TRANSFORMING SECURITY OPERATIONS
CONTENTS

The FireEye advantage 3
  How FireEye benefits organizations 4

Shrinking security problems with an intelligence-led approach 6
  FireEye iSIGHT Intelligence 6
  Why does an Intelligence-Led approach matter? 7

Innovations that solve big security problems 8

Introducing FireEye Helix 9
  What FireEye Helix includes 10
  The roadmap to FireEye Helix 11

FireEye expertise delivered 14

FireEye: a trusted security partner 15
  Different security vendors, differing visions 16
  Breach resilience as a core philosophy 17
  An evolved security strategy 18
The FireEye advantage

FireEye understands cyber attacks better than anyone else and uses that knowledge to remove complexity from security. The company has built an intelligence-led, security-as-a-service approach that blends innovative security technologies, nation-grade FireEye iSIGHT Intelligence and world-renowned expertise from Mandiant. This seamless and scalable extension of customer security operations alleviates the burden of cyber security for organizations struggling to prepare for, prevent, respond to and remediate cyber attacks in cloud, on-premise and hybrid environments. FireEye has over 5,300 customers across 67 countries, including more than 825 of the Forbes Global 2000.
HOW FIREEYE BENEFITS ORGANIZATIONS

FireEye empowers organizations to go from detecting a threat to defeating it quickly at a low total cost of ownership. FireEye directly tackles the challenges organizations face when they attempt to operationalize their security programs. This, in turn, resolves their concerns about whether their resources are effectively allocated and whether they have truly improved their security posture.

FireEye solutions simplify, integrate and automate components of an organization’s security program. A combination of technology, intelligence and expertise delivers capabilities that span the entire security operations lifecycle from assessing, preparing for, detecting, preventing, analyzing and responding to threats. These capabilities allow organizations to shift from a reactive state of constant busy work to proactive security.

Since priorities differ across organizations, this is not a “one size fits all” solution — FireEye enables organizations to decide how many of the capabilities they want to use and to what degree. The company can enhance existing security infrastructures by managing and processing the data from those solutions to augment them, or displace inadequate functionality.
If an organization has invested in a security operations center

FireEye can provide the central operations console that extends their current capabilities with:

- The ability to integrate, orchestrate and automate effective response across existing components of the infrastructure
- Instant access to the expertise of approximately 1,000 incident responders, malware researchers, intelligence analysts and security consultants through program assessments and features such as a live chat interface
- High-fidelity detection, visibility and threat intelligence context across network, email, endpoint and event data, including the ability to detect non-malware-based attacks

This approach eliminates activities in tiered security operations that often result in excessive and error-prone human effort, such as validating and prioritizing threats, eliminating false positives and gathering threat intelligence for alert context. It can also accelerate the pivot from detection to investigation. FireEye integrates its solutions with an organization’s existing products and processes and augments their entire security ecosystem by applying FireEye iSIGHT Intelligence and expertise to all event data in the environment.

If an organization does not have a security operations center or cannot afford to build one

FireEye can provide them with security operations center (SOC) functionality. FireEye as a Service and associated partner offerings can act as their SOC to enable:

- Rapid detection of the threats that matter to the organization by using analytics, machine learning and threat intelligence
- Investigation and triage of potentially malicious events to give specific response recommendations
- Proactive analyst-driven hunting for signs of compromise
- Remediation through the expertise of the same incident responders who work on the most consequential breaches or through the codification of their techniques into orchestrated and automated processes

Organizations benefit from the global network of seven FireEye advanced threat research centers that combine technology, intelligence and expertise to assess whether threats detected against other organizations will affect them, and provide proactive protection as necessary.

Irrespective of an organization’s security maturity, FireEye can help guide organizations toward intelligence-led security to reduce their overall level of cyber risk.
Intelligence has been a longtime building block of FireEye DNA, delivering critical capabilities to organizations’ security operations. Detailed knowledge of the threat landscape and cyber-attack countermeasures ensures that FireEye offerings directly address today’s threat actors and the techniques they employ. This intelligence guides FireEye as the company designs and builds products, analyzes and produces FireEye iSIGHT Intelligence and helps the Mandiant team prepare for, respond to and remediate breaches.

FireEye believes that intelligence begins with the breadth and depth of visibility into the threats and threat actors that an organization would face. This FireEye visibility:

- Begins with over a hundred intelligence analysts who have spent close to a decade deeply embedded across the globe, wherever attackers plan, design and execute their attacks from the Far East and Eastern Europe to the Americas. This gives FireEye early visibility into threat initiation — in many cases even before these attacks are launched.

