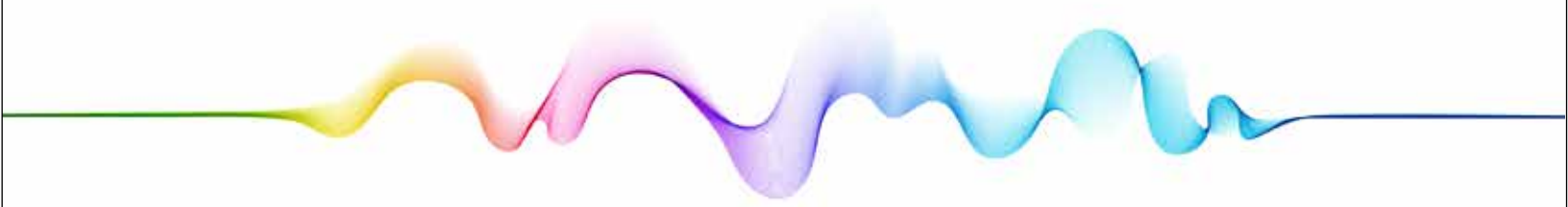
INSIGHT REPORT

AN OVERVIEW OF ENDPOINT PROTECTION PLATFORM (EPP) COMMERCIAL MARKET



TAG

CYBERSECURITY

focuses on a special subcase of endpoint protection that is referred to as *endpoint protection platform (EPP)* and that includes many aspects of the subcategories listed above.

Figure 1. TAG Taxonomy for Cybersecurity

A future TAG Insights Report will provide guidance on the more generalized endpoint protection solutions available today. This report sticks to the narrower view of EPP as a solution selected by many enterprise teams for protecting their endpoints from compromise and malware.

Overview of EPP

EPP refers to a comprehensive cybersecurity solution designed to protect Internet-connected hardware such as desktops, laptops, servers, and mobile devices from various cyber threats, especially viruses and malware. EPP is mostly an enterprise solution, but there are certainly many personal tools that might be used to protect home PCs and laptops from compromise, usually via malware.

Commercial EPP solutions typically combine multiple security tools and features to provide a layered defense approach against malware, ransomware, advanced persistent threats, zero-day exploits, and other malicious activities. The following capabilities involving EPP solutions are considered in-scope to the vendors listed in this report:

1. *Antivirus and Anti-Malware*: EPP solutions incorporate robust scanning engines to detect and remove known malware and viruses from endpoint devices. They use

signature-based detection as well as heuristics and behavioral analysis techniques to identify suspicious or malicious files.

2. *Firewall*: EPP solutions also often include a host-based firewall that monitors and controls incoming and outgoing network traffic to and from the endpoint. It helps protect endpoints from unauthorized access, network-based attacks, and data exfiltration attempts.
3. *Intrusion Detection and Prevention Systems*: These systems monitor network traffic and endpoint activities to detect and prevent intrusion attempts. They can identify and block suspicious network packets, known attack patterns, and other indicators of compromise.
4. *Data Leakage Prevention (DLP)*: DLP features prevent sensitive data from being leaked or exfiltrated from endpoints. They employ content analysis, data encryption, and access control mechanisms to safeguard data and ensure compliance with privacy regulations.
5. *Device Control*: This feature allows administrators to define and enforce policies regarding the use of external devices such as USB drives, printers, and mobile devices. It helps prevent data theft, malware introduction, and other risks associated with unauthorized device usage.
6. *Behavioral Analysis and Machine Learning*: EPP solutions leverage advanced techniques like machine learning and behavioral analysis to detect and block previously unseen or zero-day threats. By analyzing patterns of behavior, these systems can identify suspicious activities and take preventive actions.
7. *Centralized Management and Reporting*: EPP technology typically offers a centralized management console that allows administrators to deploy, configure, and manage security policies across multiple endpoints. It also provides real-time monitoring, alerts, and detailed reporting on security events and incidents.

