FireEye

FINANCIAL ANALYST DAY 2018

MARCH 1 | SAN FRANCISCO

WELCOME

Today’s Agenda

			TOPIC	SPEAKER
8:25 am	-	8:30 am	Welcome/Safe Harbor Statement	Kate Patterson, Investor Relations
8:30 am	-	9:15 am	Built to Last	Kevin Mandia, CEO
9:15 am	-	9:45 am	Built to Innovate	Grady Summers, CTO
9:45 am	-	10:00 am	Break	
10:00 am	-	10:30 am	Built to Protect	Kevin Mandia, CEO
10:30 am	-	11:00 am	Built to Win	Bill Robbins, EVP Worldwide Sales
11:00 am	-	11:30 am	Built to Last (Financial)	Frank Verdecanna, CFO & CAO
11:30 am	-	12:00 pm	Executive Panel / Q&A	
12:00 pm	-	1:00 pm	Lunch & Demos (Innovation Hub)	FireEye Solutions Experts

Additional Information

Go to investors.fireeye.com/events to download:

- Event Slides (pdf format)
- GAAP to non-GAAP reconciliations
- Historical financial results and breakouts recast under 606 for Fiscal Years 2016 and 2017 plus unaudited recast results for Q1’17, Q2’17, Q3’17, Q4’17

Wi-Fi: FireEye   Password: March2018

Safe Harbor Statement

This presentation contains forward-looking statements within the meaning of Section 27A of the Securities Act of 1933, as amended, and Section 21E of the Securities Exchange Act of 1934, as amended. These forward-looking statements are based on management's beliefs and assumptions and on information currently available to management. Forward-looking statements include information concerning: possible or assumed future results of operations, financial metrics and goals; our path to profitability; our priorities, plans, initiatives and investments; threat landscape; industry environment; customer buying preferences; growth drivers; competitive position; market opportunities; future and enhanced offerings; and the effects of competition.

Forward-looking statements include all statements that are not historical facts and can be identified by terms such as "anticipates," "believes," "could," "seeks," "estimates," "intends," "may," "plans," "potential," "predicts," "projects," "should," "will," "would" or similar expressions and the negatives of those terms. Forward-looking statements involve known and unknown risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from any future results, performance or achievements expressed or implied by the forward-looking statements. Forward-looking statements represent our management's beliefs and assumptions only as of the date of this presentation. You should read our filings with the SEC, including the Risk Factors set forth therein, completely and with the understanding that our actual future results may be materially different from what we expect. Except as required by law we assume no obligation to update these forward-looking statements publicly, or to update the reasons why actual results could differ materially from those anticipated in the forward-looking statements, even if new information becomes available in the future.

Any future offering, feature, or related specification that may be referenced in this presentation is for information purposes only and is not a commitment to deliver any offering, technology or enhancement. We reserve the right to modify future product and service plans at any time.

This presentation includes certain non-GAAP financial measures as defined by the SEC rules. As required by Regulation G, we have provided a reconciliation of those measures to the most directly comparable GAAP measures, which is available in the appendix.

FireEye

BUILT TO LAST

KEVIN MANDIA CEO

FireEye knows more about

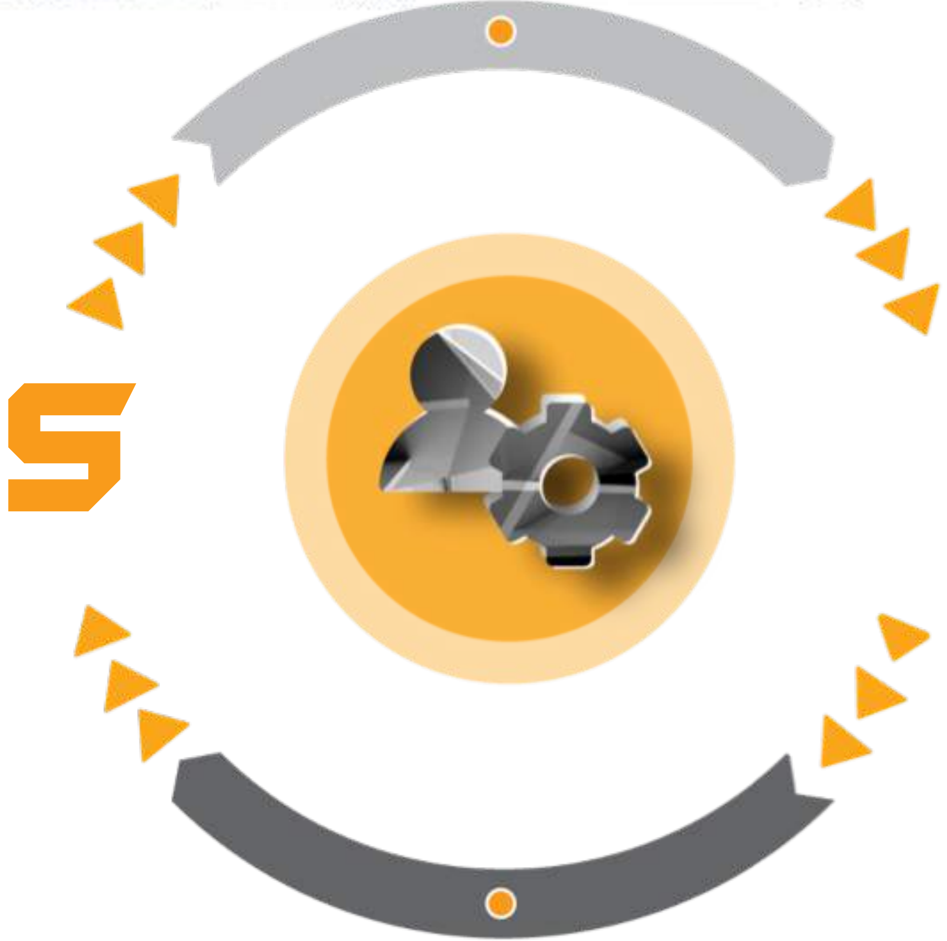
CYBER THREATS

than anyone.

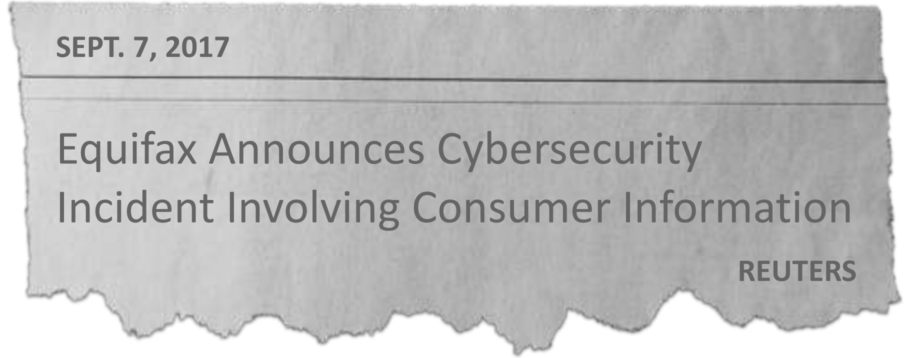
FireEye

INNOVATES

Rapidly to Combat These Threats



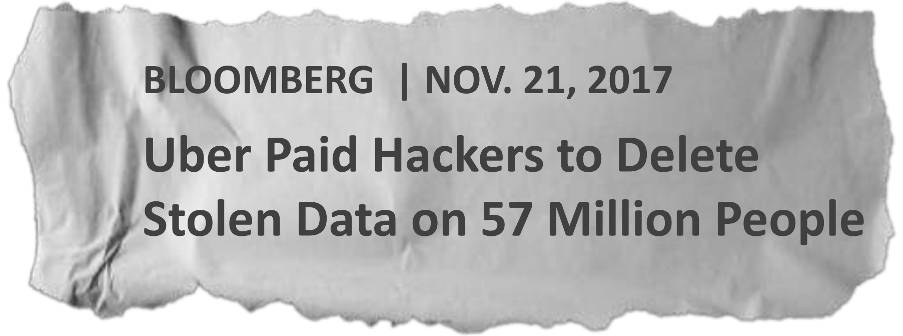
Cyber Attacks in 2017



SEPT. 7, 2017

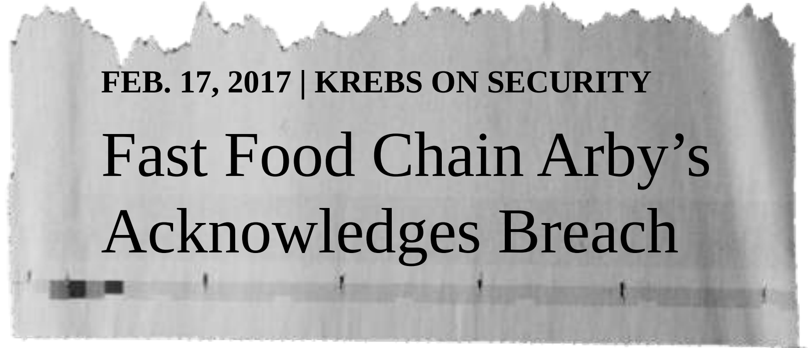
Equifax Announces Cybersecurity Incident Involving Consumer Information

