FireEye
SECURITY REIMAGINED

Assess, Respond & Insure

Reducing the Impact of Security Incidents

SOLUTIONS BRIEF

SECURITY REIMAGINED

FireEye finds and stops advanced attacks that other security technologies cannot see. And cyber insurance provides another layer of protection.

HIGHLIGHTS : TODAY'S REALITY[1]

- **205 Days: Median number of days that threat groups were present on a victim's network before detection**
- **69% of victims were notified by an external entity**
- **78% of observed phishing emails were IT or security related**
- **72% of phishing emails were sent on weekdays**

Your network has all the latest security features to keep bad guys out: anti-virus (AV) software, web gateways, anti-spam systems, next-generation firewalls, and intrusion prevention systems.

But even organizations that make responsible and sustained investments in IT are routinely compromised by attackers seeking everything from customer data to trade secrets. Network breaches have become regular front-page news—and those reports are just the tip of the iceberg.

Organizations need a fundamentally new approach to cyber security. With a powerful blend of technology, intelligence, and expertise, FireEye finds and stops advanced attacks that other security technologies cannot see, let alone stop. And cyber insurance provides another layer of protection to reduce the financial risks of those attacks.

ASSESS YOUR SECURITY TO MEASURE AND MINIMIZE RISK

Now may be the time for a serious talk with your IT security leader about today's cyber threats. Start with this question: "What are you doing to protect against advanced attacks?"

Your answer may start with an outside assessment. FireEye can help evaluate your security program and answer a range of questions: Am I compromised? How can we improve our security program?

We give you a full picture of your security posture and tailored, actionable advice to help you improve. Armed with this information, you can create a roadmap to reduce risk and avert the worst outcomes of security incidents.

[1]Mandiant M-Trends Report 2015, A View From the Front Lines.

ADAPTIVE STRATEGY

We help you build an adaptive strategy that prevents, detects, analyzes, and responds to attacks quickly

Reduced Impact of Security Incidents

By catching an incident early, organizations can minimize the overall impact. This impact includes economic loss, stolen intellectual property, damaged reputations, and disrupted business.

Reduced Risk

With FireEye, security teams can identify when attackers are operating in their network. We actively hunt down attackers that other security products miss.

Improved Efficiency of Security Teams

FireEye automates the process of detecting threats and responding to incidents. We help front-line security analysts discover and scope security incidents faster so they can better decide how to respond. With FireEye, they know what threats really matter, and the impact of any breach.

Improved ROI on Security Spending

By integrating with our partners, FireEye helps security teams get more from their existing security tools. We help turn the data you already collect into actionable intelligence to find and stop attacks.

For more information, contact
CREATE@fireeye.com
#FireEyeCyberRisk

When attacks do succeed, incident response services from Mandiant, a FireEye Company, can help you respond aggressively to minimize impact and re-secure your network

REDUCE THE IMPACT WITH A DETECT-AND-RESPOND MINDSET

Most cyber security vendors still focus on the old "prevent, prevent, prevent" mantra. This approach isn't realistic—and it clearly doesn't work. Conventional security tools are failing in the vast majority of networks[2]. And nothing can stop every threat. Detecting attacks quickly and resolving them effectively is a far better approach.

FireEye Adaptive Defense™ focuses instead on stopping attackers before they reach their goal. Prevention is about averting many attacks outright and avoiding the worst outcomes of attacks that slip through.

FireEye enables teams to limit any damage by reducing two key metrics: time to detect and time to resolve.

LIMIT FINANCIAL DAMAGE WITH CYBER INSURANCE

FireEye has partnered with cyber insurance brokers and underwriters to create financial resiliency and recovery after an attack. Should the worst happen, a cyber insurance coverage can help you limit your exposure and get you back to business.

Policies can help cover losses incurred from incident response, disrupted business and physical damage to both IT enterprise and industrial control systems. No one looks forward to making an insurance claim. But when disaster strikes, cyber insurance can be a vital part of your total security strategy.

With a cyber threat assessment, you have a blueprint to prioritize your short- and long-term technology investments. With FireEye Adaptive Defense, you have the tools you need to prevent, detect, analyze, and respond to threats. And with cyber insurance, you can complement these investments with a layer of financial peace-of-mind.

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

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