By combining these features, EPP technology provides a holistic approach to endpoint security, helping organizations protect their devices and data from a wide range of cyber threats. Most enterprise teams today, certainly in larger companies and often for mid-sized companies, will employ a commercially supported EPP platform. This decision has always been mandatory for Microsoft Windows environments, but MacBook deployments also benefit from EPP.

The related commercial solution known as endpoint detection and response (EDR) is sufficiently close to EPP that many practitioners might not draw much distinction between the two. Technically speaking, we view at TAG the use of EDR as including a managed service component, often involving the collection of telemetry from endpoints into a shared SOC that offers real-time analysis and reporting.

Increasingly, however, it's become harder to find EPP solutions that do not have some degree of collection, analysis, and notification – so the differences between EPP and EDR are less easy to identify. We try here to provide practical guidance on commercial endpoint security solutions that focus primarily on the features and functions listed above, even though considerable overlap will inevitably emerge between EPP and EDR.

Market Overview of EPP

The EPP commercial market refers to the industry that provides EPP solutions to organizations and businesses. It encompasses a wide range of vendors, products, and services aimed at protecting endpoint devices from various cyberthreats. Here is an overview of the EPP commercial market:

1. *Market Growth*: The demand for EPP solutions has been steadily increasing due to the growing sophistication and frequency of cyberattacks. The market is driven by factors such as the rise in targeted attacks, data breaches, and the need for robust endpoint security in the face of evolving threats.
2. *Competitive Landscape*: The market is highly competitive, with numerous vendors offering EPP solutions. Prominent players in the market include well-established cybersecurity companies, traditional antivirus vendors, and emerging startups specializing in endpoint security.
3. *Solution Differentiation*: EPP vendors differentiate their offerings through a combination of features, capabilities, and the effectiveness of their threat detection and prevention mechanisms. Differentiating factors may include the use of artificial intelligence and machine learning, behavioral analysis, integration with other security tools, ease of use, scalability, and support for diverse endpoint platforms.
4. *Cloud Adoption*: The adoption of cloud based EPP solutions is gaining momentum. Cloud-based EPP offers benefits such as centralized management, automatic updates, scalability, and easier deployment across distributed environments. Organizations are increasingly leveraging cloud based EPP to streamline their security operations and reduce infrastructure costs.
5. *Integrated Security Suites*: Many EPP vendors have expanded their offerings to provide integrated security suites that combine EPP with other security components such as endpoint detection and response, secure web gateways, and identity and access management. These suites offer a more comprehensive and cohesive security approach, enabling organizations to manage multiple security aspects from a single platform.
6. *Shift to Endpoint Detection and Response (EDR)*: As suggested above, EDR solutions, which provide advanced threat detection, incident response, and forensic capabilities, are gaining prominence alongside EPP. While EPP focuses on prevention, EDR focuses on detection and response. Some vendors offer combined EPP-EDR solutions to provide a more comprehensive approach to endpoint security.
7. *Compliance and Regulations*: Compliance requirements and data protection regulations, such as the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), are driving the adoption of robust endpoint security solutions. EPP solutions help organizations meet regulatory requirements and safeguard sensitive data.
8. *Managed Security Services:* The market also includes managed security service providers (MSSPs) that offer EPP as part of their cybersecurity offerings. MSSPs provide

organizations with outsourced security expertise, monitoring, incident response, and ongoing management of EPP solutions.

Overall, the EPP commercial market is dynamic to address the evolving threat landscape. Organizations are increasingly recognizing the importance of robust endpoint security and are investing in EPP solutions to protect their device and sensitive data from cyber threats. This will continue, particularly as smaller companies begin to deploy EPP and EDR for threat management and compliance support.

