Tomorrow's Endpoint Protection Platforms

Emergence and evolution

WHITE PAPER

FireEye

CONTENTS

The Technology Behind Endpoint Protection Platforms

Endpoint protection platforms (EPPs) detect and stop known cyber threats with signature or pattern-based antivirus (AV) and antimalware software technology. This was part of their original design decades ago and it persists today. However, the definitions and capabilities of EPPs continue to expand and evolve to meet new and more serious endpoint threats.

EMAIL

ATTACHMENT

DOWNLOAD

A file may be introduced to the computing environment in several ways, such as malicious email, email attachment or website downloads. This file is compared against a list of known threats. If the file is on the list it is blocked.

A file may be introduced to the computing environment in several ways, such as malicious email, email attachment or website downloads. This file is compared against a list of known threats. If the file is on the list it is blocked.

390

SIGNATURE-BASED SECURITY

Here's how signature-based endpoint protection typically works: a file may be introduced to the computing environment in several ways, such as malicious email, email attachment or website downloads. This file is compared against a list of known threats. If the file is on the list it is blocked.

These lists of known threats are normally located on a local endpoint in a threat file database. But these days, there are far too many threats to be stored locally. For example, there are nearly one billion known threat signatures identified by the AVTest Institute[1] which also registers more than 390,000 new threat samples every day. So endpoint security must compare suspicious files against threat lists stored on a server or in the cloud.

To be effective, signature databases must be continually and promptly updated. This is a challenge for EPPs because there are simply too many threats that are evolving too quickly.

390,000

NEW THREAT SAMPLES EVERY DAY

MACHINE LEARNING PROGRAMMING-BASED SECURITY

A few companies have developed non-signature-based technologies for AV protection. One such solution is to apply machine learning programming (MLP) with flexible rules and policies to address the signature gap. Vendors who utilize MLP rules and policies refer to it as next generation antivirus (NGAV) technology in contrast to traditional AV technology.

However, even MLP doesn't necessarily improve the overall efficacy of detection and prevention when compared to top performing AV solutions. With machine learning, rules and policies are programmed based on elements of a known attack or methodology. The system isn't nuanced enough to detect or classify elements outside its primary programming. Machine learning may have some advantages over file-based AV technology, but security staff pay a price in wasted time due to high false positive rates. And although machine learning implies learning, the system must be periodically updated, just like signature-based systems. MLP systems must be "taught" new algorithms promptly as new information and guidance becomes available to be effective. Regardless of whether signature-based or machine learning is the basis for the AV portion of EPPs, attacks continue to bypass EPPs.

1 AV-TEST Institute

The Endpoint Security Gap

Given the increasing volume and sophistication of cyber threats, EPPs must do much more than they do today. The recent Gartner "Magic Quadrant for Endpoint Protection Platforms"[2] report provides one definition of EPPs that reflects the addition of many capabilities over the past 20 years, including encryption, vulnerability assessment and data loss prevention (DLP). But many of these capabilities have yet to address proactive detection and response for unknown threats, the core weakness of EPPs.

[2] Gartner, Inc. (January 30, 2007). Magic Quadrant for Endpoint Protection Platforms.