REUTERS



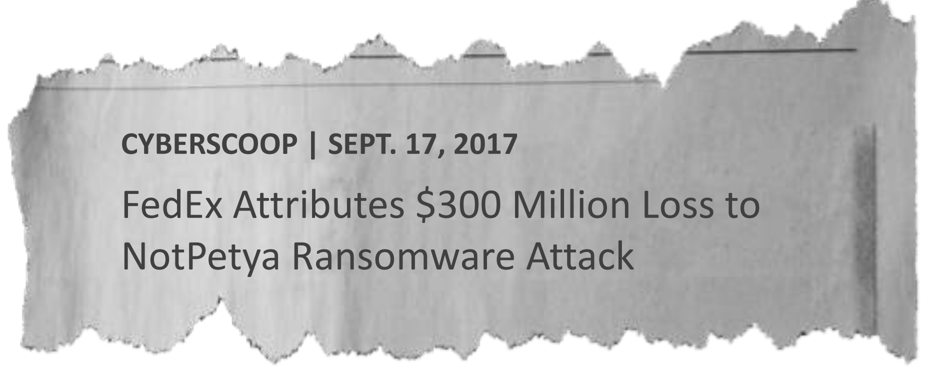
BLOOMBERG | NOV. 21, 2017

Uber Paid Hackers to Delete Stolen Data on 57 Million People



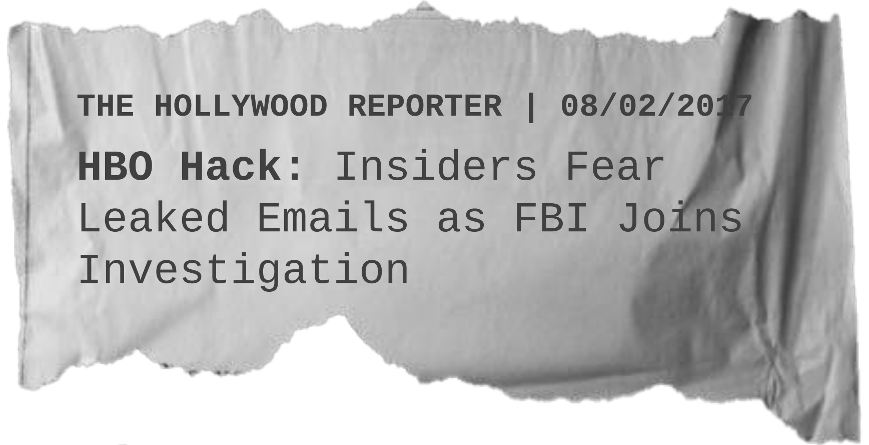
FEB. 17, 2017 | KREBS ON SECURITY

Fast Food Chain Arby's Acknowledges Breach



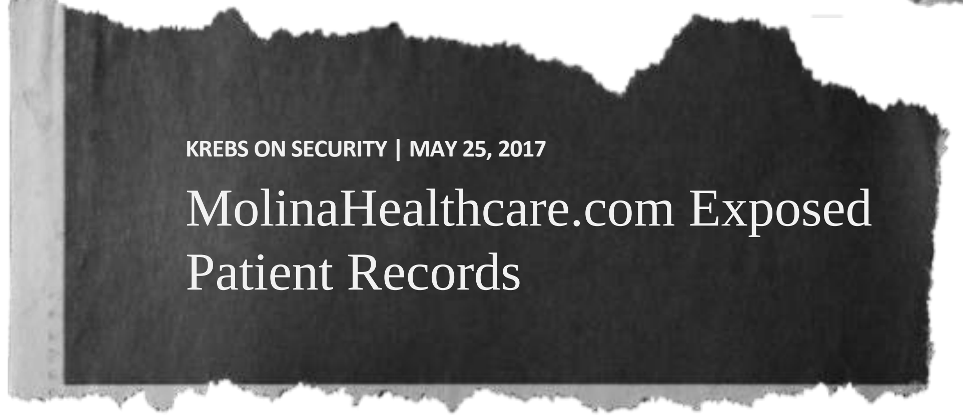
CYBERSCOOP | SEPT. 17, 2017

FedEx Attributes $300 Million Loss to NotPetya Ransomware Attack



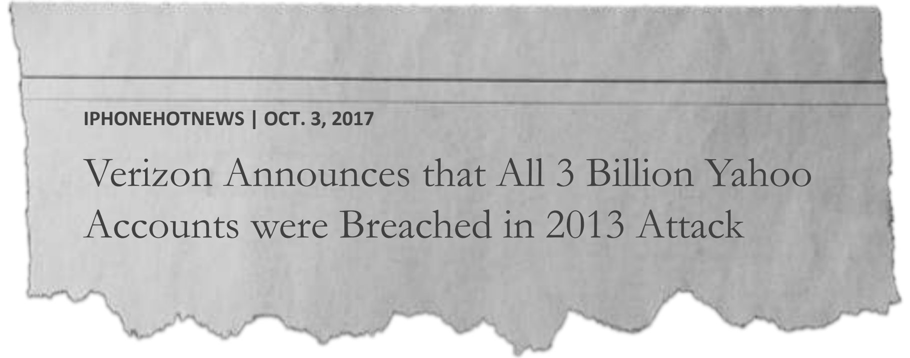
THE HOLLYWOOD REPORTER | 08/02/2017

HBO Hack: Insiders Fear Leaked Emails as FBI Joins Investigation



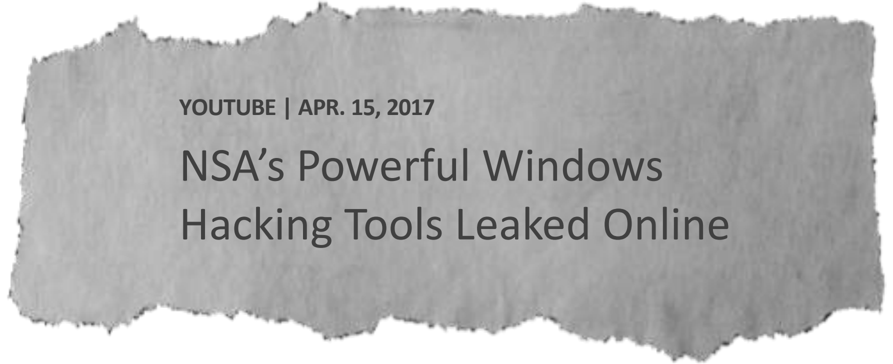
KREBS ON SECURITY | MAY 25, 2017

MolinaHealthcare.com Exposed Patient Records



IPHONEHOTNEWS | OCT. 3, 2017

Verizon Announces that All 3 Billion Yahoo Accounts were Breached in 2013 Attack



YOUTUBE | APR. 15, 2017

NSA's Powerful Windows Hacking Tools Leaked Online

300+ INCIDENT INVESTIGATORS

20+ COUNTRIES

BASED ON 2017 STATS

600+ INVESTIGATIONS

200K+ HOURS

BASED ON 2017 STATS

100+ INTELLIGENCE ANALYSTS

32 LANGUAGES

18 COUNTRIES

BASED ON 2017 STATS

300+ RED TEAM ENGAGEMENTS

60K+ HOURS

BASED ON 2017 STATS

1 MILLION+ UNIQUE MALWARE SAMPLES PER DAY

BASED ON 2017 STATS

60,000+ MALWARE SAMPLES FROM INVESTIGATIONS

BASED ON 2017 STATS

10 REPORTED ZERO DAYS BY FIREEYE

BASED ON 2017 STATS

150+ MALWARE TRAFFIC DECRYPTION/ DECODING SCRIPTS

100+ ATTACKER SESSIONS DECODED/ MONTH IN SUPPORT OF INVESTIGATIONS

BASED ON 2017 STATS

Agenda

1. Conclusions
2. How Is FireEye Different
3. 2018

CONCLUSIONS

1

There Will ALWAYS Be a Security Gap That Can Be Exploited

2

Technology Alone Is NOT ENOUGH to Combat Cyber Attacks

3

There Are NO RISKS or REPERCUSSIONS for the Attackers

4

Attackers Continue to Exploit HUMAN TRUST

5 Cyber Criminals Are Getting BETTER

6

Cyber Attacks Reflect Geopolitical CONDITIONS

CHINA

APT1
APT3
APT10
APT12
APT16
APT17
APT18
APT19
APT30

RUSSIA

APT28

APT29

IRAN

APT33
APT34

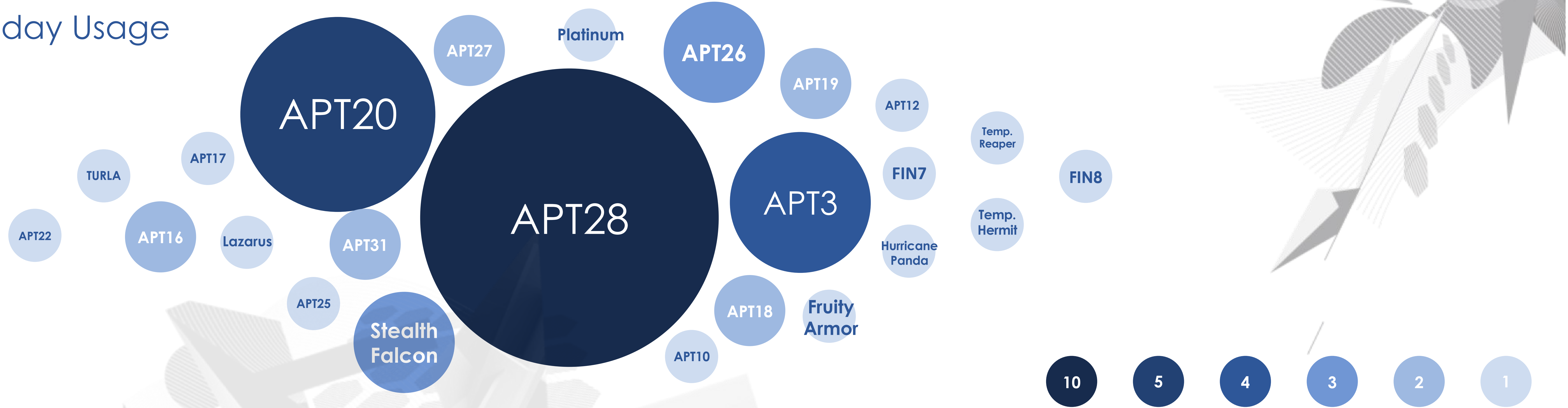
NORTH KOREA

APT37

VIETNAM

APT32

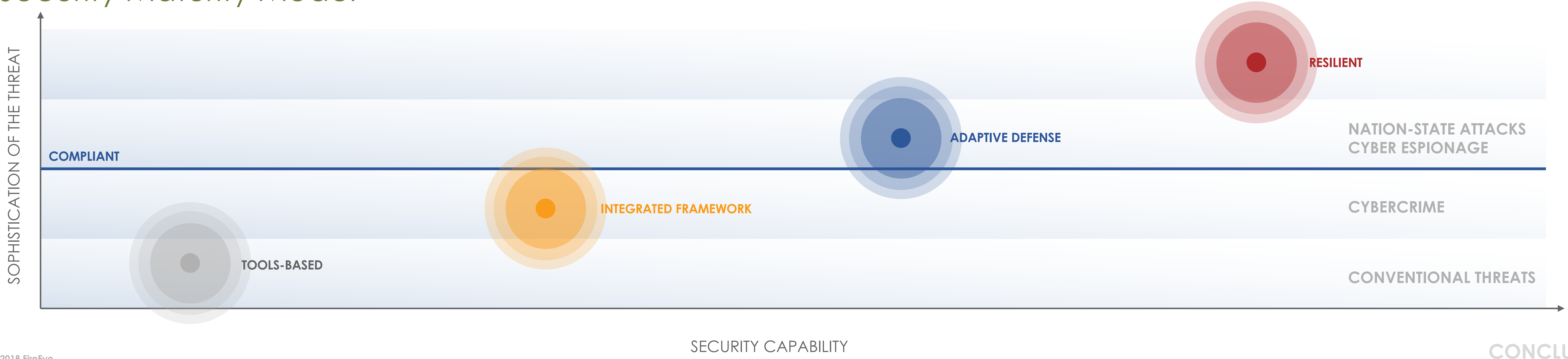
APT Groups Zero-day Usage



7 DISCLOSURE

Is More Probable

8 Security Maturity Model



9

80% of CapEx Budgets are Spent on **Detection & Prevention**

80% of Security Team Time Spent on **Analysis & Response**

10

The Outcome CISOs Want Delivered:

ALERT → FIX IN LESS THAN 7 MINUTES

How Is FireEye DIFFERENT

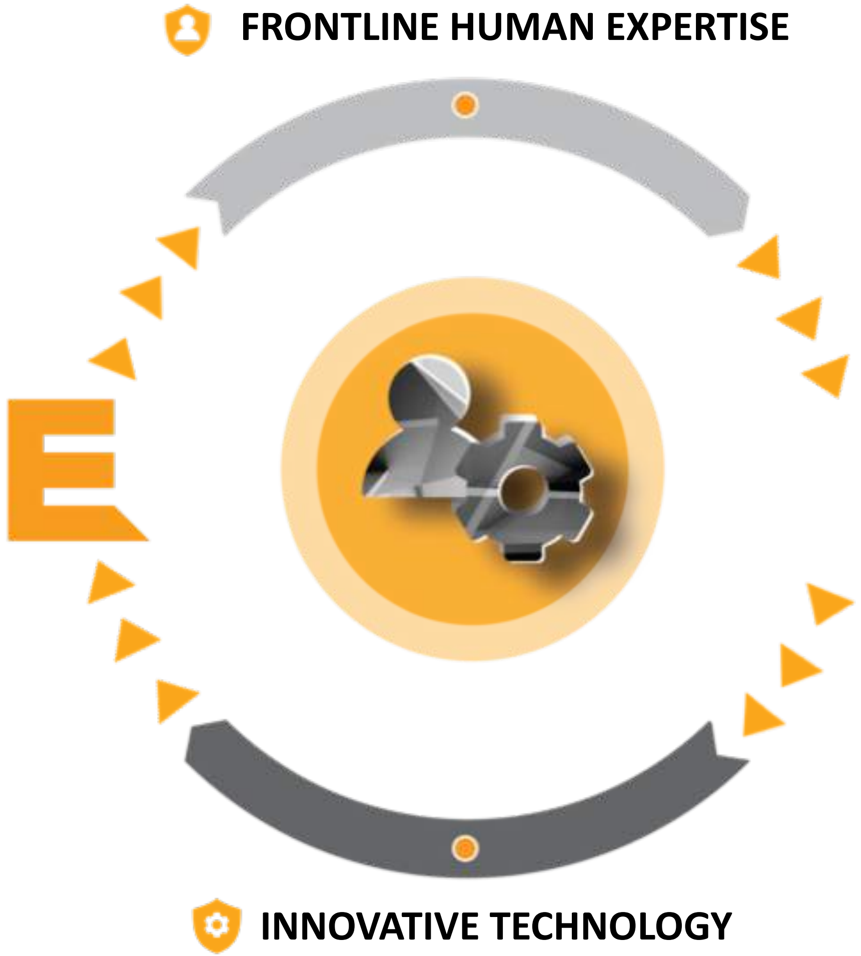
FireEye knows more about

CYBER THREATS

than anyone.

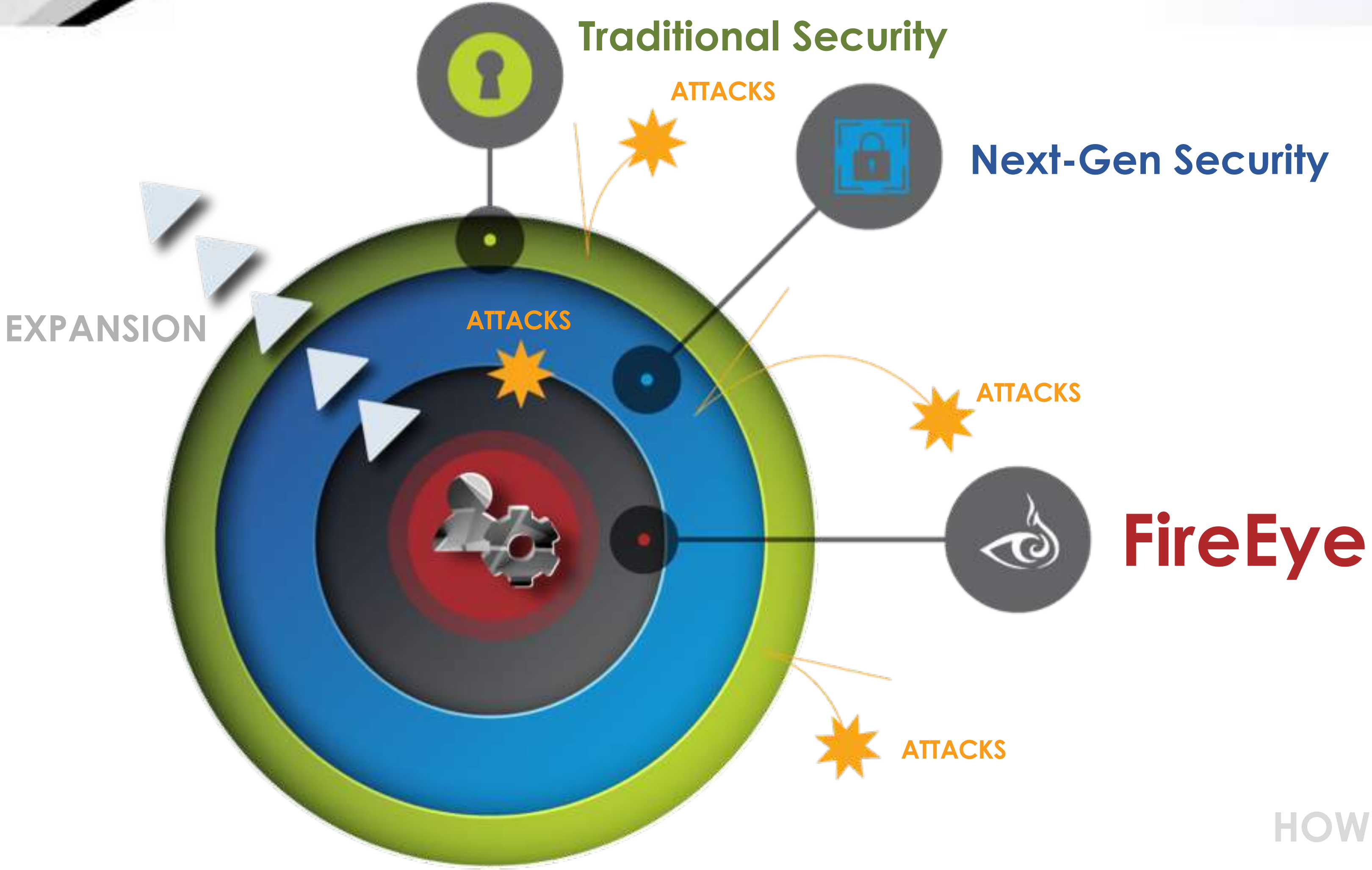
MEDIA REEL

The FireEye INNOVATION CYCLE



This innovation cycle cannot exist without our experts embracing the technology we build as their own, and our product teams embracing the **world-class expertise** provided by our frontline teams.

