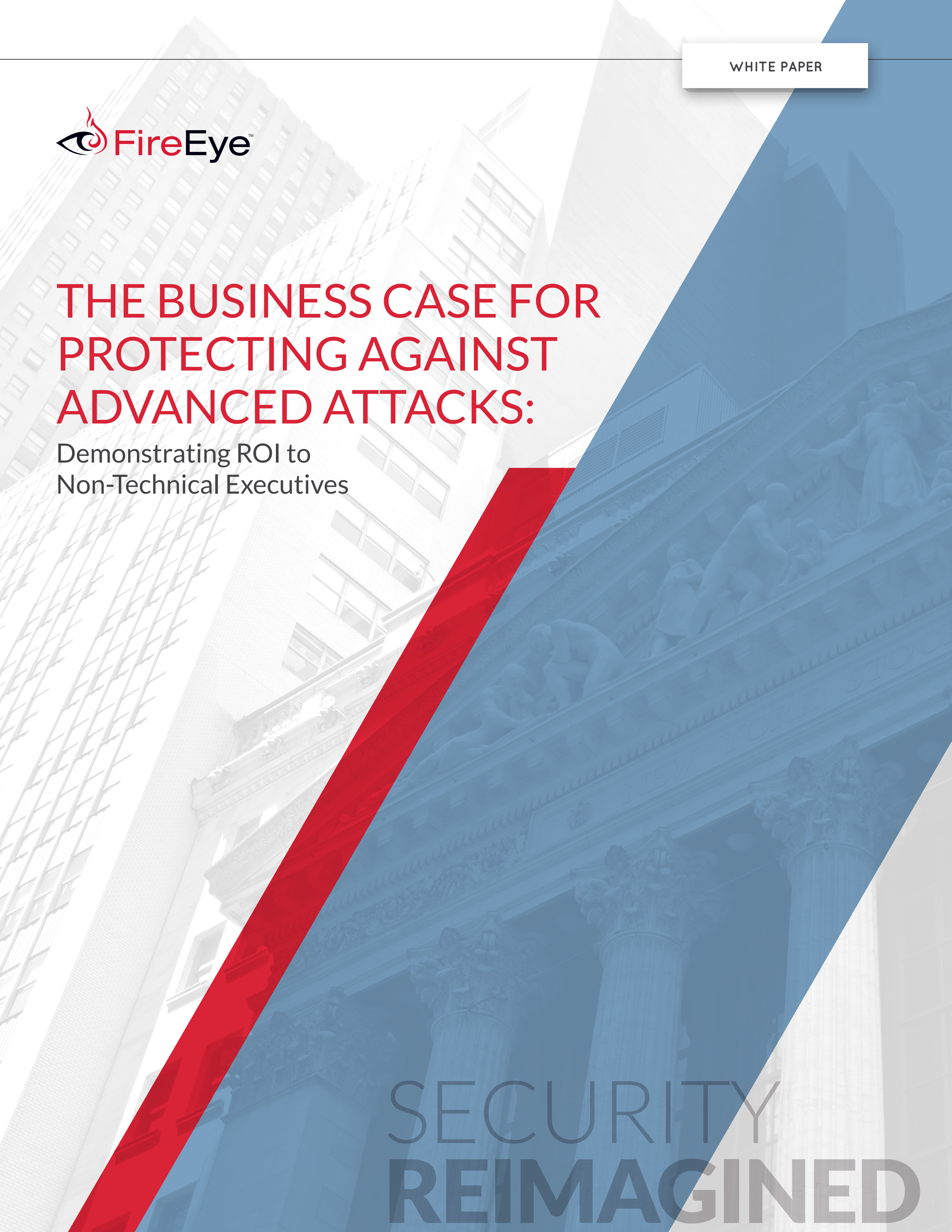


WHITE PAPER

THE BUSINESS CASE FOR PROTECTING AGAINST ADVANCED ATTACKS:

Demonstrating ROI to Non-Technical Executives

SECURITY
REIMAGINED

CONTENTS

Executive Summary

We know you get it. Today's cyber threats require advanced security. Our traditional network and endpoint defenses are clearly outmatched and don't stand a chance at preventing, investigating, or remediating today's targeted attacks.

But why doesn't your company get it? And more importantly, why doesn't your boss or the board of directors get it? Perhaps you're not making your case using language that they can easily understand—money.