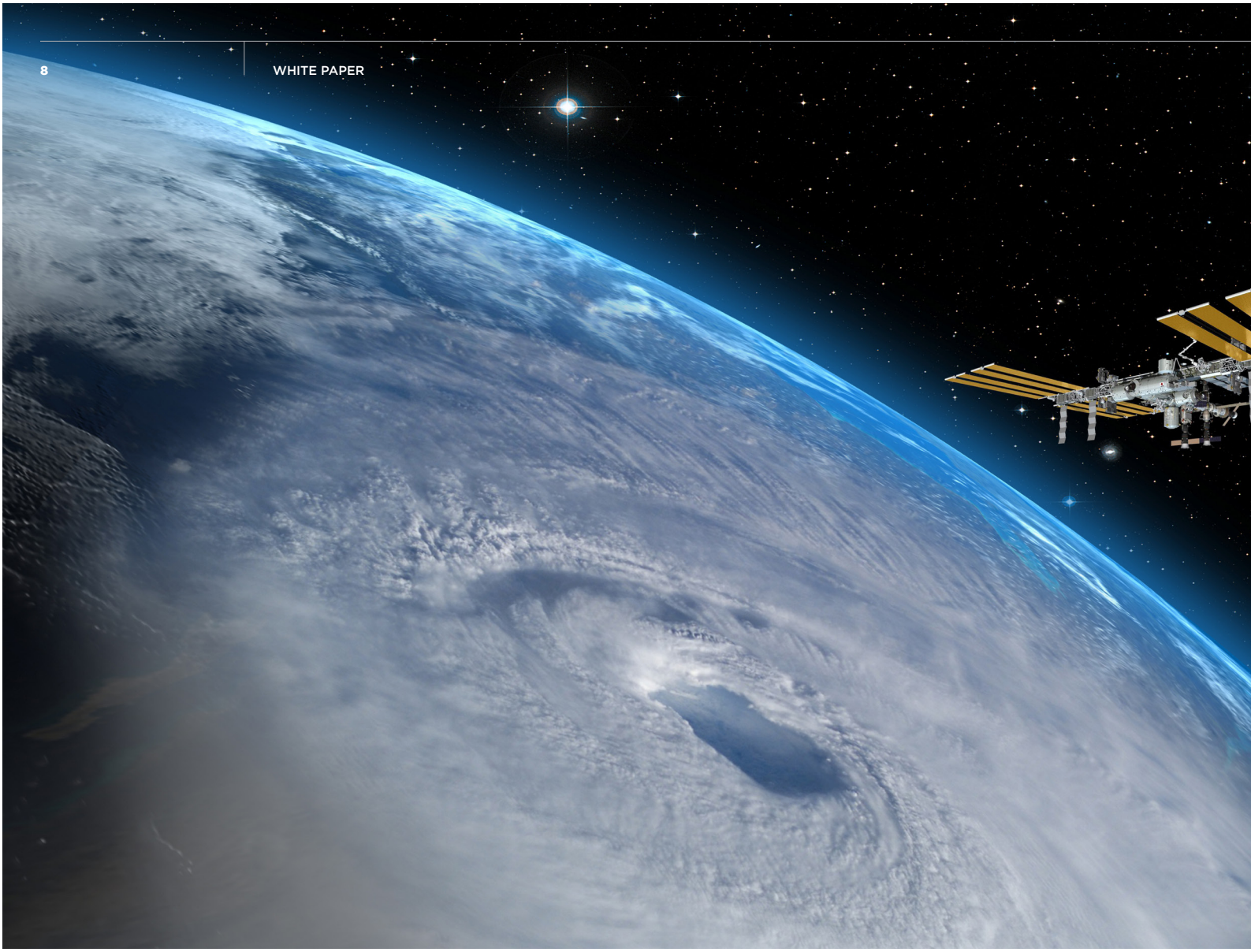
The Evolution of Attacks on Endpoints

To close the endpoint security gap, organizations should understand how cyber threats have changed over the years. Historically, attacker methods and technologies didn't vary much and weren't particularly sophisticated. In fact, they were reminiscent of phone scams. They used broad campaigns with generic messages against large groups of nonspecific targets. They adhered to the volume rule: if you make enough calls pretending to be an IRS agent and tell targets they need to pay taxes or go to jail, sooner or later someone will take the bait. They were brazen in their attempts to spoof or scare a victim to act; fear and intimidation played a major role. And like phone scams, attackers hid behind technology, with little risk of discovery or punishment from victims who had few means to protect themselves.

However, this general attack methodology was problematic for attackers. Their main issue was that they could not target specific victims or even know if victims had anything of value. They had to spend a lot of time sifting through responses to identify high-value targets.

Attackers didn't shift away from these more brute force type attacks because defenses had improved; they changed tactics because they wanted better results. Even though it required more initial effort, identifying high-value targets in advance generated a significantly higher overall return. Attackers also realized that though they were faced with more complex corporate defenses, these were generally inflexible. Attackers can test what signature- or MLP-based systems could or couldn't block based on their pattern files and programming, and then bypass them with an attack designed to evade current detection capabilities. After breaching one victim's network, they could reuse much of their work for the next target. By limiting their attacks to targets with known value, they could achieve better results for their effort. In fact, since they could target specific networks, they could develop specific goals, moving beyond money to data theft, espionage, vandalism and hacktivism.

This targeted approach required attackers to spend more time assessing and gathering information about a target and its security environment. They needed to not only penetrate an endpoint, but figure out how they could stay undetected in the corporate network long enough to achieve their goals. Targeting corporate environments drove substantial change in the attack lifecycle and the use and application of tools and sophisticated methodologies. Attacks became less brazen to avoid detection. As attackers began to understand the lack of flexibility in corporate defenses, they realized how these limitations handicapped their target's ability to detect their presence. They evolved to use techniques such as spear phishing, which were far more subtle, sophisticated, targeted and professional.



