FireEye Helix

Customer Presentation

Challenges in Security Operations

80

Average number of security tools

10K

Number of security alerts daily

20min

Time required to triage a single alert

78days

Average time it takes to discover a breach

30days

Average time it takes to respond to a breach

Current State

Using legacy SIEMs to centralize security operations

Lack of visibility across threat vectors

Lack of context and inability to prioritize threats

Negative Consequences

Increased probability of missing an alert that matters

Wasted time and resources from tools that don't work together

Slow response due to lack of threat prioritization

Desired Outcomes

Accelerated response and minimized impact of incidents

Holistic visibility and alert prioritization across threat vectors

Centralized security management and monitoring

Positive Business Outcomes

Minimize impact of a security incident

Maximize value of existing investments

Reduced risk of legal liability and business downtime

Focus on proactive security

Required Capabilities

Consolidate process management, technology and expertise

Centralize asset monitoring

Enrich alerts with contextual intelligence

Automate response and perform inline blocking

Measuring Success

Number of separate tools you employ

Mean time to respond

Time spent on remediation and related activities

FireEye Helix Overview

Technology

- Next-Gen SIEM
- Behavior Analytics
- Cloud Visibility

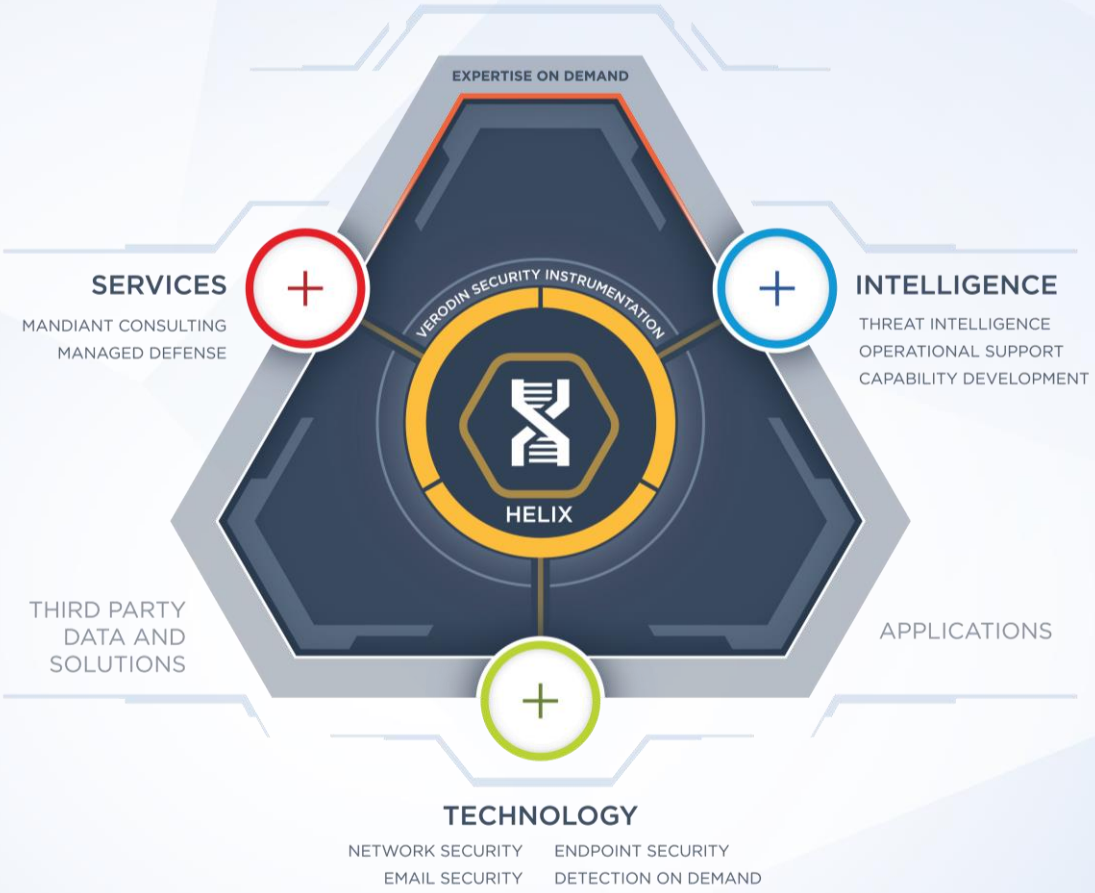
Processes

- Automation
- Guided Investigation
- Compliance Reporting

Expertise

- Expertise On Demand
- Threat Intelligence
- Risk Prioritization

The FireEye Ecosystem



FireEye Helix in Action

Collect Match Automate Prioritize Investigate Remediate

FireEye Helix in Action

Detect Advanced Threats

- Alert prioritization
- Next-Gen SIEM
- Intelligence matching

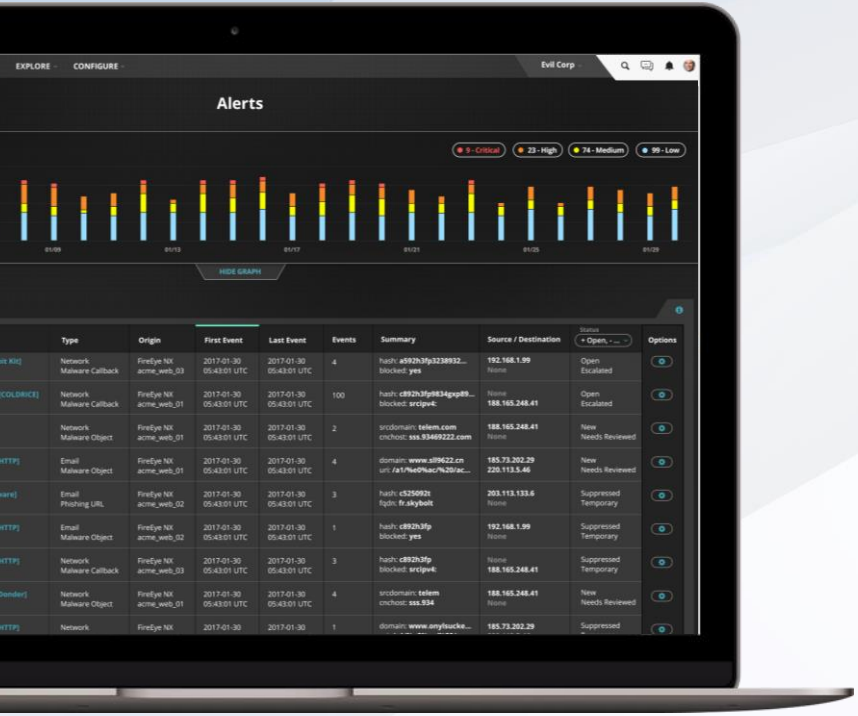
Accelerate Response

- Investigative Workbench
- Workflow Management
- Orchestration

Centralize and Gain Visibility

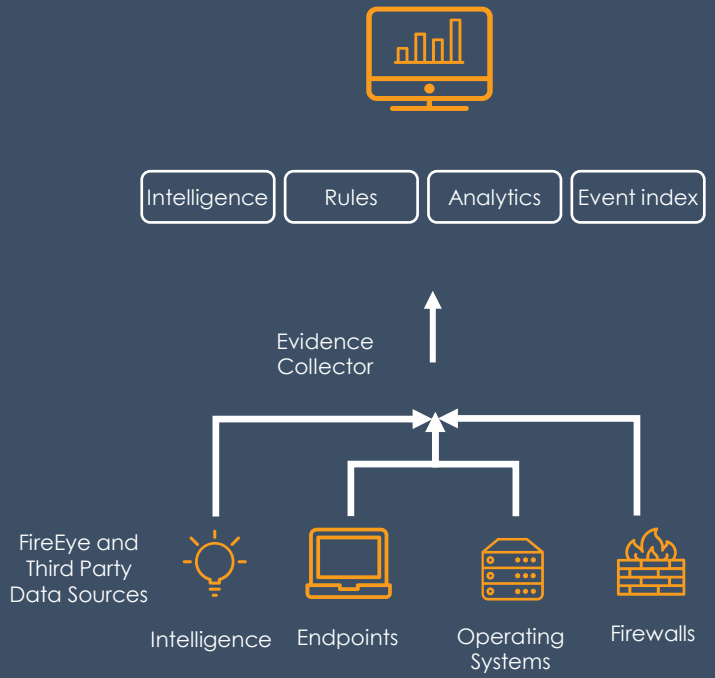
- Tool consolidation
- Flexible deployment
- 3-rd party integrations