Given today's sophisticated threat landscape—and how difficult it is to prevent, investigate, and remediate targeted attacks—advanced security solutions should be viewed as a strategic business investment, with a typical payback period between one and two years.

If you want to make your case for investing in advanced threat protection to your company's executives, then you'll need to think like your executives. We'll show you how.

Life Without an Advanced Security Solution

Before demonstrating the potential return on investment (ROI) of an enterprise-class advanced security solution, you'll need to properly set up the problem. Your executives need to know the challenges you face and the risk if you don't find solutions. Start by describing what life is like without advanced security. Here are three key points you should make:

"Like malware with no known signature, traditional defenses also cannot detect or prevent zero-day exploits or multi-stage attack methods."

Point #1: Our existing defenses can't detect or prevent the targeted tactics used by adversaries.

Most executives have heard about antivirus (AV), but they may not understand how signatures limit the scope of what can be detected. You need to educate them that traditional network and endpoint security products—such as endpoint AV and intrusion prevention systems (IPS)—are designed to detect known threats through pattern-matching signatures. Unfortunately, advanced threat actors often customize malware to evade signature-based detection. Custom malware sails past most signature-based defenses—through web, email, and other attack vectors—as if they weren't even there.

If the executive you're speaking with is a little more technical than most, you could make a stronger case by explaining that malware is often not even used in targeted attacks! Attackers with advanced skills are patient enough to wait for an initial entry point, assemble a toolkit and formulate an attack plan over time as they watch and learn about your employees and your network. These multi-stage methods often involve exploiting unknown vulnerabilities (the so-called zero-day threats), stealing authorized credentials and using benign utilities for malicious purposes.

Remind the executive that there's a whole underground market for the latest operating system or application vulnerability that can be exploited. Like malware with no known signature, traditional defenses also cannot detect or prevent zero-day exploits or multi-stage attack methods.

Point #2: We don't have the tools to properly investigate and prioritize alerts.

Once evidence indicates that your network or systems are compromised—perhaps through a security alert or notification from a third-party —it's important to investigate quickly to determine the scope (Is it just one machine? Or thousands?) and severity of the compromise (Is the attacker merely observing a host? Or in the act of stealing confidential data?) Unfortunately, many organizations lack the tools needed to validate threats and determine their impact.

> "Rapidly investigating attacks when an incident does occur can mean the difference between defeating your cyber adversaries and making headlines."

When speaking with your executives, be frank with them. Explain that no matter how much money a company spends on security, the potential for compromise by a determined attacker always exists. There are no guarantees in life (okay, aside from death and taxes) and there are certainly no guarantees with IT security. Rapidly investigating attacks when an incident does occur can mean the difference between defeating your cyber adversaries and making headlines.

Point #3: Compromised endpoints are difficult to identify and contain, especially for remote employees.

The third challenge you'll want to highlight is your organization's inability to quickly identify, analyze, and contain hosts that are compromised. The typical "whack a mole" approach – reimaging machines as signs of compromise are randomly discovered— is not effective. It is particularly disruptive for remote employees, who often have to ship IT assets back to headquarters. Really nail the point home with executives by explaining the amount of downtime that occurs when a patient zero connects to the network and infects hundreds or thousands of other machines. With no ability to contain the spread or know exactly which machines are compromised, the under-staffed IT team mandates a rebuild of all systems, halting productivity for hours or days!

Simply having the ability to proactively look for signs of compromise on all IT assets, whether they are on the corporate network or connected via a public hotspot, can go a long way in identifying problems early and preventing the spread. An advanced security solution would take that one step further to allow remote analysis and response.

What your organization really needs

Of course, no executive wants to hear about problems without proposals to fix them. Thankfully, modern-day advanced security solutions provide the answers to these three challenges, and much more.

A full-fledged advanced security solution solution shares intelligence across all three of its major components, including:

- **Network-based threat visibility—**for detecting and preventing attempts to compromise your network through web and email tactics.
- **Endpoint threat visibility—**for identifying and containing malicious activities and compromised endpoints, whether mobile, in the office or around the globe.
- **Analysis and investigative forensics—**for validating suspected threats and determining the event chain, scope, and impact of an attack.

To learn how to assess the business impact of security incidents targeting your organization and to build your own business case, read on.

