FORTIFYING ENDPOINTS AGAINST MODERN THREATS

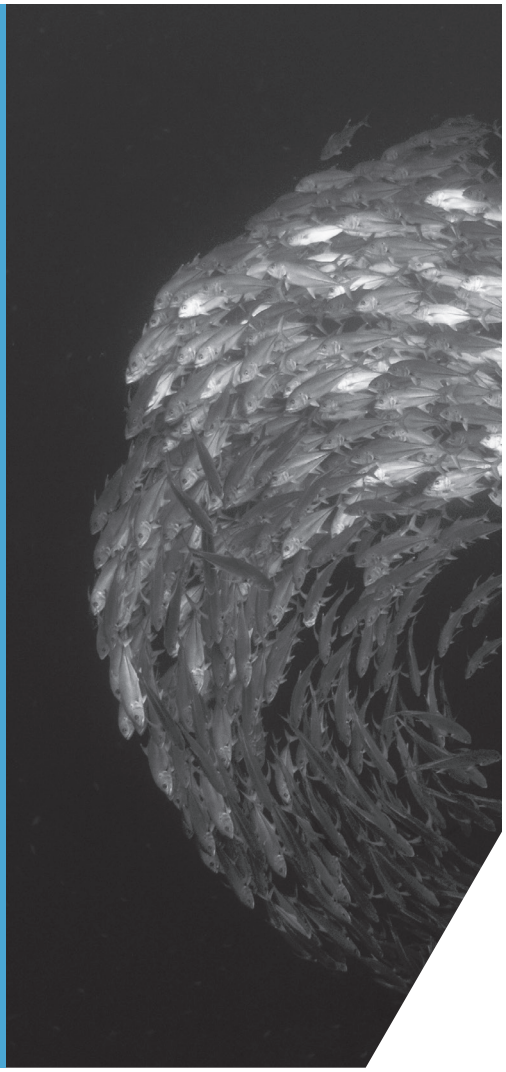
WHITE PAPER

FireEye

CONTENTS

INTRODUCTION

IN THE LAST SEVERAL YEARS, MANY COMPANIES AND THE PRESS HAVE SUGGESTED THAT ANTIVIRUS (AV) SOLUTIONS ARE OBSOLETE. IT'S TRUE THAT MODERN COMPUTER THREATS CAN BYPASS MOST AV AND ANTI-MALWARE TECHNOLOGIES. BUT ORGANIZATIONS CAN'T JUST THROW THESE PRODUCTS AWAY. SIMILAR TO LOCKS ON CAR DOORS, SIGNATURE AND PATTERN-FILE TECHNOLOGIES ARE STILL NECESSARY. THEY ACT AS AN OBSTACLE AND INITIAL LINE OF DEFENSE AGAINST UNSOPHISTICATED CRIMINALS AND COMMODITY THREATS. ALSO, REGARDLESS OF EFFECTIVENESS, PRODUCTS THAT USE AV AND ANTI-MALWARE TECHNOLOGIES GENERALLY COST LESS AND ARE ACCEPTED BY LOCAL, STATE, NATIONAL AND INTERNATIONAL GOVERNMENTAL AGENCIES AS COMPLIANCE SOLUTIONS FOR REGULATIONS SUCH AS PAYMENT CARD INDUSTRY (PCI) COMPLIANCE, THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) AND THE SARBANES-OXLEY ACT (SOX).



The threat landscape has changed dramatically since the 1980s. When AV and anti-malware solutions, intrusion detection systems (IDS), intrusion prevention systems (IPS) and cloud-based solutions were introduced, they all relied on a static view of threats — signatures, pattern files and written policies. However, these solutions were not designed to deal with today's more sophisticated attacks. Solutions designed as massive catalogs of threats have no way to identify new and unique threats designed to avoid discovery by static defenses.

"Antivirus is dead."

— Brian Dye,
Senior VP forInformation Security, Symantec
The Wall Street Journal, May 2014.

CHALLENGES FOR ENDPOINT PROTECTION

Traditional endpoint protection was never designed to deal with sophisticated or advanced persistent threat (APT) attacks. Those defenses are based on frequently updated static pattern or signature files, which was an effective tactic for quite a while. Once a virus or malware had been identified and all systems were updated, that threat was effectively blocked. Whether a threat was in an attachment, a URL, link or other delivery vector, pattern matching was a very straightforward and successful methodology. For known pattern scenarios, the method still works.

