Hewlett Packard Enterprise | FireEye

Proactively detect attacks and breaches

Advanced Compromise Assessment from HPE and Mandiant, a FireEye Company

You're under attack. Knowing your risk and addressing it is vital.

Insights

- 146—median number of days attackers are present before being detected.[1]
- 46 days—average time it takes to remove an attacker from an environment once discovered.[2]
- $15.4 million—average annual cost of cybercrime per U.S. company.[3]
- 56 percent—executives who say their response to security is reactive, not proactive.[4]

Know the gap in your network defenses

Understanding the risk of a cyberattack on your business, personal, financial, and proprietary data is essential. The cyber-threat landscape is rapidly evolving, and the sophistication of attacks has increased—worryingly. The sources of attacks are now from highly motivated, well-funded adversaries, often supported by crime syndicates and nation states. This new generation of cyberattacks is highly targeted and seeks to remain undetected to perform cyber-sabotage activities or acquire intellectual property (IP), financial data, and confidential or sensitive personal information over an extended period of time.

Traditional security controls, such as firewalls, intrusion prevention systems, anti-virus, and web gateways—although still necessary—are no longer sufficient. They are failing to protect enterprises from advanced targeted attacks and the broader problem of advanced malware. They rely on signatures and known patterns to identify and block threats, but are ineffective in detecting unknown threats.

This leaves a significant gap in network defenses, leaving enterprises vulnerable to zero-day and targeted advanced persistent threat (APT) attacks with their custom developed malware. Once inside, malware uses several persistence mechanisms seeking to remain completely undetected. It can then infect other endpoints, do further reconnaissance, steal credentials and data, or simply lie dormant until the attacker is ready to strike.

Get the help you need

With HPE and Mandiant security consultants, you gain true visibility into risks of potential security breaches through uncovered advanced threats and indicators of compromise within your network and endpoints. They are also equipped with FireEye proprietary technology and apply their expertise to hunt down evidence of past and current attacks.

By using Advanced Compromise Assessment (ACA) from HPE and Mandiant, a FireEye Company, you can detect, prevent, and manage risk from cybersecurity incidents. ACA provides early detection of a potential security breach involving APTs. The service combines HPE and Mandiant consulting experience, methodology developed over hundreds of investigations, the latest threat intelligence, and specialized knowledge of advanced attacker's tools and techniques.

See us in action

- **Prioritize security—**An ACA helped a financial services client prioritize security budgets and review its prevention-focused security strategy. Results contributed valuable input for the security strategy review and ensured a business case for prioritized investment in a detect-and-respond capability.

[1,2] M-Trends 2015: A view from the Front Lines, Mandiant, February 24, 2015.

[3] 2015 Cost of Cyber Crime Study: United States, Ponemon Institute, October 9, 2015.

[4] The Importance of Senior Executive Involvement in Breach Response, Ponemon Institute, October 29, 2014.

- **Protect brand reputation—**An ACA uncovered significant breaches across users and the infrastructure of this global retailer. The client responded and recovered from the breaches and prevented sensitive customer data exfiltration, protecting its brand reputation.
- **Protect intellectual property—** A communications, media, and entertainment client gained evidence of advanced attacker activity following their ACA. Follow-up actions helped the client avoid exfiltration of valuable IP and improved their detect-and-respond capabilities, protecting the organization against future cyberattacks.

Be protected

No matter where you are, or how big your organization is, with our combined experience and technology, you get help protecting critical information and processes while keeping your operations flexible, efficient, and responsive. With HPE, you get help to:

- Protect your brand, reputation, and revenue from targeted cyberattacks
- Understand risk through greater visibility of active threats
- Benefit from scalable, globally available 24x7 protection

Know you're covered

When you discover a system breach, you want the best to help mitigate and recover from the damage. Look to HPE and FireEye security experts. We have hands-on experience in differing industries, and adjust our solutions to address your concerns in a way that best works for your business.

[5] Frost and Sullivan recognize HP Security Research, July 2014.

Sign up for updates

We cover:

- Financial services
- Consumer goods
- Communications, media, and entertainment
- Energy, mining, and utilities
- Public sector
- Healthcare and life sciences

Benefit from our size, partnership, and experience

- **Global reach, availability, and scale—**HPE serves 1000+ managed services clients, has 3000 security researchers, and operates 10 Security Operations Centers worldwide. Global 24x7x365 managed services manage 1.8 million+ security devices. Expert incident response teams are available 24x7x365 to address critical security breaches.
- **Leadership in security intelligence and threat research—**HPE finds more than four times more critical vulnerabilities than the rest of the market combined[5], employs a unique methodology resulting from 1000s of high-profile investigations, and analyzes 23 billion+ correlated security events every month.
- **Unique partnership**—A unique combination—HPE and Mandiant security consultants have experience and skills developed over hundreds of investigations, some dealing with multiple attack groups and very large and complex environments. FireEye proprietary technology automates investigative activities, enabling rapid assessment for even the largest, most complex networks.
- **The adversary disrupted—**HPE is a trusted partner to global enterprises and national governments, delivering security solutions with measurable business outcomes. We leverage the latest threat intelligence, profile key attack groups, have specialized knowledge of advanced attacker's tools and techniques, and offer extensive, flexible consulting and managed services for advanced threat protection and incident response.
- **End-to-end security services—**HPE is one of very few companies offering a single source for security consulting services, managed services, and third-party technology, enabling end-to-end delivery of a complete security strategy and transformation programs.

Know the details

- 4600+ security and privacy professionals worldwide
- Combined security intelligence based on 4 million virtual machine sensors and 100,000+ hours of incident response annually
- Industry-recognized consultants hold certifications, including CHECK, CLAS, CISSP, CISM, CISA, IISP, ISO 27001 Lead Auditor, and PCI QSA
- 10 HPE Security Operations Centers—global 24x7x365 managed services, 1000+ clients, 500,000+ security devices, 23 billion+ security events monthly
- 5 worldwide FireEye Service Centers

Next steps

No matter where you are, or how big your organization, work with us to protect your critical information and processes while keeping your operations flexible, efficient, and responsive.

Learn more at
hpe-enterpriseforward.com/fightback/

Hewlett Packard Enterprise | FireEye

4AA5-8352ENW, August 2016, Rev. 5