Business Value



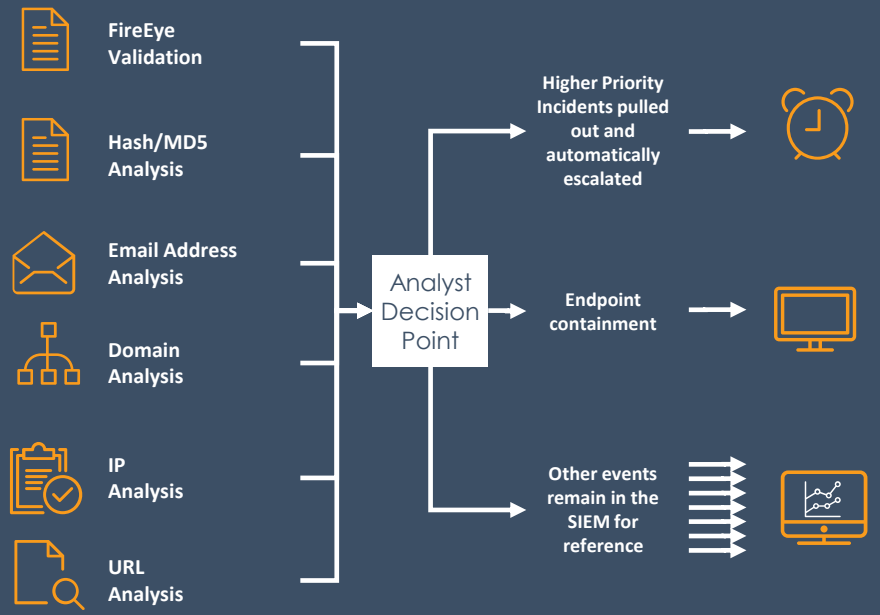
1. **Detect advanced threats** by correlating data from multiple tools
2. **Minimize the impact of an incident** by accelerating response with orchestration and automation
3. **Gain visibility** by centralizing security data and infrastructure

SIEM



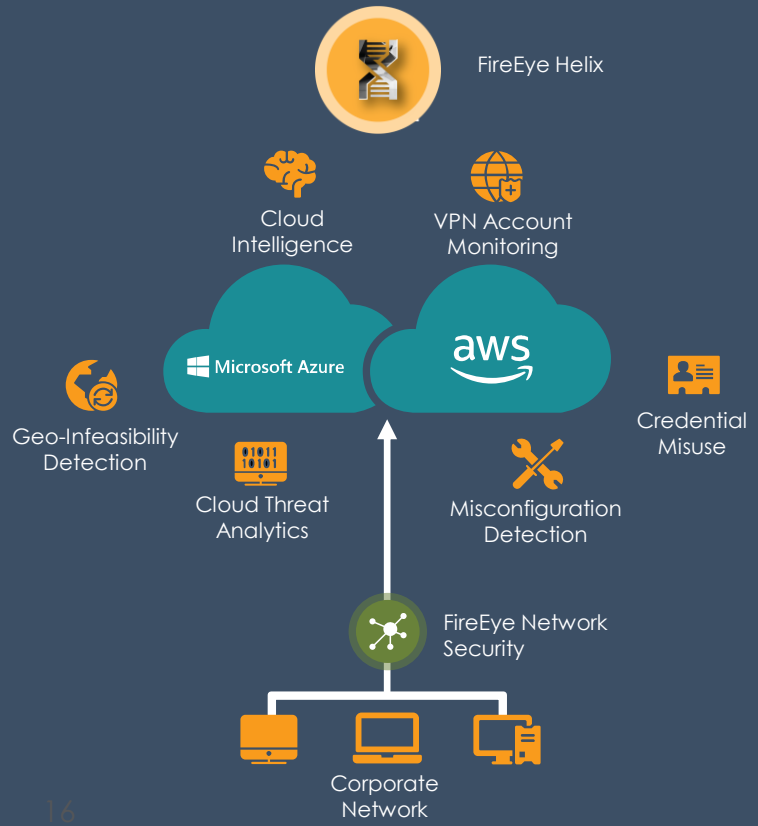
- Real-time threat intelligence
- Codified expertise from FireEye
- Sub-Second search
- Single log source
- Guided investigations
- Compliance reporting

