NETWORK SECURITY

A Buyer's Guide

How to evaluate network security for advanced threat protection

FireEye

Since January 1, 2016, more than 4,000 ransomware attacks have occurred daily, a **300% increase in attacks** since 2015.

U.S. Department of Justice

Introduction

Cyber criminals are targeting vulnerable network security systems across the world, costing global organizations billions in data breaches.[1] In the United States alone, the average total organizational cost was $7.35 million in 2016.[2] As seen in the media with the WannaCry ransomware attack, cyber crime continues to rise dramatically.

Since January 1, 2016, more than 4,000 ransomware attacks have occurred daily, a 300% increase in attacks since 2015.[3] In 2016, 1.4 billion global records were lost or stolen due to data breaches, and the United States reported the highest number of breaches with 858 million compromised records.[4] As a result, the total global cost of data breaches due to cyber crime was more than $450 billion in 2016.[5] Not only are these malicious attacks costly, they also negatively impact an organization's reputation, brand and customer and client trust.

Today's cyber attacks are more sophisticated than ever, cutting across multiple attack vectors — such as web, email, file and system exploits — and unfolding in multiple stages. Traditional, signature-based defenses such as firewalls, intrusion prevention systems (IPS) and anti-virus solutions cannot protect against all of these continuously evolving threats. They can only stop known threats. But since 80% of malware is used only once and 68% of malware is unique to a single organization, they are ineffective against today's attacks.[6]

These solutions can't stop attacks as they happen. Just as bad, they inundate security teams with inconsequential or false alerts. Most organizations only have resources to investigate approximately 4% of alerts,[7] so there's a good chance a true threat will slip through.

To stop today's attacks, you need a different approach to network security that doesn't rely on signatures or other historical data. But how do you know if a network security solution is up to the task? This guide can help. It provides a list of requirements to look for and questions to ask when evaluating or purchasing a network security solution.

[1] Graham, L. (February 7, 2017). Cybercrime costs the global economy $450 billion: CEO.
[2] Ponemon Institute (2017). Cost of Data Breach Study: Global Overview.
[3] U.S. Department of Justice, Computer Crime and Intellectual Property Section (2016). How to Protect Your Networks from Ransomware.
[4] Gemalto (2016). Breach Level Index Report.
[5] Roberts, J.J. & Lashinsky, A. (June 22, 2017). Hacked: How Business is Fighting Back Against the Explosion in Cybercrime.
[6] FireEye (2016). Network Security: Effective Protection Against Cyber Breaches for Organizations of All Sizes.
[7] Ponemon Institute (2015). The Cost of Malware Containment.