Challenges to Overcome

Over the last decade, cyber threat detection and prevention technologies have not kept pace with attacker tactics, techniques and procedures (TTPs). Securing endpoints has become extremely difficult, given the rapidly increasing number of endpoints as well as a bring-your-own-device mentality. While EPP technology has continued to improve, it still deals with two basic challenges:

Its AV technology is static and reactive.	Its limited visibility mean that analysts must work with incomplete intelligence.

Many defenses are cumbersome and lack flexibility; their automated detection and prevention processes can create a lot of noise and alert volume. These issues, compounded with their lack of visibility into threat actions makes it difficult for targets to gather important information such as who might be attacking, what they're after, when an attack may have taken place and the origin an attack. Defenders are forced to manually work through a huge volume of conflicting incident information. They must often guess at the nature of the critical threats, which both slows and reduces the effectiveness of any response.

Limitations of AV technology

A strong AV technology, whether pattern- and signature-based or MLP, has historically been the core of EPPs. But both methodologies are static and require timely updates to catch new threats. These updates have always lagged behind actual threats, but they do help reduce a lot of the more mundane attacks. As attackers improved and automated their attack procedures, new malware creation and specific victim targeting, traditional EPP solutions have struggled to keep up.

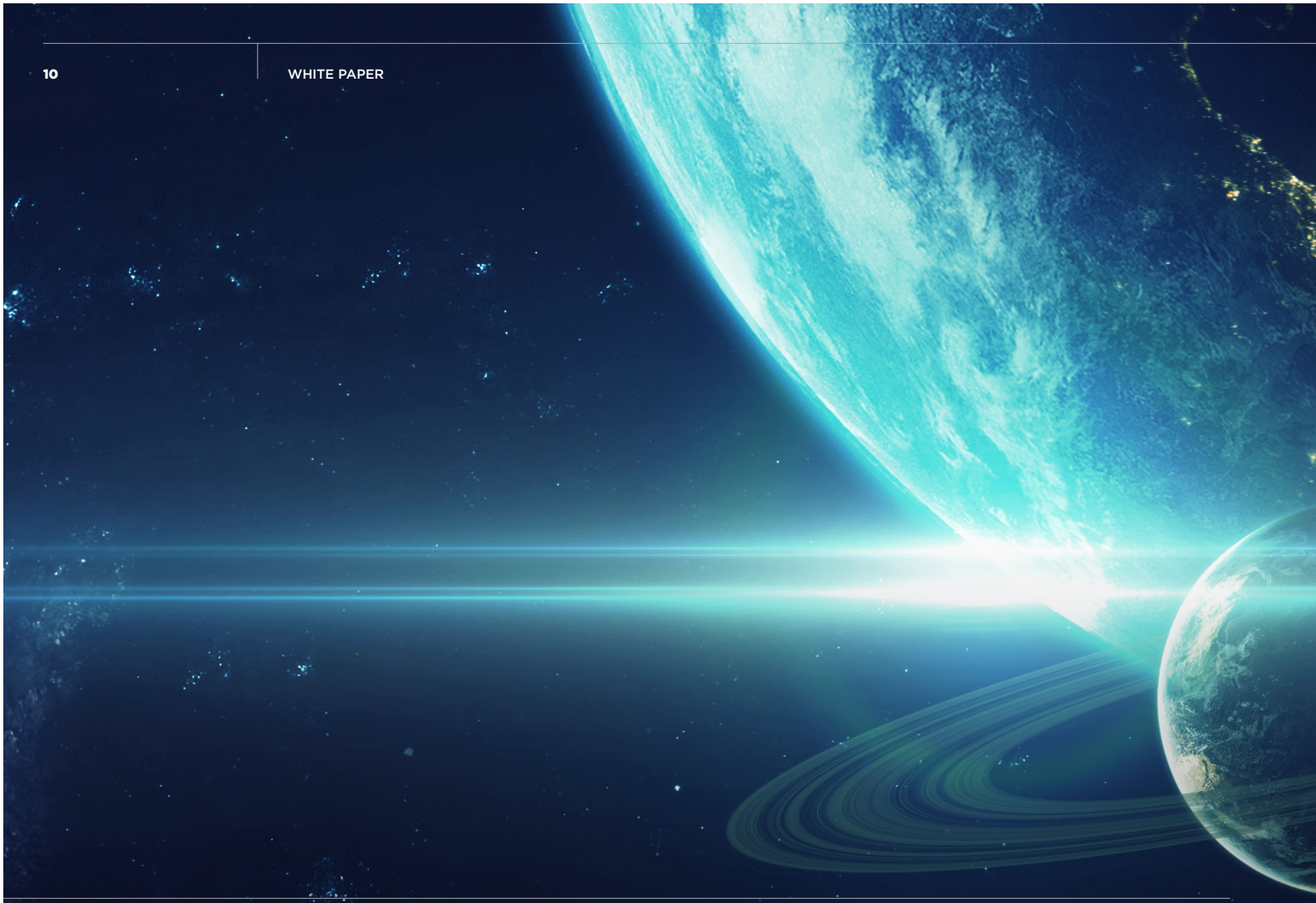
Increasing the types and number of applications in EPPs did not close the protection gaps. Because EPPs were designed to be reactive, they used fixed identifiers or rules to detect and react to a threat. These were reasonably effective against known threats and continue to be required today. But without known information, or the intelligence to evaluate complex application or system interactions, current EPPs cannot deal with highly targeted and unknown threats. The AV technologies EPPs depend on can't protect against the unknown.

