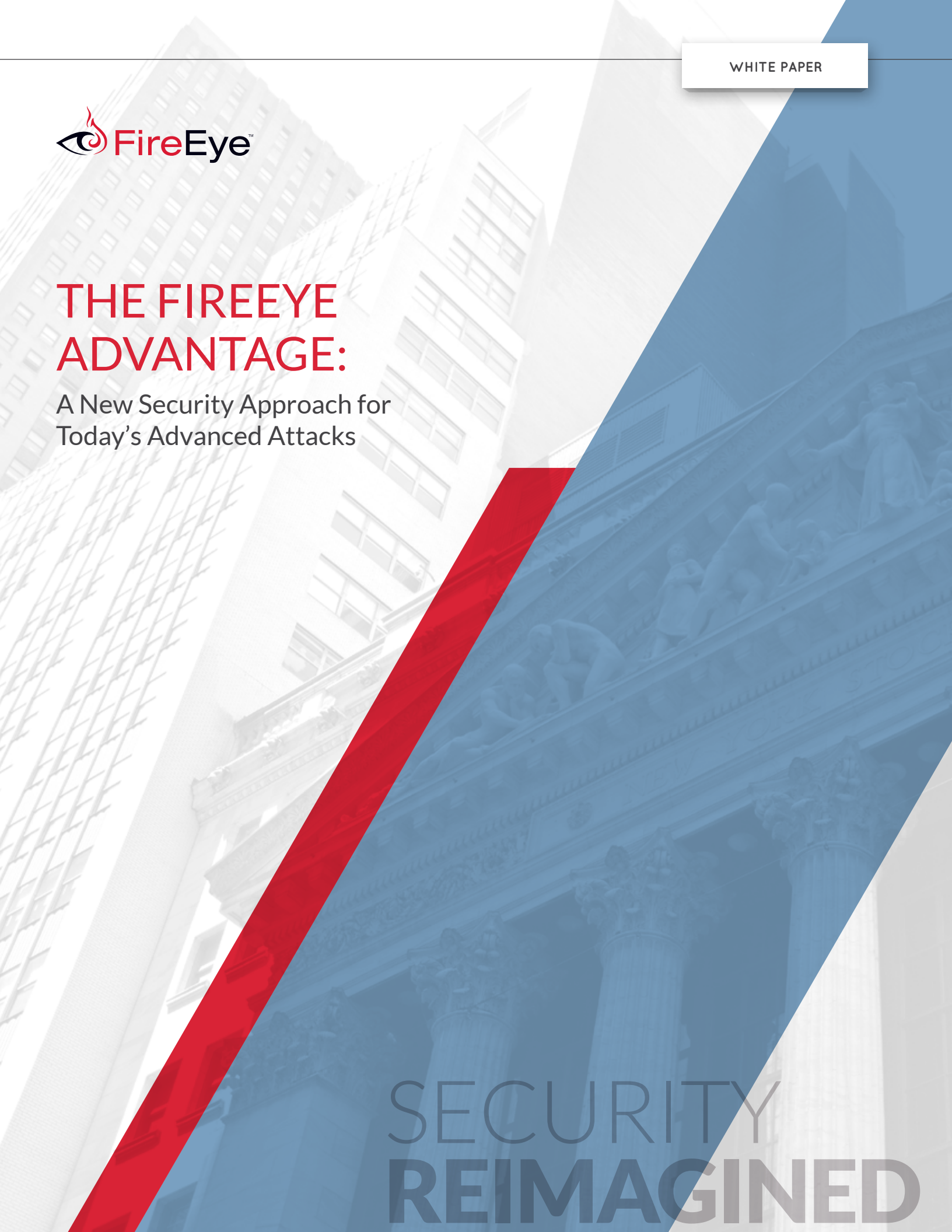
WHITE PAPER

FireEye

THE FIREEYE ADVANTAGE:

A New Security Approach for Today's Advanced Attacks



CONTENTS

Introduction

Organizations face a new breed of cyber attacks that easily thwart traditional defenses. These advanced attacks are targeted. They are persistent. And they are devastatingly effective at breaching your systems and stealing your sensitive data.

