Transforming
Security Operations

SPECIAL REPORT

FireEye

CONTENTS

5,000
CUSTOMERS

67
COUNTRIES

940
FORBES GLOBAL 2000

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 approach that blends innovative security technologies, nation-grade contextual 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 5,000 customers across 67 countries, including more than 940 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 by helping 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 extend 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.

Shrinking Security Problems with an **Intelligence-Led Approach**

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 iSIGHT Intelligence

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:

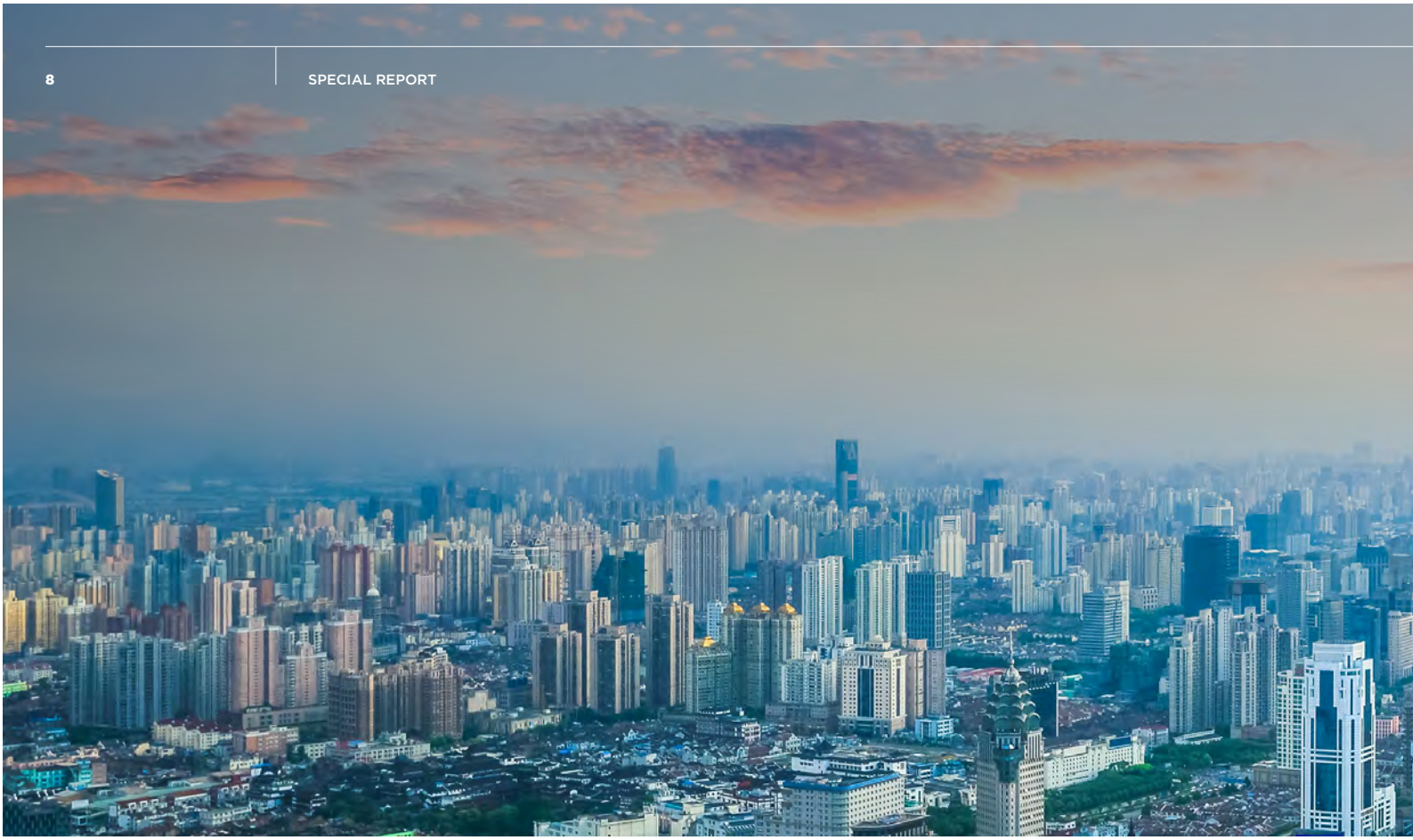
Begins with over a hundred intelligence analysts who have spent close to a decade deeply embedded across the globe, wherever attackers plan, design and execute their attacks from the Far East and Eastern Europe to the Americas. This gives FireEye early visibility into threat initiation — in many cases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