FireEye
Solves the Hard Problems First



So What?

- We Know **What Our Customers Need**
- We Know the **Security Gaps**
- We **Detect** What Other Products Miss
- Our **Alerts Matter**
- We Are Always **Adapting** to Current Threats
- Provide Not Just Alerts, But **Answers**
- **Trusted Partner** Before, During and After an Event
- Expertise **When You Need It Most**

FireEye is

BUILT TO LAST

We believe that by doing the right thing for our customers and employees, we will amass value for all shareholders.

FireEye

BUILT TO INNOVATE

GRADY SUMMERS CTO

INTELLIGENCE - LED
Advantage

NATION - GRADE
Capability

MACHINE INTELLIGENCE

INCIDENT RESPONSE

ADVERSARIAL INTELLIGENCE

CAMPAIGN INTELLIGENCE

Continuous learning system to make sure we know more about cyber threats than anyone else.

The FireEye **INNOVATION CYCLE**

FRONTLINE HUMAN EXPERTISE

INNOVATIVE TECHNOLOGY

FIREEYE SUSTAINED DIFFERENTIATOR

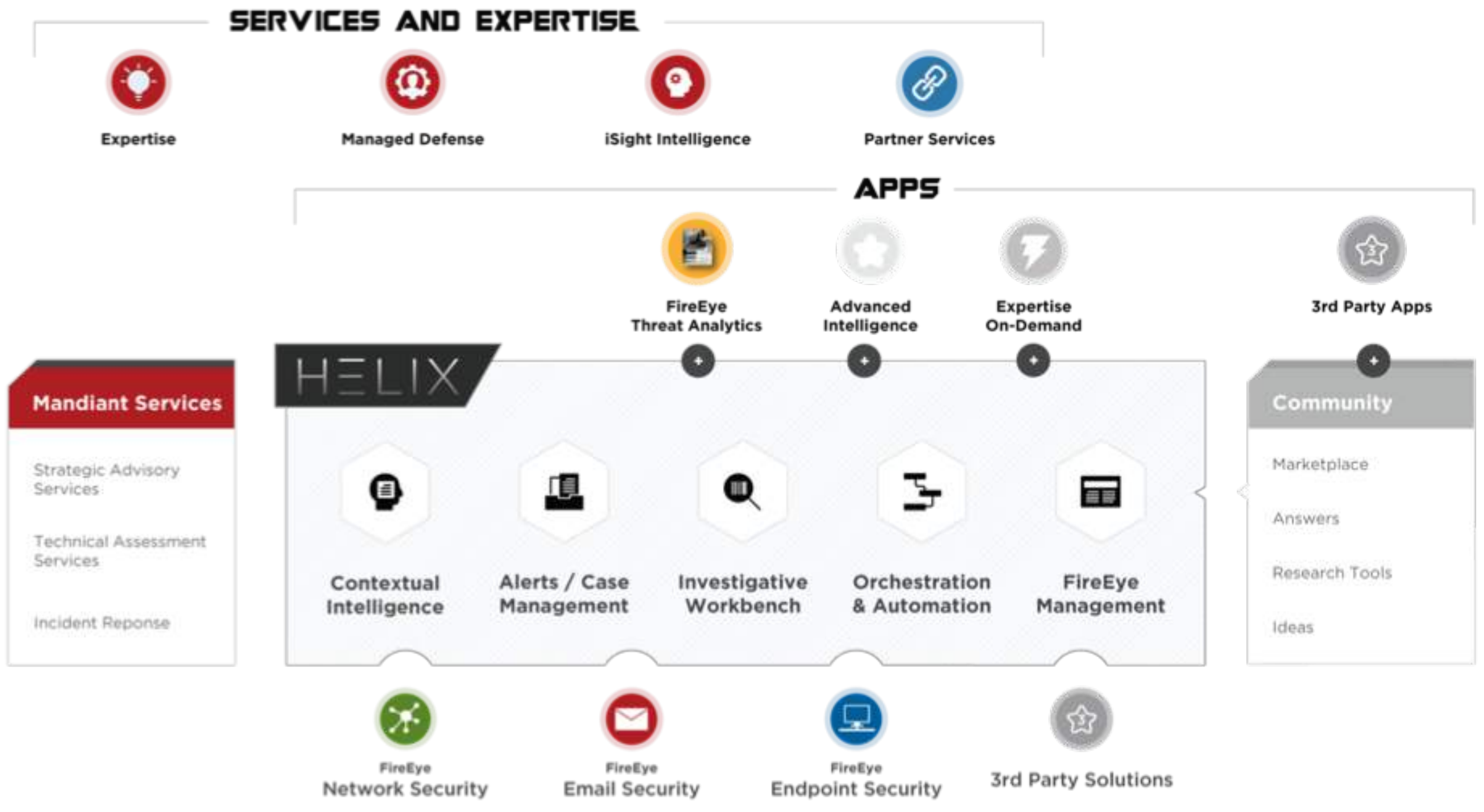
Designed with Real-time, First-hand Knowledge of the Global Threat Landscape

Architected to Be Open, Modular, Extensible

Built for What We KNOW Our Customers Need

FireEye

The FireEye ECOSYSTEM



SERVICES AND EXPERTISE

Expertise

Managed Defense

iSight Intelligence

Partner Services

APPS

FireEye Threat Analytics

Advanced Intelligence

Expertise On-Demand

3rd Party Apps

Mandiant Services

- Strategic Advisory Services
- Technical Assessment Services
- Incident Reponse

HELIX

Contextual Intelligence

Alerts / Case Management

Investigative Workbench

Orchestration & Automation

FireEye Management

Community

- Marketplace
- Answers
- Research Tools
- Ideas

FireEye Network Security

FireEye Email Security

FireEye Endpoint Security

3rd Party Solutions

FireEye

UNDERLYING **TECHNOLOGY INNOVATION**

UNDERLYING **TECHNOLOGY INNOVATION**

MVX

UNDERLYING **TECHNOLOGY INNOVATION**

MVX → Indicators

UNDERLYING **TECHNOLOGY INNOVATION**

MVX → Indicators → Heuristic, Behavioral

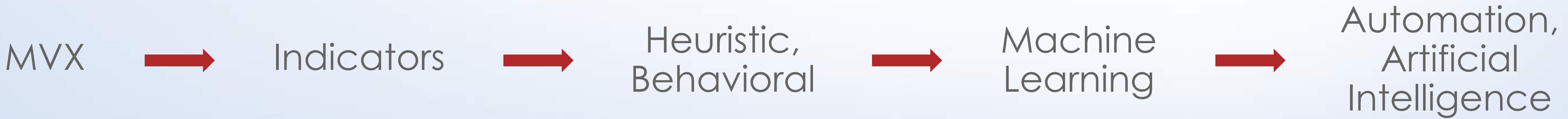
FireEye

UNDERLYING **TECHNOLOGY INNOVATION**

MVX → Indicators → Heuristic, Behavioral → Machine Learning

FireEye

UNDERLYING **TECHNOLOGY INNOVATION**

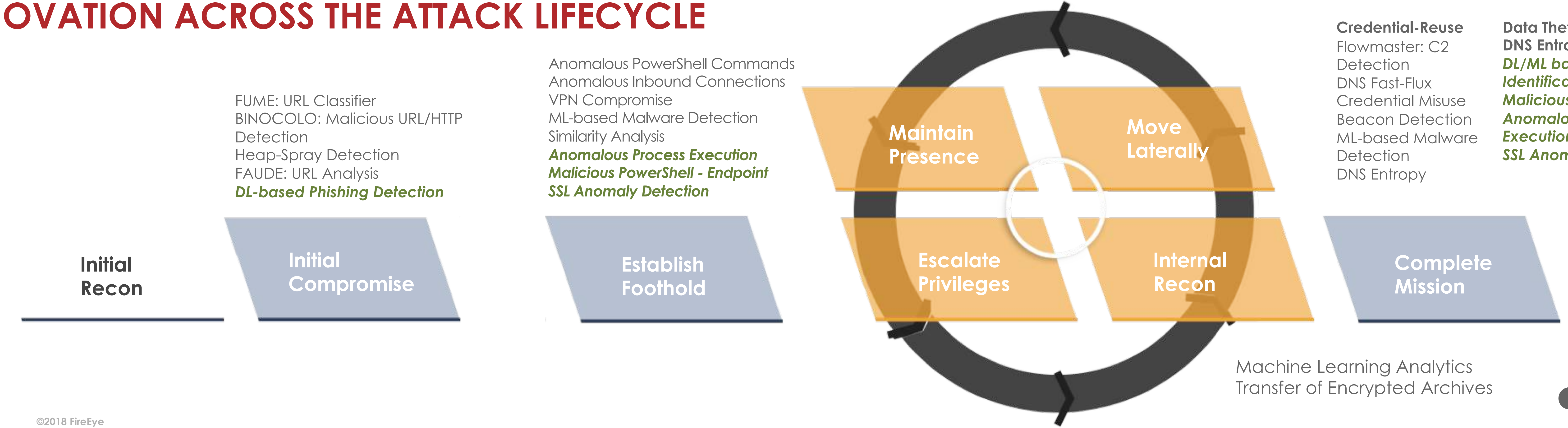


MVX → Indicators → Heuristic, Behavioral → Machine Learning → Automation, Artificial Intelligence

FireEye

INNOVATION IN ANALYTICS

INNOVATION ACROSS THE ATTACK LIFECYCLE



FUME: URL Classifier
BINOCOLO: Malicious URL/HTTP Detection
Heap-Spray Detection
FAUDE: URL Analysis
DL-based Phishing Detection

Anomalous PowerShell Commands
Anomalous Inbound Connections
VPN Compromise
ML-based Malware Detection
Similarity Analysis
Anomalous Process Execution
Malicious PowerShell - Endpoint
SSL Anomaly Detection

Credential-Reuse
Flowmaster: C2 Detection
DNS Fast-Flux
Credential Misuse
Beacon Detection
ML-based Malware Detection
DNS Entropy

Data Theft Detection
DNS Entropy
DL/ML based Malware Identification
Malicious PowerShell
Anomalous Process Execution
SSL Anomaly Detection

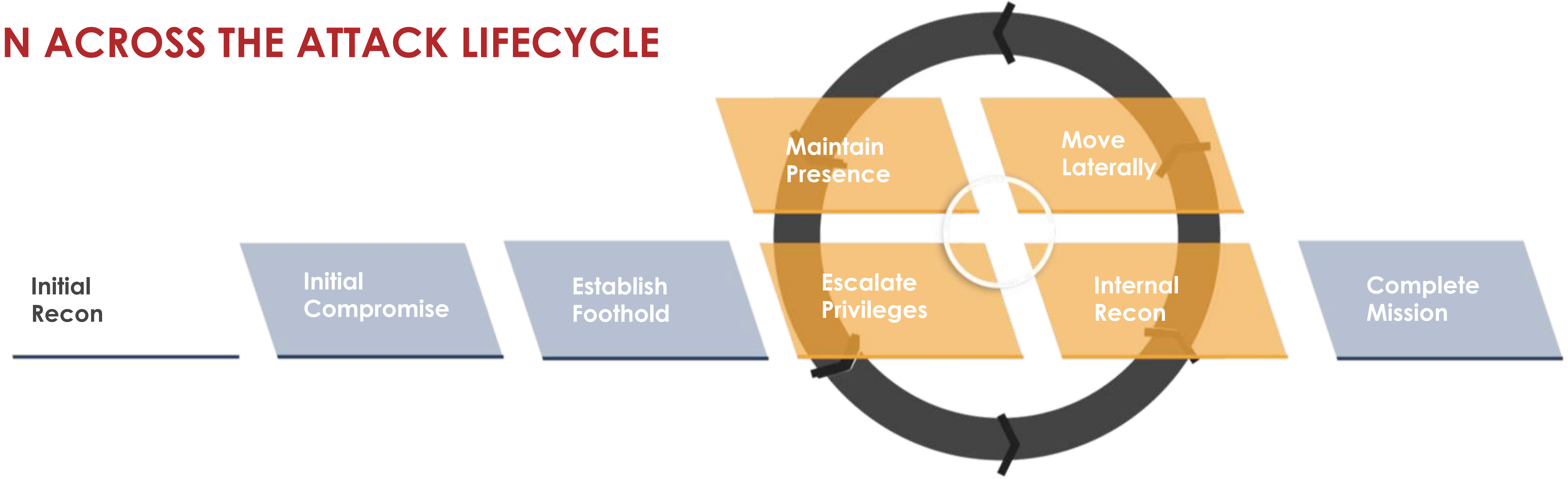
Machine Learning Analytics
Transfer of Encrypted Archives