Total Cost of Ownership (TCO) for EPP

Calculating the total cost of ownership (TCO) for an EPP solution involves considering various cost components associated with implementing, maintaining, and operating the platform. While the specific costs may vary based on your organization's requirements and the EPP provider (or EDR provider with an EPP component), here are some common factors to consider when calculating the TCO:

1. *License Fees*: Evaluate the licensing model offered by the EPP vendor. Determine whether it is per device, per user, or another metric. Consider the cost implications based on the number of endpoints or users in your organization. Also, determine if the licensing fees include ongoing updates and support or if they are separate.
2. *Maintenance and Support*: Assess the costs associated with ongoing maintenance and support. Understand the support levels provided by the EPP vendor and any associated fees. Consider factors such as access to technical support, response times, and the availability of software updates, patches, and upgrades. Determine if these services are included in the initial license fees or if they require additional payments.
3. *Implementation and Deployment*: Account for the costs related to the implementation and deployment of the EPP solution. This includes activities such as installation, configuration, integration with existing infrastructure, and any professional services required. Consider whether the EPP vendor offers implementation assistance or consulting services and the associated costs.
4. *Training and User Education*: Factor in the costs associated with training and educating your organization's IT staff and end-users on using the EPP solution effectively. Determine if the EPP vendor provides training resources, documentation, or on-site training sessions, and evaluate any additional costs for these services.
5. *Hardware and Infrastructure*: Assess whether the EPP solution requires additional hardware or infrastructure investments. Determine if any hardware upgrades or additions are necessary to support the deployment and operation of the EPP solution. Consider the costs of server hardware, network infrastructure, storage, and any other required components.
6. *Operational Costs*: Consider ongoing operational costs associated with running the EPP solution, such as electricity, cooling, maintenance of hardware infrastructure (if applicable), and any additional software licenses required to support the EPP solution.

7. *Management and Administration*: Evaluate the costs related to managing and administering the EPP solution. Consider the time and resources required for tasks such as policy configuration, threat response, incident management, and reporting. Assess whether the EPP solution offers centralized management capabilities that streamline administrative tasks to potentially reduce costs.
8. *Product Upgrades and Enhancements*: Consider the costs associated with product upgrades and enhancements. Determine if the EPP vendor regularly releases new versions or feature updates and whether these updates are included in the licensing fees or require additional payments. Consider the frequency of upgrades and any associated costs for migration or implementation of new versions.
9. *Integration Costs*: Assess the costs associated with integrating the EPP solution with other security technologies and infrastructure within your organization. Determine if there are any costs associated with implementing APIs, connectors, or custom integrations with other systems such as SIEM, SOAR, or network infrastructure.
10. *Product Lifecycle*: Consider the anticipated product lifecycle of the EPP solution. Evaluate how often the EPP vendor releases major updates or new versions and assess the costs associated with migration or implementation of these updates. Also, consider the long-term support and end-of-life plans for the EPP solution and any potential costs associated with transitioning to a new solution in the future.

By considering these factors, organizations can calculate a comprehensive TCO for an EPP solution and make more informed decisions when comparing different vendors and their offerings. It is essential to evaluate both the direct costs and the indirect costs associated with implementing, managing, and maintaining the EPP solution over its lifecycle.

Companies and Contributions

The companies listed below emerged in our research at TAG. Our goal in listing these fine firms is to provide a starting point for buyers, advocates, stakeholders, and researchers trying to make sense of the commercial landscape for companies using EPP solutions to support enterprise.

Our set of criteria for inclusion below is that a vendor must either be prominent in the interactions we have with enterprise and government practitioners or must have engaged with our analyst team to provide information onto our TAG Exchange, which does include a 100% free option for listing. We decided to keep the list to 50 vendors here, but our private Research as a Service (RaaS) portal for TAG subscribers includes many, many more.

1. Absolute: Absolute provides endpoint security and data risk management solutions for enterprise.
2. Antiy Labs: Antiy Labs is a vender of antivirus engine and solution, providing the best-in-breed antivirus engine and next generation antivirus services.
3. Arcabit: Arcabit specializes in providing antivirus and endpoint protection solutions including for enterprise.