But we can no longer simply hope or expect that all signature files will be up to date. Even if they are, with current software and hardware computing power sophisticated hackers can create attacks designed to bypass static defenses. Endpoints definitely need help to address today's more sophisticated attacks.

Casual hacker activity forces security professionals to spend their limited resources on traditional perimeter defenses instead of on discovering and stopping critical attacks.

CHANGES IN THE THREAT LANDSCAPE

Threat actor motivations vary. They can include economic or political advantage, financial gain, theft of intellectual property or disruption of a target's operations. Any computer-literate hacker can use many free and commercial tools with varying degrees of effectiveness. They don't need a high success rate or the ability to do much damage. Hacker activity forces security professionals to spend their limited resources and time deploying and managing traditional perimeter defenses. This, in turn, impacts the time available to perform comprehensive assessments, inspect and analyze security alerts and look for potential threats. Perimeter defense becomes even more difficult for security experts who lack visibility into endpoints and access to threat intelligence. Adding fuel to that fire, there are hundreds — or even thousands — of bring your own device (BYOD) technologies in the network environment, and the organization may only have limited control. With so many possible points of entry that are blind to active threats, it's no surprise that attacks break through.

Organizations must come to terms with the fact that breaches will happen. But if they are caught early enough, the organization can avoid substantial loss or damage. This doesn't mean everyone should get rid of existing endpoint protection because it can't stop certain types of attacks. It means that the real problem needs to be recognized and dealt with: stopping critical attacks that can bypass traditional endpoint protection systems.

The priority should be to minimize the time an attacker can stay in a compromised system to cause damage or access and steal data. If an organization is slow to discover or remove a threat, it puts itself and its data at risk. Threat discovery, the first step, includes understanding what cyber criminals may have done or what they are trying to do.

Being able to apply flexible endpoint defense and response capabilities can help. Security experts dedicated to endpoint protection enable organizations to more easily adapt their defenses against high-risk attackers. A key benefit is that organizational staff can continually inspect and assess endpoints and security practices, past and present. This means security teams can shorten the cycle of discovery and containment with faster and more appropriate responses that maintain endpoint and data integrity.

THREAT INTELLIGENCE AT THE ENDPOINT

Traditional static endpoint protection technologies can only protect against known threats. Of course, static security systems do get periodic updates to their threat knowledge bases. After a threat is discovered and a signature created, a central system is updated with this information. From that central system, updates are then distributed to customers who then distribute them to their respective endpoints. The updates may include known viruses, malware, different types of threat patterns and threat signature files. Obviously, it takes time to create the update and distribute it through all the systems to endpoints. At the same time, without a current database file, these systems cannot identify or stop a corresponding threat.

Systems require an administrator to set up and constantly update policies or rules for firewalls, IDS or IPS. This creates a protection gap based on not only the administrator's skills, but also on how much time administrators have to test changes and confirm that they work as designed without causing other problems. This confirmation is required because there is no system with adaptable signatures or policies that can stop an unknown threat. For instance, a system with machine learning, heuristics or other similar capabilities still requires static rules or files and can be bypassed by skilled hackers.

In fact, cyber attackers alter their attacks specifically to bypass deployed static defenses. Attackers know that systems with static defenses can't deal with a threat unless it is in their threat database or addressed in a policy. So hackers take the time to test against those defenses; if a specific attack is blocked, the attacker knows the threat database contains the corresponding signature for their malware and they can try something else. And even if these probing attacks are blocked by a static system, they don't necessarily reveal any intelligence about attacker motives or techniques, which makes it difficult to defend against "real-world" active attacks.

Skilled cyber attackers test static defenses and alter their attacks to bypass threat databases.

A NEED FOR CONSISTENTLY STRONG PROTECTION

Large and small organizations must deal with the same threat landscape. Smaller partners and suppliers provide a wide range of services to large organizations but often can't deploy the same level of protection. An attacker targeting a large organization often starts by attacking a smaller partner that they know has less robust defenses and uses the partner's access to penetrate the primary target. The grim reality is that cyber security protection is only as strong as the weakest link between interconnected systems.

When an organization is designing its cyber security solution, it must consider its entire system, including partners with connections to its network. While a solution shouldn't necessarily control what a partner does, it should consider who has access to different areas of the network and whether they can access high-risk areas. In all cases, user endpoints are crucial access points because they usually involve the least sophisticated users and represent the largest attack surface visible to hackers.

Cyber security solutions must consider the entire system, including partners with connections to organizational networks.