● Available Now ● ***Coming Soon***

FireEye

DETECTION EVOLVES WITH SMARTVISION

DETECTION ACROSS THE ATTACK LIFECYCLE



Initial Recon

Initial Compromise

Establish Foothold

Escalate Privileges

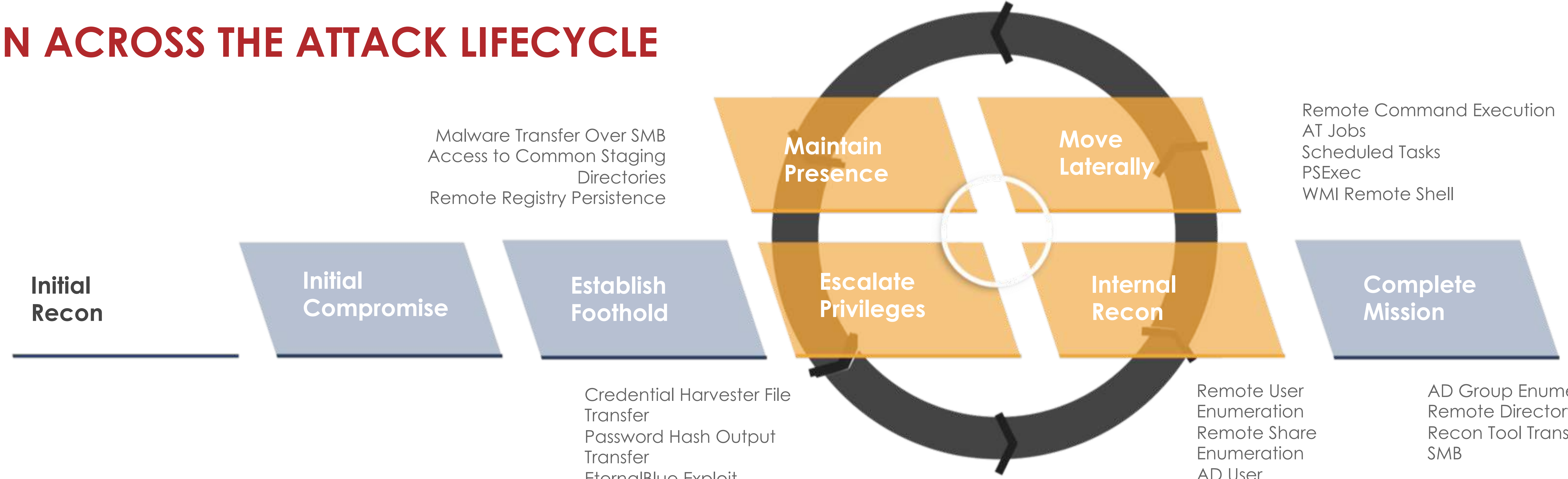
Internal Recon

Move Laterally

Maintain Presence

Complete Mission

DETECTION ACROSS THE ATTACK LIFECYCLE



Initial Recon

Initial Compromise

Establish Foothold

Credential Harvester File Transfer
Password Hash Output Transfer
EternalBlue Exploit Detection

Malware Transfer Over SMB
Access to Common Staging Directories
Remote Registry Persistence