Assessing the Business Impact of Advanced Security Solutions

Once you've established a basic understanding as to why your organization lacks the tools necessary to prevent, investigate, and remediate advanced threats, it's now time to shift the discussion from bits and bytes to dollars and cents. As with any ROI analysis, there are financial costs and financial benefits associated with an advanced security solution. The former is very straightforward. The latter is a bit more complex. Let's explore both.

Avoid Costs Resulting from a Breach:

- revenue hits
- public relations
- customer notification
- incident response
- regulatory or other fines
- legal fees
- competitive displacement

Financial costs

The financial costs of purchasing an advanced security solution that protects against targeted attacks are straightforward and reasonably easy to quantify:

- **Product or service licensing costs.** Most advanced security solutions are packaged in purpose-built, high-performance rack-mountable appliances. These products carry a perpetual usage license and usually require annual subscriptions or maintenance plans to supply customers with up-to-the-minute threat intelligence, technical support, and ongoing software updates.
- **Supplemental components.** Be sure to factor in costs of certain supplemental components needed to deploy your advanced security solution, including network TAPs, appliance racks, uninterruptable power supplies (UPS), and anything else needed to keep your solution up and running.
- **Product deployment costs.** Whether you leverage experienced consultants supplied by the vendor or your vendor's reseller, or you decide to in-source it, there is always a cost to deploying an advanced security solution.
- **Employee training costs.** All IT personnel responsible for advanced IT security will need to be trained on how to use the products and perhaps also learn new skills related to investigating and responding. The costs associated with training include classroom training, on-site training, and/or internal knowledge exchange.

Some vendors offer their web and email-based security solutions as a hosted cloud service. Such solutions usually increase the cost of advanced threat protection because significantly more Internet bandwidth is required to support the upload of suspicious content to the vendor's cloud-based malware analysis system. They also fail to identify the signs of a multi-stage attack and are, therefore, less effective.

Financial benefits

Although the financial costs associated with your advanced security solution are fairly easy to quantify, assessing the financial benefits is a bit more challenging. The best way to think about the financial benefits is to group them into three categories: preventing, investigating, and remediating advanced threats.

Improve Ability to Investigate:

- alert validation
- root cause determination
- impact assessment

Category #1 – Avoiding costs resulting from a breach. The most effective way to avoid costs associated with data breaches is to avoid a breach altogether. Although there is no 'silver bullet' defense against determined attackers, a multi-faceted solution capable of evaluating threats across multiple vectors—web, network, and email—and detecting signs of compromise on mobile devices, endpoints, and files at rest, is the most effective way to keep your company's network and IT assets out of harm's way.

The following financial benefits are actually costs you can avoid by experiencing far fewer—or hopefully no—data breaches as a result of your investment in an advanced security solution.

- **Avoiding revenue hits.** A major data breach can have a dramatic effect on revenue. If a national retailer experiences a large credit card data breach, for example, a portion of its customers may shop elsewhere for fear of having their credit card data compromised.
- **Avoiding public relations costs.** Every publicly disclosed data breach spawns damage control by the victimized companies. Companies often recruit the expertise of public relations firms to craft customer-facing messages to help restore the company's image and arrest falling stock prices.
- **Avoiding customer notification costs.** Companies affected by a large-scale data breach must proactively notify customers and business partners potentially affected by the breach and reactively respond to concerned calls and emails.
- **Avoiding incident response and remediation costs.** When victimized by an extensive data breach, many companies employ the services of expert incident response consultants—such as those from Mandiant—who are equipped with special tools and training to uncover the root cause of an attack, ensure the attack has been terminated, and aggregate forensically sound evidence that may be used to identify and convict the perpetrators.
- **Avoiding regulatory fines.** Breaches that occur at organizations found to be non-compliant with industry regulations (e.g., PCI, HIPAA) may be subject to regulatory fines and increased scrutiny from regulators. In some instances, fines may accumulate into the millions of dollars.
- **Avoiding legal fees and punitive damages.** A frequent outcome of large-scale data breaches is class-action lawsuits by customers /or investors. After spending millions on attorney and court fees, your organization may be subject to punitive damages if your organization is found negligent.
- **Maintaining competitive advantage.** In the event proprietary data is stolen pertaining to the company's core products (e.g., software source code), the company may lose a competitive advantage that it's never able to regain.