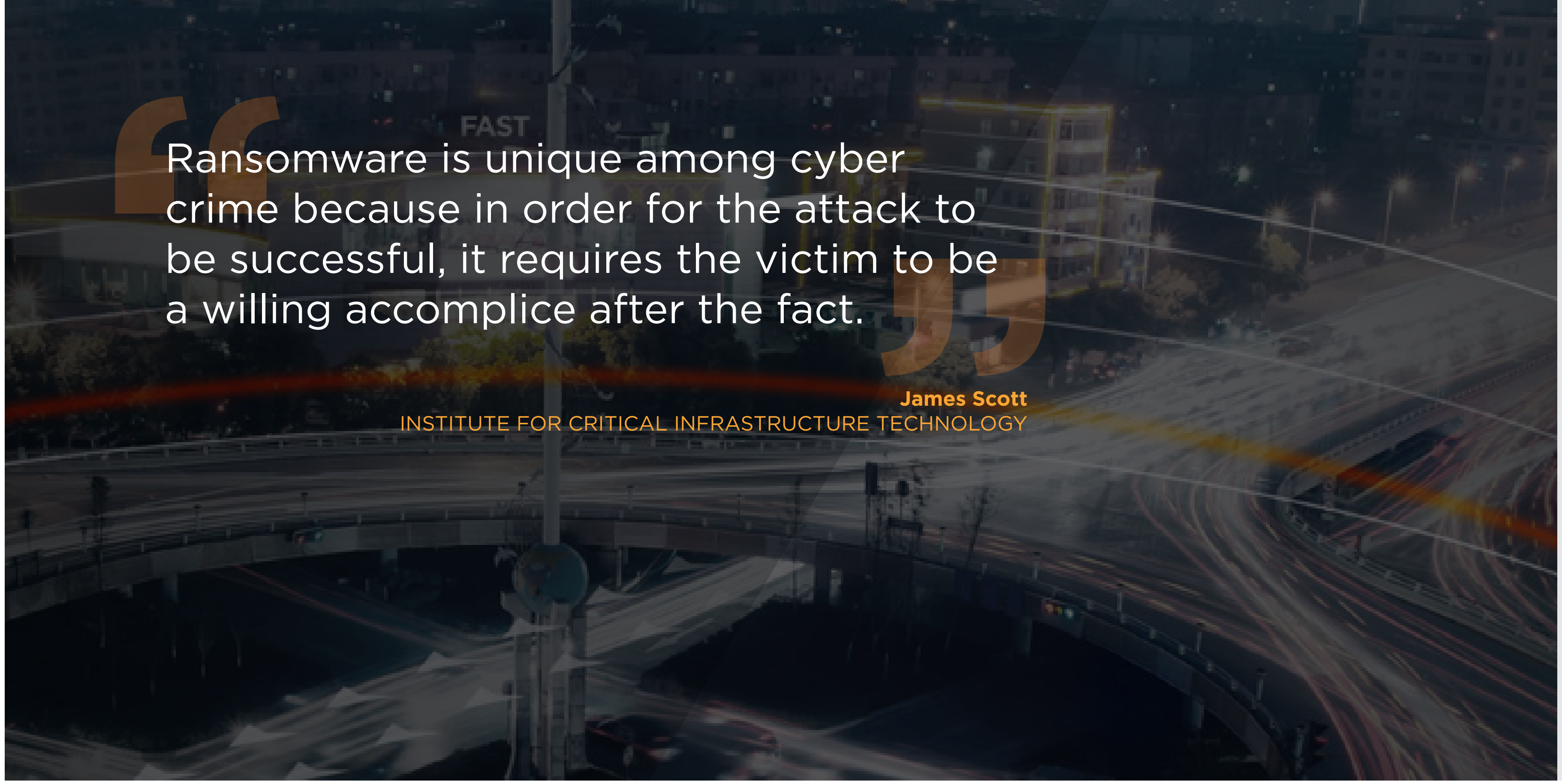
< PREVIOUS NEXT >

Capability #1

Detect and Stop Attacks, Including Zero-Day Exploits and Custom Malware

Despite organizations spending billions to prevent malicious attacks, sophisticated cyber criminals manage to stay one step ahead of traditional, signature-based network security solutions. They use advanced tactics such as zero-day exploits and customized malware to exploit vulnerabilities in operating systems and applications to gain access to resources and steal information.

Because sophisticated exploits and malware may not be immediately detected and contained, you may not realize that your network has been breached. Once bypassed, traditional network security solutions such as firewalls and secure web gateways are mostly ineffective, leaving your organization exposed to a serious data breach.