Maintain Presence

Escalate Privileges

Move Laterally

Remote Command Execution
AT Jobs
Scheduled Tasks
PSExec
WMI Remote Shell

Internal Recon

Remote User Enumeration
Remote Share Enumeration
AD User Enumeration

AD Group Enumeration
Remote Directory Listings
Recon Tool Transfer Over SMB

Complete Mission

Machine Learning Analytics
Transfer of Encrypted Archives

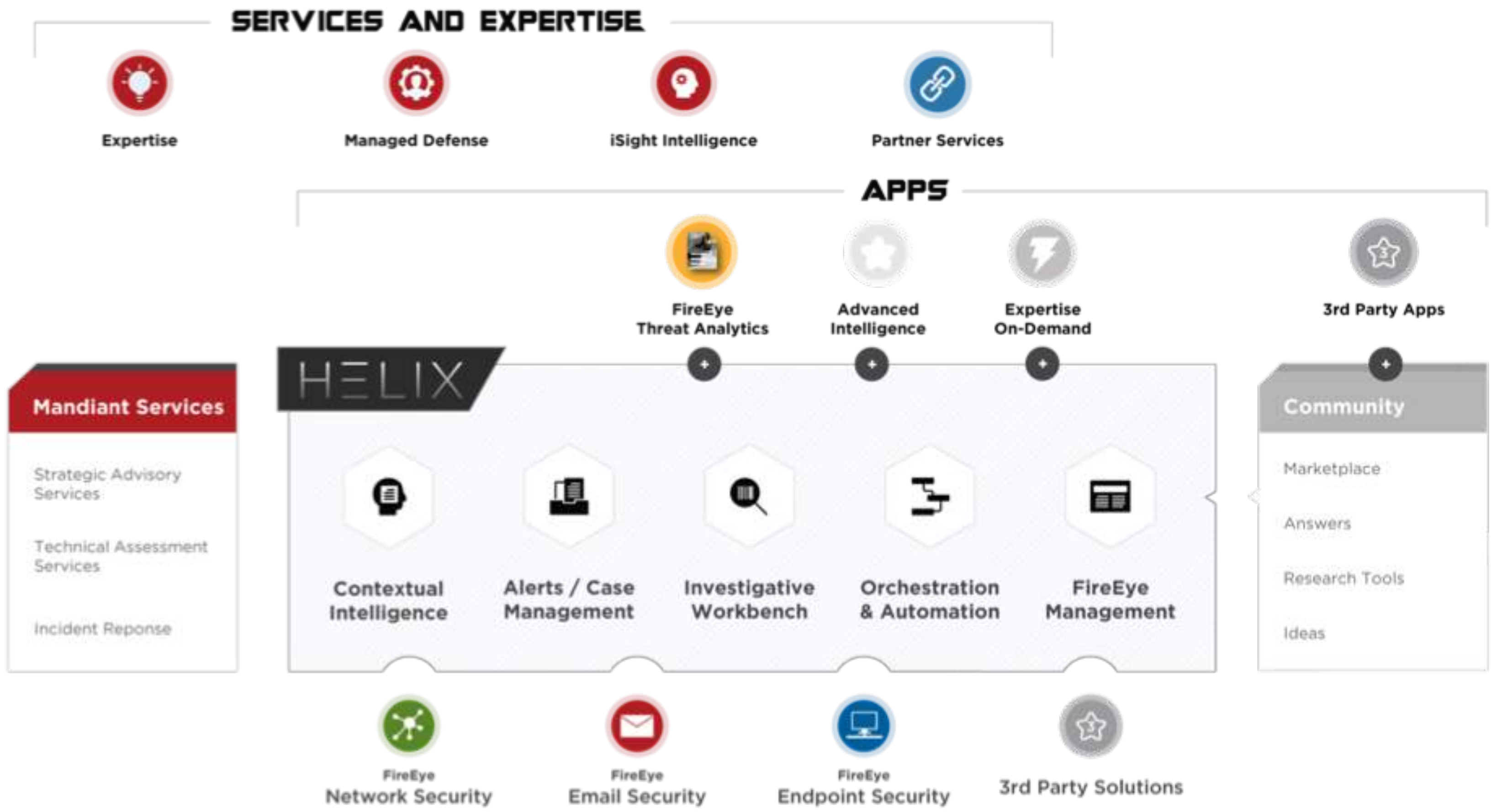
FireEye

INNOVATION IN PRODUCTS & SERVICES

ACCOMPLISHMENTS AND UPCOMING FEATURES

FireEye

The FireEye ECOSYSTEM



SERVICES AND EXPERTISE

Expertise

Managed Defense

iSight Intelligence

Partner Services

APPS

FireEye Threat Analytics

Advanced Intelligence

Expertise On-Demand

3rd Party Apps

Mandiant Services

Strategic Advisory Services

Technical Assessment Services

Incident Reponse

HELIX

Contextual Intelligence

Alerts / Case Management

Investigative Workbench

Orchestration & Automation

FireEye Management

Community

Marketplace

Answers

Research Tools

Ideas

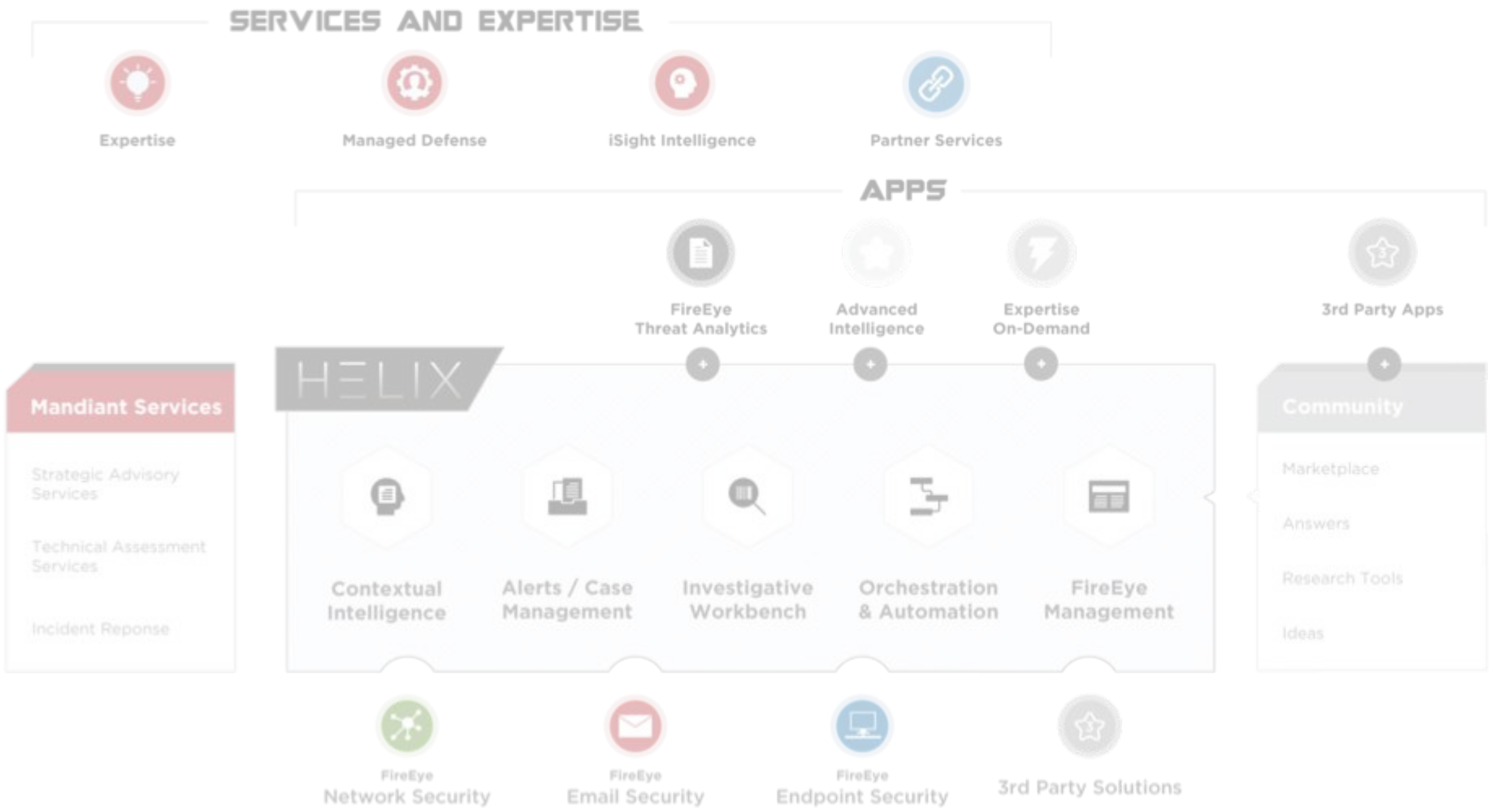
FireEye Network Security

FireEye Email Security

FireEye Endpoint Security

3rd Party Solutions

FireEye



SERVICES AND EXPERTISE

Expertise

Managed Defense

iSight Intelligence

Partner Services

APPS

FireEye Threat Analytics

Advanced Intelligence

Expertise On-Demand

3rd Party Apps

Mandiant Services

Strategic Advisory Services

Technical Assessment Services

Incident Reponse

HELIX

Contextual Intelligence

Alerts / Case Management

Investigative Workbench

Orchestration & Automation

FireEye Management

Community

Marketplace

Answers

Research Tools

Ideas

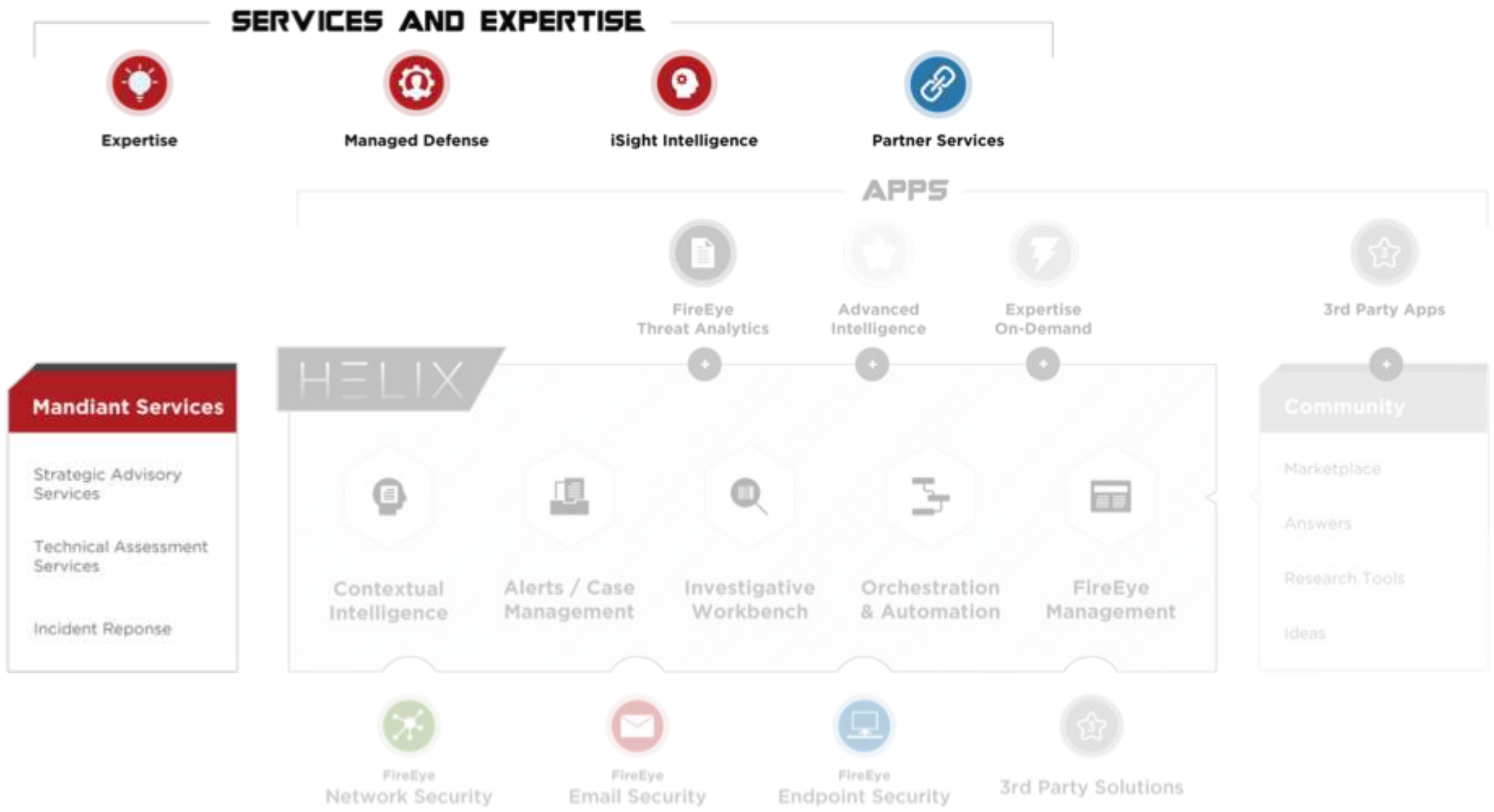
FireEye Network Security

FireEye Email Security

FireEye Endpoint Security

3rd Party Solutions

FireEye


SERVICES AND EXPERTISE
Expertise
Managed Defense
iSight Intelligence
Partner Services
APPS
FireEye Threat Analytics
Advanced Intelligence
Expertise On-Demand
3rd Party Apps
Mandiant Services
Strategic Advisory Services
Technical Assessment Services
Incident Reponse
HELIX
Contextual Intelligence
Alerts / Case Management
Investigative Workbench
Orchestration & Automation
FireEye Management
Community
Marketplace
Answers
Research Tools
Ideas
FireEye Network Security
FireEye Email Security
FireEye Endpoint Security
3rd Party Solutions

Managed Defense & iSIGHT

2017 ACCOMPLISHMENTS

- Automated triage increased analyst efficiency by 5x
- Created more than 1,000 product detections
- Launched new bundle for midmarket
- Successful first sales of FaaS for ICS
- Largest ever iSIGHT deal to a government agency

LOOKING AHEAD

- New interlock between FaaS and Managed Defense creates simpler sales motion and faster onboarding
- iSIGHT providing expanded context for Helix
- Expanding our iSIGHT intelligence offerings to provide statistical analysis and trends
- Providing new tailored, real-time intelligence alerting
- Machine learning to model and automate predictive alert scoring for Helix and FaaS

FireEye

Mandiant Consulting

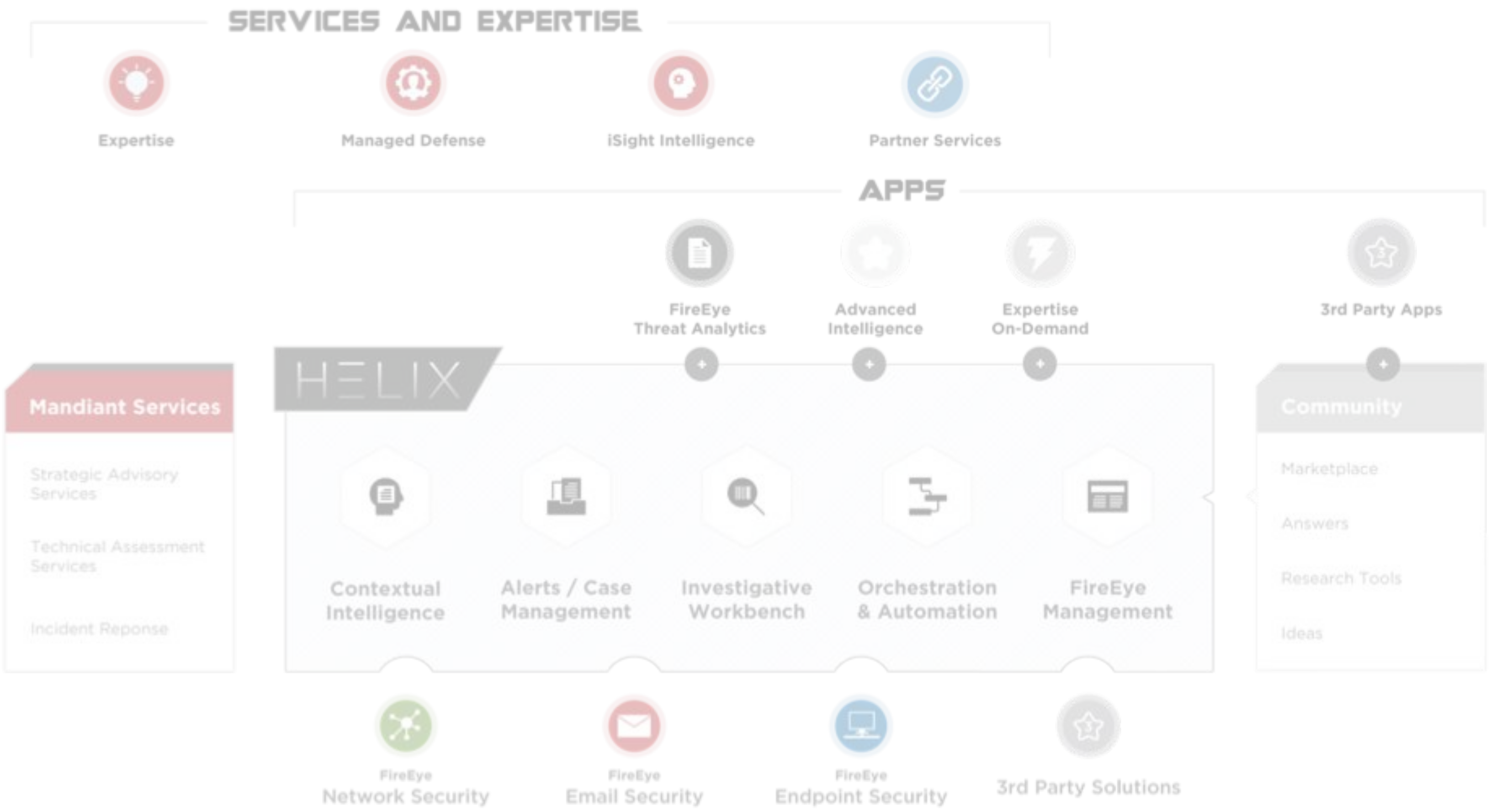
2017 HIGHLIGHTS

- Record year for Professional Services and Incident Response
- Continue to be the go-to trusted advisor for the world's most significant breaches at the most critical customers
- Continued focus on improving FireEye technology
- Conducted more training in 2017 than any year in Mandiant history
- New Security Transformation offering seeing large-deal traction
  - $12M SLED customer: Security Transformation deal that included Product, FaaS, Intel, and Consulting Services
  - $6M Financial Customer, Security Transformation deal that included Consulting and Intel Services

LOOKING AHEAD

- Launch Mandiant-on-Demand subscription offerings
- Continued international expansion
- Continued training expansion
- Increased investment in government and strategic transformation services

FireEye



SERVICES AND EXPERTISE

Expertise

Managed Defense

iSight Intelligence

Partner Services

APPS

FireEye Threat Analytics

Advanced Intelligence

Expertise On-Demand

3rd Party Apps

Mandiant Services

- Strategic Advisory Services
- Technical Assessment Services
- Incident Reponse

HELIX

Contextual Intelligence

Alerts / Case Management

Investigative Workbench

Orchestration & Automation

FireEye Management

Community

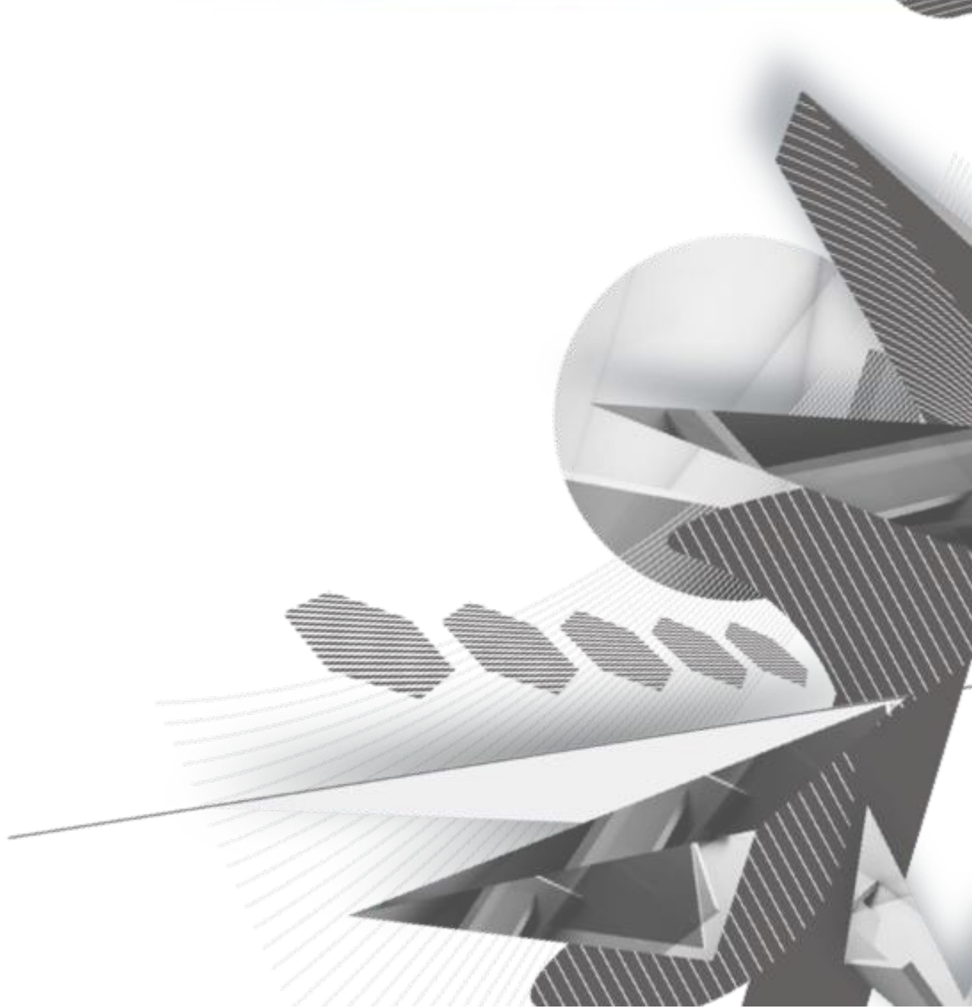
- Marketplace
- Answers
- Research Tools
- Ideas