4. Avast: Avast offers antivirus software and cybersecurity solutions for individuals and businesses.
5. Bitdefender: Bitdefender GravityZone provides advanced cybersecurity solutions, including endpoint security and threat detection.
6. BlackBerry: BlackBerry offers AI-driven cybersecurity solutions.
7. Broadcom: Symantec, now part of Broadcom, provides cybersecurity and information protection solutions.
8. Check Point: Check Point Harmony Endpoint provides endpoint security and threat prevention solutions.
9. Cisco: Cisco Secure Endpoints offers advanced security solutions for endpoint protection.
10. Comodo: Comodo offers a range of endpoint security solutions for use by enterprise teams.
11. Crowdstrike: Crowdstrike Falcon offers cloud-native endpoint security and threat intelligence.
12. Cybereason: Cybereason provides a popular endpoint detection and response (EDR) solution.
13. Cynet: Cynet provides an autonomous commercial breach protection platform for enterprise teams.
14. Deep Instinct: Deep Instinct specializes in AI-driven endpoint protection against cyber threats.
15. Doctor Web: Doctor Web is a Russian cybersecurity company offering antivirus and anti-malware products.
16. Emsisoft: Emsisoft provides real-time antivirus and anti-malware solutions for endpoints.
17. eScan: eScan offers endpoint security solutions, including antivirus and anti-malware software.
18. ESET: ESET is a well-known vendor that provides antivirus and internet security software.
19. F-Secure: F-Secure is a popular commercial vendor that provides cybersecurity and privacy solutions.
20. Fortinet: Fortinet's Endpoint Visibility and Control offers endpoint security solutions, including visibility and control.
21. Fortra: Fortra (formerly HelpSystems) provides a large suite of cybersecurity and endpoint protection solutions.
22. Heimdal Security: Heimdal EDR provides a range of endpoint detection and response solutions.
23. Joe Security: Joe Security offers advanced threat analysis and endpoint protection solutions.
24. K7 Computing: K7 Computing provides antivirus and internet security solutions for endpoints.
25. Kaspersky: Kaspersky a vendor headquartered in Russia that offers cybersecurity and antivirus software.
26. MacPaw: CleanMyMac X is a Mac optimization and cleaning software that will help teams who prefer to use Macs.
27. MalwareBytes: MalwareBytes provides a suite of anti-malware and anti-spyware solutions.

28. ManageEngine (Zoho): ManageEngine offers a wide range of IT management and security solutions.
29. Microsoft: Microsoft Defender for Endpoint provides advanced threat protection for Windows-based systems.
30. Morphisec: Morphisec offers various advanced endpoint protections against cyber threats.
31. N-able: N-able RMM provides remote monitoring and management solutions for IT professionals.
32. Norton: Norton (a Gen-Digital Company) offers cybersecurity and identity theft protection services.
33. OpenText: OpenText is a popular vendor that offers enterprise information management solutions including an endpoint security tool.
34. OPSWAT: OPSWAT provides cybersecurity solutions, including endpoint protection and threat detection.
35. Palo Alto Networks: Palo Alto Networks provides cybersecurity solutions, including firewalls and network security.
36. REVE: REVE Antivirus offers antivirus and endpoint security solutions for business.
37. SentinelOne: SentinelOne is a top security provider that offers autonomous endpoint protection.
38. Sophos: Sophos Intercept X provides advanced endpoint security and threat prevention.
39. Stormshield: Stormshield Endpoint Security offers advanced cybersecurity solutions.
40. Syxsense Secure: Syxsense Secure offers a suite of endpoint security and management solutions.
41. Trellix: Trellix FireEye Endpoint Security provides advanced threat intelligence and protection.
42. Trend Micro: Trend Micro offers various cybersecurity solutions for individuals and businesses.
43. Vipre: Vipre provides antivirus and endpoint security solutions that can be deployed for enterprise.
44. VMware: VMware offers cloud-native endpoint protection and security solutions.
45. WatchGuard: Watchguard offers endpoint security solutions required to stop advanced cyberattacks.
46. WithSecure: WithSecure provides cybersecurity solutions that include support for endpoint security.
47. Xcitium: Xcitium Endpoint offers a suite of commercial endpoint security solutions.

About TAG

TAG is a trusted next generation research and advisory company that utilizes an AI-powered SaaS platform to deliver on-demand insights, guidance, and recommendations to enterprise teams, government agencies, and commercial vendors in cybersecurity, artificial intelligence, and climate science/sustainability.