Solutions Review

Endpoint Security Buyer's Guide

Includes a Category Overview; the Top 10 Questions to Ask; Plus, a Capabilities Reference of the Leading 24 Providers for Endpoint Security Solutions

INTRODUCTION

Malware co-developed almost simultaneously with the advent of the Information Age. Creeper, the first known computer virus, was developed in 1971, just three years after the creation of the ARPAnet. Creeper would not look unfamiliar to a modern information security professional. It spread unchecked through the primitive internet, displaying the text "I'm the Creeper. Catch me if you can!" on affected mainframes. Shortly after that, a different program—Reaper—was developed. Its only purpose was to delete Creeper. It was the first antivirus software. From that playful beginning, malware detection and interception developed into its present-day arms race.

As of 2017, endpoint protection has moved far beyond basic malware scanning. It's a commodity of information security, but its exact definition is a moving target. Compare this to other information security products: An Intrusion Protection Systems (IDS) lets you know when bad packets or weird connections threaten the integrity of your perimeter. Identity and Access Management (IAM) lets you manage user accounts. Endpoint protection used to only mean antivirus, but now even a basic product will include a personal firewall and the ability to control ports and devices.

"As of 2017, Endpoint Protection has moved far beyond basic malware scanning."

Organizations also use endpoint protection to enforce compliance policies, preventing end-users from installing programs that they consider unsecure. Other products also cover laptops and cellphones. Yet more variants of endpoint protection bundle in data loss prevention and vulnerability scanning. Basically, endpoint protection means different things to different people, and there's no standard definition in place.

Maybe, with all the shifting going on in the endpoint protecting space, you should stick to the traditional definition of EP as an antivirus platform? Unfortunately, you might not find yourself well-served by this plan. Malware scanning, on its own, can't currently keep up with the volume of new viruses that are being written every day, and many products simply don't update their malware signatures fast enough to remain relevant. The actual concept of signature-based detection is in fact quickly dying out, replaced by concepts such as whitelisting and behavioral detection.

For those seeking to buy or update an endpoint protection product, there are even more issues to consider. For one thing, this product may now include functionality such as firewalls, GRC, DLP, and more. You may have standalone systems that accomplish these functions already. If so, learning whether these products will play nicely together becomes your first priority. You'll want to consider how your endpoint protection product can provide or accept data from other applications and security tools. Given that a layered approach to security is paramount; your endpoint protection product must be considered from a holistic point of view.

The good news is that if you need endpoint protection, there's a thriving and competitive marketplace awaiting your custom. As for bad news, the loose definition of the product will have you poring through a lot of product descriptions on a search to find the one solution that fits the bill. Fortunately, our 2017 Endpoint Protection Buyers Guide is here to help.

Our Capabilities Reference offers a profile of the leading 24 providers for endpoint protection solutions. Editors at Solutions Review cut through the rhetoric to provide an unbiased rundown of unique product key features. Provider profiles aim to illustrate company objectives and background in a snapshot, and unearth the technical capabilities of each endpoint protection product and service. Additionally, we provide consumers the bottom line- our take on what make the featured providers unique, distinctive or exceptional. Before you begin your research, here are a few key questions to ask yourself and your vendors before you make your decision.

Jeffrey Edwards
Editor
Solutions Review

5 Questions You Should Ask Yourself Before Selecting an Endpoint Security Solution

QUESTION 1 What size solution do I need?

If you're running a thirty-person company, you're going to need a different solution than if you're overseeing security for an enterprise of five thousand. You can't laugh off security if you're a small company—no one is too small to target—but you might be able to get away with using an all-in-one solution that bundles in DLP, vulnerability scanning, and asset tracking along with the basic functionality. When you're at the helm of a larger organization, you may be more likely to have a pre-existing network architecture that would make a broader endpoint protection product redundant.

QUESTION 2 How will I educate my users?

One of the biggest concerns that's overlooked when onboarding a new solution is, "how are my users going to respond to this?" This is a huge problem with endpoint protection because an endpoint is any device that connects to your corporate network. Your users' laptops and personal devices need to have endpoint protection installed for your network to be truly secure. If your users aren't security-aware, however, they might ignore the malware scanners warnings, circumvent its firewall, or even just uninstall it. How will you make your end-users aware that endpoint protection is critical?

QUESTION 3 How do I implement the product?

This is another question that depends on the systems that you have up and running before choosing a new endpoint protection strategy. If you're just setting up an organization, you won't have to worry much about your product conflicting with pre-existing systems. In a more established organization, you'll have to wonder about conflicts, not just with existing security applications, but also with applications currently employed by your end users. For users to buy into information security, you must implement endpoint protection in a way that doesn't interfere with day-to-day activities.

QUESTION 4 How does this affect my team?

A common misconception about endpoint protection is that it is fundamentally a "set it and forget it" kind of product. It's not—endpoint protection requires a modicum of human interaction to remain functional. For example, most signature-based products will automatically update their list of known malware, but certain kinds of malware can disable the update process. To prevent this and other forms of malfunction, you need to divert resources to review logs, apply patches, and check for infection. This will necessarily take time and effort away from other projects, so plan accordingly.

QUESTION 5 What is my contingency plan?

Even the smartest and most cutting-edge behavioral recognition algorithms are going to eventually trip up and fail to recognize malware. Implementing a new endpoint protection product is the perfect time to re-evaluate your incident response and digital forensics plan. You'll also need to understand how to integrate your new endpoint protection product into your overall incident response. This may be something as simple as dumping the logs from a personal firewall for analysis, or as complicated as purchasing an endpoint protection product with dedicated incident response capabilities.

5 Questions You Should Ask Your Potential Endpoint Security Solution Provider

QUESTION 6 How good is the core functionality?

Apart from all the bells and whistles that are tacked on, endpoint protection includes three basic things: a malware scanner, a personal firewall, and the ability to control ports and devices. So, how well does your endpoint protection product perform those three basic functions? Does it rely on outdated methods such as signature-based detection? Does it incorporate new techniques like sandboxing, whitelisting, or behavioral detection? How well does it execute on these concepts?

