FireEye™

White Paper

Protecting Your Data, Intellectual Property, and Brand from Cyber Attacks

A Guide for CIOs, CFOs, and CISOs

Contents

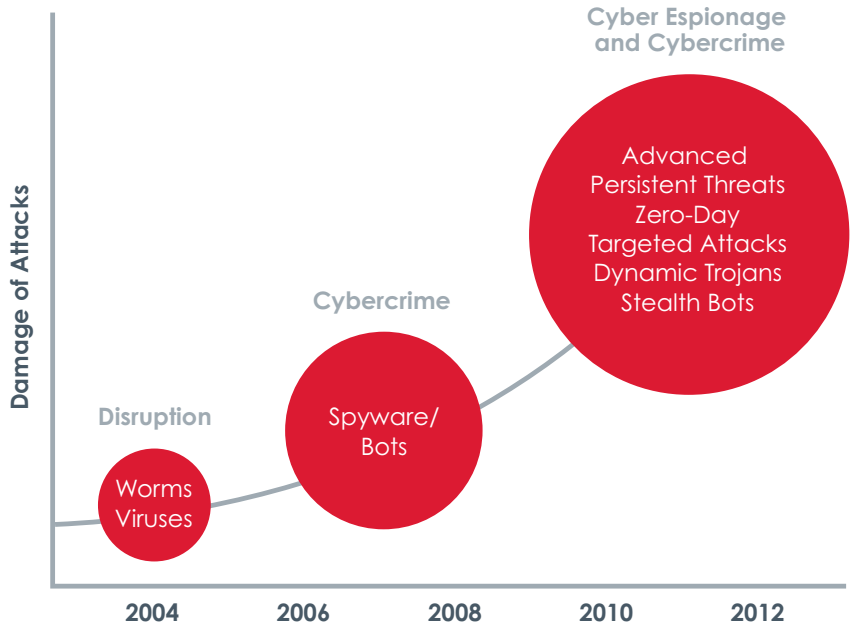
The Problem

Enterprises and government agencies are under virtually constant attack today. Significant breaches at RSA, Global Payments, ADP, Symantec, International Monetary Fund, and a number of other organizations have made headlines—and undoubtedly thousands more have occurred that we haven't even heard about. Flame, Stuxnet, and a number of other cyber attacks have been uncovered that set an entirely new standard for complexity and sophistication.

Fundamentally, these developments make clear that the cybercriminals, nation-states, and hacker activists waging these attacks are growing increasingly sophisticated and more effective in their efforts to steal and sabotage. Leveraging dynamic malware, targeted spear phishing emails, elaborate Web attacks and a host of other tactics, these criminals know how to bypass traditional security mechanisms like firewalls and next-generation firewalls, IPS, anti-virus (AV), and gateways. Think your organization is immune? If so, it's in the vast minority: ninety five percent of organizations are routinely compromised, with the theft of intellectual property, customer records, and other sensitive data increasingly common.

Here's how a 2012 Gartner report put it: "There is widespread agreement that advanced attacks are bypassing our traditional signature-based security controls and persisting undetected on our systems for extended periods of time. The threat is real. You are compromised; you just don't know it."

Why are today's security defenses failing? In this battle, your security teams are using an outdated arsenal: legacy security platforms based on technology that originated many years ago using signatures. These tools are good at blocking basic malware that is known and documented, such as viruses, but they are incapable of identifying today's dynamic, multi-pronged cyber attacks, which are often called advanced malware or advanced persistent threats (APTs).



