have difficulty in identifying positive impact. Enterprises have two areas where MTD tools can immediately demonstrate value. The first is device vulnerability assessment where MTD solutions can be used to identify unpatched and vulnerable devices and rank them in terms of severity. The second area has to do with reducing app risk: MTD solutions can identify apps that conflict with an enterprise's security and privacy policies, even when these applications are not malicious. Enterprises in regulated industries such as financial services, insurance, healthcare, government and energy, as well as enterprises with high-security requirements, such as defense contractors and consulting firms are typical adopters of MTD.

**Benefit Rating:** Moderate

**Market Penetration:** 5% to 20% of target audience

**Maturity:** Adolescent

**Sample Vendors:** BETTER Mobile Security; Check Point Software Technologies; Lookout; Microsoft; Pradeo; Sophos; Symantec; Wandera; Zimperium

**Recommended Reading:** “Market Guide for Mobile Threat Defense”
“When Android Is Secure Enough for the Enterprise”

“iPhone and iPad Security FAQs”

“Advance and Improve Your Mobile Security Strategy”

Zero Trust Network Access

Analysis By: Steve Riley

Definition: Zero trust network access (ZTNA) creates an identity- and context-based, logical-access boundary around an application or set of applications. The applications are hidden from discovery, and access is restricted via a trust broker to a set of named entities. The broker verifies the identity, context and policy adherence of the specified participants before allowing access, and prohibits lateral movement elsewhere in the network. This removes the application assets from public visibility and significantly reduces the surface area for attack.

Position and Adoption Speed Justification: ZTNA is a synthesis of concepts promulgated by the Cloud Security Alliance’s software-defined perimeters (SDP) project, by Google’s BeyondCorp vision, and in O’Reilly’s *Zero Trust Networks* book. Early products on the market tended to focus on use cases involving access to web applications. Newer, more complete products work with a wider range of applications and protocols.

As more organizations suddenly find themselves transitioning to much more remote work, hardware-based VPNs exhibit limitations. ZTNA has piqued the interest of those seeking a more flexible alternative to VPNs and those seeking more precise access and session control to applications located on-premises and in the cloud. ZTNA vendors continue to attract venture capital funding. This, in turn, encourages new startups to enter an increasingly crowded market and seek ways to differentiate. Merger and acquisition (M&A) activity in this market is underway, with several startup vendors now having been acquired by larger networking, telecommunications and security vendors.

User Advice: Organizations should evaluate ZTNA for any of these use cases:

- Opening up applications and services to collaborative ecosystem applications, such as distribution channels, suppliers, contractors or retail outlets without requiring the use of a VPN or DMZ.
- Normalizing the user experience for application access — ZTNA eliminates the distinction between being on and off the corporate network.
- Application-specific access for IT contractors and remote or mobile employees as an alternative to VPN-based access.
- Extending access to an acquired organization during M&A activities, without having to configure site-to-site VPN and firewall rules. The merged companies can quickly and easily share applications without requiring the underlying networks and/or identity systems to be integrated.
- Enabling users on personal devices — ZTNA can improve security and simplify bring your own device (BYOD) programs by reducing full management requirements and enabling more-secure direct application access.
- Cloaking systems on hostile networks, such as systems facing the public internet used for collaboration.
- Carrying encryption all the way to the endpoints for scenarios where you don’t trust the carrier or cloud provider.
- Permitting users in potentially dangerous areas of the world to interact with applications and data in ways that reduce or eliminate risk prone to originate in those areas.
- Securing access to enclaves of IoT devices if the device can support lightweight SDP agent or a virtual-appliance-based connector on the IoT network segment for connection.

**Business Impact:** The benefits of ZTNA are immediate. Similar to a traditional VPN, services brought within the ZTNA environment are no longer visible on the public internet and, thus, are shielded from attackers. In addition, ZTNA brings significant benefits in user experience, agility, adaptability and ease of policy management. For cloud-based ZTNA offerings, scalability and ease of adoption are additional benefits. ZTNA enables digital business transformation scenarios that are ill-suited to legacy access approaches. As a result of digital transformation efforts, most enterprises will have more applications, services and data outside their enterprises than inside. Cloud-based ZTNA services place the security controls where the users and applications are — in the cloud. Some of the larger ZTNA vendors have invested in dozens of points of presence worldwide for low-latency access.