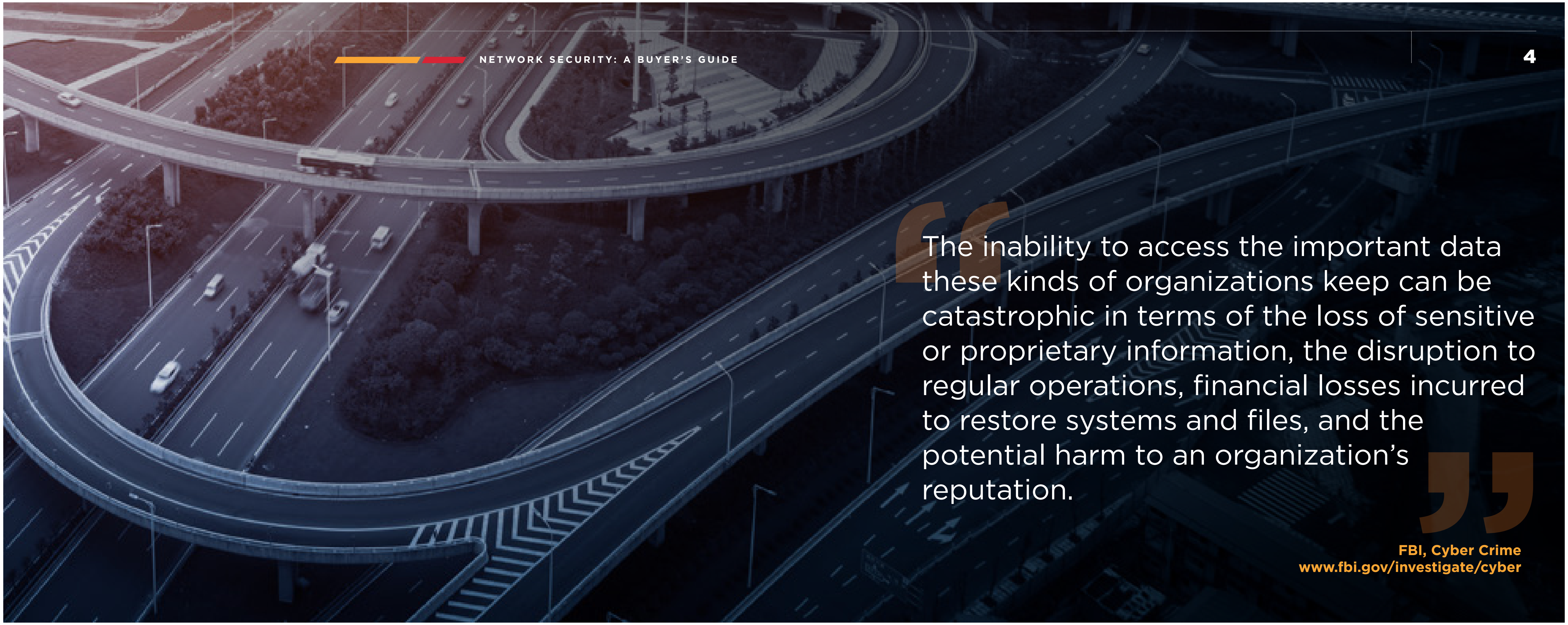


> Ransomware is unique among cyber crime because in order for the attack to be successful, it requires the victim to be a willing accomplice after the fact.
>
> **James Scott**
> INSTITUTE FOR CRITICAL INFRASTRUCTURE TECHNOLOGY

? Ask these questions when evaluating network security solutions

- Does it use multiple threat analytic techniques to accurately detect both known and unknown threats with a low rate of false alerts?
- Does it prevent cyber criminals from exploiting vulnerabilities in Windows® and macOS,® along with a variety of applications and application versions?
- Does it protect distributed offices with different WAN link speeds and provide a consistent level of protection across the entire organization?

< PREVIOUS NEXT >



> The inability to access the important data these kinds of organizations keep can be catastrophic in terms of the loss of sensitive or proprietary information, the disruption to regular operations, financial losses incurred to restore systems and files, and the potential harm to an organization's reputation.

FBI, Cyber Crime
www.fbi.gov/investigate/cyber

Capability #2

Quickly Recognize and Respond to High-Priority Threats

Security teams receive thousands of threat alerts on a daily basis. Of these fake malware alerts received by security operations teams, 81% are considered false positives and only 4% are investigated.[8] Because signature-based network security solutions do not quickly recognize and prioritize critical threat alerts, your organization is at greater risk for a calculated, malicious attack.