FireEye Network Security

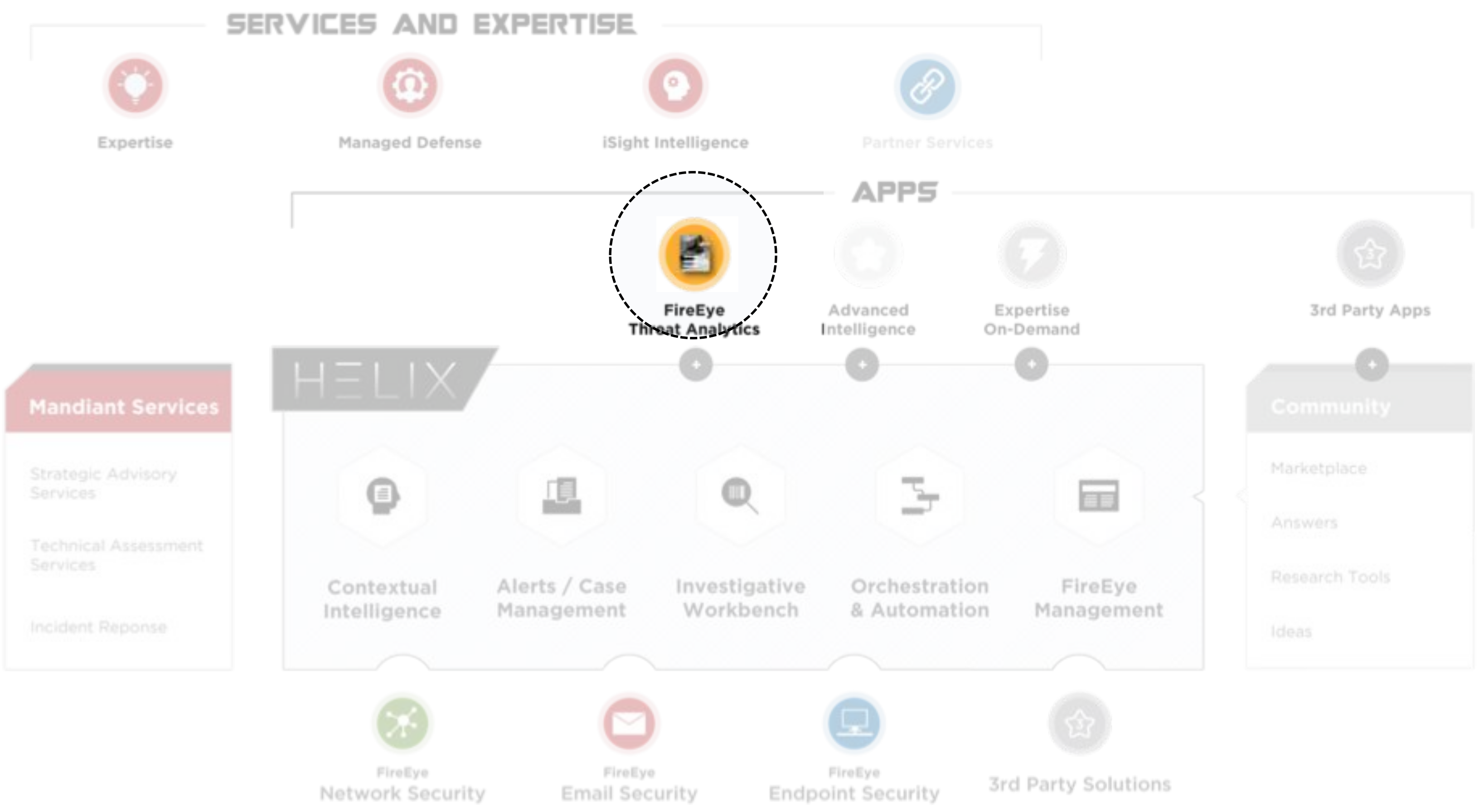
FireEye Email Security

FireEye Endpoint Security

3rd Party Solutions



FireEye


SERVICES AND EXPERTISE
Expertise
Managed Defense
iSight Intelligence
Partner Services
APPS
FireEye
Threat Analytics
Advanced
Intelligence
Expertise
On-Demand
3rd Party Apps
Mandiant Services
Strategic Advisory Services
Technical Assessment Services
Incident Reponse
HELIX
Contextual Intelligence
Alerts / Case Management
Investigative Workbench
Orchestration & Automation
FireEye Management
Community
Marketplace
Answers
Research Tools
Ideas
FireEye
Network Security
FireEye
Email Security
FireEye
Endpoint Security
3rd Party Solutions

FireEye

THREAT ANALYTICS

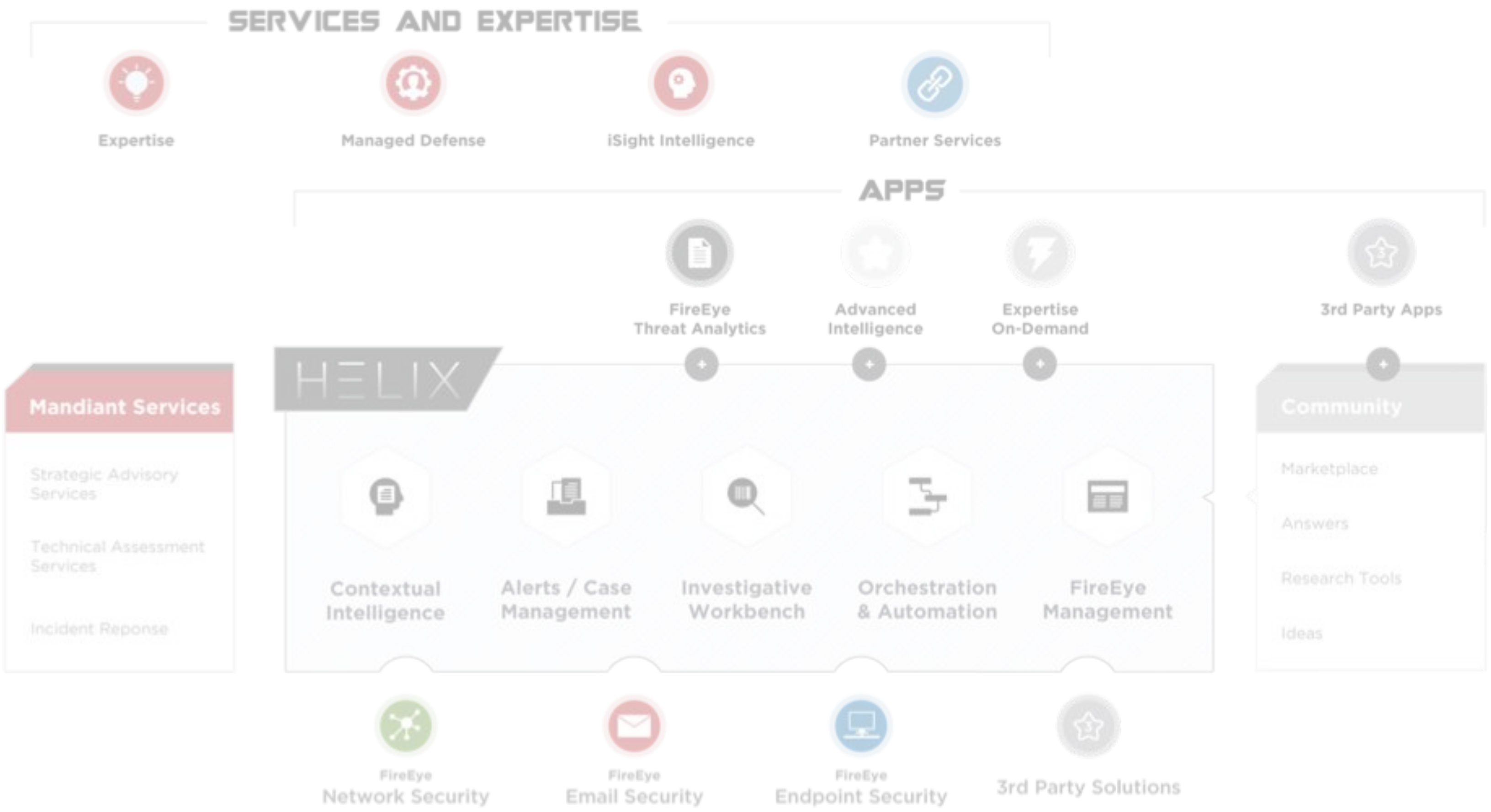
2017 ACCOMPLISHMENTS

- Identified as Best User Behavioral Analytics (UBA) and Best Threat Hunting in the SIEM space, by Frost & Sullivan
- Large and mature security organizations adopting TA to replace legacy SIEM
- First TA + ICS monitoring deals in 2017

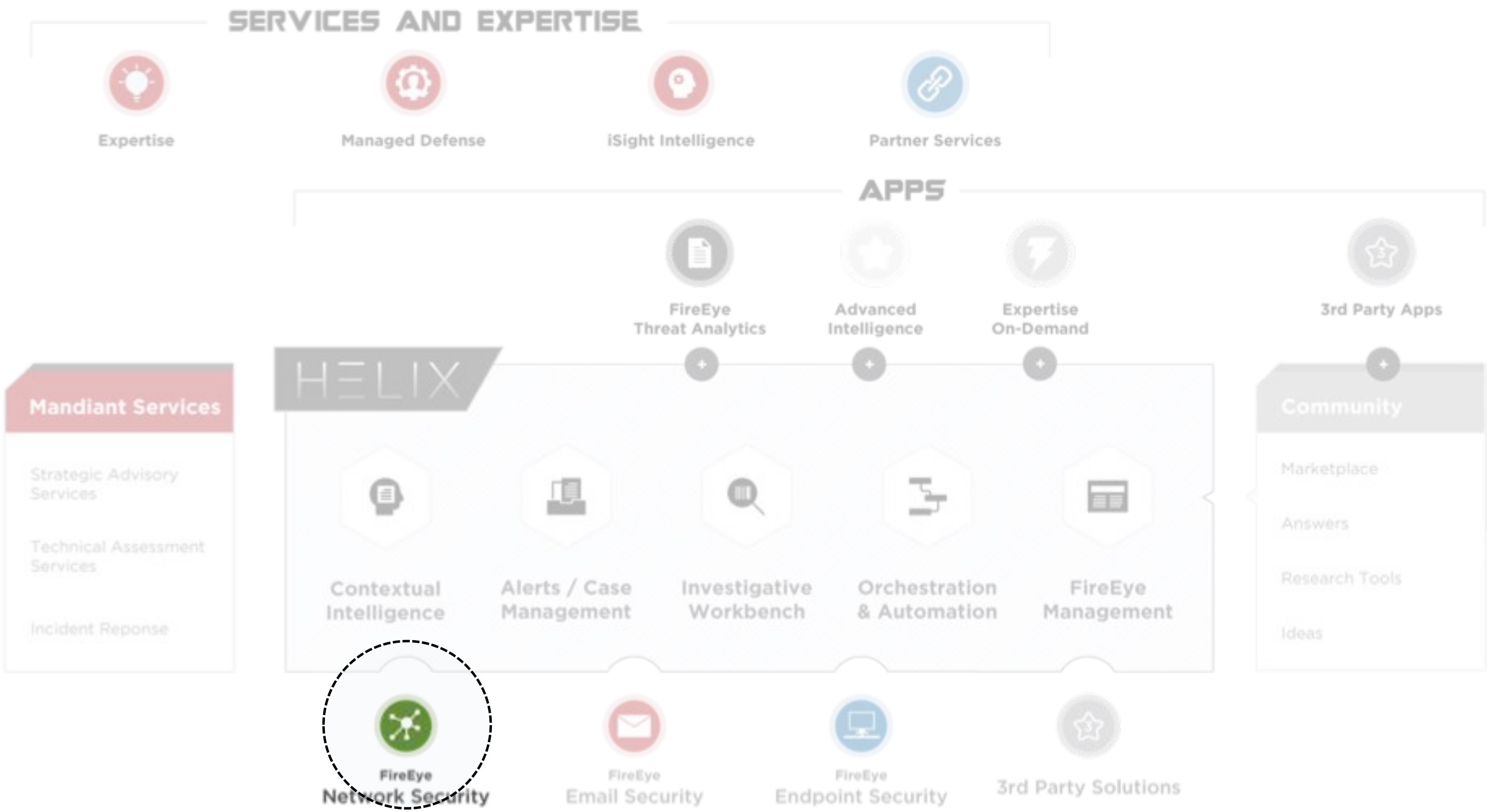
LOOKING AHEAD

- Compliance reporting
- Automatic coverage recommendations to maximize EPS value
- Major improvements in context, case management, intel attribution

FireEye


SERVICES AND EXPERTISE
Expertise
Managed Defense
iSight Intelligence
Partner Services
APPS
FireEye Threat Analytics
Advanced Intelligence
Expertise On-Demand
3rd Party Apps
Mandiant Services
Strategic Advisory Services
Technical Assessment Services
Incident Reponse
HELIX
Contextual Intelligence
Alerts / Case Management
Investigative Workbench
Orchestration & Automation
FireEye Management
Community
Marketplace
Answers
Research Tools
Ideas
FireEye Network Security
FireEye Email Security
FireEye Endpoint Security
3rd Party Solutions