- Is extended with insights derived from 10+ years of experience responding to the world’s most consequential breaches and Multi-Vector Virtual Execution (MVX)-driven technology that identifies never-before-seen attacks. This allows FireEye to understand how attackers infiltrate an organization, what they do once inside and how victim security controls fail.

- Has insight into the impacts of a breach (e.g., if stolen credit cards are sold on the dark web) through visibility into the attacker ecosystem. This helps influence strategic risk management decisions based on an assessment of attack severity beyond just the technical details; prioritization of resources and the focus of response.

Subject matter experts — malware analysts, geopolitical experts and linguists — who understand the context behind the threats then analyze and correlate the observed activity within a highly flexible and scalable threat analysis and machine-learning infrastructure. These experts map and continue to track nearly 600 million interconnections between threats, the actors and sponsors behind them and their tactics, techniques and procedures. This analysis has enabled FireEye to study close to 16,000 threat actors, including more than 30 nation-state sponsored groups, ranging from the China-based APT1 to Russia-based attackers making headlines today. These threat actor dossiers enable organizations to include the threats from these actors in their risk assessment and influence the design and operation of their security program. FireEye uses this knowledge to build the industry’s most effective products and services against these threats.

No competitor has frontline experience comparable to FireEye. They cannot claim the same level of intelligence. For FireEye competitors, intelligence is, at best, a tactical list of previously known malware or bad IP addresses. FireEye builds its intelligence on a deep understanding of adversaries and their tactics, techniques and procedures to ultimately help deliver solutions that shrink the security problems organizations face.
For organizations looking to enhance their existing security operations

An intelligence-led approach:

• Enhances the effectiveness of their existing detection solutions by isolating the alerts that truly matter from the thousands of unreliable ones

• Prioritizes alerts by highlighting those that pose the greatest risk to the organization

• Identifies necessary proactive actions based on knowledge of the threats and threat actors that target the organization

• Drives an assessment of business risk so organizations can develop proactive security strategies

The benefits of this intelligence-led approach lie in the ability to take an existing investment and get more out of it: shrinking the day-to-day operational problem and decreasing current manual efforts forced on the security operations team.

WHY DOES AN INTELLIGENCE-LED APPROACH MATTER?

For organizations looking to build or rebuild parts of their security operations program

An intelligence-led approach pairs FireEye iSIGHT Intelligence with:

• Technology solutions that use machine learning and behavioral analytics to rapidly detect threats that present the greatest risk to the organization without the noise of false positives and overwhelming alerts

• FireEye as a Service, which uses intelligence to drive proactive hunting and monitoring of threats

• Mandiant incident responders who fuse knowledge of the latest threat actor tactics with the techniques necessary to quickly eject attackers from an environment and keep them out

• Mandiant consultants who use the knowledge of the threat landscape to help design, build and expand organizational security operations or simulate attacks to test effectiveness of existing controls

• Orchestration and automation, to enable intelligence-driven workflows and automated response.

Organizations can benefit from the instant and automatic operationalization of intelligence within their end-to-end security operations center. This, in turn, ensures they have the fastest time to protection.
Innovations that solve big security problems

Intelligence is a core building block of the FireEye solution set. It is what enables the company to deliver effective security capabilities rather than just individual point products. FireEye believes that this intelligence enables the delivery of a solution that combines innovative technology with expertise learned on the front lines and a solution that spans the entire operations process from alert to fix.

Historically, FireEye innovations have solved pressing security problems that lacked effective solutions. For instance:

• 10+ years of research and development delivered a virtualization-based solution that created and advanced the technology landscape to detect threats that were bypassing traditional signature based defenses. Today, this capability has become a must-have part of any security program.

• The Mandiant team pioneered rapid incident response technologies that allowed incident responders to be far more effective and efficient at dealing with large enterprise-wide breaches involving tens of thousands of victim machines. The traditional approach relied on dead disk forensics which could not scale.

FireEye acquisition strategies have been equally innovative, complementing organic development with companies that delivered high speed network forensics, human intelligence and security orchestration — all critical to the ability to maintain pace with the attacker.