**Benefit Rating:** Moderate

**Market Penetration:** 5% to 20% of target audience

**Maturity:** Adolescent

**Sample Vendors:** Akamai; AppGate; Cato Networks; Cisco; Netskope; Perimeter 81; Proofpoint; Pulse Secure; SAIFE; Zscaler

**Recommended Reading:**
- “Market Guide for Zero Trust Network Access”
- “Zero Trust Is an Initial Step on the Roadmap to CARTA”
- “Solving the Challenges of Modern Remote Access”
- “Quick Answer: Cost Effectively Scaling Secure Access While Preparing for a Remote Workforce”
- “The Future of Network Security Is in the Cloud”
Data Sanitization

**Analysis By:** Rob Schafer; Christopher Dixon

**Definition:** Data sanitization is the disciplined process of deliberately, permanently and irreversibly removing or destroying the data stored on a memory device to make it unrecoverable. A device that has been sanitized has no usable residual data, and even with the assistance of advanced forensic tools, the data will not ever be recovered (see the International Data Sanitization Consortium).

**Position and Adoption Speed Justification:** Growing concerns about data privacy and security, leakage, regulatory compliance, and the ever-expanding capacity of storage media and volume of edge computing and IoT devices make robust data sanitization a core C-level requirement for all IT organizations.

This requirement for comprehensive data sanitization should be applied to all devices with storage components (e.g., enterprise storage and servers, PCs, mobile devices, and increasingly, edge computing and some IoT devices). Where organizations lack this robust data sanitization competency, it is often due to handling the asset life cycle stages as isolated events, with little coordination between business boundaries (such as finance, security, procurement and IT).

For mobile devices, a remote data-wiping capability is commonly implemented via a mobile device manager (MDM). Although such a remote capability should not be considered a fail-safe mechanism, reliability should be adequate for a significant majority of lost or stolen mobile devices.

**User Advice:** Follow a life cycle process approach to IT risk management that includes making an explicit decision about data archiving and sanitization, and device reuse and retirement.

Implement policies that assign explicit responsibility for all sensitive or regulated data-bearing devices to ensure that they are properly wiped or destroyed at the end of their productive use.

Collaborate with data sanitization stakeholders (e.g., security, privacy, compliance, legal, IT) to create appropriate data sanitization standards that provide specific guidance on the end-to-end destruction process, based on data sensitivity.

As different media (such as magnetic HDD storage vs. semiconductor-based NAND flash memory) require different sanitization methods, ensure your IT asset disposition (ITAD) vendor provides a certificate of data destruction with a serialized inventory of the data-bearing assets sanitized. Include a clause within your ITAD contract giving you the right to audit the ITAD vendor’s data sanitization processes/standards to ensure its compliance with your security and industry standards (e.g., NIST 800-88).

Regularly (e.g., annually) verify that your ITAD vendor consistently meets your data sanitization security specifications and standards.
Understand the security implications of personal devices and plug-and-play storage. Organizations that have yet to address portable data-bearing devices (e.g., USB drives, IoT devices) are even less prepared to deal with these implications.

Consider using whole-volume encryption for portable devices and laptops and self-encrypting devices in the data center.

Consider destroying storage devices, versus reusing them, if they contain highly sensitive and/or regulated data (e.g., organizations in the financial and healthcare industries).

For externally provisioned services (e.g., SaaS, IaaS), understand end-of-contract implications, and ask current and potential providers for an explanation of their storage reuse and recycling practices.

**Business Impact:** At a relatively low cost, the proper use of encryption, data sanitization and, when necessary, destruction will help minimize the risk that proprietary and regulated data will leak.

By limiting data sanitization to encryption and/or software-based wiping, organizations can preserve the asset’s residual market value. The *destruction* of data-bearing devices within an IT asset typically reduces the asset’s residual value to salvage, incurring the cost of environmentally compliant recycling.

The benefit rating is moderate, because data sanitization has become an increasingly accepted process to minimize the material business risk of data security. While data sanitization will not necessarily result in increased revenue or cost savings, it will minimize the risk of significant monetary and brand damage that can result from serious ITAD-related data breaches.

**Benefit Rating:** Moderate

**Market Penetration:** 20% to 50% of target audience

**Maturity:** Early mainstream

**Sample Vendors:** Blancco Technology Group; ITRenew; WhiteCanyon Software

**Recommended Reading:** “Mobile OSs and Device Security: A Comparison of Platforms”

**Secure Instant Communications**

**Analysis By:** Dionisio Zumerle

**Definition:** Secure instant communications provide confidentiality and data retention for instantaneous forms of communication such as instant messaging, text messaging, voice and video communications. The solutions support smartphones, tablets and personal computers.