FireEye



SERVICES AND EXPERTISE

Expertise

Managed Defense

iSight Intelligence

Partner Services

APPS

FireEye Threat Analytics

Advanced Intelligence

Expertise On-Demand

3rd Party Apps

Mandiant Services

Strategic Advisory Services

Technical Assessment Services

Incident Reponse

HELIX

Contextual Intelligence

Alerts / Case Management

Investigative Workbench

Orchestration & Automation

FireEye Management

Community

Marketplace

Answers

Research Tools

Ideas

FireEye Network Security

FireEye Email Security

FireEye Endpoint Security

3rd Party Solutions

NETWORK SECURITY

2017 ACCOMPLISHMENTS

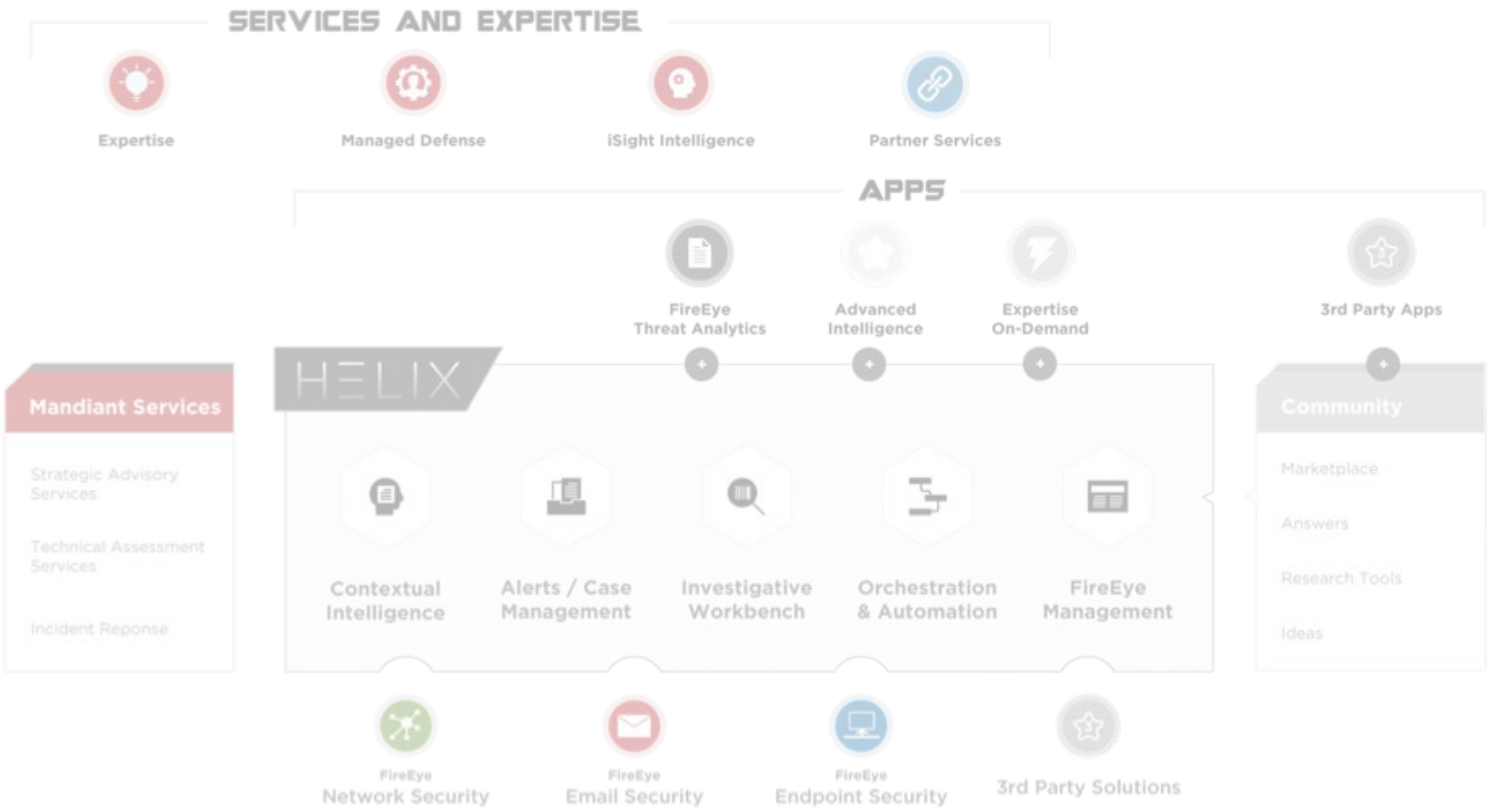
- SmartVision
- Strong growth in lightweight network sensors
- ICE data theft detection capability
- Over 40 new riskware hunting classifications (encrypted office docs, PDF with network connectivity, non-exe communicating on non-standard high port, etc)

LOOKING AHEAD

- New lower-priced form factor for SmartVision
- Expansion of lateral move detection capabilities
- Subscription packaging
- Network sensor for AWS & Azure

50 million

Network malware analyses performed every hour



SERVICES AND EXPERTISE

Expertise

Managed Defense

iSight Intelligence

Partner Services

APPS

FireEye Threat Analytics

Advanced Intelligence

Expertise On-Demand

3rd Party Apps

Mandiant Services

Strategic Advisory Services

Technical Assessment Services

Incident Reponse

HELIX

Contextual Intelligence

Alerts / Case Management

Investigative Workbench

Orchestration & Automation

FireEye Management

Community

Marketplace

Answers

Research Tools

Ideas

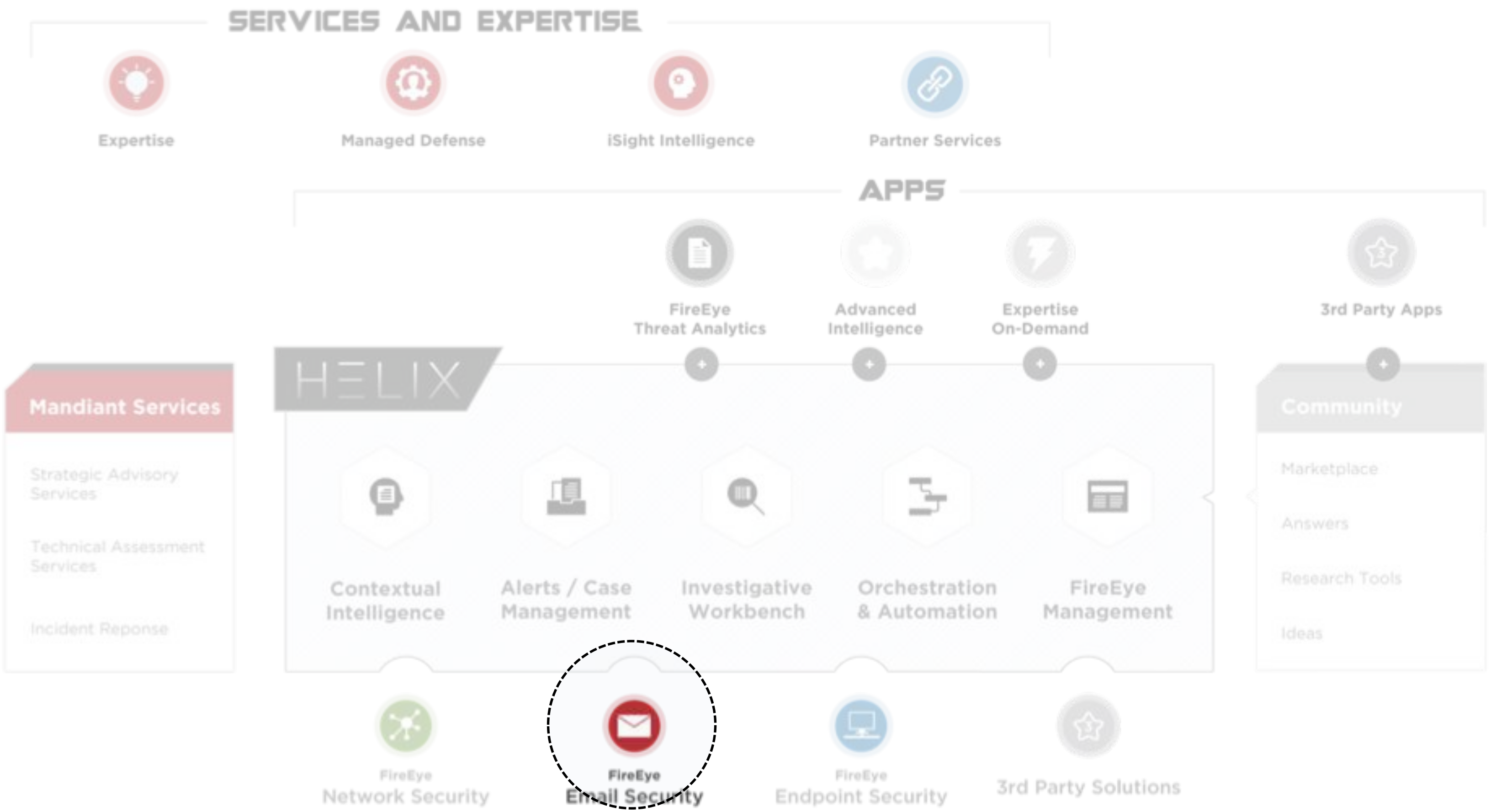
FireEye Network Security

FireEye Email Security

FireEye Endpoint Security

3rd Party Solutions

FireEye


SERVICES AND EXPERTISE
Expertise
Managed Defense
iSight Intelligence
Partner Services
APPS
FireEye
Threat Analytics
Advanced
Intelligence
Expertise
On-Demand
3rd Party Apps
Mandiant Services
Strategic Advisory Services
Technical Assessment Services
Incident Reponse
HELIX
Contextual Intelligence
Alerts / Case Management
Investigative Workbench
Orchestration & Automation
FireEye Management
Community
Marketplace
Answers
Research Tools
Ideas
FireEye
Network Security
FireEye
Email Security
FireEye
Endpoint Security
3rd Party Solutions

EMAIL SECURITY

2017 ACCOMPLISHMENTS

- Integrating The Email Laundry's AV/AS
- New Business Email Compromise (BEC) and improved content analysis
- Major malware and URL detection improvements (FAUDE 3.0)

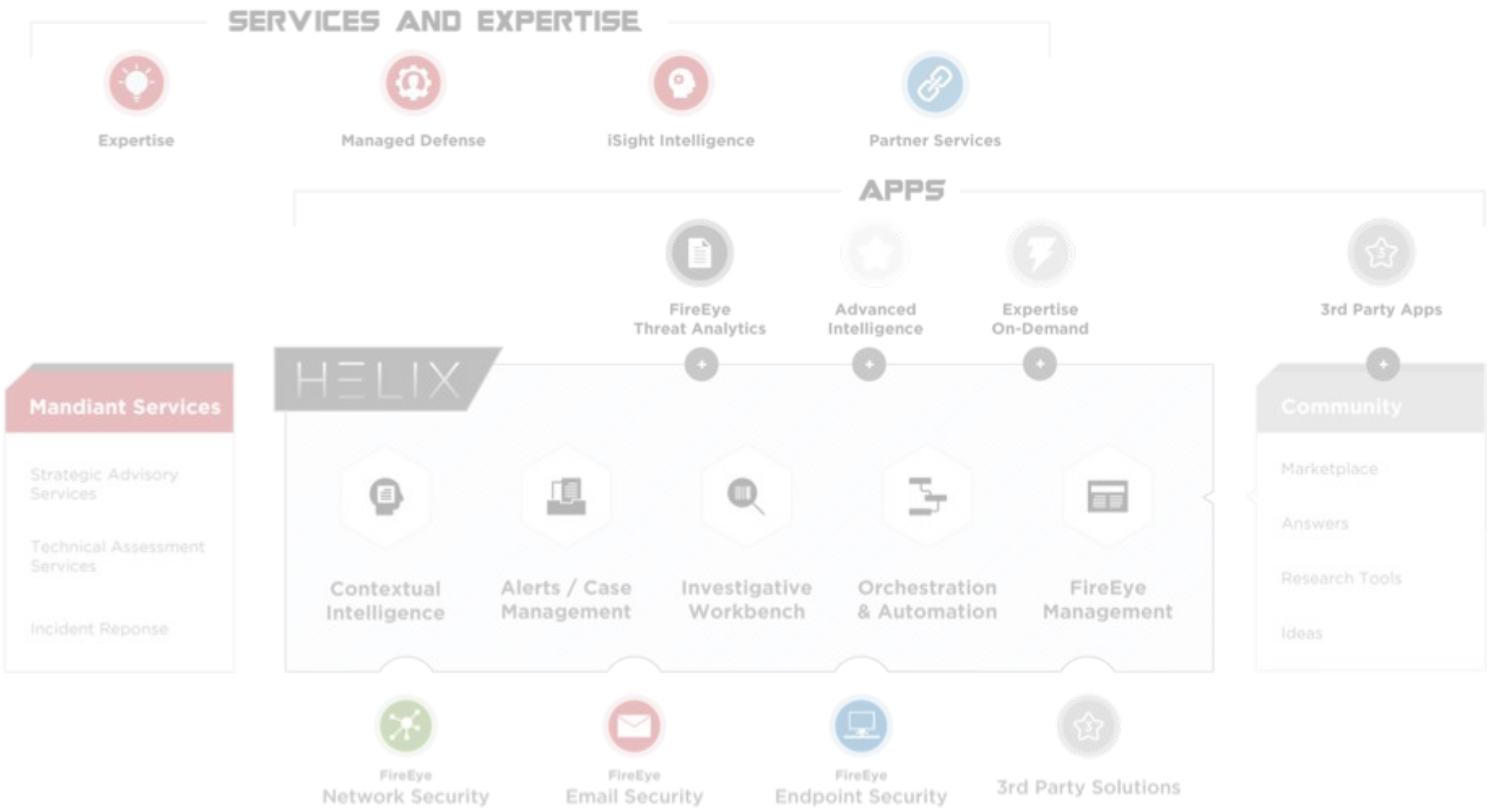
LOOKING AHEAD

- PenPal Personal Trust Matrix
- Threat Campaign Tracking
- Outbound detection
- Secure Email Gateway features
  - DLP, Encryption, Archive, E-Discovery

