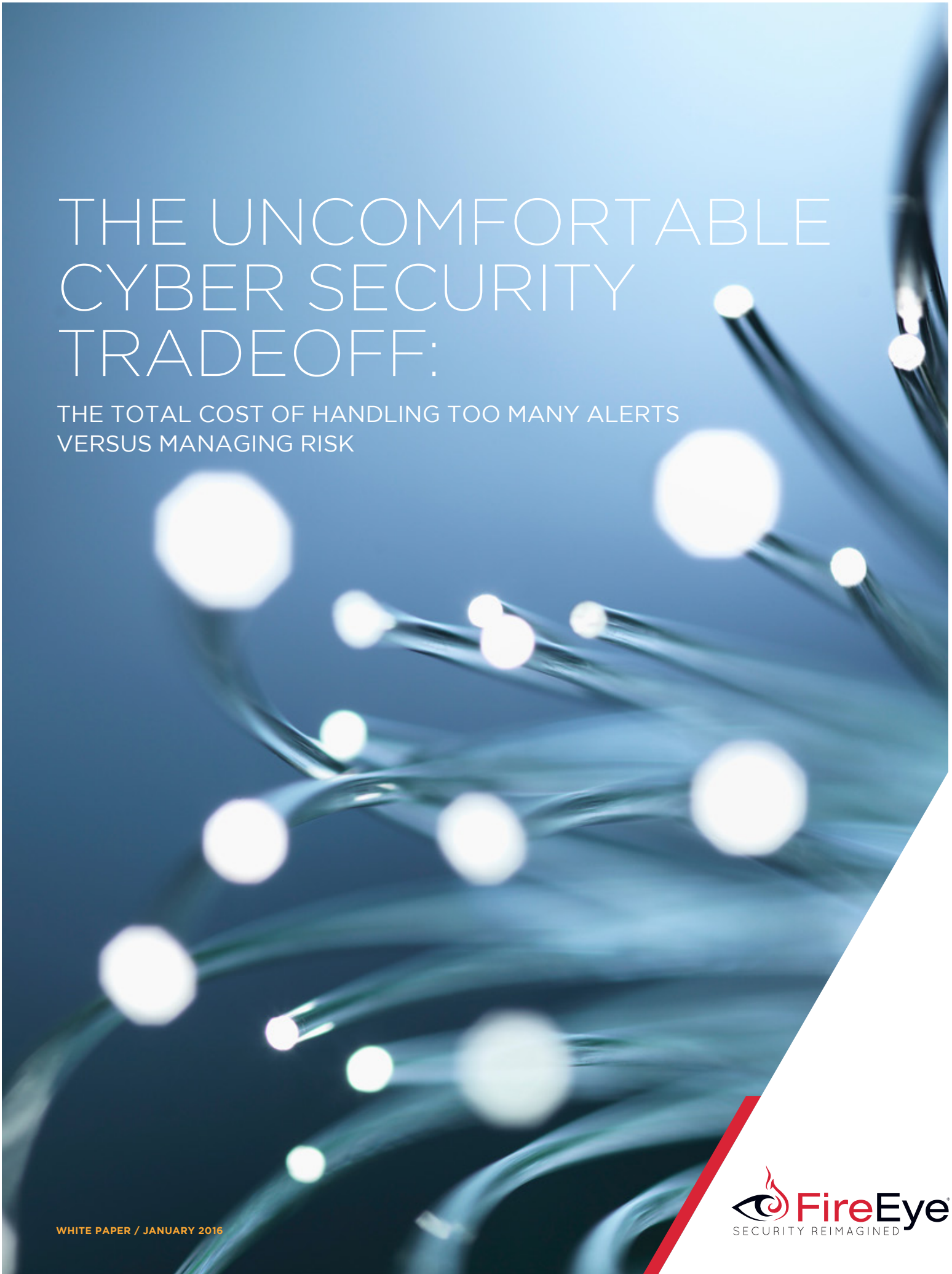

THE UNCOMFORTABLE CYBER SECURITY TRADEOFF:

THE TOTAL COST OF HANDLING TOO MANY ALERTS VERSUS MANAGING RISK

WHITE PAPER / JANUARY 2016

FireEye
SECURITY REIMAGINED

CONTENTS

INTRODUCTION

RECENT HIGH-PROFILE SECURITY BREACHES INVOLVING MAJOR RETAILERS, FINANCIAL SERVICES PROVIDERS, AND GOVERNMENTAL AGENCIES UNDERSCORE HOW DESTRUCTIVE A BREACH CAN BE TO AN ORGANIZATION'S REPUTATION AND FINANCIAL STABILITY.