**Position and Adoption Speed Justification:** Most solutions are implemented as apps installed on a device and use encryption over the data channel. Some solutions increase their security assurance by adding a hardware-based root of trust. This can be the secure enclave or trusted execution environment (TEE) natively available on mobile devices, or a microSD card. Some
solutions are instead part of stand-alone hardened smartphones. The solutions provide encryption of both the exchanges in transit and the communications stored in the device.

Secure instant communications solutions have matured along with the underlying mobile operating systems on which they operate and are able to deliver acceptable network performance, battery consumption, and efficiency in key management and encryption. User experience is the main aspect on which these solutions are trying to improve, to compete with mainstream enterprise communications solutions.

Revelations about pervasive surveillance and privacy-invasive apps have led enterprises to be concerned about confidentiality of their information. In some industries, regulations — such as the Health Insurance Portability and Accountability Act (HIPAA) and the regulations issued by the Financial Industry Regulatory Authority (FINRA) — encourage or require protection, auditing and archiving of communications. Still, adoption is limited to fulfilling regulatory obligations, or mitigating particularly sensitive scenarios.

Data retention is an increasingly important feature, as it enables monitoring and archiving for regulatory compliance purposes, and instant deletion for security assurance. Some solutions are delivered as part of broader archiving suites, and are starting to extend archiving to third-party instant messaging apps, such as WeChat and WhatsApp.

**User Advice:** For most organizations, the security provided by commercial enterprise communications solutions, such as unified communications, is enough to meet their confidentiality requirements. However, some organizations with high-security requirements will need a specialized, hardened instant communications solution. Typically, these are organizations at risk of industrial espionage or state-sponsored attacks and will deploy the solution to a restricted pocket of the user population that needs the solution (e.g., high-level executives). With the surge in remote work in 2020, there is a mild increase in these use cases.

Enterprises in regulated industries such as healthcare, finance, government and energy are typical adopters of secure instant communications solutions for compliance purposes. Increasingly this functionality is provided by more suitable options for the long term, namely enterprise information archiving vendors and industry-specific suites such as clinical communication and collaboration platforms, and equivalent financial services solutions.

Software-only solutions in the form of an application are the easiest to deploy and run. While hardware-based solutions offer better performance, they impact user experience and are limited to well-defined use cases with strict security requirements.

It is not advised to rely on free consumer-grade instant communications apps that claim to offer end-to-end encryption. In addition to the lack of enterprise-grade features, these solutions are rarely a defensible choice in the event of a security incident.

**Business Impact:** Secure instant communications solutions protect organizations against leaks of sensitive information, and can address risks of the interception of communications in cases of industrial espionage and/or hacktivism. When used for compliance purposes, they can satisfy regulatory requirements that would otherwise have led to penalties. Outside regulated verticals and
organizations with high-security requirements, mainstream organizations favor user experience and hence, when they do not use consumer solutions, they select general-purpose UC solutions or broader industry-oriented suites that include secure instant communications functionality.

**Benefit Rating:** Moderate

**Market Penetration:** 5% to 20% of target audience

**Maturity:** Early mainstream

**Sample Vendors:** Adeya; BlackBerry; CellTrust; KoolSpan; SafeGuard Cyber; Smarsh; TeleMessage; TigerConnect; Virtual Solution; Wickr

**Recommended Reading:**

- “Market Guide for Instant Communications Security and Compliance”
- “Take These Four Steps to Securely Use WhatsApp, WeChat and Other Instant Communication Apps”
- “Advance and Improve Your Mobile Security Strategy”

### Endpoint Detection and Response

**Analysis By:** Paul Webber

**Definition:** EDR solutions provide capabilities to detect and investigate security events, contain the attack and produce guidance for remediation. EDR solutions must identify and analyze activity and device configuration. Visibility and reporting of user and device activity are combined with direct intervention when abnormal activity is detected. Automated response and rollback of threats are highly desirable EDR features. Integration and automation with other tools are key. Cloud hosting is predominant, with on-premises hosting also offered.

**Position and Adoption Speed Justification:** Endpoint detection and response (EDR) is a mainstream part of any endpoint security strategy and is not limited to organizations with mature security operations. Adoption of EDR grew because of increasingly advanced threats, but also the added appeal of automation, orchestration and managed EDR features built into EDR products. EDR innovation is increasingly included in broader endpoint protection platforms (EPPs) adding behavior-based detection and basic threat hunting. This convergence also came from the EDR side of the market, where EDR vendors added protection capabilities to their core detection and response functions. Cloud-delivered endpoint security solutions will replace traditional on-premises (host server) architectures for the mainstream market within the next two to three years.