EPPs that rely on pre-programmed rules, policies and signature files can't always instantly protect against all threats. The number and type of threats is wildly dynamic and based on an unknowable array of skilled attackers, powerful tools, complex networks and constantly changing environments.

Limitations due to low visibility

Analysts need to be able to inspect endpoints and gather details of threat activity to understand who attacked, what they were after, when they attacked and where the attack originated. Without understanding the real nature of a threat, blocked or not, analysts can't alter their protection to address current threat activity. For critical, comprehensive threat intelligence, analysts need inclusive visibility into endpoint activity, processes and timelines as well as correlation of relevant threat activity across every endpoint.

Neither standard nor next-generation AV have endpoint visibility so they can't apply real-time threat intelligence to an unknown threat to optimize responses and defend against it. Even when any type of AV solution blocks a threat, they have minimal visibility into the specifics of the threat, such as its attack methodology or whether it's one of a series of attacks. Therefore, they cannot provide the details analysts need to determine threat actor TTPs. Gartner and other analyst firms have added endpoint visibility with Endpoint Detection and Response (EDR) to EPP to highlight these intelligence needs.



Required Capabilities for Better Endpoint Protection Platform

For EPPs to remain effective and relevant, the security industry has been forced to redefine them over the years with additional capabilities. AV has always remained a core function of EPPs. An EDR capability with comprehensive visibility has become another critical component. Given the ever-increasing numbers of persistent and creative attacks, there are three more essential elements to EPPs: contextual intelligence, behavior analysis and automation. Intelligence provides insights into TTPs. Behavior analysis helps better distinguish real threats from false positives and provides a baseline to identify both subtler attacks as well as internal attacks. Automation offloads more mundane security activities to security systems.

AV has always remained a core function of EPPs.

The interaction of these elements delivers even more capabilities.

Combining threat intelligence with automated detection and prevention helps block threats as early as possible.	Combining AV detection with relevant intelligence and real-time behavior analysis of complex endpoint activity can help identify threats and reduce gaps in endpoint protection.	Automation can remove lower risk threats quickly and free analysts to use EDR visibility to investigate and determine the nature of threats of consequence.

A defense enhanced with intelligence and visibility gives analysts the means and time to better understand a threat and adapt defenses as needed.

No single defense or combination of endpoint solutions can detect and stop every threat every time. But when added to AV detection, a combination of layered endpoint auto-detection and prevention technologies and threat intelligence, behavior analysis and visibility can address a much broader range of discreet and unknown threats and their methodologies. These capabilities should also correlate data with local and network threat behavior analysis engines to build case and response data in real time on the risk and threat activity at any endpoint.

Secured and expanded boundaries

Organizations are constantly under intense, methodical, coordinated attacks on multiple fronts. EPPs need to more proactively address these threats. If a threat gets through, the best possible protection comes from real-time endpoint interrogation and investigative capabilities that can uncover active attack operations quickly and reduce the severity of their impact.

Threat actors employ powerful tools and skilled individuals to conduct their work. To defend against them, organizations need comprehensive visibility from EDR and added layers of automated protection such as behavioral analysis detection and prevention in addition to common AV software. These capabilities provide detailed endpoint information so analysts can filter out network noise and false alerts and determine the exact threat state of every endpoint to build an ongoing comprehensive picture of threats. The expectation is that EPPs have to continually adapt their protection capabilities to contend with immediate and future risks.

To learn more about endpoint protection that goes from prevention to investigation and remediation, visit:

www.FireEye.com/endpoint

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

www.FireEye.com

FireEye is the intelligence-led security company. 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 5,300 customers across 67 countries, including more than 845 of the Forbes Global 2000.

FireEye