Contain Cost of Remediation:

- identify infected hosts
- quarantine to stop spread

Category #2 – Reducing costs associated with investigating and remediating suspected incidents. This second category of financial benefits relates to cost savings realized by automating key activities performed by security analysts, such as validating security alerts and determining the root cause and material impact of successful data breaches.

- **Improved ability to validate security alerts.** Security analysts monitor hundreds (and sometimes thousands) of alerts from security products each day. Having rich intelligence at your fingertips dramatically improves your analysts' ability to validate security alerts.

- **Improved ability to investigate root cause.** Once an alert has been validated and a compromised host has been identified, the analyst should identify the root cause of the attack to learn from the incident and take measures to prevent follow-on attacks. Network and endpoint forensics provides incident responders with a treasure trove of data enabling them to determine the root cause of attacks within hours instead of days or weeks.

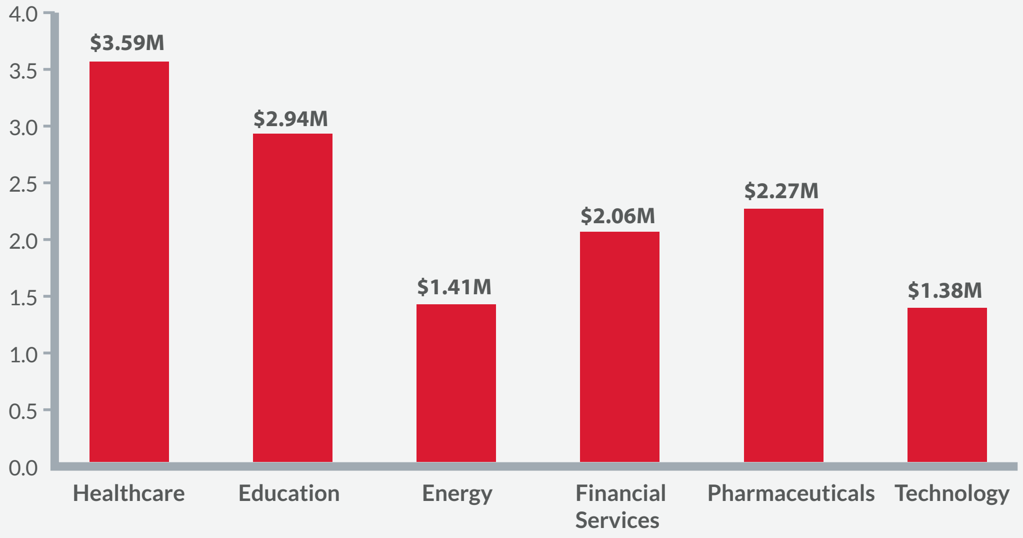
- **Improved ability to quantify material impact.** Assessing what, if any, data was actually stolen as a result of a data breach is difficult at best. Most companies lack the tools and just "assume" that the attacker stole all data on a compromised host. Forensic tools help take the guesswork out of quantifying the material impact of data breaches.

Category #3 – Containing the cost of a breach by improving remediation. The third and final category is associated with remediating infected hosts. Although an advanced security solution doesn't aid in the removal of malware or the re-imaging of hosts, it does assist with two important remediation tasks:

- **Improved ability to identify infected hosts.** Advancements in host-based security solutions enable security professionals to identify the scope of a breach by looking for indicators of compromise on corporate IT assets across the enterprise. In this way, they know precisely which machines need remediation, saving time and effort (and money) in the clean-up phase.

- **Newfound ability to quarantine infected hosts.** Whether an infected endpoint is connected to the corporate network or a Wi-Fi hot spot in a coffee shop around the world, today's advanced host-based security solutions can effectively quarantine endpoints to prevent communication with other systems (with the exception of the endpoint monitoring appliance). Containing the incident minimizes data theft and the spread of malware, which minimizes the overall cost of a breach.

Figure 1: Global average cost (in millions) by industry. Based on an average of 10,000 records compromised.



Building Your Own Business Case

Measuring ROI for a security product is often compared to measuring the ROI of automobile insurance. How can you measure the return on your automobile insurance policy if you've never been involved in a car accident? And, of course, not all car accidents are the same—just like not all data breaches are the same.