Organizations have many choices when it comes to security solutions: products, vendors, implementation and managed security services as well as investments in personnel. Larger organizations generally seek feature-rich systems; smaller organizations may look towards simpler and more automated solutions. No matter what, organizations must consider vendor access points as significant vulnerabilities. It is an area where static defenses can provide a misleading sense of security.

A LIFECYCLE APPROACH FOR ENDPOINT SOLUTIONS

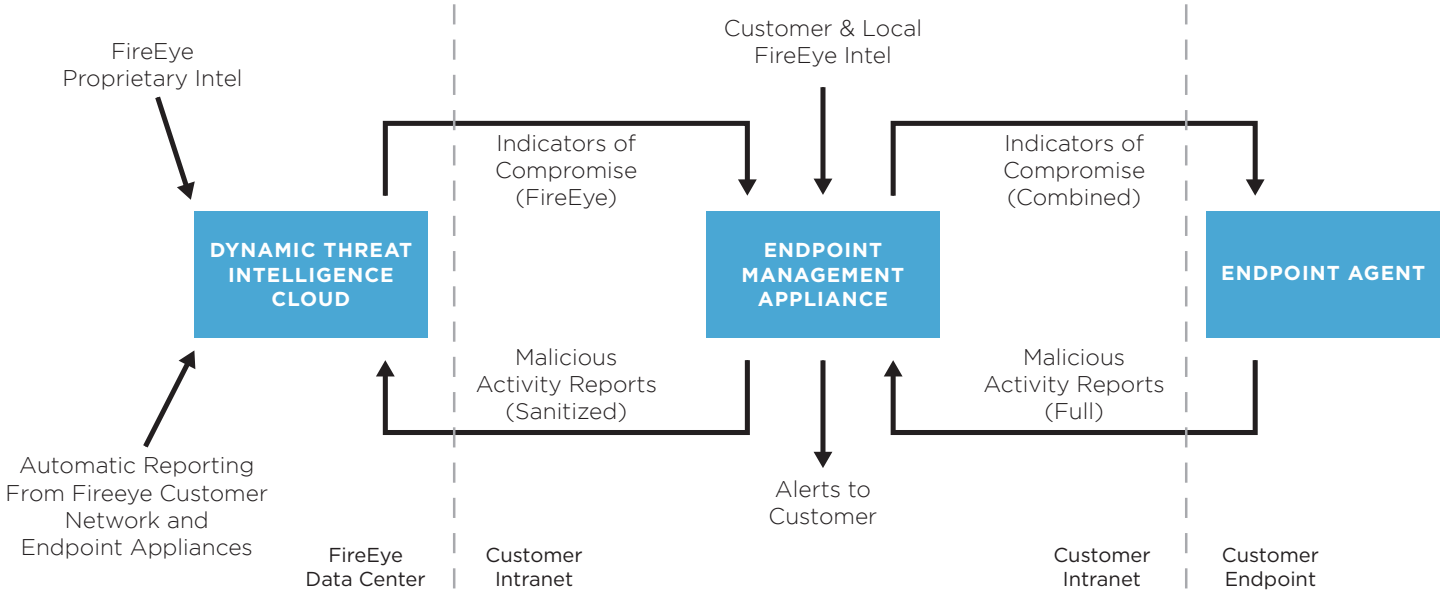
Organizations generally consider two security models to protect endpoints. The traditional and most common is endpoint protection (EPP). These are usually the static type of defense systems being discussed here. A newer type of system is endpoint detection and response (EDR), which is better able to deal with modern threats, including APT attacks. Regardless, both security models need to be in place. The best security solutions are able to detect, prevent, investigate, analyze and respond to known and unknown threats.

To enable threat discovery, endpoints need to be integrated into an overall network intelligence workflow. By correlating endpoint activity with overall network activity, enterprises can better review and analyze data to uncover threat activity on endpoints. The resulting intelligence includes a timeline of events, file registry processes and incident information. Throughout any inspection, review and analysis, organizations do not want to risk further infection from a compromised endpoint, so an analyst must be able to contain a compromised endpoint until it can be certified as clean.