Emerging FireEye pricing and packaging innovations bring these capabilities to a broader range of customers with varying maturity levels, different budgets and adoption paths. Organizations can therefore leverage as many FireEye capabilities to the degree they need now and seamlessly add more in the future.
FireEye’s goal is to reduce the cost and complexity of security operations and give organizations the best possible risk posture. Therefore, starting in the first quarter of 2017, FireEye will be enhancing the customer experience as individual products merge into FireEye Helix, a unified platform for network and endpoint security delivered on premise, in the cloud or as a hybrid deployment.

The platform is unified in how organizations acquire, deploy and use it on a day-to-day basis. Interaction takes place through a single console for your entire security operation, deployment occurs with speed and at scale, and procuring the platform is eased by a simple, low, recurring operational cost model.

FireEye Helix offers organizations of all sizes proven, signature-less, real-time prevention, detection, response and remediation capabilities against all threats. It is the foundation upon which any organization can simplify, integrate and automate their security program and it is designed to be delivered everywhere at the speed of software. FireEye expertise can always be a click away whether organizations need quick advice on a particular alert or deep analysis.
FireEye Helix delivers a new, unified user experience across the FireEye product portfolio. Organizations will also be able to send event data from non-FireEye components of their IT and security infrastructure into FireEye Helix. They can then overlay FireEye iSIGHT Intelligence on that data to triage buried threats. By centralizing security data from across the infrastructure, FireEye Helix can also perform rich analytics to detect lateral movement, data exfiltration, account abuse and user behavior anomalies. All of these are important components of the attack lifecycle that traditional security products such as firewalls cannot see.

The visibility FireEye Helix offers will enable organizations to use the unified dashboards, search and reporting capabilities to easily pivot from detection to investigation to response, or from network to endpoint.

APIs will allow organizations to customize capabilities and integrate FireEye Helix into existing processes. Combined with the ability to ingest their own sources of threat intelligence in STIX format, FireEye customers and partners can gain the extensibility they desire.

FireEye is committed to supporting this platform extensibility by working with channel partners to customize customer implementations, management and support of FireEye Helix. FireEye will engage with technology partners to ensure that FireEye Helix seamlessly integrates into their solutions. FireEye will also work with solution providers across the globe to deliver the capabilities as a hosted service to their customers. By strategically partnering across the cyber security ecosystem, FireEye can offer customers more value and compelling reasons to manage more of their security operations through FireEye Helix.

FireEye Helix was based on a simple value proposition — extract the value of an organization’s overall heterogeneous security ecosystem through a singular view of event data, enriched with FireEye iSIGHT Intelligence. This helps drive down the cost of operations by leveraging orchestration and expert-designed processes to efficiently handle incidents.

**WHAT FIREEYE HELIX INCLUDES**

FireEye Helix provides the following capabilities for one subscription price:

- **Detect what others miss:** FireEye Helix combines FireEye network and endpoint detection with industry-leading FireEye iSIGHT Intelligence.

- **Make other security products better:** FireEye Helix applies FireEye intelligence, rules and analytics to existing security and IT products. With broad support for hundreds of devices, any log source becomes more valuable.

- **Work faster from a unified console:** FireEye Helix features a single console for each of the major SOC use cases such as alert management, search, analysis, rules, analytics, investigations and reporting. And with single sign on and common cloud components, for organizations using these capabilities in the cloud, FireEye Helix will eliminate friction for the security analysts.

- **Analyst-focused:** FireEye Helix powers the SOC with tools that emphasize response speed, including sub-second search across all events, context on every alert, simple pivot and analysis tools, drill-down to forensic captures and malware analysis reports on any hash.

- **Automate the response:** FireEye Helix orchestration lets SOC teams take advantage of pre-developed FireEye playbooks with Mandiant best practice response processes that can be run automatically based on a combination of events and alerts.

- **Broad situational awareness:** FireEye Helix reports and dashboards allow an organization to customize views and gain quick insights into any part of their environment.

- **Achieve compliance:** FireEye Helix reports help show auditors the data needed for compliance. The initial release will include basic alert aggregation reports (useful for a variety of compliance regimes), with additional reports released throughout 2017 for specific compliance frameworks.

- **Product entitlement:** FireEye Helix provides customers with entitlements to FireEye Network Security (NX), Endpoint Security (HX), Threat Analytics Platform (TAP), Advanced Threat Intelligence (ATI) and limited use of FireEye Security Orchestrator (FSO).
Delivering on the FireEye Helix vision requires innovation across multiple foundational elements. Detection and visibility are the first two. Without deep visibility across the enterprise, reporting and analytics capabilities cannot be effective. Without high fidelity detection, it is hard for dashboards to consistently provide a list of prioritized, active and relevant threats with enough context for effective response.