Today's threat landscape demands a fundamentally new approach, one that does not rely on binary signatures, lists, or rules to detect threats. Organizations need protection that is powerful enough to block today's fast-moving, constantly changing attacks—especially those that exploit zero-day vulnerabilities.

Many security vendors insist that their timeworn approaches are equipped to combat today's advanced threats. Others, aware that yesterday's defenses are no match for today's attacks, have begun hawking sandbox-based products as the answer. But most are bolt-on additions to legacy offerings—encumbered by technologies that simply are not architected for new threats.

This paper examines several security architectures, including sandbox-based products, and the limitations of these approaches. It also reveals the FireEye advantage—an architecture built from the ground up to truly protect against today's advanced attacks and evolve as threats change.

The Limitations of Existing Security Solutions

Organizations like yours have spent millions of dollars on classic defense-in-depth layered approaches to protect their business. Traditional environments start by deploying firewalls and gateways (email or Web) at the edge to filter and reduce malicious traffic (both inbound and outbound) using rule sets, reputations, and blacklists. The next level of protection may include intrusion prevention systems (IPS) that use signatures and rules to identify and block attacks over the network. The last line of defenses typically comprises standard signature-based endpoint anti-virus (AV) software or whitelisting. These traditional security tools are designed to protect your business from known threats. The problem: none of these measures can effectively protect against unknown threats. Unlike traditional defenses, FireEye protects against both known and unknown threats from harming your business.

Signature-based technology

- Rules-based technology
- List-based technology
- Multitude of malware
- Vulnerable to evasion
- Lack of correlated protection
- No real-time protection

Signature-based technology

Signature based technology is the most common form of malware detection used in AV software, IPS devices, and Web gateways. Unfortunately for organizations that rely on these defenses, signatures are woefully ineffective. Today's malware is polymorphic, changing constantly. Binary signatures reflect only the malware's state when first identified—not new variants. Because of this mismatch, binary signatures fail to detect most malware samples—about 60,000 new malware variants are released daily.[1] Making matters worse, cybercriminals use a bevy of techniques to evade signature-based detection.

[1] Jon Clay (Trend Micro). "Big Data Analytics and the Smart Protection Network." August 2012.

Common evasion tacks include file encryption and portable executable packers. Signature-based defenses are not effective against these tactics.

Rules-based technology

Rules-based technology includes everything from firewalls to data loss prevention (DLP) systems. This approach requires users to manually configure rules based on known threats. Organizations create firewall rules to block a subset of known malicious IP addresses. Or they employ Web-content rules to block known malicious domains or websites. But these tacks are only as good as the information supporting them. If the underlying technology cannot detect unknown threats, these technologies are of little use.

List-based technology

List-based technology has grown popular in recent years. Commonly used lists are cloud-based blacklist of IP addresses, Web domains, and even malware itself. Most security professionals recognize that signatures, rules, and blacklists are not effective against advanced threats, so many are shifting to whitelisting. Whitelisting technology allows only preapproved connections and files—essentially, what is known to be good—on sensitive computer systems. The problem: environments change so quickly that whitelisting technologies cannot keep up. And managing whitelists is a nightmare, especially in large environments.

Lack of correlated protection

When examining how today's attackers operate, FireEye researchers have observed a disturbing trend: adversaries know the protection technology better then the organizations implementing it. Threat actors understand what it takes to bypass signature-, rules-, and list-based security. A typical scenario: a component of advanced malware enters targeted systems through one vector (such as email) and communicates externally through another (such as the Web). It downloads only small pieces of code to camouflage its activities. And it changes every time it executes.

FireEye has detected advanced malware connections that use cloud-hosting companies to hide communications with the attacker's command-and-control (CnC) server. These sophisticated multivector attacks are why correlating threat information across multiple vectors is critical.