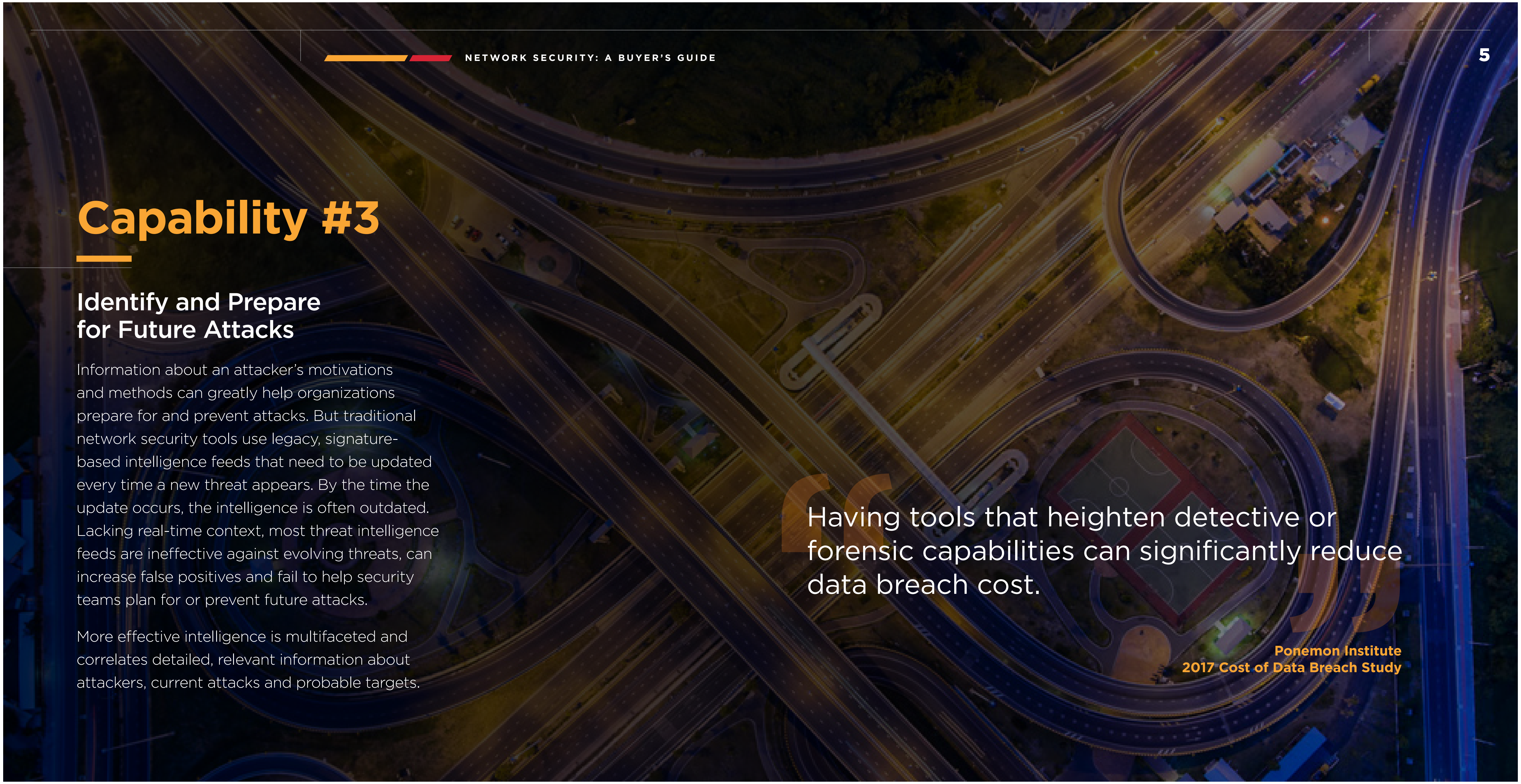
Once you experience an attack, the time it takes to recognize and respond to the breach is critical. Faster access to more accurate intelligence can greatly reduce further threat exposure and impact of a breach. When companies cut the time they need to detect and respond to breaches by 50%, they can reduce the business impact of those breaches by up to 70%.[9]

? Ask these questions when evaluating network security efficacy

- Does it deliver a less than 1% false positive rate?
- Does it use inline blocking to immediately stop attacks?
- Does it help you prioritize and immediately respond to threats by providing real evidence and contextual intelligence?
- Does it automatically validate and correlate alerts to help you quickly identify and protect against multi-vector attacks?

[8] Ponemon Institute (2015). The Cost of Malware Containment.
[9] Aberdeen Group (June 2017). The Need for Speed: Faster Detection Requires a New Type of Platform.

< PREVIOUS NEXT >



Capability #3

Identify and Prepare for Future Attacks

Information about an attacker's motivations and methods can greatly help organizations prepare for and prevent attacks. But traditional network security tools use legacy, signature-based intelligence feeds that need to be updated every time a new threat appears. By the time the update occurs, the intelligence is often outdated. Lacking real-time context, most threat intelligence feeds are ineffective against evolving threats, can increase false positives and fail to help security teams plan for or prevent future attacks.