QUESTION 7 Will it run on all of my devices?

A typical enterprise has a veritable zoo of devices that are connected to its network—not just Windows and Apple computers, but cell phones running iOS, Android, Windows Phone, and even the occasional senescent Blackberry. That's not even counting the servers. Can your endpoint protection product run on all these devices? Does it run well on different platforms? If the answer is no, you'll need to either find a solution that's platform-agnostic, or resign yourself to finding a second solution that will cover the platforms that the first one can't.

QUESTION 8 Will it provide granular data?

Many endpoint protection solutions now provide asset tracking functionality, and enterprise products will include a visor where you can survey all connected devices. How much information can you get out of these viewpoints? If you have many servers and workstations, it may be useful to collect and track statistics on how many computers are running on outdated hardware. Another time-saver is the ability to remotely push updates to connected devices, or push notifications to users and admins. Even if you don't need these capabilities right away, these features may become more practical as the size of your enterprise increases.

QUESTION 9 How does it react to the unexpected?

Let's say that tomorrow morning, you find that a new piece of malware can exploit a vulnerability in an application you use—a Zero Day has emerged. How long does it take for your endpoint protection to react?

In a 2015 study by Damballa, seven percent of dangerous malware went unrecognized by signature-based detection systems for longer than a month, and for as long as six months. More up-to-date methods look for suspicious behavior to trigger alerts. Whatever solution you choose, endeavor to understand how fast they can react to new threats.

QUESTION 10 Is the product well supported?

Aside from all the discussion about feature sets, capabilities, and detection methods, support is the last important question. Emergencies don't happen on a schedule, so can the vendor get you on the phone with an engineer at the drop of a hat? If not, can they train your staff to support the product on their own?

Lastly, is training bundled into the price of the product, or offered separately? As always, having well-trained staff and a thorough knowledge of a security tool is equally as important as the tool itself.

Endpoint Security Solution Profiles

Bit Defender

Romanian information security company Bitdefender's GravityZone Security for Endpoints is a modular solution delivers centralized management and deployment under the umbrella of various virtualization vendors, cloud providers, servers, desktops, laptops, and mobile devices. Bitdefender invests a quarter of its R&D budget in 'disruptive ideas,' and has become a player in 'next generation' technologies such as machine learning and threat detection. Recently released products includedBitdefender BOX, a solution that protects all of a user's connected devices; and Hypervisor Introspection (HVI), a framework to secure virtualized environments from advanced targeted cyberattacks.

From the Company

"Bitdefender's GravityZone is Bitdefender's Enterprise security solution for medium to large organizations. It's redesigned from the ground up with a fresh, but proven private cloud computing architecture that takes full advantage of virtualized infrastructures. GravityZone leverages Bitdefender's acclaimed antimalware technologies and provides a centralized security management platform for physical, virtualized, and mobile endpoints. It is a business-agile solution that implements a holistic approach. Not just antivirus, but an enterprise-grade solution that helps organizations to attain their virtualization projects' objectives and secure data, while preserving the systems' performance and users' productivity."

Key Features

Global Protective Network (GPN) – Performs 7 billion queries daily; uses reflective models and machine learning algorithms to extract malware patterns

Photon™ – Optimizes scanning processes by examining unknown, suspicious, or modified files, and can adapt to each computer within networks throughout the process

Firewall – Provides a fully-featured two-way personal firewall with Intrusion Detection to block attacks and hijack attempts

Multilanguage Support – Available in English, German, French, and Romanian

Bottom Line

Bitdefender's solution is supported by Windows, Mac, and Linux operating systems. GravityZone is an on-premise console and is delivered as a virtual appliance that is compatible with OVA, XVA, and VHD formats.

Carbon Black

Formerly Bit9 + Carbon Black, this Massachusetts-based security company stepped up its game in 2016, with multiple key acquisitions and an IPO. Carbon Black's endpoint security software detects malicious behavior and prevents malicious files from attacking an organization. Software consistently records all endpoint activity making it easy to track potential security threats and determine root causes. Carbon Black offers custom API's, giving IT teams the ability to integrate security capabilities from a variety of solutions.

From the Company

"Carbon Black leads a new era of endpoint security by enabling organizations to disrupt advanced attacks, deploy the best prevention strategies for their business, and leverage the expertise of 10,000 professionals from IR firms, MSSPs, and enterprises to shift the balance of power back to security teams. Only Carbon Black continuously records and centrally retains all endpoint activity, making it easy to track an attacker's every action, instantly scope every incident, unravel entire attacks and determine root causes. Carbon Black also offers a range of prevention options so organizations can match their endpoint defense to their business needs."

Key Features

Detect and Disrupt Attacks - Respond instantly by leveraging a recorded history of all endpoint data, along with active banning and live response remediation.

Real-Time Visibility - Continuously record critical endpoint data—even while devices are offline or outside your corporate network to quickly detect infected systems and identify unpatched endpoint vulnerabilities

Improve Control and Security- Greatly reduce your attack surface while ensuring the right balance between protection and access.

Eliminate Reimaging- The powerful combination of advanced threat prevention with the ability to remotely isolate and remediate attacks before they occur dramatically reduces malware infections and eliminates the need for reimaging.

Bottom Line

Carbon Black offers multiple deployment options and minimizes zero-day exploits with continuous real time monitoring. Products retain a persistent history of attackers' every action, the cause of their attacks, and patterns of behavior then Isolate, terminate, remediate and ban endpoint threats.

Check Point

California-based Check Point Software provides a security solution that combines data and network security with threat prevention technologies, as well as remote access VPN for both Windows and Mac software. Their solution prevents potential security threats and can provide visibility into network worms through malware detection for signatures and behavioral analysis, which can help prevent significant damage before it occurs.