No real-time protection against unknown threats

Real-time protection is difficult for vendors due to the demands required on their technology. Blocking attacks in real time is impossible if security products do not support the common threat vectors, correlate information internally and externally, and detect unknown threats. These obstacles play right into the hands of the bad actors who understand what security vendors are up against.

The Limitations of On-Premise Sandboxes

On-premise sandboxes typically are built on top of individual appliances or servers and deployed in the customer's local network. Sandbox appliances analyze file objects for known malicious content and behavior. Suspicious files execute within the sandbox to be analyzed either automatically or manually by security professionals. The idea is to assess whether changes to the original system version indicate malicious behavior.

On-Premise Sandboxes Weaknesses

- Hypervisors vulnerable to evasion
- Limited in scope
- File-centric approach
- Focused on a single vector
- Limited utility of hashes
- Slow to respond

Hypervisors vulnerable to evasion

Many sandboxes use off-the-shelf hypervisors, such as VMware, Xen, and Hyper-V. Threat actors have access to these hypervisors—including source code in some cases— and write their malware to exploit or evade detection in these environments.

Limited in scope

Sandboxes replicate the environment of a single user system, typically the organization's so-called gold image. But most organizations have a multitude of operating system and application versions in their environment. Malware often targets vulnerabilities in specific combinations of environments and software. Files that appear innocuous when tested in the gold-image environment can exploit vulnerabilities in other configurations.

File-centric approach

Sandboxes focus on individual files. Depending on the solution and configuration in place, a platform may cache and upload specific file types, such as all EXE and DLL files. But malware can arrive in an array of file types. And given the multi-vector nature of today's attacks, inspecting a file on its own may have limited value. Malicious code in a PDF, for example, may execute only when triggered by HTML parameters. So a PDF inspected on its own in a sandbox will not exhibit any signs of malware and go undetected.

Focused on a single vector

On-premise sandboxes reside on a host agent or individual appliance. They typically protect a single threat vector, such as email or Web traffic. Because these solutions do not track multiple vectors, they cannot correlate activity across these channels or provide the insight required to identify a multi-vector attack. Take a malicious PDF. Users may not realize that by opening the file, they have inadvertently executed JavaScript code that begins downloading a malware payload from a malicious website. Lacking the correlation between email and Web vectors, the sandbox-based analysis does not detect the malicious callback. And most sandboxes lack any useful mechanism for sharing threat intelligence across the enterprise.

Limited utility of hashes

Sandbox solutions use message-digest algorithm (MD5) hash codes to identify malicious files. Like binary signatures, these hashes have limited value. For example, a malicious PDF named "salary-guide. pdf" is sent with dummy content to a human resources (HR) representative. An attacker embeds the same malware into a different PDF and sends it to someone else in the HR department. Because the file attributes are different, the sandbox generates a different hash value for each file—even though they contain the same malicious code. Even if the sandbox identifies the malware in the first PDF, that knowledge does not help in identifying the same malware in another file.

Slow to respond

For manual analysis, security professionals run code in a sandbox environment and observe changes to the environment to spot suspicious behavior. When security teams discover an exploit, they manually generate signatures. The process is essentially a new software release. First, the team submits suspected malware to a security vendor. From there, the vendor must examine the suspected code sample, generate a signature, document it, test it, and finally, release it to customers. This process can take hours, days, or even weeks in many cases. The process is far too slow for today's fast-moving, constantly evolving attacks.

The Key Architectural Advantages of FireEye

Thousands of permutations

In a typical organization, users can run a wide range of operating systems, applications, software versions, security patches, and so on. This variety can make detecting threats much more complex. For example, an exploit may only work on a specific application version, such as Adobe Acrobat version 9. The FireEye platform analyzes each piece of potentially malicious code within hundreds of potential environmental variables using the patented FireEye Multi-Vector Virtual Execution™ (MVX) engine.

Hardened proprietary hypervisor

Many security platforms leverage commercially available virtualization technologies such as VMware, Xen, and Hyper-V to run malware analysis. Aware that their code may be scrutinized in a sandbox environment, threat actors are creating malware that can detect the presence of a common virtual environments to evade detection.