More effective intelligence is multifaceted and correlates detailed, relevant information about attackers, current attacks and probable targets.

> "Having tools that heighten detective or forensic capabilities can significantly reduce data breach cost."
>
> **Ponemon Institute**
> **2017 Cost of Data Breach Study**

? Ask these questions when evaluating network security intelligence

- Is the intelligence derived from thousands of hours of incident response engagements, a global network of sensors collecting real-time intelligence and hundreds of analysts and researchers to provide contextual insights to alerts that identify the most critical threats for response?
- Does it quickly protect against evolving threats by using real-time machine intelligence and analytics about recent attacks gathered from millions of sensors deployed around the globe?
- Does it provide frequently updated information about attacker tools, techniques and procedures (TTPs) to help you anticipate and respond to attacks?
- Does it share victim intelligence and provide best practices to help you improve defenses and quickly respond to and prevent attacks?

< PREVIOUS NEXT >

> The biggest victims of (cyber) crime are in the most developed economies, including the U.S., China and Germany.
>
> **Adam Segal**
> DIRECTOR OF THE DIGITAL AND CYBERSPACE POLICY PROGRAM, COUNCIL ON FOREIGN RELATIONS

Capability #4

Protect Your Entire Environment by Working with Multiple Solutions

When your network security doesn't integrate smoothly with email and web security it can cause problems and increase the risk of a successful attack. It limits the ability to create integrated workflows, increases complexity and reduces visibility. The result? Your network is left exposed. It can take weeks and even months before exploits and malware are finally discovered and investigated, leaving cyber criminals plenty of time to do damage.

? Ask these questions when evaluating email security solutions

- Is it part of a comprehensive security platform that integrates email with other critical security components, such as network and endpoint security?
- Does it share threat information with network and endpoint security products?
- Can you create integrated, automated workflows to speed up the detection-to-resolution process?

< PREVIOUS NEXT >

Capability #5

Grow and Adapt to Your Business Needs

As your business expands, you need a network security solution that rapidly adapts and evolves as you grow, with as little cost and impact as possible. Over time, traditional, signature-based tools struggle to protect your organization's existing investment. Because these tools lack flexibility and are managed independently, the end result is extra work for your teams with more chances of system misconfigurations. Your organization is open to future malicious attacks and unnecessary, additional costs.

? Ask these questions when evaluating network security extensibility

- Does it protect your existing security investment by providing expandable hardware and software capabilities?
- Does it offer flexible deployment options that grow with your network traffic needs?
- Does it future-proof your investment by allowing you to easily and cost-effectively increase performance and expand system deployment?

Summary

By 2020, global organizations are expected to spend more than $100 billion on cyber security solutions.[10] Despite the money and resources invested in traditional signature-based network security, these outdated defenses cannot stand up to today's complex and constantly evolving cyber attacks.

Your network security solution should:

- Rapidly detect and stop attacks from exploit- and malware-based threats
- Quickly recognize and respond to high-priority threats
- Prepare for future cyber attacks
- Work with other security solutions to protect your environment
- Adapt and grow with your business needs

Today's sophisticated multi-vector, multi-stage attacks can cost your organization hundreds of thousands or even millions of dollars. A network security solution that offers advanced defense capabilities is the most effective way for you to efficiently identify and quickly stop these malicious attacks.

120 countries currently have or are developing offensive cyber attack capabilities, which are now viewed as the fifth dimension of warfare after space, sea, land and air.[11]

[10] International Data Corporation (2016). Worldwide Semiannual Security Spending Guide.
[11] Defense Systems (March 25, 2010). Future hostilities to begin with cyber attacks, NATO official says.

< PREVIOUS NEXT >

About FireEye Network Security

FireEye Network Security is designed for high-performance, pervasive and consistent protection against threats across your organization. It offers an integrated security workflow, advanced sandboxing and actionable contextual intelligence to help organizations stop targeted, highly evasive and APT attacks.

To learn more, visit
fireeye.com/nx

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 940 of the Forbes Global 2000.

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

fireeye.com

FireEye®