ENDPOINT SECURITY

A Buyer's Guide

How to evaluate endpoint security solutions for advanced threat detection and response

FireEye

> 81% see endpoint security tools as the most helpful for threat detection.

Respondents from the SANS 2017 Threat Landscape Survey: Users on the Front Line

Introduction

Over the past decade, cyber threat detection and prevention technologies haven't kept pace with the increasingly-sophisticated tools and procedures used by today's global cadre of hackers and cyber criminals. Consequently, it's become considerably more difficult to achieve truly effective endpoint protection. While technical progress has been made, a number of deficiencies continue to plague contemporary solutions:

- Traditional, signature-based solutions such as antivirus (AV) tools do a good job detecting and blocking threats that are already known. However, they can't proactively identify and block those bearing unknown signatures.
- Legacy solutions don't provide details about threat activities, nor are they integrated into a holistic platform where log data can be analyzed to obtain a deeper understanding of new threats.
- Legacy platforms offer very little visibility into the security landscape, so your technical analysts are typically left in the dark, with scant intelligence to guide them toward proactive intervention or effective response to security incidents.

In short, traditional solutions, and even so-called next-generation AV, do not provide integrated protection. This puts your security staff in the position of trying to integrate and correlate a patchwork of multiple endpoint agents along with their associated information, which can actually leave the enterprise exposed to new vulnerabilities and attacks. In our current security environment, what's needed are advanced endpoint protection solutions that enable security personnel to inspect, detect and remediate a broader spectrum of threats than ever before—comprehensive solutions that provide both superior automated protection and robust, pervasive threat monitoring capabilities. That is, solutions that catch what legacy platforms catch—as well as what they miss—and are capable of answering the "who, what, when, where and how" pertaining to each and every security event.

Clearly, a new approach is needed to stop today's constantly evolving threats. But how can you know if a given solution will offer the requisite capabilities to protect your organization amid an increasingly complex and changing environment? This Buyer's Guide includes a checklist of pertinent questions to ask while evaluating endpoint security offerings, and is designed to help you make a well-informed decision.

Capability #1

Protect against known threats and those not yet identified

To stop today's creative and persistent attacks, organizations need to understand how attackers think, how they operate and what they're after. Most legacy endpoint protection products rely on signature-based intelligence feeds that only look backwards, and can only react based on the characteristics of past attacks. They can't anticipate or block previously unknown threats introduced via a malicious email attachment, website download or other threat vectors. Their signature databases have to be updated continually, in near real time, to keep up with known threats. It's a constant challenge since there are so many threats—and they are constantly evolving. For example, the AV-TEST Institute has identified nearly one billion known threat signatures and registers more than 390,000 new ones daily.

To keep pace, the industry has, over time, extended the capabilities of endpoint security offerings beyond their core AV protection. Thankfully, AV products are largely effective for tackling known threats, whether by means of signature or machine-learning capabilities. But to combat the latest unknown threats and respond proactively requires behavior analysis, local endpoint visibility and Intelligence-based protection backed by global analysts who can provide contextual insights into the nature of the threat and the attackers behind it.

1 AV-TEST Institute (September, 2017). AV-TEST - The Independent IT-Security Institute Malware Statistics

? Ask These Questions When Evaluating Endpoint Security Solutions

- Does it gather real-time intelligence from multiple sources to detect attacks before they hit?
- Does it provide proactive threat inspection to gather data that helps analysts determine the best response?
- Does it offer dynamic behavior analysis of threat processes and access to in-depth information about attacks and the attackers' motivations, characteristics and methods?
- Can it automatically prevent known attacks quickly and stop complex attacks before they cause damage?