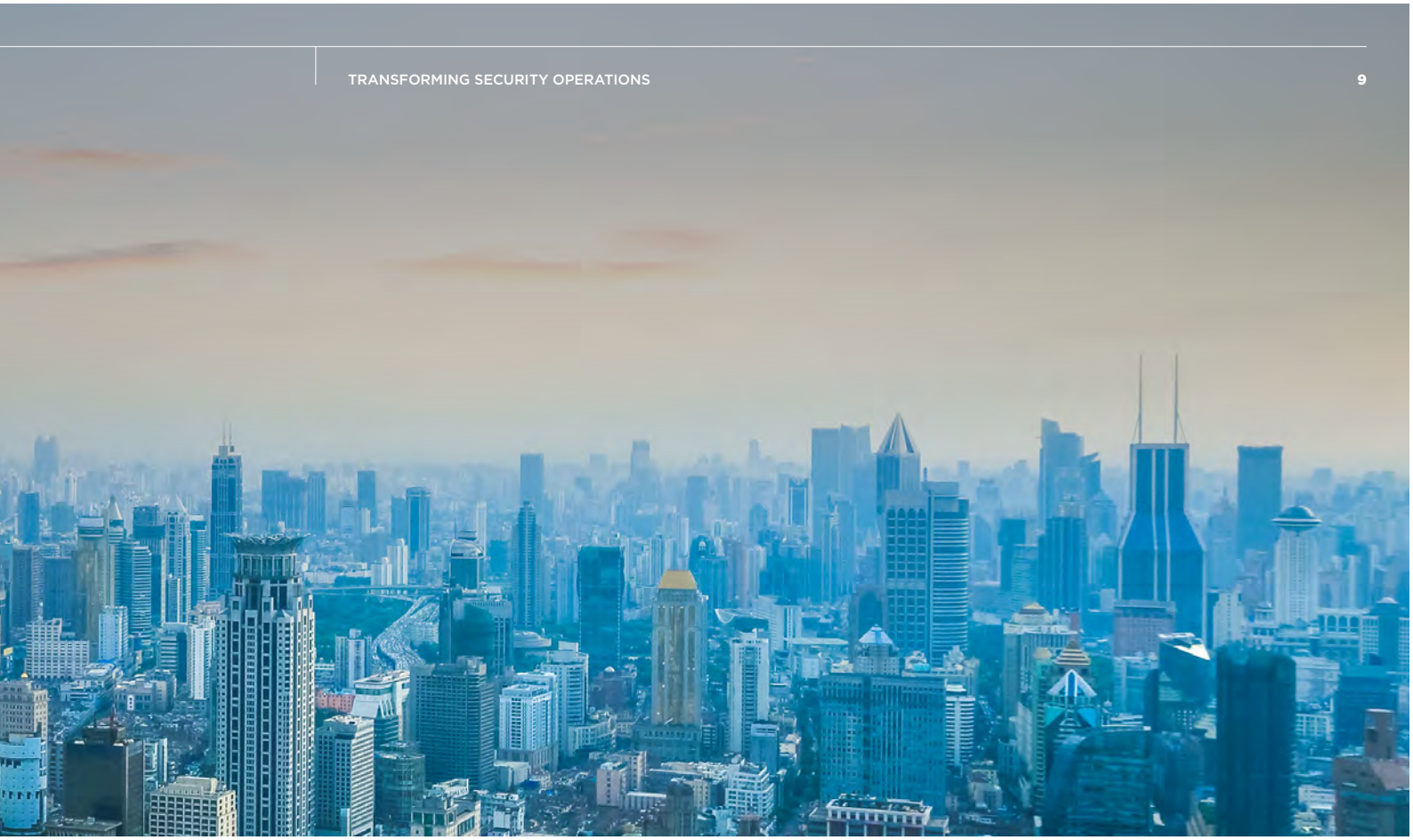


Why does an intelligence-led approach matter?