With so many variables to consider, how can one build a solid business case for investing in an advanced security solution? We have two suggestions—a basic, "back of the cocktail napkin" level of analysis and a more detailed, comprehensive analysis.

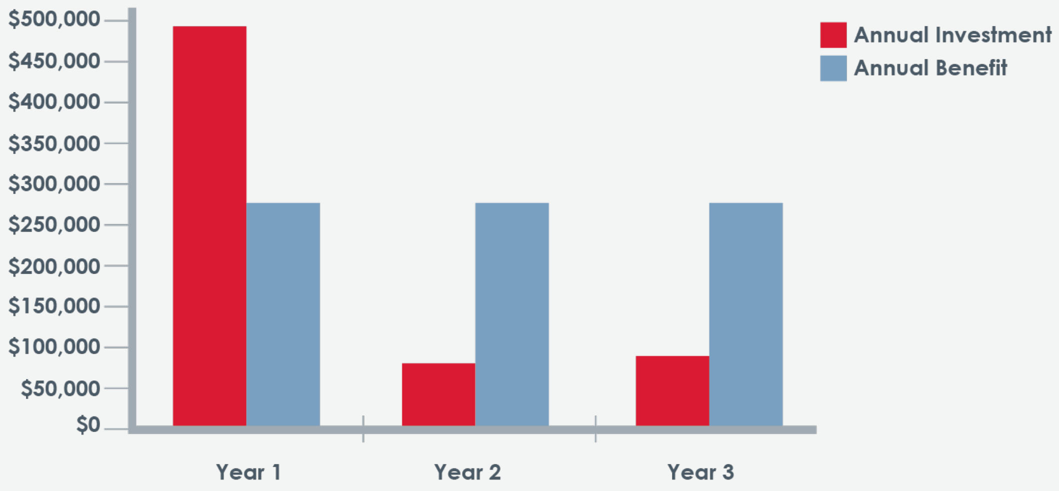
Cocktail napkin ROI analysis

Let's begin our basic analysis by focusing exclusively on the benefits achieved by detecting and preventing targeted attacks (depicted in Category 1). Rather than estimating avoided costs, let's make it even simpler.

Ponemon Institute is a well respected IT research firm. Each year, it publishes the "Cost of Data Breach Study" to that assesses the total cost of corporate data breaches. Ponemon's May 2014 report finds the average cost of a data breach (that occurred in 2013) across 314 companies in 10 countries to be $3.5 million, which is an increase of 15% over the prior year's finding. As you can see in Figure 1, the average varies by industry across the globe but is dependent on the number of records compromised.

So, in the spirit of keeping things simple, let's calculate ROI of a network-based advanced security solution designed to detect and block threats found in web and email traffic. (We'll address financial gains achieved from investigating and remediating advanced threats in the next section.) But first, we'll need a few assumptions:

Figure 2: Comparison of annual investment and benefit over three-year period

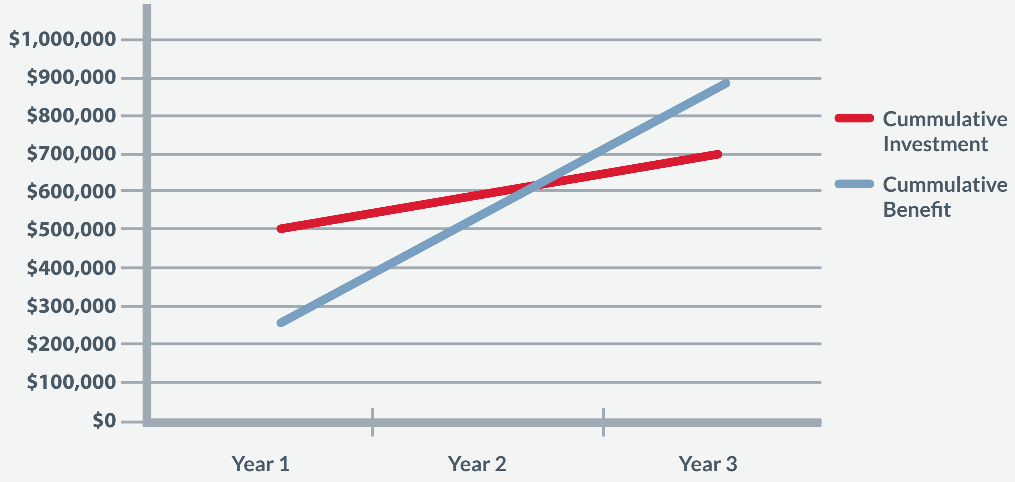


The 2014 Ponemon report mentioned above estimates the probability of a company experiencing a data breach involving a minimum of 10,000 records over a 2-year period at 22.2%. Putting the odds of a similar data breach over a three-year period at 25% seems reasonable.