> Every IT position is also a cybersecurity position now. Every IT worker, every technology worker, needs to be involved with protecting and defending apps, data, devices, infrastructure, and people.
>
> **Cybersecurity Jobs Report**
> 2017 Edition

Capability #2

Improve staff efficiencies and move from detection to remediation quickly

When it comes to security, enterprises have to get by on limited resources. The sky is not the limit. Facing such constraints, organizations seek solutions that enable IT security personnel to scale their capabilities. However, most endpoint defenses have a narrow focus, which makes it difficult for them to detect threats outside their defined protection parameters. And even when they do, they can't get the relevant information—the who, what, when, where and how—to detect and block future threats bearing similar characteristics. Thus, remediation efforts are stalled, and your security staff diverts its attention trying to figure out what happened.

Speeding up the process requires automated tools for detecting and preventing threats plus integrated intelligence and visibility for rapid analysis and response. Automation, intelligence and visibility provide a pathway to greater efficiency, enabling your staff to offload mundane tasks to security systems, overcome resource limitations and do more with less.

Ask These Questions When Evaluating Endpoint Security Solutions

- Does it include multiple detection and prevention engines to accelerate response?
- Can it detect and prevent known and unknown threats automatically and remediate them?
- Does it quickly validate threats and reduce incident overhead by automatically eliminating lower level ones?
- Does it provide continuous visibility into endpoint threat status so analysts can know the past and current state of endpoints and be better prepared to respond to any changes?

< PREVIOUS NEXT >

Capability #3

Reduce overall risk with integrated workflows

Today's cyber attacks are multi-stage and multi-vector, often incorporating spear-phishing emails, viruses and other malware. Unfortunately, security infrastructures that consist of disjointed point products that aren't integrated into a comprehensive whole often miss multi-stage attacks because of a lack of correlation between attack vectors. A disjointed solution also makes it impossible for analysts to leverage an integrated workflow that can dramatically reduce the time it takes to go from detection to investigation to response. The result? Your organization is exposed to greater risk.

Integrating endpoint protection technologies and intelligence into an automated solution enables your security staff to inspect incidents within a single workflow and connect the dots. Every suspicious activity—even in the absence of a security alert—can be correlated and evaluated in real time to find and then block a threat before it does any harm.

? Ask These Questions When Evaluating Endpoint Security Solutions

• Can you create integrated, automated workflows to speed up detection to resolution?	• Does it combine threat intelligence with automated detection and prevention?	• Is the intelligence feed updated in real time with validated evidence of newly detected attacks?	• Can it distinguish real threats from false positives and provide a baseline to gauge the severity of an attack?

> The ideal Endpoint Detection and Response (EDR) system should be capable of self-detection using its own built-in detection techniques, analytics and behavioral indicators.
>
> **Gartner Market Guide**
> for Endpoint Detection and Response Solutions

Capability #4

Increase visibility with endpoint detection and response capabilities

To fully understand the nature of an attack, analysts need complete visibility into endpoint activity, processes and timelines, as well as the ability to correlate relevant threat activity across every endpoint. Without being able to inspect endpoints and gather details, they can't alter their protection strategies to address current threat activity or better prepare for future events.

AV solutions—legacy or next-generation—do not provide visibility into endpoints, so analysts can't apply real-time intelligence to defend against heretofore-unknown threats. And even if an AV product successfully blocks a threat, it provides few details into its specifics, and not the kind of information analysts need to determine a threat actor's modus operandi and prepare an effective response. That's why Gartner and other analyst firms now consider endpoint visibility to be an essential component of an effective endpoint detection and response system.

? Ask These Questions When Evaluating Endpoint Security Solutions

- Does it provide deep visibility, enabling analysts to search, hunt and investigate incidents?
- Can analysts quickly and easily see the threat state of every endpoint to enable a fast, informed response?
- Can you conduct forensic investigations and root cause analyses of endpoint threat activities?
- Does it provide visibility into the entire lifecycle of an attack?