Some vendors are combining telemetry from network, email, and web security products, to enrich data and derive stronger detections from weak signals. These extended detection and response (XDR) solutions leverage advanced analytics to identify unknown threats and reveal tactics and techniques. They provide integrations with other security tools to allow faster detection for additional efficiency gains.

**User Advice:** Organizations should:
First, look for EDR capabilities in their incumbent EPP solution delivered via the same agent, management console and service wherever possible.

Prefer cloud-hosted EDR solutions, placing a premium on vendors that provide automation and managed features/services around the detection of suspicious and anomalous behavior.

Target vendors that provide additional managed services themselves (versus via channel partners or MSSPs) including alerting and monitoring, incident response and managed detection and response.

Favor vendors that can help remove vulnerabilities, misconfigurations and harden the endpoint against attack, as well as providing the facility to rapidly respond to issues with direct access to remediate issues in near real time.

Ensure they are also applying foundational basics (such as vulnerability, patch and configuration management) before taking on EDR projects that require some security capabilities to be already in place for the project’s success.

As threat actors continue to mature and evolve campaigns using stealthier fileless attacks, living-off-the-land techniques and other hard-to-detect exploits, vendors must provide advanced analytics facilities that can identify anomalous activity and patterns of behavior, revealing the tactics and techniques of advanced persistent threats.

**Business Impact:** It isn’t practical to achieve 100% prevention and protection, and older EPP tools should be updated with ones that have EDR functionality. Adding detection and response features is now considered mainstream, though many organizations still lack the skills to fully leverage them. Adoption of EDR must be accompanied by investment in training of responders to recognize threats, identify remediations and transition from reactive processes to proactive threat hunting and rapid response. Organizations with few skilled staff should opt for managed detection and response (MDR) services that provide monitoring, alerting and often triaging of alerts.

Some EDR tools can automatically contain an attack and prevent malware from spreading, especially when the system “learns” from historical operator actions or has external threat intelligence feeds.

For organizations lacking expert teams to build complex playbooks and assimilate the tradecraft of advanced attackers, automated and already fully integrated “XDR” platforms are preferable. These allow faster and more effective detection and response without investment in the sophisticated SIEM and SOAR tools used by larger enterprises.

**Benefit Rating:** High

**Market Penetration:** 20% to 50% of target audience

**Maturity:** Early mainstream

**Sample Vendors:** Cisco; CrowdStrike; Cybereason; FireEye; Microsoft; Palo Alto Networks; SentinelOne; Tanium; Trend Micro; VMware Carbon Black
Secure Web Gateways

Analysis By: Lawrence Orans; Peter Firstbrook; John Watts

Definition: Secure web gateways (SWGs) utilize URL filtering, advanced threat defense (ATD) and malware detection to protect organizations and enforce internet policy compliance. SWGs are delivered as on-premises appliances (hardware and virtual), cloud-based services or hybrid solutions (cloud and on-premises).

Position and Adoption Speed Justification: SWGs have progressed to the Slope of Enlightenment, as the trend toward cloud-based services continues to strengthen. Gartner’s volume of inquiries for cloud-based SWG services outpaces the inquiry volume for appliance-based SWGs by a factor of more than four-to-one.

The market outlook for SWG is positive, and new competitors have emerged. CASB vendors Bitglass and Netskope have begun to offer SWG functionality. Palo Alto Networks is also emerging as a competitor with its firewall-based Prisma Access solution. And, Akamai has introduced a proxy-based SWG cloud service. In the midmarket, SWGs face some pressure from firewall vendors that offer basic URL filtering (not complete SWG functionality) as an optional feature. Cloud-based recursive DNS solutions have also become a popular solution with midmarket customers.

As highlighted by Gartner’s SASE framework (see “The Future of Network Security Is in the Cloud”), enterprises continue to seek a broader menu of security services from their cloud security service providers. The SWG market continues to evolve as vendors add services such as CASB, zero trust network access (ZTNA), remote browser isolation (RBI) and others to their list of available offerings.