Figure 2 offers a year-by-year comparison of the annual investment and potential annual benefit forecasted from your investment in web- and email-based advanced security solutions solutions.

FINANCIAL COSTS:	
Advanced network security solution cost	$500,000
Annual maintenance	20%
FINANCIAL BENEFITS:	
Average data breach cost (avoided) (Ponemon Institute, 2014)	$3,500,000
Odds of average-size breach over three-year period (without an advanced security solution)	25%
Financial benefit by avoiding a data breach for 3 years ($3,500,000 x 0.25)	$875,000

Figure 3: Comparison of investment and benefit over three-year period



To better visualize the break-even point, where avoided breach costs surpass the advanced security solution investment, refer to Figure 3. This illustration depicts the cumulative (i.e., since inception) investment and benefits by year as measured by "avoided costs" over the same three-year period.

As you can see in Figure 2, the break-even point for recouping your up-front investment in year 1 occurs mid-way through the second year. In this basic example, the company yields a positive return of $175,000 over three years for an ROI of 25%. Of course, this doesn't take into account the many cost-saving benefits of automating advanced threat investigation and remediation processes. Perhaps that's a good segue to the next section.

Comprehensive ROI analysis

Okay, maybe "cocktail napkin analysis" wasn't the right term for the prior section. But as you'll discover in the next section, calculating a complete ROI for a full-featured advanced security solution can get pretty complicated.

FINANCIAL COSTS:	
Advanced security solution investment (network- and host-based advanced security plus forensics and intelligence)	$1,000,000
Annual maintenance	20%
Supplemental components	$300,000
Product deployment costs	$200,000
Employee training costs	$100,000

FINANCIAL GAINS:	
Average data breach cost (avoided) (Ponemon Institute, 2014)	$3,500,000
Odds of average-size breach over three-year period (without an advanced security solution)	25%
Financial benefit by avoiding a data breach for 3 years ($3,500,000 x 0.25)	$875,000
Increase in incident response team productivity (benefits of automating investigation and remediation tasks as described in Categories 2 and 3)	50%

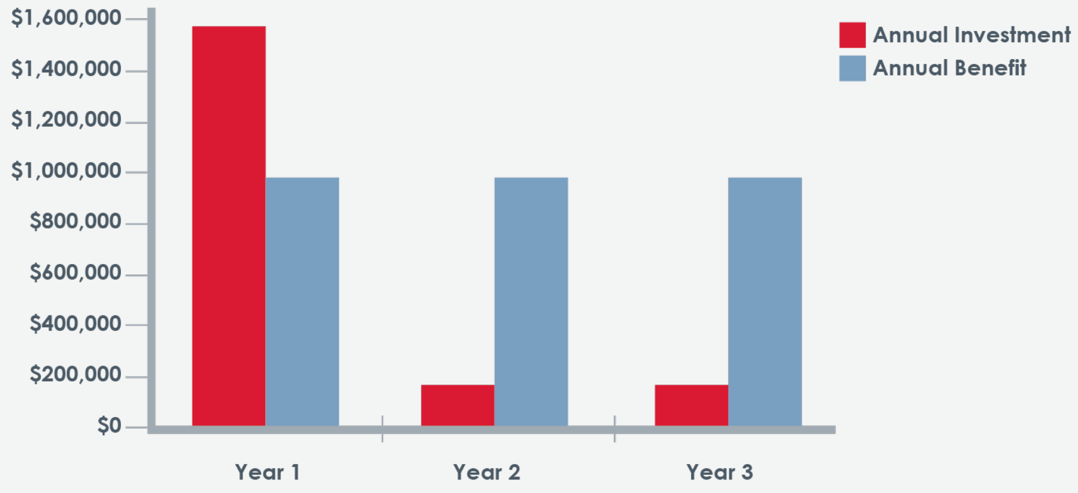
OTHER ASSUMPTIONS:	
Number of full-time security analysts and incident responders	10
Average hourly rate (in U.S. dollars)	$75
Hours worked per worker per week	40
Weeks worked per worker per year	48

Although the itemized financial gains in Category 2 (investigating) and Category 3 (remediating) are completely valid, it's virtually impossible to quantify those gains before implementing your advanced security solution. Of course, if you'd like to try, go for it!