Capability #5

Streamline efficiencies with a single-agent solution

As attacks became more sophisticated, the industry responded by layering new technologies atop AV capabilities. Adding firewalls, intrusion detection and protection (IDS/IPS), data loss prevention (DLP) and features to protect against key loggers, spyware, Trojans, adware, phishing, ransomware and more created a suite of individual product silos commonly referred to as an endpoint protection platform. In most cases, the result was greater complexity without greater protection. Many of these add-ons sat on the shelf unused, doing little more than racking up costly licensing fees and giving administrators another thing to worry about. Gartner's "Magic Quadrant for Endpoint Protection Platforms" notes that the addition of capabilities such as encryption, vulnerability assessment and DLP, have yet to address proactive detection and response for unknown threats. The reason? Lack of integration.

While no combination of technologies can detect and stop every threat every time, a solution that integrates each protection engine into a single endpoint agent tied into auto-detection and prevention technologies, threat intelligence and visibility can efficiently address a much broader range of threats. And enable a much more timely and effective response.

2 Gartner, Inc. (January 30, 2017). Magic Quadrant for Endpoint Protection Platforms.

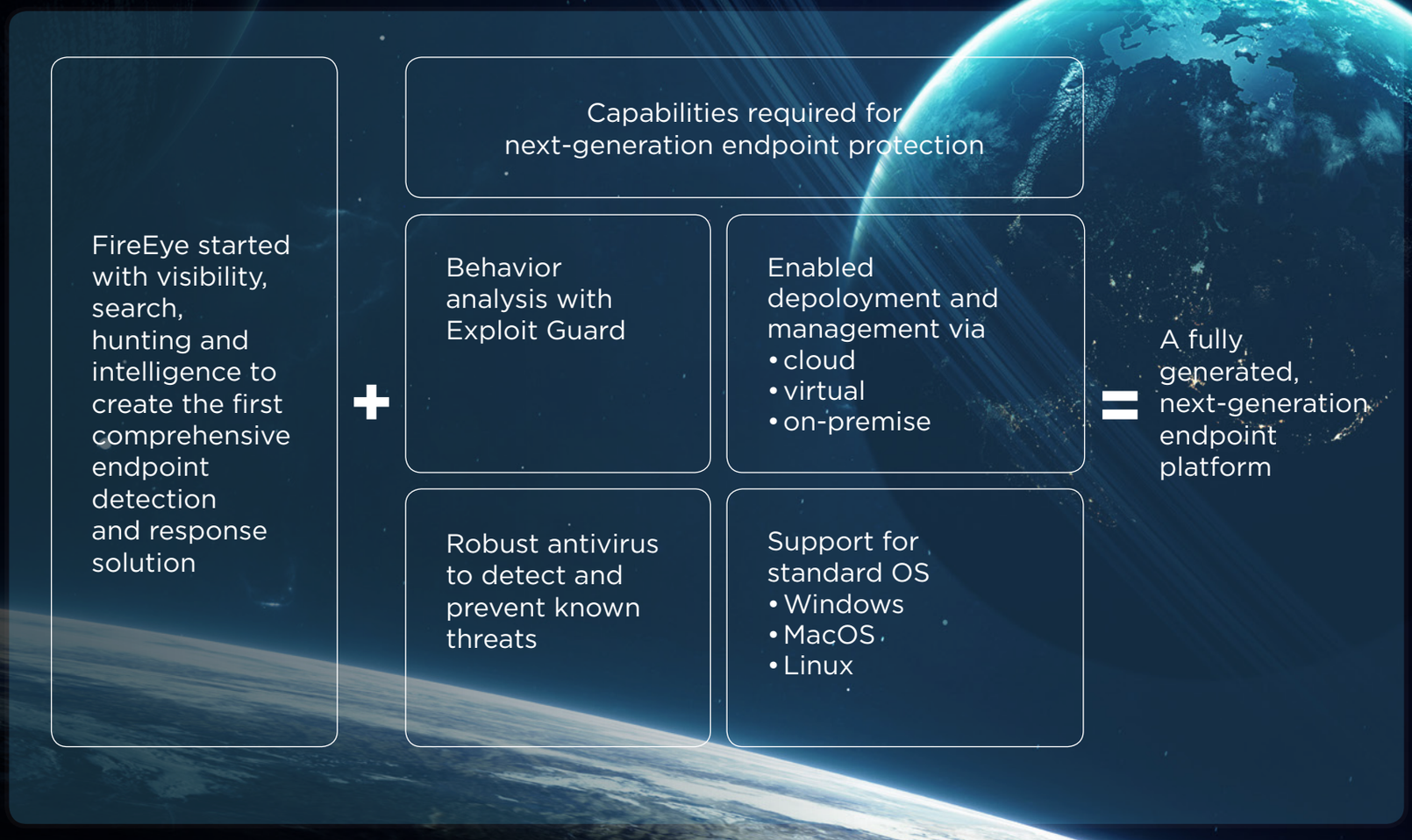
? Ask These Questions When Evaluating Endpoint Security Solutions