User Advice: Security and risk management leaders responsible for endpoint and network security should take a fresh look at the SWG market and not automatically renew traditional approaches. Critical capabilities to seek out include purpose-built cloud solutions, advanced threat protection (for example, sandboxing), and CASB services to control and monitor access to SaaS applications. Some cloud SWG services offer outbound firewall functionality. Also, many SWGs can now apply policy to SaaS applications (including shadow IT) by integrating with CASB solutions (the CASB services share their cloud application discovery and risk database with the SWG providers). ZTNA functionality (primarily implemented as an alternative to traditional VPNs) is another important feature to consider. Enterprises may adopt or change SWG providers to accommodate growth or improve risk posture by applying best-of-breed security to web traffic.
Business Impact: Secure web gateways provide an additional layer of protection against destructive attacks such as ransomware, and enable safer and more efficient adoption of cloud-based services. Cloud-delivered SWGs can also reduce branch office networking costs by using commodity internet access (instead of backhauling web traffic over MPLS links to a centralized data center). When the SWG service also includes a firewall-as-a-service option, it can be used to eliminate branch office firewalls. Also, cloud SWG services can provide protection for mobile users that are off the corporate network.

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Sample Vendors: Cisco; ContentKeeper; Forcepoint; iboss; McAfee; Menlo Security; Netskope; Sangfor Technologies; Symantec; Zscaler

Recommended Reading: “Magic Quadrant for Secure Web Gateways”
“Critical Capabilities for Secure Web Gateways”
“How to Avoid Failures When Migrating to a Cloud-Based Secure Web Gateway”
“The Future of Network Security Is in the Cloud”

Cloud Access Security Brokers

Analysis By: Steve Riley

Definition: Cloud access security brokers (CASBs) provide crucial cloud governance controls for visibility, data security, threat protection, and compliance assessment in SaaS and IaaS. CASBs consolidate multiple types of security policy enforcement into one place. Examples include authentication, single sign-on, authorization, device profiling, data security, logging, alerting, and malware removal. Most CASB deployments are cloud-based; on-premises deployments are rare.

Position and Adoption Speed Justification: Vendors offer feature-rich products to increase cloud visibility and apply consistent policy across multiple providers. Execution across all vendors is variable: while some have incrementally improved and added new capabilities, the leading vendors continue to make significant investments that have contributed to the rapid maturation of the market. The acquisition phase of the market has ceased. Major incumbent security vendors now offer a CASB, either stand-alone or as part of a product portfolio; integration with other products in portfolios is inconsistent but improving. While the number of independent vendors has stabilized, the most relevant independent vendors demonstrate sustained innovation and broad market reach. Differentiation among vendors is becoming difficult, and several have branched beyond SaaS governance and protection to include custom application support in IaaS clouds, cloud security posture management (CSPM) capabilities, and user and entity behavior analysis (UEBA) features. The most relevant independent vendors continue to receive venture capital funding, while funding
for the less well-known private vendors remains uncertain. The pace of client inquiry indicates that CASB is a popular choice for cloud-using organizations. Gartner’s 4Q19 security spend forecast predicts a significant but slowing growth rate for CASB: 45.3% in 2020, 40.7% in 2021, 36.7% in 2022, and 33.2% in 2023. While the forecast predicts slowing spend for all security markets, CASB’s growth remains higher than any other information security market (see, “Forecast: Information Security and Risk Management, Worldwide, 2017-2023, 4Q19 Update”).

**User Advice:** Examine vendor capabilities in four functionality areas: visibility, data protection, threat detection and compliance. All relevant CASB vendors interact with SaaS applications via APIs and can be positioned in-line for real-time traffic visibility. CASB proxies may or may not require endpoint agents for traffic steering outside proxied networks; factor this into your evaluation. Increasingly, CASB vendors offer remote browser isolation as an adjunct to in-line deployments.

Common deployment scenarios that deserve special scrutiny include:

- **Cloud discovery and risk assessment.** Evaluate the thoroughness of the CASB’s analysis of an organization’s cloud security posture. The CASB should discover every cloud service in use and assign each one a risk score (ask vendors for information about how often this is updated), gleaned from attributes whose weights can be modified by customers. Evaluate the CASB’s CSPM capabilities for assessing risk in IaaS storage, compute, and virtual network configurations.

- **DLP.** Evaluate whether CASB capabilities are sufficient or require augmentation with deployed enterprise DLP product, either via ICAP or RESTful API integration. In-line CASB DLP capabilities should provide a mechanism to control the movement of sensitive information into and out of cloud services in real time. Examine CASB support for data classification features that can link to existing enterprise classification tools.