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.



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.

Introducing **FireEye Helix**

FireEye's goal is to reduce the cost and complexity of security operations and give organizations the best possible risk posture. FireEye Helix is a security operations platform that makes it simple to deliver advanced security to any organization. FireEye Helix surfaces unseen threats and empowers expert decisions with frontline intelligence to take back control of your defenses and capture the untapped potential of your security investments.

FireEye Helix offers organizations of all sizes proven, 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 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 intelligence on that data to triage buried threats. By centralizing security data from across the infrastructure, FireEye Helix can 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 enables organizations to use the unified dashboards and search and reporting capabilities to easily pivot from detection to investigation to response, or from network to endpoint.

APIs 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 by working with channel partners to customize implementations, management and support of FireEye Helix. FireEye engages with technology partners to ensure that FireEye Helix seamlessly integrates into their solutions. FireEye also works 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 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:

Enhance all security products
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.

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.

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, investigation and reporting. It also eliminates friction for security analysts with single sign-on and common cloud components for organizations that need cloud functionality.

Achieve broad situational awareness
FireEye Helix reports and dashboards allow an organization to customize views and quickly gain insights into any part of their environment.

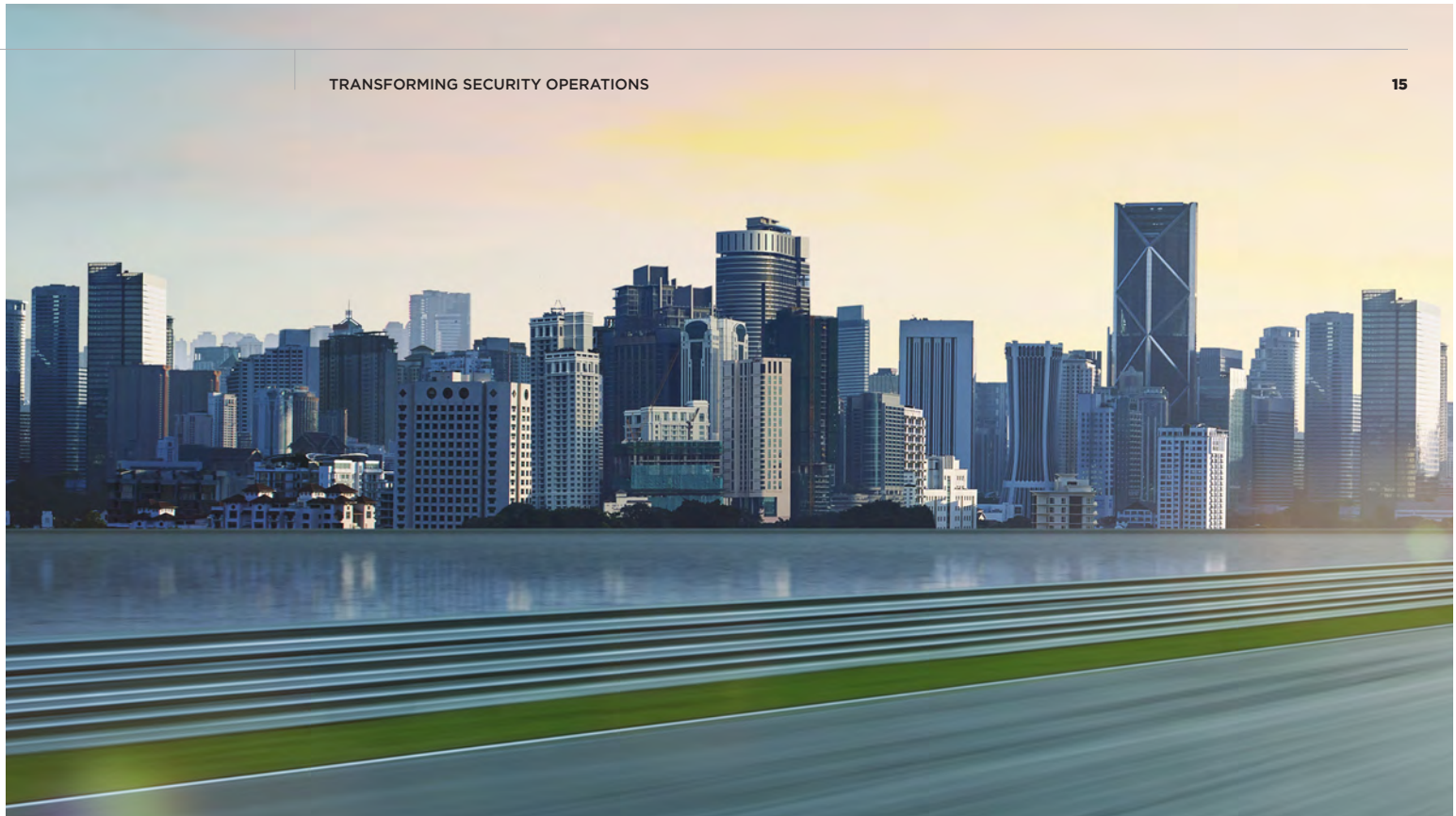
Augment operational capabilities
FireEye Helix powers the SOC with tools that emphasize response speed, including sub-second search across all events, context on every alert, simple pivot and analysis tools, drill-down to forensic captures and malware analysis reports on any hash.