From the Company

"Since 1993, Check Point has provided protection against threats, reduced security complexity and lowered total cost of ownership. Since its inception, their pure focus has been on IT security and adapting to customers' changing needs. They have developed numerous technologies to secure the use of the Internet by corporations and consumers when transaction and communicating. Their unified security architecture is operated through a single console that unified security gateways and remains to be their single agent for endpoint security protection."

Key Features

Software Blade – A single management platform that can monitor, manage, and enforce policies via At-a-Glance Dashboard to manage 6 Endpoint Software Blades

Single Console – Enables central policy management, enforcement, and logging from centralized console, and can control security policies as well as multiple deployment options

Compliance Check – Provides network surveillance before users log into the network to monitor appropriate security, correct OS service packs, approved applications, whether anti-malware is intact, etc.

Encryption – Enables full disk and media encryption for secure information on all existing drives, as well as multi-factor pre-boot authentication

Bottom Line

Check Point's Endpoint Security is centrally managed by their Endpoint Policy Management Software Blade, which enables central policy administration, enforcement, and logging from a single console. Their software supports Microsoft Windows 7 & 8 (Enterprise and Professional), Microsoft Vista, and Microsoft Windows XP Pro, as well as Mac OSX operating systems.

Code42

Code42 is a global enterprise SaaS provider of endpoint data protection and security. Headquartered in Minneapolis, Minnesota, their cloud solutions enable IT teams to meet data privacy regulations, recover from data loss, and limit risk. Code 42 protects users from 'Datastrophe" with enterprise grade security, desktop OS protection, data storage in private, public or hybrid cloud, and secure mobile file access.

From the Company

"We're best known for CrashPlan, an enterprise SaaS solution that backs up all distributed end-user data on a single, secure platform. Through continuous, automatic collection via a lightweight agent on the device, CrashPlan protects every file on Apple OS X®, Windows and Linux laptops and desktops. Our platform enables IT security and business teams to limit risk meet data privacy regulations and recover from data loss, no matter the cause."

Key Features

GI Enterprise-Grade Security – File encryption for all files on devices remain encrypted in-transit and at rest with AES 256-bit encryption.

Protect Every Device - Protect all major desktop operating systems and provide file access on all major mobile platforms with a single solution.

Cloud Choice for Security and Availability- CrashPlan's flexible data storage and security architecture lets you choose where to keep your data and encryption keys in a private, public or hybrid cloud.

People-Friendly, Enterprise-Approved - CrashPlan meets IT needs and provides employees continuous backup, secure mobile file access, intuitive self-service restore.

Bottom Line

Traditionally enterprises needed to build custom API's to leverage several identity management solutions to connect with their data protection technologies. Code42's broadened support for SAML 2.0 enables IT organizations utilizing several identity providers to integrate these solutions using Code42's EDGE Platform. Code42 System Engineers can assist you in gathering requirements and developing specifications and have designed solutions that have been successful for organizations ranging in size from startups to global enterprises.

Comodo

Founded in 1998, Comodo operates out of Clifton, New Jersey and offers consumers a range of Endpoint Security solutions. Comodo's Endpoint Security Manager provides centralized management of a 7-layered security suite that protects endpoints and their applications against malware and threats. System administrators can terminate suspicious network connections, force-close processes, stop services and uninstall applications. The administrator is also able to resolve processes causing CPU or RAM saturation and quickly establish the largest files on the endpoint's hard-drive and selectively delete them.

From the Company

"The Comodo organization is a global innovator and developer of cyber security solutions, founded on the belief that every single digital transaction deserves and requires a unique layer of trust and security. Building on its deep history in SSL certificates, antivirus and endpoint security leadership, and true containment technology, individuals and enterprises rely on Comodo's proven solutions to authenticate, validate and secure their most critical information. With data protection covering endpoint, network and mobile security, plus identity and access management, Comodo's proprietary technologies help solve the malware and cyber-attack challenges of today."

Key Features

Host Intrusion Protection System (HIPS) – A rules-based intrusion prevention system that monitors all activities of applications and processes.

Containment with auto-sandboxing – A preventative layer that auto-sandboxes files that have yet to be reported to any known blacklist.

Comodo Firewall – A highly configurable packet filtering firewall that constantly defends inbound and outbound Internet attacks.

Comodo Antivirus – A proactive antivirus engine that automatically detects and eliminates viruses, worms, and other malware

Bottom Line

Comodo combines endpoint security management with system monitoring tools by managing endpoint network connections, processes and services, applications, CPU, RAM and hard-disk usage and bandwidth consumption. Administrators are alerted in real-time program detects deviations from acceptable or pre-defined standards.

CounterTack

Headquartered in Massachusetts, CounterTack leverages big data and behavioral analytics with a next-generation endpoint security solution called Sentinel. Sentinel fuses efficient threat detection, data collection and correlation with Big Data technology to scale endpoint detection and response-countering threats based on unprecedented endpoint intelligence. Sentinel is built on four foundational concepts as part of the, "Continuous Endpoint Threat Detection and Response Lifecycle"- Detect, Analyze, Respond and Resist.

From the Company

"Built on Big Data architecture to counter endpoint threats at-scale and leveraging tamper-resistant collection for pure behavioral capture on enterprise endpoints, (laptops, servers, workstations, mobile devices) CounterTack dramatically reduces the impact of advanced threats in real-time and post-incident, giving teams an opportunity to defend the enterprise across the entire cyber kill chain."

Key Features

Detect - Detect advanced threats through behavioral-based monitoring. Through its proprietary endpoint data collection process, Sentinel detects the key behaviors that define an incident for teams. Sentinel detects known, unknown and previously unseen attacker behavior.

Analyze - Analyze threats to fully understand potential impact across all endpoints. Sentinel provides the capability to analyze threats against proprietary and open-source compromise indicators, with the ability to isolate threats on the host.