- **Adaptive access control (AAC).** Examine techniques vendors provide for altering the behavior of governed applications based on signals observed during and after login. AAC allows for shades of access (e.g., read-only access to content on unmanaged devices) that are more useful to the business than blocking access completely.

- **UEBA.** Evaluate how CASBs detect and isolate risky users and devices. Insider threats and compromised accounts are common attack vectors. Seek mechanisms that build baseline behavior profiles (such as typical upload/download amounts and user locations) and alert and mitigate when behavior deviates from baselines. Step-up authentication is an important capability to test with whatever IAM vendor is already deployed.

- **Third-party app discovery and control.** Ensure that the CASB can detect all third-party apps that have been granted access to SaaS applications (almost always via OAuth). Look for more than single yes/no controls for each app and instead favor the ability to group third-party apps into categories based on OAuth scopes.

- **Regulatory compliance.** Determine whether the CASB offers sufficient visibility and control for aspects such as user privacy and data residency. Carefully scrutinize encryption mechanisms. Encrypting data before sending it to a cloud service might negatively affect certain functionality.
in the service. Evaluate the CASB’s CSM capabilities for comparing IaaS workload configurations to common regulatory baselines.

**Business Impact:** CASBs are uniquely positioned to enable organizations to achieve consistent security policies and governance across many cloud services. Unlike traditional security products, CASBs are designed to protect data that’s stored in someone else’s systems. CASBs are suitable for organizations of all sizes in all industries and are uniquely positioned to help demonstrate that cloud use is well-governed. Given the expected continued feature expansion and relative ease of switching, favor one-year contract terms over lengthier ones.

**Benefit Rating:** High

**Market Penetration:** 20% to 50% of target audience

**Maturity:** Early mainstream

**Sample Vendors:** Bitglass; Censornet; CipherCloud; Forcepoint; McAfee; Microsoft; Netskope; Proofpoint; Symantec; Zscaler

**Recommended Reading:** “Magic Quadrant for Cloud Access Security Brokers”

“Critical Capabilities for Cloud Access Security Brokers”

“Peer Lessons Learned: Implementing Cloud Access Security Brokers”


“Best Practices for Planning, Selecting, Deploying and Operating a CASB”

---

**Secure Enterprise Data Communications**

**Analysis By:** Rob Smith

**Definition:** Secure enterprise data communications solutions provide encrypted and authenticated “virtual” connections for networks and apps. It is a broad category that supports site-to-site bridging, as well as individual remote and mobile users, and relies typically on IPsec and Transport Layer Security (TLS) for confidentiality.

**Position and Adoption Speed Justification:** The recent surge in remote working has made virtual private network (VPN) one of the most important technologies in IT, as the need for remote work reached unprecedented levels. The VPN aspects of this profile are mostly mature with little change and are heading rapidly to plateau. For example, site-to-site secure connections based on traditional VPN are barely considered competitive. Although in extremely high demand, remote PC access methods have not changed noticeably for more than a decade. Remote-access VPN access has proved challenging, due to limited bandwidth and hardware constraints, forcing the push of infrastructure into the cloud. This means that secure browser apps and other apps using TLS under the hood become the de facto standard. Software-defined perimeter (SDP), software-defined WAN (SD-WAN) and cloud app providers are offering their own virtual privacy connections. Cloud access
security brokers (CASBs) are creating the equivalent of the enterprise gateway in the cloud, complete with centralized identity management and managed encrypted connections to business user destinations. Zero-trust network access (ZTNA) is also a potential replacement for VPN, as users migrate to cloud applications and no longer need traditional on-premises access.

**User Advice:** Companies that find themselves needing to renegotiate legacy VPN contracts should take a careful look at the timing of their cloud strategies. In many cases, site-to-site and end-user VPNs will be short-term investments, which will be replaced by cloud services that include data-in-transit encryption. In other cases, the transition could take many years. As migration to the cloud is completed, legacy VPNs will serve decreasing needs for on-premises services and servers, while the main business processes are incrementally modernized, web-enabled and migrated to the cloud. Secure communications between apps and servers in the cloud context will increasingly be handled directly by the apps and will not be managed under legacy VPN configurations.

**Business Impact:** Enterprises are putting their business infrastructures in the cloud, while their endpoint business processes are, in many cases, still designed for local, on-premises services and company endpoints. Security and risk management (SRM) leaders should ensure that architectural changes preserve security, while minimizing impacts on usability. Cloud-first companies must conduct an end-of-life analysis of legacy secure communications needs before investing further in conventional solutions.