Security Orchestration



- 150+ pre-defined integration plug-ins
- 400+ supported devices, actions and playbooks
- Expertise codified by Mandiant
- Built-in playbook builder
- Role-based actions

Cloud Security

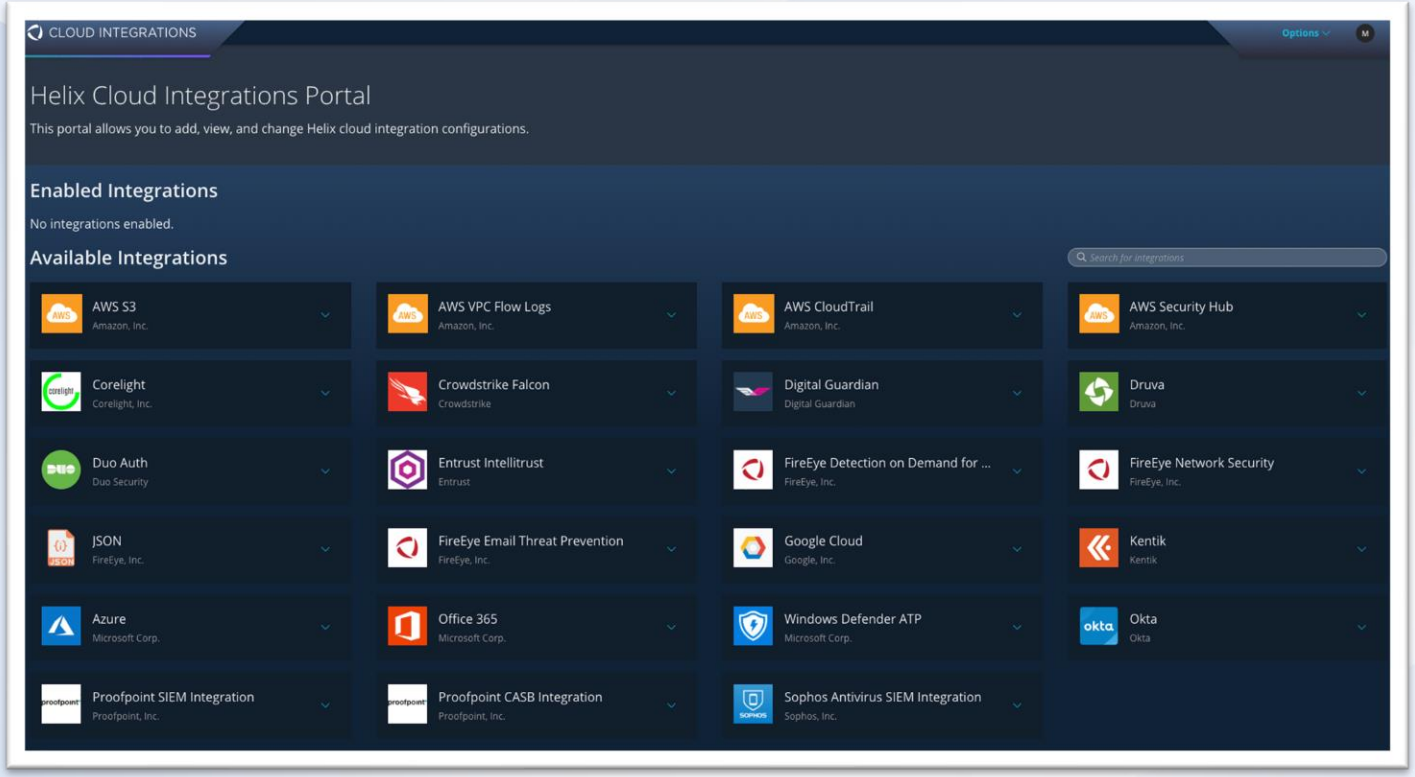


- Guard against credential abuse
- Single pane visibility across your enterprise
- Prevent accidental misconfigurations that lead to attacker compromise

FireEye Cloud Security Solutions

- Ultimate cloud visibility and centralized monitoring
- Simplified integration via Cloud Integration Portal