Respond - Use actionable intelligence for a continuous response to incidents and threats. Sentinel lets operators deny advanced threats from fully executing to machines with real-time remediation capabilities so teams can prevent the full attack from impacting the production system.

Resist - Prevent threats once detected by Sentinel from ever running again with the capability to dramatically reduce the time associated with incident investigation and research.

Bottom Line

CounterTack puts power back in the hands of IT teams by offering a custom, expansible combination of tamper-resistant OS surveillance. Security Teams are provided the remediation capabilities required to mitigate the impact of incidents and malicious events on laptops, devices, workstations and servers.

CrowdStrike

CrowdStrike, a California-based company, offers its endpoint solution, Falcon Host, which provides visibility in real-time and detects attacks within your software. Their solution integrates into your current environment and enables your IT team to detect and block suspicious activity in order to prevent damage to your business. Their solution covers Windows desktop and servers as well as Mac computers, whether on or off the network.

From the Company

"CrowdStrike Falcon Host integrates seamlessly into your current environment, enabling your security team to effectively and efficiently detect and block adversary activity - -ultimately preventing damage to your organization through Saas-based next-generation endpoint protection. The solution provides real-time visibility into adversary activity on every endpoint, and the lightweight Falcon sensor immediately detects attacks and protects your data without having to rely on 'sweeps and scans' of the environment. Their Advanced Threat Intelligence Cloud combines advanced machine learning and can graph data models to analyze billions of endpoint events, spotting and correlating anomalies to alert you when an attack is underway."

Key Features

Indicators of Attack – Allows you to focus on proactive indicators of attack vs. indicators of compromise to gain effective insight into your business activities.

Visibility – The Advanced Intelligence Cloud enables detection of who is attacking you, and where the attack is coming from.

Falcon API - Provides simple integration of CrowdStrike's endpoint protection with your existing security architecture and SIEM tools

Custom Blocking – Enables users to set up custom blocking via whitelisting or blacklisting and provides control over what can or cannot run on endpoints.

Bottom Line

CrowdStrike provides native cloud architecture to ensure zero hardware, software, and maintenance costs. Their interface consists of nine components: Whitelisting, Micro VM, virtual detonation, machine learning (AV 2.0), exploit mitigation, HIPS, IOC detection, containment, and forensics.

ESET

ESET is headquartered in Bratislava, Slovak Republic, and offers software programs for malware detection and protection. Their Endpoint Security solution detects and blocks Trojans, adware, viruses, worms and other forms of malware, including emerging threats. The software includes a firewall, which can help block malicious traffic and prevent the accidental spread of malware. The anti-theft feature can help protect mobile devices and, in the event that a device is stolen, can lock down device or wipe it, ensuring that unauthorized persons cannot access information.

From the Company

"ESET provides proactive threat protection and develops software that reacts immediately to new and emerging threats. They also ensure protection through two methods of detection (comparing known virus signatures and using heuristics to anticipate new ones) as opposed to one. Their software is built to run unnoticed in the background and to deliver scanning with little system footprint to reduce compromised performance."

Key Features

Antivirus and Antispyware Protection - Eliminates all types of threats, including viruses, rootkits, worms and spyware with optional cloud-powered scanning for better performance and detection.

Advanced Memory Scanner - Monitors the behavior of malicious processes and scans them, allowing for effective infection prevention.

Exploit Blocker - Detection technology that strengthens protection against targeted attacks and previously unknown exploits.

Optimized for the Virtual Environment - ESET Shared Local Cache stores the metadata of scanned files, so replica files on one machine are not scanned again on other virtual machines.

Bottom Line

ESET offers easy to implement advanced security for mobile workforce and network, in addition to protecting computers, tablets and file servers from malware. Protection includes firewall, antispam and content filtering for data access protection while Antispam monitors email traffic for spam that may carry malware.

F-Secure

F-Secure Corporation is an online security and privacy company based in Helsinki, Finland. F-Secure Client Security is endpoint protection for PCs running Windows. Client Security offers proactive, heuristic protection against the latest emerging threats, complete with automated software updates, and continuous endpoint protection against known vulnerabilities.

From the Company

"F-Secure Client Security is award-winning endpoint protection for PCs running the Windows® operating system. It's much more than just Anti-Virus. Client Security is proactive, heuristic protection against the latest emerging threats. Complete with automated software updates, Client Security provides the ultimate endpoint protection against known vulnerabilities."

Key Features

Info Protection and Wi-Fi Security - DeepGuard provides proactive on-host protection against new and emerging threats. Its dynamic, proactive behavioral analysis technology efficiently identifies and intercepts malicious behavior. Connect to any hotspot, public or private and surf without exposing your traffic.

Remove geo-blocking - Access geo-restricted content by changing your virtual location.

Safe Transactions - Connection Control prevents banking Trojans from sending sensitive information to online criminals. It does this by automatically closing network connections to unknown sites and preventing new ones during business-critical actions such as online banking. You can enable Connection Control to sites that support HTTPS.

Bottom Line

F-Secure's products and business solutions are ideal candidates for SMBs looking for efficient systems with a low overhead. F-Secure's strong track record on anti-malware technology makes the company a good chose for SMBs for whom malware protection is a high priority.

FireEye

Hailing from California, FireEye is renowned for having invented a purpose-built, virtual machine-based security platform that provides real-time threat protection to enterprises and governments worldwide, against the next generation of cyber-attacks. Most sophisticated cyber attacks easily circumvent traditional signature-based defenses, so FireEye retaliates with next-generation firewalls, IPS, anti-virus, and gateways. FireEye platform utilizes a virtual execution engine, armed with dynamic threat intelligence, to quickly expose and obstruct cyber-attacks in real time.

From the Company

"Many vendors differentiate between the risks of organization-owned and bring-your-own-devices (BYOD), remote and onsite devices, and even connected and disconnected devices. But really, they are all part of the soon-to-be worldwide collection of 50 billion connected devices. Every one of those endpoints is a cyber security risk: the first point of attack and network vulnerability. An attacker only needs to breach one, but you have to protect them all. To protect those endpoints, and your network, FireEye offers a unified endpoint defense: the Secure Endpoint and Mobility solution."