**Benefit Rating:** High

**Market Penetration:** More than 50% of target audience

**Maturity:** Mature mainstream

**Sample Vendors:** Check Point Software Technologies; Cisco Systems; F5; Microsoft; NetMotion Software; Palo Alto Networks; Pulse Secure

**Recommended Reading:** “Solving the Challenges of Modern Remote Access”

“Market Guide for Secure Enterprise Data Communications”

“Market Guide for Zero Trust Network Access”

“Recreate Desktop Security After Users Move to the Cloud”

Entering the Plateau

**Endpoint Protection Platforms**

**Analysis By:** Paul Webber

**Definition:** Endpoint protection platforms provide protection from malware, usually via the installation of an agent on the endpoint. This must protect against existing and emerging threats and exploits including protection against malware, both file-based and fileless exploits,
identification and prevention of threats using behavioral analysis, whitelisting of known applications, processes and scripts, and investigation and reporting of the configuration of the endpoint.

**Position and Adoption Speed Justification:** The EPP market has adapted to more advanced threats and stealthier attackers. Organizations currently place a premium on preventing unknown and non-file-based attacks, and the addition of machine learning and cloud-based look-up as an alternative to local signature-based identification. Ease of use, low resource utilization and reduced maintenance are still expected.

Principal evolutions in the EPP market are cloud-native solutions that are easier to deploy and manage, plus advances in behavior-based detection and analytics, that allow identification of zero-day threats.

Improvements in native OS security protect credentials, prevent kernel attacks and can isolate browser and applications, together with vulnerability management and hardening. These advances are eroding the scope for EPP vendors. It is shifting the focus of attackers toward application security weaknesses and fallibility of the end user. More stealthy attacks mean that EDR features are required to detect and respond to advanced threats that would otherwise bypass EPP tools reliant on prevention and protection alone.

**User Advice:** Because of the shift of attacks toward more advanced and stealthy techniques, security and risk management leaders responsible for endpoint security should look for products with these capabilities:

- A single agent with a combination of protection against known threats and exploits with behavioral analysis, preferably cloud-hosted, plus associated look-up of unknown items.
- Ability to report internet, network and application activity to derive additional indications of potentially malicious activity and identify unknown threats or anomalous activity.
- Facilities to scan systems for vulnerabilities and report/manage the installation of security patches, in order to improve hardening and reduce attack surface.
- A capability to rapidly contain threats when identified and to remediate systems remotely, preferably with optional automation for each of these features.
- The provision of managed services offerings to augment in-house teams where organizations lack internal resources or skills to manage advanced EPP solutions.

**Business Impact:** EPP is still a commonly deployed layer of malware prevention and is considered basic security hygiene for all organizations. Self-propagating, indiscriminate malware is now joined by attacks that focus on individuals and organizations. Attackers exploit poor configuration, unpatched systems and steal credentials to gain entry, then use living-off-the-land attacks and fileless malware to bypass security controls. Despite sophisticated, stealthy attackers, a well-configured and maintained EPP product can still significantly lower the risk of malware and targeted attacks. All industry sectors and scales of organization must reexamine their endpoint protection approach and invest in additional capabilities and layers of protection for the endpoint.
Advanced adversaries targeting the organization can evade protection solutions, making detection and response capabilities critical to identifying attacks, fraud and breaches. Therefore, EPP solutions should not be the only layer of endpoint protection but be part of a wider set of security controls.

**Benefit Rating:** Moderate

**Market Penetration:** More than 50% of target audience

**Maturity:** Mature mainstream

**Sample Vendors:** Cisco; CrowdStrike; Cybereason; McAfee; Microsoft; SentinelOne; Sophos; Symantec; Trend Micro

**Recommended Reading:** “Critical Capabilities for Endpoint Protection Platforms”

“Magic Quadrant for Endpoint Protection Platforms”

“Top Security and Risk Management Trends”

“Innovation Insight for Extended Detection and Response”
Figure 3. Hype Cycle for Endpoint Security, 2019

Hype Cycle for Endpoint Security, 2019

Source: Gartner
ID: 369962
**Hype Cycle Phases, Benefit Ratings and Maturity Levels**