Many of these headline-grabbing targeted attacks are based on monetary profit, political gain, or data theft, and are a result of an active, persistent pursuit with the intent to compromise the target's infrastructure.

When customer data is stolen, the damage to an organization can be swift – and costly. With awareness of cybersecurity risks at all-time highs, investments are pouring into security technologies. But how do you know if you are investing in the right set of security tools and threat intelligence, getting the best return on your investment, and if those investments enable you to respond swiftly in the moment of crisis? Often an organization's security technologies miss the critical threats entirely or bury the threat with little or no context in a sea of noise.

But how do you know if you are investing in the right set of security tools and threat intelligence, getting the best return on your investment, and if those investments enable you to respond swiftly in the moment of crisis? Often an organization's security technologies miss the critical threats entirely or bury the threat with little or no context in a sea of noise.

A broader defensive response

Today's attacks are highly specialized and precise in nature, which means there is insufficient history to generate a signature that can identify an attack. However, the total volume of threats has gone up dramatically with millions of unique malware samples showing up each day. Therefore, it is practically impossible for security vendors to create signatures for every potential piece of malware. In response, vendors have broadened the aperture of signatures to catch multiple pieces of malware – perhaps an entire malware family – with a single signature. Further, they have lowered the threshold for when alerts are triggered.

Buried in alerts

For security teams, the broadening of the aperture combined with lower alerting thresholds means that even benign activity generates alerts. One of the most well known examples of this came from McAfee a few years ago, where a misconfigured DAT update rendered Windows workstations inoperable. While this is an extreme example, a recent set of tests conducted by FireEye found that most security vendors generated more unreliable alerts than reliable ones.[1] This means the average security team would need to investigate large volumes of benign triggers before a real threat is found, during which time an attacker could be advancing through a network and creating havoc.

Compounding the problem is the fact that not all alerts are the same. Security teams must sort through the thousands of alerts generated by high volume, but relatively low-threat viruses, worms and spyware, to identify and isolate the more infrequent, but dangerous targeted attacks. The result is that many security teams are now awash in alerts and lack resources to scale their response effectively. Excessive alerts thus create a new operational security problem: How to manage all security alerts effectively on a given day?

[1] Cutting through the Clutter, FireEye, 2016

While most alerts are simply noise, security teams can't easily determine which ones are false positives or benign events. Therefore, they can't prioritize the alerts and focus their investigations. The same FireEye report found that vendors primarily fall into two buckets:

- Those that miss the true attacks
- Those that miss the true attacks but generate large numbers of alerts (with high false positives) in an attempt to "catch something"

Organizations are thus faced with either missing true threats, or being buried in a large volume of alerts. In either scenario the conclusion is the same: the security operations team never gains visibility or context on the threats that presented significant risk.

The cost of ineffective security

According to recent research by the Ponemon Institute, the average company unnecessarily spends over $1.2 million[2] annually responding to erroneous or inaccurate alerts. And security analysts waste two-thirds of their time chasing down the wrong alerts due to faulty intelligence – two-thirds of the time of a resource whose fully loaded cost to your organization can be $150,000 or more.

The average organization receives hundreds of thousands of alerts a week, of which an estimated nineteen percent or less are reliable, and the organization's resources only allow it to investigate four percent[2]. But how can you know if you are focusing on the right four percent of threats? Even more importantly, how do you prioritize the alerts to focus on, especially if you do not have the capacity to handle even the true alerts?

Security teams are left with an uncomfortable and expensive tradeoff: either scale their operations at considerable cost or increase the risk of missing a critical alert and exposing the company to a costly security breach. Depending on the size of the organization, bulking up the security team could cost tens of millions of dollars – an inefficient proposition. On the other hand, according to IDC, financial damages to the business due to targeted threats range from $10,000 to more than $100,000 per hour in post breach[3] costs. In many cases, threats remain undetected for days, or sometimes even months, driving potential costs into millions of dollars.