- Cloud-focused threat rules, analytics, dashboards
- Single pane visibility across cloud vendors

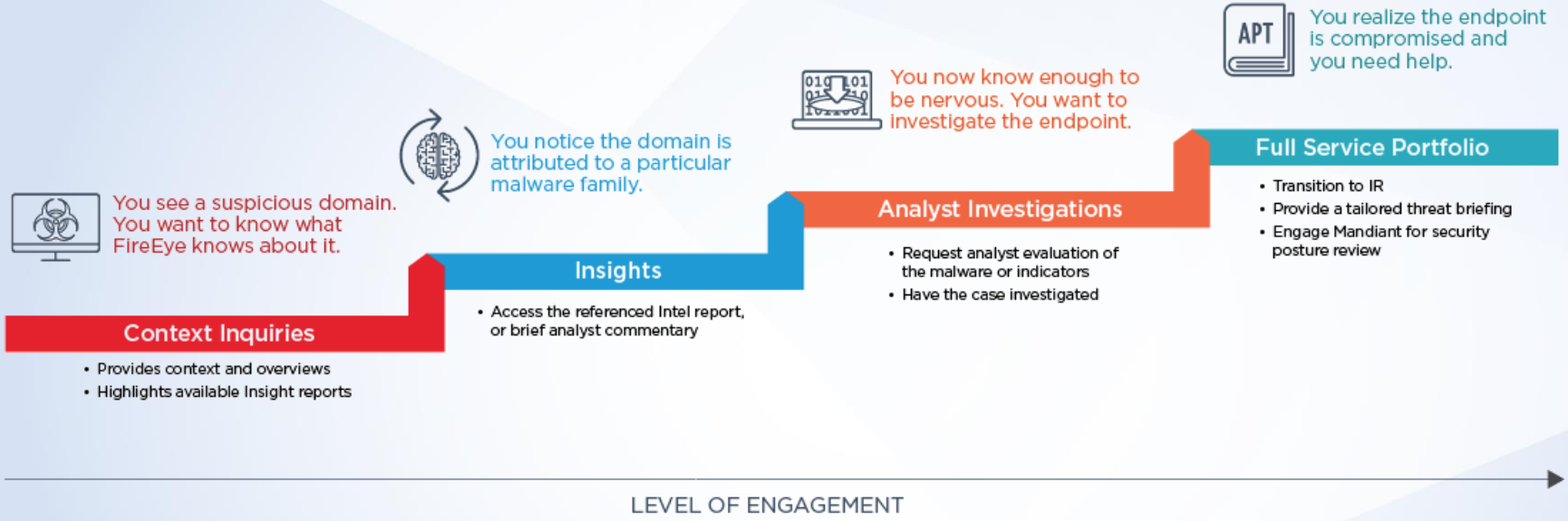
Self-Service Portal for Cloud Data Integration



Expertise on Demand

- Amplify your team with side-by-side access to proven skills and threat insight
- Increase situational awareness via daily news analysis, quarterly threat briefings and finished threat intelligence
- Advance your security program and capabilities via training and consulting services
- Gain a single, trusted partner with unrivaled breadth and depth of cyber security experience and skills