**Table 1. Hype Cycle Phases**

<table>
<thead>
<tr>
<th>Phase</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Innovation Trigger</strong></td>
<td>A breakthrough, public demonstration, product launch or other event generates significant press and industry interest.</td>
</tr>
<tr>
<td><strong>Peak of Inflated Expectations</strong></td>
<td>During this phase of overenthusiasm and unrealistic projections, a flurry of well-publicized activity by technology leaders results in some successes, but more failures, as the technology is pushed to its limits. The only enterprises making money are conference organizers and magazine publishers.</td>
</tr>
<tr>
<td><strong>Trough of Disillusionment</strong></td>
<td>Because the technology does not live up to its overinflated expectations, it rapidly becomes unfashionable. Media interest wanes, except for a few cautionary tales.</td>
</tr>
<tr>
<td><strong>Slope of Enlightenment</strong></td>
<td>Focused experimentation and solid hard work by an increasingly diverse range of organizations lead to a true understanding of the technology’s applicability, risks and benefits. Commercial off-the-shelf methodologies and tools ease the development process.</td>
</tr>
<tr>
<td><strong>Plateau of Productivity</strong></td>
<td>The real-world benefits of the technology are demonstrated and accepted. Tools and methodologies are increasingly stable as they enter their second and third generations. Growing numbers of organizations feel comfortable with the reduced level of risk; the rapid growth phase of adoption begins. Approximately 20% of the technology’s target audience has adopted or is adopting the technology as it enters this phase.</td>
</tr>
<tr>
<td><strong>Years to Mainstream Adoption</strong></td>
<td>The time required for the technology to reach the Plateau of Productivity.</td>
</tr>
</tbody>
</table>

Source: Gartner (July 2020)

**Table 2. Benefit Ratings**

<table>
<thead>
<tr>
<th>Benefit Rating</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Transformational</strong></td>
<td>Enables new ways of doing business across industries that will result in major shifts in industry dynamics</td>
</tr>
<tr>
<td><strong>High</strong></td>
<td>Enables new ways of performing horizontal or vertical processes that will result in significantly increased revenue or cost savings for an enterprise</td>
</tr>
<tr>
<td><strong>Moderate</strong></td>
<td>Provides incremental improvements to established processes that will result in increased revenue or cost savings for an enterprise</td>
</tr>
<tr>
<td><strong>Low</strong></td>
<td>Slightly improves processes (for example, improved user experience) that will be difficult to translate into increased revenue or cost savings</td>
</tr>
</tbody>
</table>

Source: Gartner (July 2020)
Table 3. Maturity Levels

<table>
<thead>
<tr>
<th>Maturity Level</th>
<th>Status</th>
<th>Products/Vendors</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Embryonic</strong></td>
<td>■ In labs</td>
<td>■ None</td>
</tr>
<tr>
<td><strong>Emerging</strong></td>
<td>■ Commercialization by vendors  ■ Pilots and deployments by industry leaders</td>
<td>■ First generation  ■ High price  ■ Much customization</td>
</tr>
<tr>
<td><strong>Adolescent</strong></td>
<td>■ Maturing technology capabilities and process understanding  ■ Uptake beyond early adopters</td>
<td>■ Second generation  ■ Less customization</td>
</tr>
<tr>
<td><strong>Early mainstream</strong></td>
<td>■ Proven technology  ■ Vendors, technology and adoption rapidly evolving</td>
<td>■ Third generation  ■ More out-of-box methodologies</td>
</tr>
<tr>
<td><strong>Mature mainstream</strong></td>
<td>■ Robust technology  ■ Not much evolution in vendors or technology</td>
<td>■ Several dominant vendors</td>
</tr>
<tr>
<td><strong>Legacy</strong></td>
<td>■ Not appropriate for new developments  ■ Cost of migration constrains replacement</td>
<td>■ Maintenance revenue focus</td>
</tr>
<tr>
<td><strong>Obsolete</strong></td>
<td>■ Rarely used</td>
<td>■ Used/resale market only</td>
</tr>
</tbody>
</table>

Source: Gartner (July 2020)

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

Understanding Gartner's Hype Cycles

Evidence

1 Gartner press release, “Gartner HR Survey Reveals 41% of Employees Likely to Work Remotely at Least Some of the Time Post Coronavirus Pandemic.”

2 Gartner’s Security and IAM Solution Adoption Trend Survey, 2020. This study was conducted to learn what security solutions organizations are benefiting from, and what factors affect their choice/preference for such solutions. The research was conducted online during March and April 2020 among 405 respondents from North America, Western Europe and the Asia/Pacific region. Companies from different industries were screened for having annual revenue of less than $500 million. Respondents were required to be at manager level or above (excluding the C-suite) and to
have primary involvement and responsibility in a risk management role for their organization. The study was developed collaboratively by Gartner analysts and the Primary Research team that follows security and risk management.