[2] The Cost of Malware Containment, Ponemon Institute, January 2015
[3] Shifting Risks and IT Complexities Create Demands for new Enterprise Security Strategies, IDC, February 2014

Focus on the alerts that matter

Security teams must cut through the clutter of alerts and enhance their security operations so that they can focus on the threats that matter the most. These guidelines can help organizations spend wisely to best manage the tradeoff between alerts and risk. The "At a Glance" sidebar quantifies an example of the operational benefit when these recommendations are implemented in a security posture. More specifically, look for a solution that provides:

1. **High fidelity, low false positive alerts**

   Organizations that manually triage through both true and false positives can spend up to 157 minutes identifying a true positive. With FireEye, false positives are eliminated by our MVX engine, which does the same in about 4 minutes on an average - compare 157 minutes of an expensive and hard to find human resource to 4 minutes within a technology solution. Owning FireEye, you not only increase security operations efficiency, but also limit risk by finding threats quickly.

2. **Contextual intelligence for alert prioritization**

   Your security technology needs to have contextual intelligence that provides details on the attacker as well as the scale and scope of the attack. With this depth of information, you will be in a better position to prioritize threats and craft proper responses. FireEye detection products deliver this context including threat severity, attack characteristics, and attacker profile with each alert. This means you can focus on the most critical alerts, a task nearly impossible with other approaches that can't distinguish alerts without deeper investigation.

   In addition, you can feed all your events and event data through the FireEye® Threat Analytics Platform and apply FireEye threat intelligence against that data to find the presence of indicators of compromise as well as build the context necessary to prioritize the alerts that present the most risk to your organization.

3. **Early detection of attacks**

   Finding threats early provides a dual benefit. First, it minimizes risks by stopping attacks before significant impact and second, it eliminates downstream alerts raised later in the attack life cycle thereby decreasing the operational cost of analysis. FireEye technology has the most comprehensive visibility across the attack lifecycle and can detect threats during the exploit phase before the attacker has a foothold in the victim environment. Moreover, it can also be deployed in-line, so that you can identify and block these attacks early in their life cycle, reducing additional alerts in later stages. FireEye customers report a 76 percent reduction in alerts.

4. **Find the Right People to Manage, Investigate, and Respond to Alerts**

   With the right technology and intelligence, you can narrow the focus area to a set of prioritized alerts with the context to investigate them. That is only part of the puzzle. Any security program will still require the right combination of experts to monitor the alerts for true threats, and subsequently triage, investigate and respond to those alerts. This requires the techniques, experience, and intuition honed over years of identifying and responding to the most consequential breaches in the world. With FireEye as a Service and our Mandiant Consulting team, you have the option to do this yourself if you have the expertise in house or partner with us and thus have the world's top security experts monitoring your network and systems around the clock to detect, prevent, analyze and respond to the security incidents in a fraction of the time it takes using conventional approaches.

AT A GLANCE

A True Cost of Ownership calculator is available online at www.fireeye.com/tco.html for each organization to customize viewpoints on the operational cost and risk created from false positives and alert volumes. The following is a snapshot of outcomes based on default values informed through common deployments, which take into account resource capacity constraints.

This example demonstrates two outcomes that quantify the impact of alert volume, and more specifically, false alerts- operational time and operational cost. Additional time is necessary to triage through alert volumes, especially false positives – that can be upwards of 80% of total alert volume when using competing solutions. FireEye alerts leverage the power of MVX to automate the identification of threats that matter. This wasted time can also be correlated to the operational cost tied to triaging and investigating alerts, a cost that can be $600 per incident or more. A solution with false positives requires security teams to wade through volumes of noise to find the weak signal, which results in the operational overhead.

An often unaccounted for consideration is the impact of detection technologies that have visibility across the entire lifecycle. By seeing and stopping attacks early (e.g. during exploit), it eliminates the alerts that would be generated from subsequent stages of the attack (e.g. callbacks) and alerts from other victims when the scope of the attack expands.

	Standard	FireEye
Average Time to Identify an Alert that Matters	157 Minutes	4 Minutes
Annual Operational Expenditure Due to Alert Volume Given Resource Capacity	$21,996,000	$1,903,200
Annual Operational Expenditure Due to Alert Volume When Deployed Inline	$21,996,000	$456,768
Annual Operational Expenditure Due to False Positives Given Resource Capacity	$17,816,760	$19,032

Find the perfect balance

Don't waste time and money sorting through and responding to a deluge of false positives. With high-fidelity, intelligent context, and early detection, you can greatly reduce the time required to identify a true positive and quickly prioritize the remaining critical alerts based on attack profile and severity. FireEye technology helps you keep operational security costs down by allowing you to quickly identify, focus on, and react to the threats that matter most. **Learn more** about FireEye's complete approach to protecting your organizations from cyber threats.

For more information on how to make the most out of your security investment, visit:
www.fireeye.com/tco.html

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

fireeye.com

FireEye