Key Features

FireEye as a Service – Offers insight and intelligence from the front lines of incident responses, and proactive hunting for indicators of compromise (IOCs) in your environment. Provides around-the-clock monitoring for indications that a cyber-attack has bypassed your technology defenses.

Enterprise Forensics - Enterprise forensics combines high-performance packet capture with analysis tools to aid investigation efforts. It complements several other FireEye threat prevention and detection capabilities.

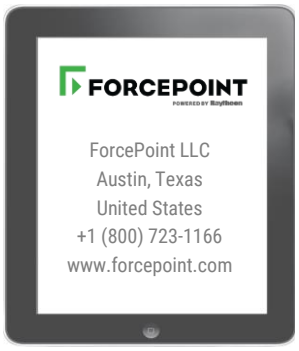
Endpoint Mobility - Detect and prevent attacks on the organization, or user-owned Android and iOS devices. Validate, interrupt or contain attacks without exposing the rest of your network.

Bottom Line

FireEye offers cyber security solution architecture with a wide range of capabilities to help security teams detect, analyze, and protect against advanced threats targeting organizations today. The solution is accommodating to businesses of all sizes while offering custom solutions for small and medium size businesses as well.

ForcePoint

In 2011, ForcePoint partnered with Facebook to provide threat intelligence and protect users from links to malware sites. ForcePoint now offers their Triton APX product to endpoint protection buyers. Users are prevented from accessing dangerous URLs, and administrators control access to data by blocking, removing, quarantining, auditing or encrypting data. Unique to most endpoint solutions, ForcePoint ensures users are adhering to company policy by monitoring endpoint use on and off the network and prevents the exfiltration of critical data.



From the Company

"We have set out to solve the intractable problem of securing users, data and networks in a world of escalating threat and dramatically changing infrastructure, compounded by the fact that most organizations have deployed dozens of disparate point products that do not communicate with each other, do not have an integrated understanding of threats, and do not share information to better piece together the full story. A key object of the Forcepoint Triton security platform is to minimize the time between compromise and remediation, known as "dwell time", and to stop theft by focusing on insider threat protection, cloud data protection and network security."

Key Features

Triton ACE – Improve your threat defenses by identifying and classifying information crossing your network to deliver real-time security ratings to all products built on the Forcepoint TRITON architecture.

ThreatSeeker Intelligence Cloud – Receives global input from over 155 countries and, working in parallel with Triton ACE, analyzes up to 5 billion requests per day.

Threat Protection Cloud - Monitor Web traffic for real-time code analysis in a behavioral sandbox for advanced threat identification.

Bottom Line

Forcepoint uses a combination of classification engines, filtering categories, data fingerprints, and word filters designated by the individual customer's network policy. Advanced technologies help to quickly identify and protect sensitive data and provide actionable forensic insight into attacks on endpoint devices on or off the network.

Heat Software

Two leading providers of hybrid service management, Lumension and FrontRange, merged in 2015, creating a company that offers buyers enhanced capabilities in the management of endpoint operations and security. Short for, *H*elpdesk *E*xpert *A*utomation *T*ool, Heat Software delivers flexible and scalable hardware security modules and user environment management solutions. The company's international headquarters is located in Milpitas, California, but is a multi-national corporation operating in Europe, Asia and Australia as well. Unified Endpoint Management products include Heat Endpoint Management, and Heat Endpoint Security.

From the Company

"Today's users expect 24/7 availability of applications and information, no matter what device they use or where the information they need physically lies. This puts pressure on IT staff to gain management control of the fast-growing heterogeneous infrastructure. However, with an increasing number of remote users, more mobile devices, and a growing use of virtual infrastructures—this is quite a challenge. IT needs a comprehensive endpoint management solution that helps them manage the infrastructure in a quick, flexible, and reliable way."

Key Features

Connect to Client Management – Heat software automates operational tasks such as maintaining virtual endpoints, improving user-end productivity, system availability, and installing applications.

Patch Management- Manages endpoint configurations and third-party applications through a single console. Automatically patches security and non-security vulnerabilities.

LANrev Enterprise Mobility Management- Manages and remotely secures mobile devices. IT teams can perform select administrative and security tasks working remotely or on-the-go by supporting employee mobile devices.

Bottom Line

Buyers will appreciate fully automated software provisioning, configuration and maintenance tasks to manage virtual and physical devices with Heat Client Management solutions. Heat Software fully protects endpoints from known and zero-day malware while enabling the use of only authorized software.

Intel Security (McAfee)

McAfee offers advanced endpoint protection for large enterprises that includes behavioral anti-malware, smart scanning, and dynamic whitelisting, in addition to essential antivirus, antispam, web security, firewall, and intrusion prevention for desktops and laptops. Power and performance is centrally managed to protect employee productivity and keep administration simple.

From the Company

"Traditional Windows, Mac, and Linux systems need essential security to block advanced malware, control data loss and compliance risks caused by removable media, and provide safe access to critical email and web applications. McAfee Endpoint Protection Suite integrates these core functions into a single, manageable, multiplatform environment ideal for safeguarding traditional desktops that have limited exposure to Internet threats. This proven enterprise and small business endpoint security solution delivers operational efficiencies and cost savings with the convenience of a single suite. It includes real-time anti-malware and antivirus protection, proactive email and web security, desktop firewall, comprehensive device control, and unrivaled centralized management."

Key Features

Easy installation and configuration – In just 20 minutes McAfee ePolicy Orchestrator streamlines and automates workflow, policy deployment, updates, maintenance, and reporting across all devices.

Reduce the attack and save time - Dynamic application control allows installation of only known good files or applications based on a flexible, automated update model.