Just as importantly, no security program can automate processes that rely on alert data with an 80%+ false positive rate.

A third foundational element is the ability for FireEye Helix to seamlessly integrate with existing infrastructure so that organizations get maximum benefit from their current security investments.
DETECTION AND VISIBILITY

On the network
The MVX engine has been the backbone of the FireEye high-fidelity detection ecosystem. It combines dynamic inspection with machine learning, analytics and threat intelligence and has allowed FireEye to detect more actively exploited zero-day threats than the rest of the industry combined.

In 2016 FireEye gave customers the ability to deploy this engine as:

- A shared and clustered resource, MVX Smart Grid, that can either be deployed in an organization’s data center as a private cloud or be made available through the FireEye public cloud infrastructure to further reduce the customer’s hardware footprint.
- A virtual or physical appliance Network Smart Node that accesses the MVX Smart Grid. These lightweight Network Smart Nodes provide intelligent filters to look for suspicious traffic. All of an organization’s existing FireEye Network Security appliances can continue to be used as is or be converted into Network Smart Nodes.

This architecture, already deployed at one of the world’s largest banks, simplifies management, consolidates hardware and improves performance significantly.

In 2017, organizations will be able to increase their visibility via virtual Smart Nodes deployed in Microsoft Azure and Amazon Web Services workloads. This will offer FireEye protection for assets hosted on those platforms. FireEye also continues to enhance and deliver new detection and analytics rulesets that focus on threats unique to these cloud environments.

Visibility must also extend beyond the perimeter. Mandiant breach response experience provides a very unique perspective on what attackers do once they are inside the perimeter. That knowledge is used to train the machine-learning algorithms that power FireEye detection. Applying these algorithms to the dozens of types of meta data collected by FireEye Helix enables the detection of lateral movement, data exfiltration and attacks on server infrastructure. Network Smart Nodes are scheduled to receive automatic software upgrades with these capabilities in 2017.

On the endpoint
Endpoints are where attacks can start and finish since they are often where assets being targeted reside. The FireEye endpoint solution integrates tightly with both FireEye iSIGHT Intelligence and network solutions. This allows organizations to pivot and quickly validate, investigate and contain threats detected on the network or elsewhere in the FireEye ecosystem. The network integration will extend into the FireEye public cloud for near real time malware analysis of suspicious artifacts found on the endpoint.

In 2016 FireEye took the first steps towards replacing legacy endpoint protection solutions such as antivirus software with the ability to detect exploitation attempts against the most targeted applications. In 2017, the company will add anti-malware capabilities that use machine learning and data science to detect adversaries based on their behavior.

However, FireEye’s philosophy on endpoint security dictates going beyond just detecting these threats to actively preventing them before they have a chance to cause any damage. FireEye also focuses on enabling organizations to remediate quickly when prevention is not an option. Threats such as ransomware that have a devastating effect on organizations are prime targets for this prevention capability.

As endpoint diversity increases, so does the list of targeted operating systems. FireEye expects to deliver endpoint protection for all major operating systems in 2017: Microsoft Windows, macOS and Linux.
FireEye recognizes that there will always be non-FireEye components in an organization’s security infrastructure. FireEye Helix capabilities can enable organizations to codify, simplify and automate many existing and often cumbersome security processes as it relates to these diverse components. FireEye will provide templated security playbooks based on years of experience battling threat actors of all types. FireEye partners can also build such playbooks for their customers or organizations can build their own using a rich business process modeling interface and drag and drop integrations into most commonly used security and IT infrastructure components. Connecting the dots across the security program ultimately lowers risk and improves time to protection, such as the time between a detection alert and a blocking action on a firewall or web proxy.

Once an organization has its processes defined, FireEye can help automate them, reducing the burden on security staff and allowing the organization to focus on higher priority tasks. However, automation requires very high confidence in the event that triggers the automated response. Given its track record for alert accuracy, FireEye is uniquely positioned to provide these high confidence automation triggers. This capability enables FireEye to combine orchestration with detection and investigation capabilities in a single unified platform.
By any measure, skilled expertise is in short supply and while every customer needs to operationalize security to truly lower risk, not every customer has a SOC and the people to operate one. FireEye Helix is designed to lower the need for skilled expertise by intelligently automating much of the security operations process. In addition, it will allow organizations to interact with FireEye experts through a click-to-chat interface. For organizations that need a higher level of engagement, FireEye as a Service can, in conjunction with partners and through a network of 7 global advanced threat research centers, deliver a spectrum of capabilities from compliance and basic threat validation to investigation and proactive hunting.