Expertise On Demand



Proof Points

Visibility

550+

Product integrations to minimize pivot points and accelerate response

Response Time:

20x

Acceleration in manual tasks like alert enrichment and triage

Value

5-7

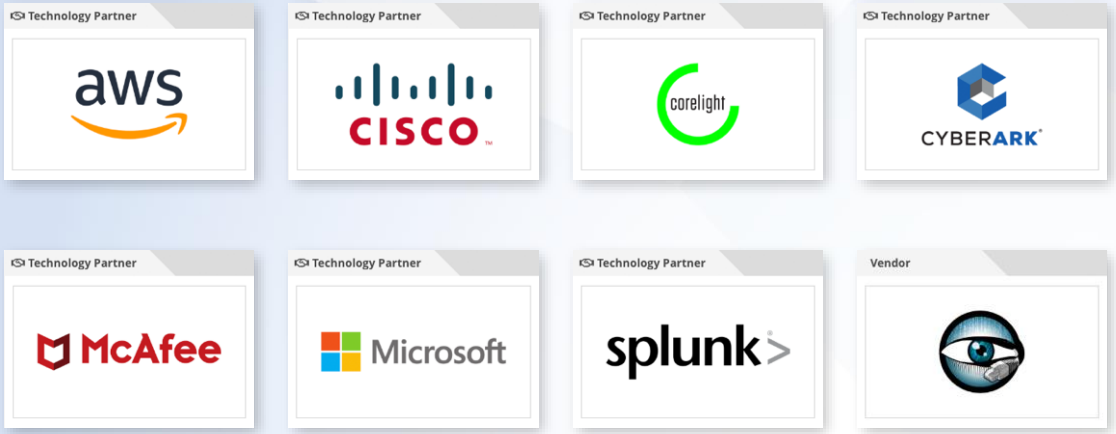
Stand-alone product capabilities combined in one platform

Efficiency

86%

Reduction in analyst time spent on non-response activities

Technology Integrations



To learn more about our product integrations, including additional tools and content to extend your FireEye experience, visit

https://fireeye.market

Parsing Integrations

As of June 2019

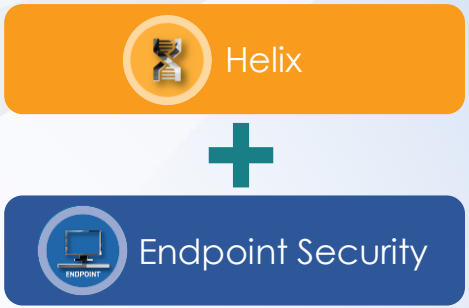
Orchestrator Plug-ins

As of June 2019

FireEye Helix With Security Solutions

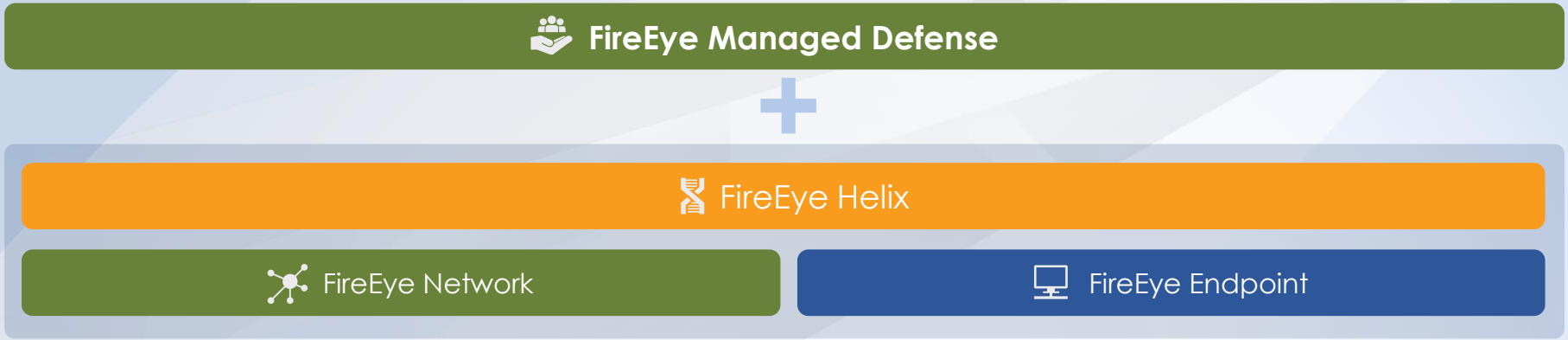
- Enhanced detection and alert fidelity
- Automation rule books
- Alert prioritization
- Contextual intelligence