In working with thousands of corporations and government agencies around the globe, we estimate an across-the-board productivity increase of approximately 50% for security operations center staff and incident response teams. This means a staff of 10 will ultimately be just as productive as a staff of 15.

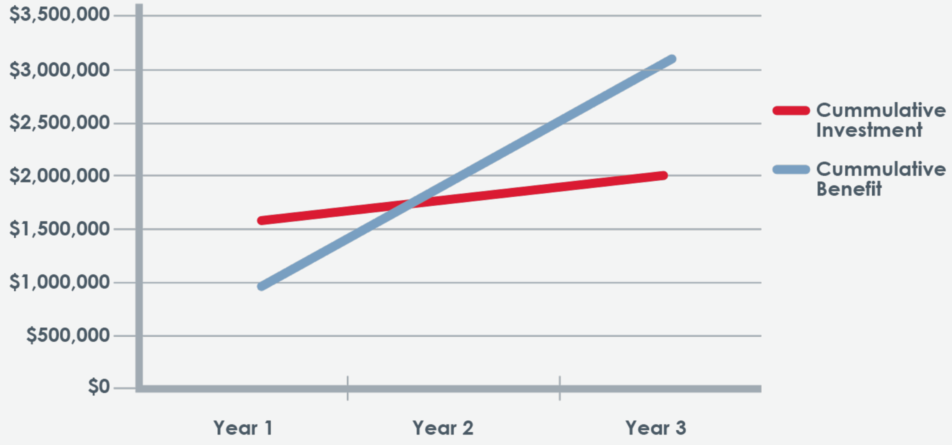
So, after crunching the numbers depicted above across a three-year period, Figure 4 depicts a year-by-year comparison of projected annual advanced security solution investments and realized benefits. As you'll soon discover, factoring in cost savings achieved by automating investigation and remediation tasks makes the three-year ROI stats even more compelling.

Figure 4: Comparison of annual investment and benefit over three-year period



Like in the prior section, Figure 5 depicts the break-even point across that same three-year period. Once again, this illustration depicts the cumulative investment and return as measured by avoided costs and productivity gains by year.

Figure 5: Comparison investment and over three-year period



If you carefully compare Figure 5 (comprehensive ROI analysis) to Figure 3 (basic ROI analysis), you can see that the break-even point occurs even earlier during the second year. That's because the incremental gains achieved through improved productivity of the security team outweigh the incremental costs of network- and host-based advanced security products, network forensics, supplemental products (e.g., TAPs), deployment costs, and training costs.

In this comprehensive ROI analysis, the company yields a positive benefit of $1,035,000 over three years for an ROI of 52%.

Conclusion

Today, savvy IT security professionals know that it's no longer a matter of "if" your network will become compromised, but "when." In fact, a research study[1] (between October 2013 and March 2014) indicates that 97% of the organizations had been breached, meaning at least one attacker had bypassed all existing network and endpoint defenses. Further, more than one-quarter of the same organizations experienced events known to be consistent with tools and tactics used by advanced persistent threat (APT) actors.

Given the modern cyber-threat landscape, IT security teams are no longer measured on their ability to prevent attacks, but on their ability to respond to attacks, as well. Fortunately, innovations in advanced security solutions are providing organizations newfound capabilities to do both.

Hopefully by now, you've concluded that whether you acquire a network-based advanced security solution for detecting and preventing web- and email-based threats, or you invest in a full-featured advanced security solution—adding network forensics and host-based protection—your investment will consistently yield a positive benefit. And now you have the methodology to demonstrate it.

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 combined with the most aggressive "boots on the ground" 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. The FireEye Global Defense Community includes more than 2,200 customers across more than 60 countries, including more than 130 companies in the Fortune 500.

[1] Cybersecurity's Maginot Line: A Real-World Assessment of the Defense-in-Depth Model," FireEye, 2014.

FireEye