That's why FireEye created the MVX engine—a hardened, proprietary hypervisor built from the ground up for automated malware analysis. The MVX engine can identify even sandboxevading malware.

Multi-flow analysis

Today's advanced threats attack in multiple phases in an orchestrated sequence of events to exploit a vulnerability and breach the network. Threat actors have often hijacked legitimate, well-known websites and embedded malicious code on high-traffic pages. Visitors to the compromised page are profiled, and only victims who match specific characteristics are attacked via a drive-by download. Without the user ever realizing it, the hidden download inserts exploit code within the user's Web browser to exploit a browser or plug-in vulnerability. Once this initial exploit is executed, the attacker can follow up with additional steps, such as delivering malware executables and callbacks to a CnC server. Although the attack appears to stem from a single Web visit, it involves multiple stages that take place in the background.

The MVX engine inspects malicious code within the context of multi-flow environments—where attacks really operate. That enables the FireEye platform to detect malicious code that basic file inspection misses.

Multi-vector analysis

The FireEye platform offers visibility across multiple threat vectors, including Web, email, and files. The platform collects and correlates this multi-vector threat intelligence within and across enterprises. When the FireEye platform detects a malicious email attachment, it executes that code to capture callback information and destination IP addresses. Then it coordinates with Web security devices to block those connections. The FireEye platform blocks attacks targeting other users and stops malware from connecting to malicious or compromised IP addresses.

FireEye Platform Benefits

- Thousands of permutations
- Hardened, proprietary hypervisor
- Multi-flow analysis
- Multi-vector analysis
- Correlation of threat intelligence
- Cloud sharing to community
- Real-time protection

Correlated threat intelligence

Through the FireEye Dynamic Threat Intelligence™ (DTI) cloud, FireEye customers can leverage real-time threat intelligence generated across thousands of appliances deployed by customers around the world. The DTI cloud correlates a range of information including:

- Malware attack profiles
- Malware code identifiers
- Exploit URLs
- Destination IP address
- Protocols used
- Ports used

Real-time protection

The FireEye platform automatically inspects suspicious code. When it detects malware, FireEye immediately blocks the inbound attack, generates alerts, and delivers the intelligence that security administrators need to bolster their defenses. And details about emerging attacks are shared anonymously in real time around the globe through the FireEye DTI cloud.

FireEye System Health Monitoring Report

FireEye offers a complimentary System Health Monitoring Report with critical information about your baseline environment. An easy-to-use executive summary outlines your security posture based on the FireEye threat scoring system, including these key indicators:

- Evidence of data theft due to malware and botnet connections
- The overall threat landscape, which covers currently infected clients, malware variants, content analysis
- Callback analysis
- Zero-day activity
- Malware forensics

The report concludes with detailed security recommendations to remediate infected systems and protect against ongoing threats.

FireEye security recommendations

The System Health Monitoring Report outlines, clear, specific advice that can help you remediate your systems, safeguard your data, and make your defenses more resilient to future attacks.

Conclusion: The FireEye Advantage

For advanced threats, security solutions must identify unknown threats and protect across multiple vectors of compromise such as: Web, email, file, and mobile. With proactive customer monitoring and alerting services—and the global DTI cloud—FireEye provides a new level of protection.

About FireEye, Inc.

FireEye has 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. These highly sophisticated cyber attacks easily circumvent traditional signature-based defenses, such as next-generation firewalls, IPS, anti-virus, and gateways. The FireEye Threat Prevention Platform provides real-time, dynamic threat protection without the use of signatures to protect an organization across the primary threat vectors, including mobile, Web, email, and files and across the different stages of an attack life cycle. The core of the FireEye platform is a virtual execution engine, complemented by dynamic threat intelligence, to identify and block cyber attacks in real time. FireEye has over 1,300 customers across more than 40 countries, including over 100 of the Fortune 500.

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

FireEye