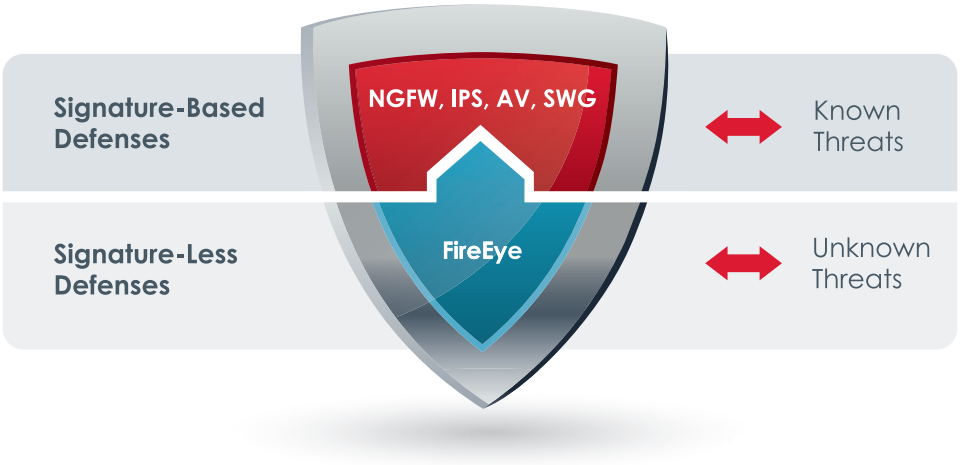
Why You Should Care

If your organization is like most you are spending a lot of money, perhaps 10-20% of your annual IT budget, on security—but it's not working against the new breed of advanced cyber attacks. If that's not enough to concern you consider how losing the security battle can hurt your business:

- **Loss of competitiveness.** When cybercriminals can circumvent your defenses, trade secrets, patents, customer records, and M&A activities can all be exposed and significantly weaken your competitive position.
- **Compliance breaches.** If you are not protected from breaches, your organization's compliance with relevant policies and mandates is in serious jeopardy. Whether you are a financial institution that needs to safeguard credit card data and stay compliant with PCI DSS, or your business is tasked with compliance with HIPAA, NERC, FISMA, privacy rules, or any of the other policies in effect around the world, data breaches can lead to fines, lost business, and a host of other penalties.
- **Damaged reputation.** Customer trust and market share are precious commodities. All it takes is a significant breach to hit the headlines, and those hard-earned assets can erode quickly. Estimates from companies that have been breached have ranged in the several millions of dollars up to 200 million dollars.
- **Lost productivity.** If your security team is finding out about breaches after the fact, they are going to be scrambling to handle forensics, shore up the vulnerability, assess where other similar gaps may be, rebuild corrupted systems, and so on. The time spent on these efforts is time your business doesn't get back—and that can't be focused on more strategic efforts.

What You Can Do About It

To combat the trends and risks outlined above, many organizations are adding a new layer of defense that complements their existing security technologies and enables security teams to effectively spot and thwart the advanced cyber attacks being waged today. With this added layer of defense, security teams can detect in real-time when code is truly malicious and has made it through all of their other defenses.



FireEye offers solutions that deliver this required layer of defense. These solutions have been proven to detect and block the advanced cyber threats your organization is facing. Featured in Forbes, Businessweek, The Wall Street Journal, and a number of other publications, FireEye helps your business effectively guard against today's advanced attacks—so you can avoid the financial, brand, and competitive damage they inflict. Further, by automating advanced malware detection, FireEye keeps your security team out of fire-fighting mode and delivers significant operational savings. The FireEye solution also eliminates false positives and negatives which saves more staff time. Given all these benefits, an independent study calculated the average return customers receive by investing in FireEye solutions to be $16,517,000.

That's why about 20% of the Fortune 500 is a FireEye customer. FireEye customers are from diverse industries including financial services, healthcare, manufacturing, and energy as well as more than 60 government agencies.

Following are quotes from a few of the decision makers that chose FireEye:

"The reason we looked into FireEye was because the traditional tools we used—firewalls, anti-virus, intrusion prevention, intrusion detection—are primarily signature based and therefore are simply impotent in terms of stopping targeted and zero-day attacks."

—Jerry Archer, SVP and CSO, Sallie Mae

"Zero-day and targeted attacks that evade simpler defenses are where you're going to need a next-generation product like FireEye. We looked at other vendors, but FireEye stood apart in its ability to detect these advanced threats and keep us secure."

—Tony Spinelli, SVP and CSO, Equifax

"We've really benefited from FireEye appliances which help us guard against the exfiltration of intellectual property. FireEye's people have also been very responsive to our requests and questions. They haven't been just a vendor, but a really great partner in helping us address our network perimeter defense issues."

—Leslie Lambert, CISO, Juniper Networks

About FireEye

FireEye is the leader in stopping advanced cyber attacks that use advanced malware, zero-day exploits, and APT tactics. The FireEye solutions supplement traditional and next-generation firewalls, IPS, anti-virus, and gateways, which cannot stop advanced threats, leaving security holes in networks. FireEye offers the industry's only solution that detects and blocks attacks across both Web and email threat vectors as well as latent malware resident on file shares. It addresses all stages of an attack lifecycle with a signature-less engine utilizing stateful attack analysis to detect zero-day threats. Based in Milpitas, California, FireEye is backed by premier financial partners including Sequoia Capital, Norwest Venture Partners, and Juniper Networks.

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