In 2017, FireEye as a Service will operate off the FireEye Helix technology stack that enables immediate service delivery without the delays hardware appliances can incur for activities such as data center planning and change control. And it will allow experts – whether internal to an organization, from FireEye or its partners – to instantly be effective in improving security.
While the vision and roadmap for FireEye Helix are clear, the same cannot always be said about the entire cyber security industry. After all, many vendors may make similar promises or talk about unique technology or perhaps even claim an “intelligence-led” approach. FireEye believes organizations should assess claims based on the vendors’ core assets and their ability to bring those assets together to deliver significant value to a customer’s security program.
DIFFERENT SECURITY VENDORS, DIFFERING VISIONS

To compare security vendors, organizations should look beyond the features and functionality of individual products, and evaluate whether a vendor’s strategic approach will result in an optimal risk posture that aligns with their requirements.

A PREVENTION-ONLY APPROACH

Many vendors try to convince customers that they can prevent all threats. This approach is especially popular with vendors whose primary business is selling policy enforcement solutions such as firewalls. This seems sound, if not for the stark reality that every breach FireEye responds to is behind a firewall and other traditional security measures.

Conventional prevention methods often fail because they are incomplete:

- Indicators of compromise are ephemeral. They can only be used to provide information about a specific point in time—a retrospective data point. They are a piece of the puzzle, but they cannot tell the entire story. Organizations need more evidence to build the context necessary to anticipate attacks.

- Integrated perimeter controls, which include firewalls and sandboxes, often execute traffic objects sequentially in siloed environments. They completely miss attacks that use multiple steps or non-digital steps.

- Security analytics can identify anomalies and activities that have previously been unseen. However, it’s critical to understand what informs these algorithms. Without knowledge of attacker behaviors, attacks can easily evade defensive measures.

As the network perimeter disappears with cloud-based applications and telecommuting, organizations gradually lose visibility and control over their environment; any combination of network or endpoint devices to prevent every possible attack therefore becomes unreliable.

THE ALTERNATIVE: JUST FOCUS ON RESPONSE

Other security vendors believe exactly the opposite—that breaches are inevitable, and that having rapid post-breach response capabilities is a core component of a modern security posture. Even then, most organizations lack the expertise to keep pace with attackers and they may not be able to scale their response, leaving their security operations team overwhelmed with the volume of incidents that must be evaluated.

These two approaches can take an organization’s security posture in completely opposite directions. Yet, many organizations don’t consider such core differences in vision and instead only evaluate security solutions on minute technical features.
FireEye believes an organization’s focus should be to prevent as many threats as possible but to have a contingency plan to quickly identify attacks that bypass security controls and respond effectively. Breach resilience offers a strategy where organizations can focus not just on stopping breaches, but rather eliminating or reducing the consequences of any breach. This empowers organizations to manage risk at the most reasonable and scalable cost structure.

As an organization pursues this goal, they should be aware that business impact typically does not occur immediately after a breach. It takes time for the attackers to map out the victim network, steal credentials, spread laterally and complete their mission. Organizations with detection, proactive hunting and response capabilities can disrupt this attack lifecycle after being breached, but before any business impact occurs.
Once an organization has decided which strategy they want to adopt, they need to evaluate their vendor options. This can be hard to do since so many security companies have similar messages. A breach resilient strategy requires organizations to have an integrated workflow that spans detection and visibility as well as response and remediation. Organizations can then engage with multiple vendors and stitch together a workflow with their own capabilities through trial and error, or leverage FireEye, an experienced security partner that has already assembled the elements necessary to deliver an end-to-end experience:

- Technology to detect and respond to threats other technologies miss
- Intelligence from the front lines with analysts deployed across the globe
- Expertise that is the first responder to many headline breaches around the world

This set of intertwined capabilities is the result of more than a decade of thinking about and building solutions to the most pressing security problems. These experiences and capabilities have culminated in FireEye’s ability to deliver intelligence-led security as a service that helps customers assess and prepare, detect and prevent and analyze and respond to security threats. FireEye Helix goes one step further to give all organizations — independent of size or security maturity — the power to enhance their existing security investments and program and deliver the outcome of more effective security.
For more information on FireEye, visit:
www.FireEye.com

ABOUT FIREEYE, INC.
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:registered: 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 825 of the Forbes Global 2000.