- Does it provide a set of integrated mechanisms within a single, consolidated agent and threat management workflow to enhance threat protection?
- Does it enable security staff to finely tune their endpoint protection efforts in real time?
- Can it detect threats that legacy platforms miss?

Summary

Over the years, the security industry has refined its endpoint protection products with supplemental capabilities in order to keep pace with a constantly evolving security landscape. While AV capabilities remain a core function, the ability to gain deep visibility into the enterprise infrastructure is now seen as critical to establishing an effective endpoint detection, prevention and response system.

Given the ever-increasing numbers of persistent attacks, contextual intelligence, behavior analysis and automation are deemed essential to address today's threat environment. Intelligence provides insights into the tactics of threat actors. Behavior analysis helps better distinguish real threats from false positives and provides a baseline to identify and prevent a wider array of attacks. And automation offloads routine prevention activities to security systems, allowing analysts to quickly and effectively deal with threats that may have bypassed initial defenses. When integrated into a single agent, these components constitute a comprehensive and adaptable endpoint protection solution that allows you to go quickly from threat detection to investigation, prevention and response—all in real time.



Neither standard endpoint protection nor next-generation antivirus products can provide a comprehensive endpoint detection and response solution

> "With the detection capabilities we have from FireEye, **we've been able to slash the industry average 'time to detection' by almost 98%!**"
>
> **Tom Webb**
> Director of Information Security Operations
> University of South Carolina

You need endpoint security that:

Protects against signature-based and the latest unknown threats and gathers real-time intelligence from multiple sources.	Improves staff efficiencies and enables security analysts to move from detection to remediation faster with multiple detection and prevention engines.	Reduces overall risk with integrated workflows that enable you to quickly identify a threat on any endpoint and easily respond to it.	Increases visibility with endpoint detection and response capabilities that are critical for a comprehensive solution.	Streamlines efficiencies with a single-agent solution that does everything required to detect and respond to known and unknown threats.

FireEye Endpoint Security provides a comprehensive, integrated solution—all in a single agent. With threat intelligence gathered from more than nine million global deployments and 10-plus years of incident response engagements built in, it's the only solution that automatically evolves at the pace of today's advanced threats. Detection, investigation and remediation—without the vulnerabilities of traditional solutions—the FireEye Endpoint Security difference.

About FireEye Endpoint Security

FireEye Endpoint Security delivers advanced detection and prevention capabilities to help respond to threats that can bypass traditional endpoint defenses. With the addition of antivirus (AV) and malware detection capabilities for known threats, along with endpoint detection and response (EDR) capabilities, analysts can now rely on a single endpoint agent for expanded visibility to quickly determine the exact scope and level of attack activities related to both known and unknown threats. With detailed context on blocked and unknown threats, analysts can adapt defenses to all cyber attacks. To learn more visit FireEye Endpoint Security.

To learn more, visit
www.fireeye.com

FireEye is the leader in intelligence-led security-as-a-service. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks. FireEye has over 5,000 customers across 67 countries, including more than 940 of the Forbes Global 2000.

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300
877.FIREEYE (347.3393)
info@fireeye.com

fireeye.com