Unify and simplify management - Flexible response and actionable threat forensics - simplify investigations so you can focus on the most critical risks by integrating with Intel Security and third-party products increase visibility and efficiency.

Bottom Line

McAfee Active Response offers continuous detection and response to advanced threats so IT can focus on expanding incident response strategies and prioritizing alerts. Provides complete real-time visibility into your endpoints to identify and remediate threats faster.

Kaspersky Lab

The company's Anti Targeted Attack Platform is a solution that enables businesses to detect attacks and other malicious actions by monitoring web, e-mail and network activity attacks at any stage. Suspicious events are processed with an Advanced Sandbox and Targeted Attack Analyzer for a final report. The technology provides an isolated environment for analyzing attacks and their intent. Platforms are available as an independent solution or in combination with expert services aimed at rapid incident detection and response.

From the Company

"When businesses face an adversary with the skill, knowledge, and determination to overcome the many existing security technologies, they need knowledge of possible attack vector details of the indicators of compromise, and the ability to distinguish normal operations from malicious activity. This is an immense undertaking which requires strong security expertise combined with technology that is capable of spotting a criminal act in the avalanche of daily activity in a large corporation. This is the challenge that is being addressed with the Kaspersky Anti Targeted Attack Platform, together with the security services aimed at sharing security intelligence with our customers faster than ever before. Today we announce our entry into a new category of security products, one that we believe will define the future of the IT security industry."

Key Features

Powerful Data Protection – File/ Folder and Full Disk Encryption can be applied to endpoints.

SIEM Integration – Support for IBM® QRadar and HP ArcSight SIEM systems.

Vulnerability and Patch Management – Automated OS and application vulnerability detection and prioritization, combined with the rapid automated distribution of patches and updates.

Host-based Intrusion Prevention System with Personal Firewall –Restricts activities according to the application's trust level – supported by an application level Personal Firewall, which restricts network activity.

Bottom Line

Kaspersky maintains an exceptional level of protection, performance and usability. The software features help you keep private data safe with antivirus applications that provide threat prevention, yet have minimal impact on system resources and usability of your PC.

LANDESK

Originally founded in 1985 as LAN Systems, the company's endpoint protection software allows users to manage, update and protect critical data. LANDESK's intuitive console integrates several security layers and enforces security policies on users and devices in the private or public cloud. Users can automate patch management and deployment, encrypt data and grant network access.

From the Company

"Your users and your enterprise's critical IT resources face an ever-evolving range of threats, from online criminals to internal mistakes. LANDESK Security Suite helps to maximize protection against those threats. It delivers multi-layered endpoint protection, even against zero-day threats, without compromising user productivity. It automates patching of critical operating systems and third-party applications, even on systems that are mobile, remote, or asleep. LANDESK Security Suite boosts compliance with industry standards, ensures your user environment is stable and secure and integrates with systems management to further reduce risk and extend protection and control."

Key Features

Patch Management - Maintain a secure, productive environment. Patch vulnerabilities in multiple operating systems and keep third-party applications up to date.

Application Control - Defend against zero-day threats and malicious software by controlling what software is allowed with Host Intrusion Protection.

Device and Connection Control - Prevent data loss and installation of malicious software by blocking access to devices and connections.

Bottom Line

LANDESK patch management can be used as a built-in component of LANDESK Security Suite to maintain baseline security, stability, and performance for your applications and operating systems. The Security Suite extends active security management to all endpoints and offers a console to discover, manage, update, and protect all of your deployed systems.

Microsoft (System Center)

Best known for its line of operating systems, Microsoft Corporation also offers endpoint protection solutions. Window's Enterprise mobility suite (EMS) provides a foundation for protection against modern threats and continuous management with greater protection of users, devices, apps, and data, while eliminating concern about scale, maintenance, and updates. Microsoft's cloud-first approach provides an integrated set of solutions that are designed to work together from the ground up, avoiding the need for complicated integration efforts across point capabilities.

From the Company

"A key concern for you continues to be security, and rightly so. Identity is the control plane at the center of our solution helping you to be more secure. Only Microsoft offers cloud identity and access management solutions running at Internet scale and designed to help secure your IT environment. Microsoft Azure Active Directory has hundreds of millions of users, is available in 35 datacenters around the world, and has processed more than 1 trillion (yes, trillion) authentications. Our innovative new technology, Microsoft Advanced Threat Analytics is designed to help you identify advanced persistent threats in your organization before they cause damage."

Key Features

Service-Oriented Threat detection: Detect abnormal user behavior, suspicious activities, known malicious attacks and security issues.

Conditional access: Control access to applications and other corporate resources like email and files with policy-based conditions that evaluate criteria such as device health, user location etc.

Single sign-on: Sign in once to cloud and on-premises web apps from any device. Pre-integrated support for Salesforce, Concur, Workday, and thousands more popular SaaS apps.

Bottom Line

The Microsoft Enterprise Mobility Suite was created to address today's move to mobile, cloud-based services and offers three core components—Microsoft Azure Active Directory Premium, Microsoft Intune, and Microsoft Azure Rights Management designed to work together, providing an integrated endpoint protection solution.

Palo Alto Networks

Based in Santa Clara, California and founded in 2005, Palo Alto Networks has combined network, cloud and endpoint security into one integrated platform that delivers automated prevention against cyberattacks. Palo Alto's Traps™ endpoint solution focuses on the attacker's core techniques and when the attacker's path becomes known, the program blocks advanced attacks originating from executables, data files or network-based exploits.

From the Company

"As the next-generation security company, we are leading a new era in cybersecurity by safely enabling all applications and preventing advanced threats from achieving their objectives for tens of thousands of organizations around the world. We are one of the fastest growing security companies in the market because of our deep expertise, commitment to innovation, and game-changing security platform focused on bringing an end to the era of breaches by uniquely integrating our Next-Generation Firewall, Advanced Endpoint Protection, and Threat Intelligence Cloud."