The illustration below shows an example of the flow of threat intelligence that can be applied to endpoints. This process needs to be a circular flow that continually improves its intelligence base and checks endpoints for threats. It shows how threat information discovered on one device can be used to see if it, or another endpoint, is compromised. The diagram also illustrates how threat information moves between the various points in the whole system:

- A starting point can be the proprietary FireEye threat intelligence accessible to customers via the FireEye Dynamic Threat Intelligence Cloud (DTI).
- These will have Indicators of Compromise (IOC) that can be used by the FireEye Endpoint Security appliance to check whether an IOC exists on any endpoint.
- The FireEye Endpoint Security appliance can use Triage Viewer to check every endpoint for a known IOC, and gather information about that IOC and what it may be trying to do.
- If something is discovered, that device can be contained for deep analysis and to prevent the spread of any possible infection.
- Beyond known IOCs, analysts can inspect and analyze other devices, using FireEye Enterprise Security Search to search every endpoint for unknown threats.
- Any suspicious result can be further inspected and analyzed with Data Acquisition to collect more detailed data, such as whether any files or registry entries were changed or created. Analysts can also determine if any unauthorized process attempted to contact internal or external networks. All this data allows analysts to create new custom IOCs as needed.

FIGURE 1. FIREEYE ENDPOINT INTELLIGENCE DATAFLOW



Integrated intelligence sharing between network, endpoint and cloud systems provides a broader protective impact than any single system can provide.

To improve endpoint protection, analysts can use network intelligence to better detect and deal with issues. FireEye endpoint visibility capabilities help analysts identify and investigate an application exploit, malware download and execution or a callback to a command and control (CnC) server. This can be a part of an integrated approach that includes dynamic, real-time malware analysis capabilities provided by the FireEye Multi- Vector Virtual Execution (MVX) engine and the investigation capabilities of the FireEye Endpoint Security solution. Together, they create a much more robust and proactive protection environment.

Integrated intelligence sharing between network, endpoint and cloud systems provides a broader protective impact than any single system can provide. This shared intelligence details attacker characteristics: their tools, techniques and procedures (TTP). TTPs give security analysts the information they need to identify and defend against attackers and their attacks. TTPs also guide defenders' ability to adapt defenses according to the demands of particular threats.

Integrated intelligence sharing dramatically reduces time to detection and response. For example, if exploit code is detected in the network, that area can be isolated and an IOC propagated to all endpoints. The converse is also true. Promptly detected threats can be prevented before they take hold. This results in significant time and overhead savings and the ability to address threats with dynamic and timely response.

Threat analysts need to be able to research blocked attacks and compromises quickly and easily. They must determine what was blocked, what attacks penetrated defenses, how they penetrated defenses and, if any malicious code was introduced, what it did in their systems. The faster they understand what happened and how it happened, the faster they can improve detection and protection practices.

Endpoint detection will never be perfect. But a better understanding of operational baselines for systems and endpoints creates the basis for stronger threat detection and analysis. Analysts combine network forensics with operational knowledge to recreate the lifecycle of an attack — the kill chain. This analysis can discover failed attack attempts before an actual breach. Combined with breach data, these failures can tell an analyst quite a bit about attacker TTPs, which provide information critical to understanding and protecting against advanced attacks.

Dynamic endpoint response involves far more than quarantining an endpoint. Based on data gathered from past and current event analyses, it can include a full analysis of any malicious artifacts found, intelligence sharing throughout the network and policy enhancement. It ultimately creates a body of actionable intelligence that tells internal and external stakeholders what must be done to deal with current and future attacks. In fact, it powers a cycle of continuous improvement where responses improve detection with shared threat intelligence.

CONCLUSION

As the threat landscape evolves, endpoints must detect and respond to new threats more effectively — something traditional static systems can't do on their own. The solution isn't to throw away traditional security but to fortify it with intelligence and visibility. Sharing intelligence with endpoints allows them to protect themselves and the entire network. Analysts can then use that shared intelligence to adapt their endpoint defenses — detection and response — in real time, based on attacks faced every day.

The solution isn't to throw away traditional security but to fortify it with intelligence and visibility.

ABOUT FIREEYE

FireEye protects the most valuable assets in the world from those who have them in their sights. Our combination of technology, intelligence and expertise — reinforced with the most aggressive incident response team — helps eliminate the impact of security breaches. We find and stop attackers at every stage of an incursion. With FireEye, you'll detect attacks as they happen. You'll understand the risk these attacks pose to your most valued assets. And you'll have the resources to quickly respond and resolve security incidents. FireEye has over 4,000 customers across 67 countries, including more than 650 of the Forbes Global 2000.

To learn more about FireEye Endpoint Security, visit:
www.fireeye.com/products/hx-endpoint-security-products.html

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

www.FireEye.com

FireEye