- Immediate correlation to the endpoint
- Automation rule books
- Alert prioritization
- Contextual intelligence



- Context from email and network
- Containment at a click
- Automation rule books
- Alert prioritization
- Contextual intelligence

FireEye Helix with Managed Defense



- Analyst-driven detection and response
- Systematic, proactive hunting investigations
- Visibility and protection from emerging threats
- Detailed reports with recommendations
- Proprietary investigative techniques
- Access to hundreds of FireEye experts

How to Get FireEye Helix

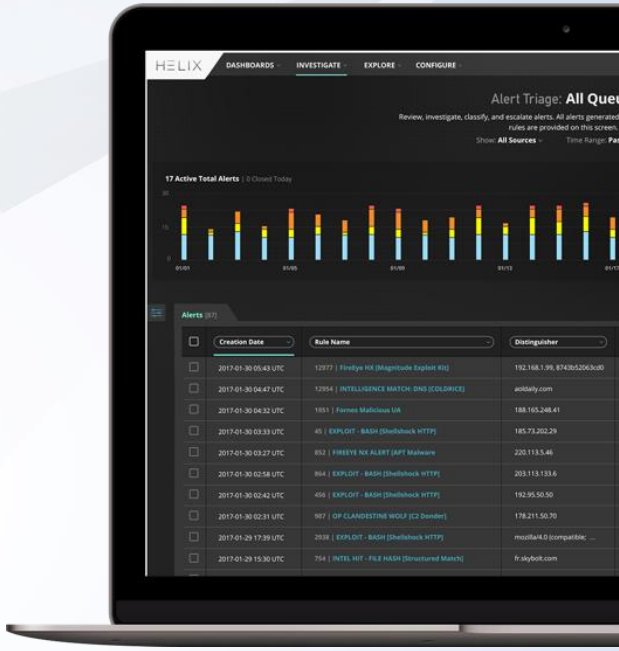
		Pricing Model
Stand-alone	FireEye Helix	Per EPS
With a FireEye Subscription Solution	FireEye Helix Network Security Email Security Endpoint Security	Priced based on respective solution - Network: $ per Mbps - Email: $ per mailbox - Endpoint: $ per Endpoint
With the FireEye Security Suite (For Mid-Market up to 2,000 users)	FireEye Helix Network Security Email Security Endpoint Security	Per connected user

Leveraging Your Entitlement

Customers of FireEye subscription products are provided with a no cost entitlement to FireEye Helix up to 100 Events Per Second (EPS). An event includes any internal or external processes affecting a network. These can include activity from firewalls, IDS/IPS, servers or any other processes that generate log data. With the 100 EPS entitlement, customers still enjoy the full functionality of Helix.

By selecting which event data is sent into Helix, customers can experience the value of the product's misconfiguration monitoring, user behavior analytics, cloud intelligence, data exfiltration detection, or malicious network traffic identification.

Talk to your FireEye account manager to identify which capabilities you are interested in trialing.



Industry Awards

- Frost & Sullivan – FireEye Threat Analytics (formerly TAP) is the Leader in key SIEM segments

- CRN – 2017 Tech Innovator Award
- ChannelNomics – 2017 Security Innovation of the Year Award
- Hosting Advice – 2018 Developers'Choice

FIREEYE™

Thank You