Key Features

Exploit Mitigation- Traps™ focuses on the core techniques leveraged by exploits in advanced cyber attacks and render these techniques ineffective by blocking the technique.

Malicious Executable Prevention - Traps prevents executable malware by preventing core malware techniques. Additionally, the WildFire™ threat intelligence cloud offers rapid analysis of executables before they can run.

Lightweight yet Comprehensive - Traps does not perform system scanning or rely on updates, so users experience minimal impact while protecting all applications.

Bottom Line

Palo Alto's endpoint solution is designed to deliver automated preventative measures against cyber threats. Businesses can implement key technology initiatives within the cloud and increasingly mobile networks, while maintaining visibility and control, to protect data assets and critical control systems.

Panda Security

Founded in 1990 in Bilbao, Spain, Panda Security Endpoint Protection Platforms embrace cloud delivery of security services. Their Collective Intelligence technology offers a security model that automatically analyzes and categorizes new malware offering effective protection against Internet threats with minimum impact on system performance. Panda Security´s portfolio of solutions include SaaS based protection of endpoints, email and web traffic, cloud-based systems management, as well as an integrated on-premises endpoint protection platform. Additionally, all products are backed by tech support services.

From the Company

"For more than 20 years, Panda Security has achieved major technological milestones in the global security industry. Today Panda is a solid, internationally acclaimed company with a direct presence in 80 countries. It protects over 10 million users in 195 countries. Our mission is to simplify complexity creating new and better solutions to safeguard the digital lives of our users. In 2009, notable international opinion leaders acknowledged Panda Security as The Cloud Security Company."

Key Features

Malware Freezer- Avoid false positives and freeze the malware detected for seven days with the option to automatically restore the file on the user's system.

Detection - Maximum malware detection, even for malware that exploits unknown (zero-day) vulnerabilities, regardless of the source of infection.

Real-time Monitoring and Reports- Carefully monitor the security of your corporate network and automatically generate easy to interpret reports and graphs or consult all of this data in real-time thorough comprehensive dashboards.

Bottom Line

Panda Security Endpoint Protection provides centralized protection for Windows, Mac and Linux workstations, including laptops, smartphones, and the leading virtualization systems.

RSA Security

RSA NetWitness Endpoint is endpoint threat detection and response solution that exposes targeted, advanced malware, highlights suspicious activity for investigation, and instantly determines the scope of a compromise to help security teams stop advanced threats faster. NetWitness Endpoint's unique behavioral-based detection identifies unknown, zero-day malware and compromises that other tools don't see.

From the Company

"Cyber criminals are becoming more creative when it comes to developing new techniques to penetrate an organization's network. If a network is infected by an unknown malware, relying on signature-based tools like Anti-Virus solutions will leave you with a false sense of security. When a network is at risk, analysts must be able to detect the issue quickly and rapidly understand the type of attack along with the affected systems to understand the extent of malicious activity at the endpoints. NetWitness Endpoint complements our network and cloud approaches to provide pervasive visibility for faster threat detection and remediation."

Key Features

Expose Advanced Threats - Real-time monitoring and alerting as well as fast, comprehensive scans provide deep visibility into Windows and Mac endpoints across the enterprise and collect all of the information needed for a complete investigation.

Analyze and Confirm Infections Quickly - Intelligent risk level scoring system prioritizes suspicious endpoint activity leveraging dynamic data trained through machine learning and focuses the analyst on real threats in the early stages.

Enterprise-Level Scalability - Each NetWitness Endpoint server supports 50,000 agents with multi-server support for larger deployments.

Bottom Line

RSA offers technology solutions, including authentication and credential management, access management, identity administration, and data protection. Also, the company provides business solutions, including regulatory compliance, password management, consumer identity protection, portal and partner integration, mobile workforce security, and credit/debit card information protection.

Sentinel One

SentinelOne offers real-time endpoint protection driven by intelligent automation machine learning. Founded in 2012 in Mountain View, California, SentinelOne uses predictive execution inspection to monitor endpoints and detect unknown threats. The solution offers real-time forensics to deliver investigative capabilities much like "sandboxing" during a breach. The technology fully automates remediation, and removes threats.

From the Company

"SentinelOne is shaping the future of endpoint security by unifying prevention, detection and response in a single platform that uses machine learning and intelligent automation to defeat even the most advanced zero-day threats. With SentinelOne, organizations can predict malicious behavior across multiple threat vectors, rapidly eliminate cyber-attacks with fully-automated, integrated response capabilities, and adapt their defenses in real-time. SentinelOne was formed by an elite team of cyber security and defense experts from IBM, Intel, Check Point, McAfee, Palo Alto Networks and the Israel Defense Forces."

Key Features

Data Attack Storyline Visualization – The software provides you with a 360-degree view of an attack, including point of origin and progression across endpoints and other systems for complete forensic insight.

Behavioral Detection of Advanced Malware - Dynamic Behavior Tracking Engine uses sophisticated machine learning to predict threats across any vector.

Auto-Immunization – When the Dynamic Behavior Tracking Engine detects new malicious binary, it is instantly flagged it and all agents on the network are notified, making other endpoints immune to the attack.

Continuous System-level Monitoring - SentinelOne's lightweight autonomous agent is deployed on each endpoint device where it monitors all activity in both kernel and user. The Agent is virtually silent will not interfere with user productivity.

Bottom Line

SentinelOne offers protection across endpoint devices running Windows, OS X, and Linux. SentinelOne off loads indicators using industry standard formats (CEF, STIX, OpenIOC) for seamless integration with SIEMs, firewalls, and leading network security solutions. Product is offered as an on-premise solution, or use as a cloud-based service.

Sophos

Headquartered in the United Kingdom with offices around the globe, Sophos develops products for communication, endpoint protection, encryption, network security, email/mobile security and unified threat management. Products offer comprehensive security for users and data protection for desktops, laptops, mobile devices, data, web and even email, all with a single license.