Achieve compliance
FireEye Helix reports help show auditors the data needed for compliance.

Third party integration to improve the effectiveness of an organization's security infrastructure

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. FireEye will provide templatized 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.



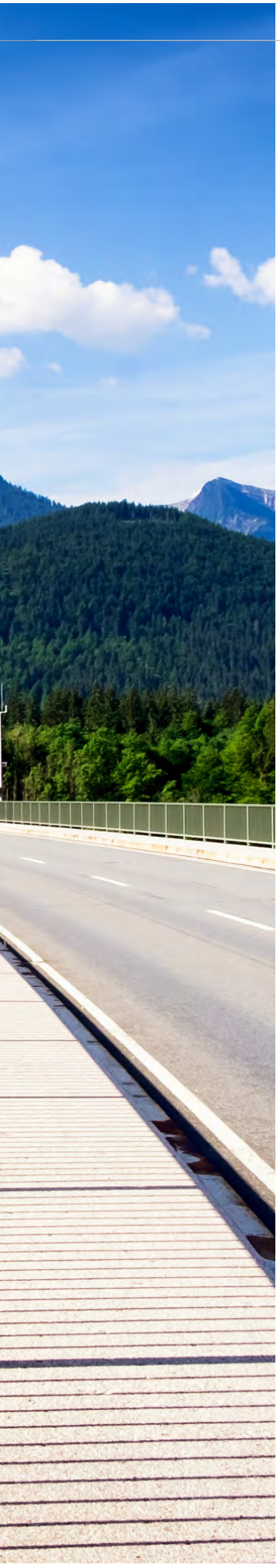
FireEye Expertise **Delivered**

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 as a Service can, in conjunction with partners and through a network of seven 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.

FireEye: **A Trusted Security Partner**

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.

Every breach FireEye responds to is behind a firewall and other traditional security measures.

Breach resilience as a core philosophy

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.

An evolved security strategy

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 resilience 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

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

www.FireEye.com

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 5,000 customers across 67 countries, including more than 940 of the Forbes Global 2000.