From the Company

"Next-Generation Enduser Protection is the integration of our innovative endpoint, mobile and encryption technologies to deliver better protection and simpler management. From malicious traffic detection integrated into the endpoint to cloud-managed policies that follow users across devices and platforms, we're redefining what it means to provide comprehensive end user security. And as we continue to innovate, you'll benefit, as it becomes easier than ever to provide sophisticated protection for your users and data."

Key Features

Security - Secure Next-generation endpoint protection including antivirus, HIPS, web security, malicious traffic detection and more

Prevention - Prevents infection, detects compromised systems and remediates threats with real-time threat intelligence from SophosLabs

Control - Web, application, device and data control for comprehensive policy enforcement within the endpoint and Fast performance, even on older systems

Bottom Line

From individual file, to device and into the cloud, users get encryption everywhere and maximum protection from web and email threats with built-in anti-malware and web protection. Users are able to protect the network from compromised devices and reduce the risk of data breaches via integration with Unified Threat Management.

Symantec

Founded in April of 1982, Symantec has more than 21,500 employees world wide working to provide information management solutions. Symantec offers a cloud-based, endpoint protection solution that monitors your computer for misbehaving programs and threats. When Threat Protection detects a file with a virus, it attempts to clean the file, and if that fails, the program quarantines it.

From the Company

"Advanced attacks are more complex and difficult to uncover than ever before. They exploit unknown vulnerabilities and are highly stealthy and persistent, using novel techniques to hide themselves while compromising critical systems and data. Symantec's Threat Protection solutions block, detect, and quickly respond to all of the today's threats across your organization, from embedded systems to mobile devices, to desktops, servers, gateways, and the cloud. These offerings combine local context from your infrastructure with global telemetry from one of the world's largest cyber threat intelligence networks to protect organizations of any size."

Key Features

Manage Endpoint Protection - includes multiple layers of protection through a single high-powered client and management console across both physical and virtual machines. We make it easy to deploy, update and manage your endpoint security across various locations, user groups, and operating systems.

Stop Advanced Threats- Designed to protect against advanced threats with powerful, layered protection backed by industry leading security intelligence.

Granular Control – Set different security policies and proactively secure your system by using policy-based system lockdown and application control allowing control over employees handling confidential data.

Bottom Line

SONAR™ behavioral analysis stops malicious files designed to appear legitimate protection includes strong antivirus, antispyware and firewall protection eradicate known mass malware.

Trend Micro

Trend Micro Inc. is a global security software company founded in Los Angeles, California with global headquarters in Tokyo, Japan. Trend Micro endpoint security solutions ensure mobile and desktop protection against everything from traditional threats to the latest sophisticated, targeted attacks. Defend against both virtual and physical endpoints with multiple layers of anti-threat capabilities that consist of four stages: prevent, detect, analyze, and respond.

From the Company

"Endpoint Security Solutions are part of the Trend Micro Smart Protection Suites. These interconnected, multi-layered security suites protect your users and their data regardless of the device they use, or where they are working. The Smart Protection Suites combine the broadest range of endpoint and mobile threat protection capabilities with multiple layers of email, collaboration, and gateway security. And, you can manage users across multiple threat vectors from a single management console that gives you complete user-based visibility of the security of your environment. Plus, we give you the ultimate flexibility to deploy your endpoint security on-premises, in the cloud, or using a combination of both. And you can make changes on the fly without the hassles of new licenses."

Key Features

Application Whitelisting - prevents your users from executing dangerous or malicious applications on your endpoints by locking down to only the legitimate applications you are allowing.

Vulnerability Shielding and Application Lockdown - protect your endpoints from vulnerabilities before there is a patch deployed, or indefinitely in cases of end-of-life or unpatchable systems.

Behavior Monitoring - provides protection against new, unknown, and emerging threats with malware behavior blocking and event monitoring.

Web Reputation - stops access to malicious websites, including those employing data exfiltration.

Bottom Line

Trend Micro endpoint security delivers protection as all layers of security work together and are managed together to better correlate threat data and give visibility to advanced malware and threats help to stop more threats, more often.

Webroot

Webroot is a private company founded in 1997 and headquartered out of Broomfield, Colorado. Webroot recently announced its BrightCloud Security Services, a new portfolio of services for enterprise-class businesses, including integration for Next-Generation Firewalls and SIEMs. Webroot Secure Anywhere Endpoint Protection works by classifying suspicious programs as malicious and rolling back all of the local changes made by the malware, making the agent lightweight and fast

From the Company

"By combining innovative SecureAnywhere file pattern and predictive behavior recognition technology with the almost limitless processing power of cloud computing, Webroot effectively stops malware and zero-day threats at the moment of attack. The smarter, next-generation Webroot® approach to malware prevention is more effective and accountable than any conventional antivirus. You no longer need to rely on an outmoded detection model that is easily overwhelmed by today's malware—a model that yields unknown dwell times and doesn't alert on attacks until long after the infiltration has occurred."

Key Features

No Reimaging – Works by journaling and rollback remediation to restore files to their uninfected state, so users don't have to reimage.

Threat Intelligence - The Webroot® Threat Intelligence Platform continuously collects, analyzes, and correlates data, ensuring complete protection.

Real-time Updates - Threat data is delivered to Webroot-protected devices from the cloud in real-time.

Bottom Line

Webroot's endpoint solution is a well-designed management console offering policy management mechanics, customizable email alerts and lightweight client with fast installation and scanning. Includes malicious URL and malware blocking with phishing protection.

About Solutions Review

Solutions Review is a collection of technology news sites that aggregates, curates and creates the best content within leading technology categories. Solutions Review mission is connect buyers of enterprise technology with the best solution sellers.

Over the past three years, Solutions Review has launched ten tech Buyer's Guide sites in categories ranging from Cybersecurity to Wireless 802.11ac as well as Mobility Management and Business Intelligence, Data Analytics, Data Integration and Cloud Platforms.