500K

Credential theft attempts stopped weekly by one new ML module

FireEye



SERVICES AND EXPERTISE

Expertise

Managed Defense

iSight Intelligence

Partner Services

APPS

FireEye Threat Analytics

Advanced Intelligence

Expertise On-Demand

3rd Party Apps

Mandiant Services

- Strategic Advisory Services
- Technical Assessment Services
- Incident Reponse

HELIX

Contextual Intelligence

Alerts / Case Management

Investigative Workbench

Orchestration & Automation

FireEye Management

Community

- Marketplace
- Answers
- Research Tools
- Ideas

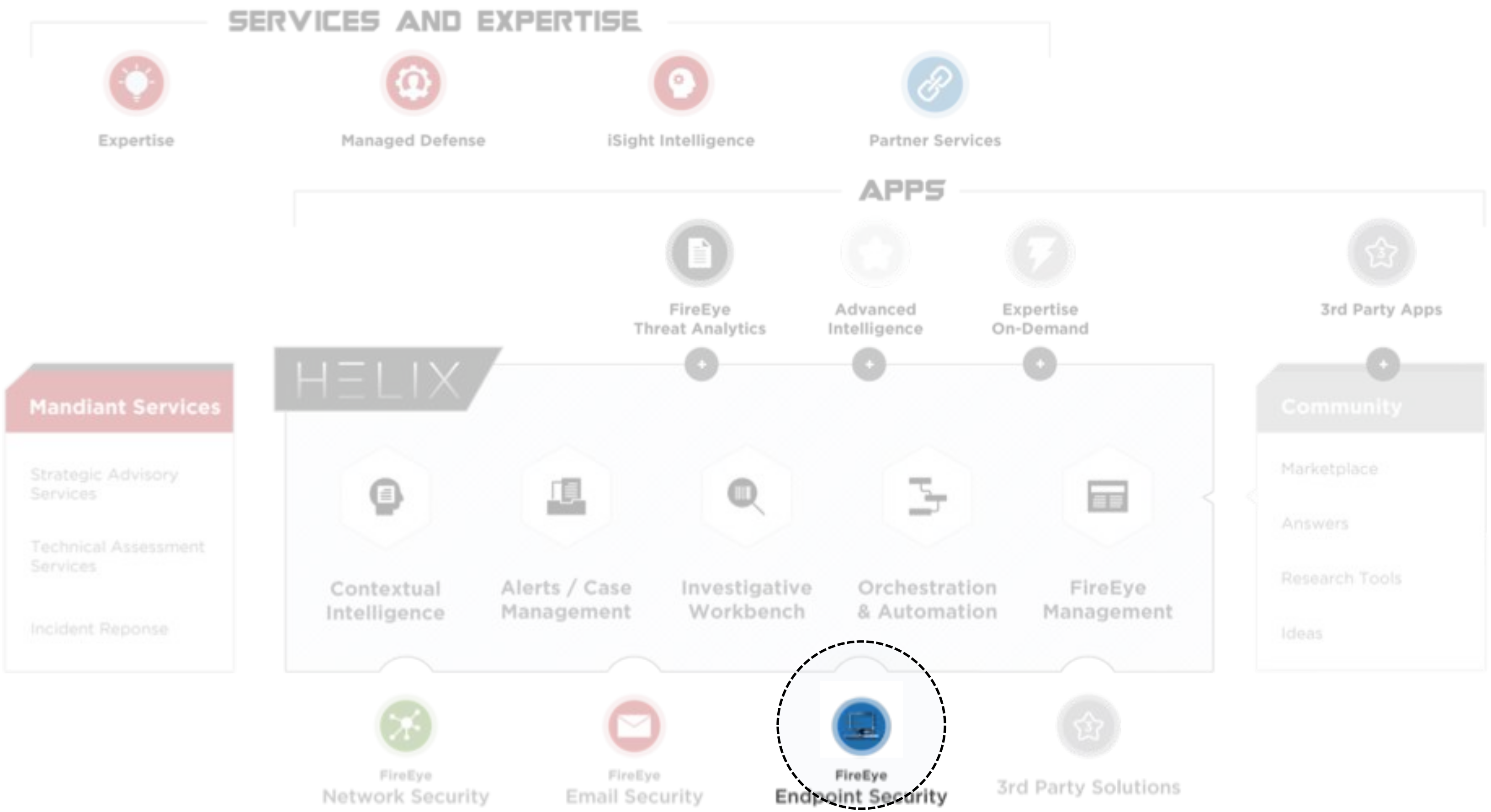
FireEye Network Security

FireEye Email Security

FireEye Endpoint Security

3rd Party Solutions

FireEye


SERVICES AND EXPERTISE
Expertise
Managed Defense
iSight Intelligence
Partner Services
APPS
FireEye Threat Analytics
Advanced Intelligence
Expertise On-Demand
3rd Party Apps
Mandiant Services
Strategic Advisory Services
Technical Assessment Services
Incident Reponse
HELIX
Contextual Intelligence
Alerts / Case Management
Investigative Workbench
Orchestration & Automation
FireEye Management
Community
Marketplace
Answers
Research Tools
Ideas
FireEye Network Security
FireEye Email Security
FireEye Endpoint Security
3rd Party Solutions

ENDPOINT SECURITY

2017 ACCOMPLISHMENTS

- Record year for bookings and customer adoption
- Delivered across hardware and virtual, as well as cloud, Windows, Mac, and Linux
- Integrated AV engine to allow us to compete in the Endpoint Protection Platform (EPP) market

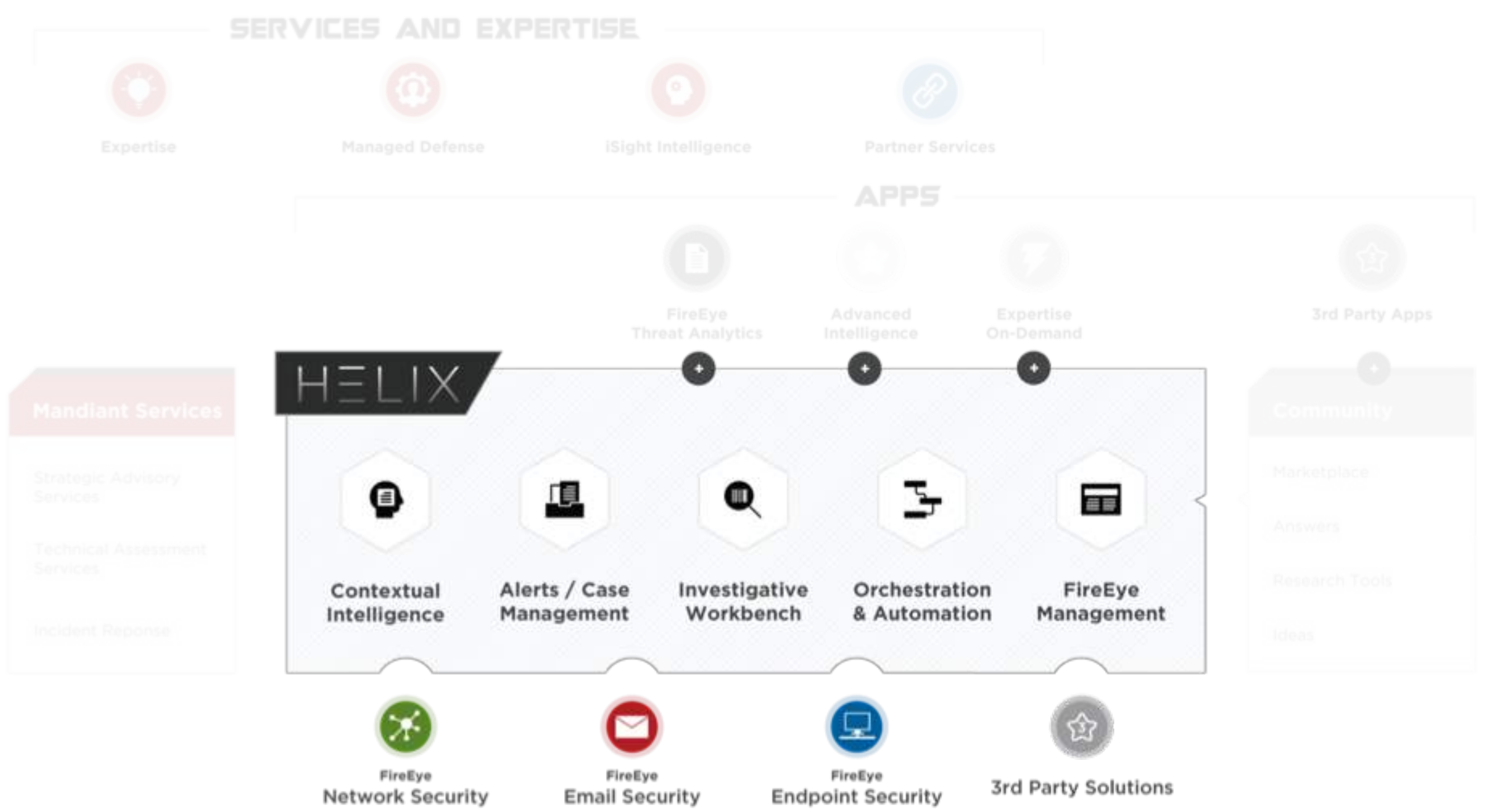
LOOKING AHEAD

- New modularity features provide rapid iteration capability for Mandiant and ICE
- MalwareGuard machine learning-based prevention of ransomware and advanced malware
- Weak Indicator Detection on Endpoint

100%

Detection of last 3 years of Office, Adobe, and browser 0-day exploits with ExploitGuard

FireEye


SERVICES AND EXPERTISE
Expertise
Managed Defense
iSight Intelligence
Partner Services
APPS
FireEye
Threat Analytics
Advanced
Intelligence
Expertise
On-Demand
3rd Party Apps
Mandiant Services
Strategic Advisory Services
Technical Assessment Services
Incident Reponse
HELIX
Contextual Intelligence
Alerts / Case Management
Investigative Workbench
Orchestration & Automation
FireEye Management
Community
Marketplace
Answers
Research Tools
Ideas
FireEye
Network Security
FireEye
Email Security
FireEye
Endpoint Security
3rd Party Solutions

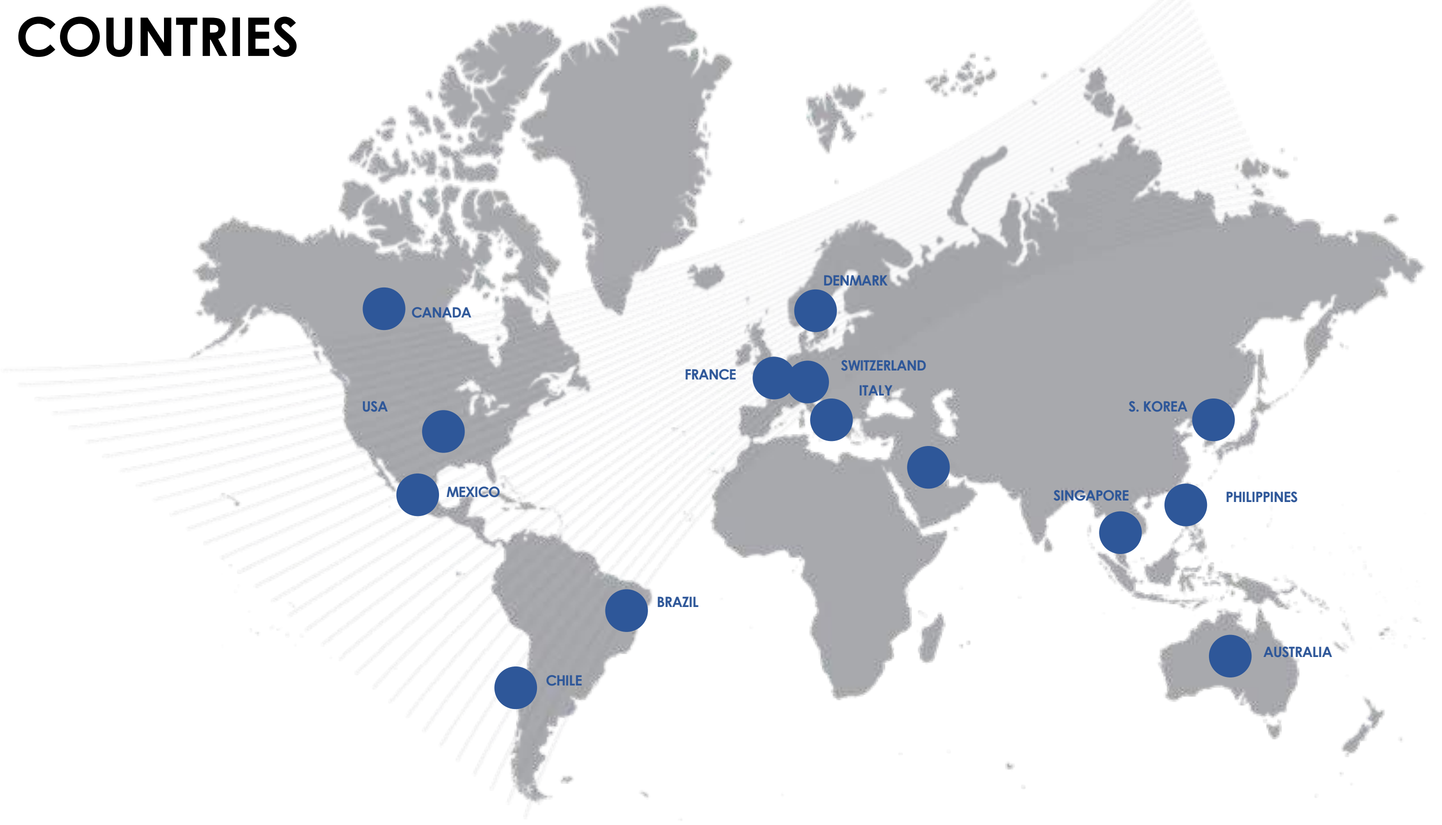
FireEye

X15

- Security orchestration and automation (SOAR) market with full integration of FSO
- Unified platform for our product and services
- Managed Defense and micro-service delivery platform
- 3rd party content and applications, community capabilities start in Q2

HELIX CUSTOMERS

COUNTRIES



240,000 EMPLOYEES

20 EMPLOYEES

INDUSTRIES

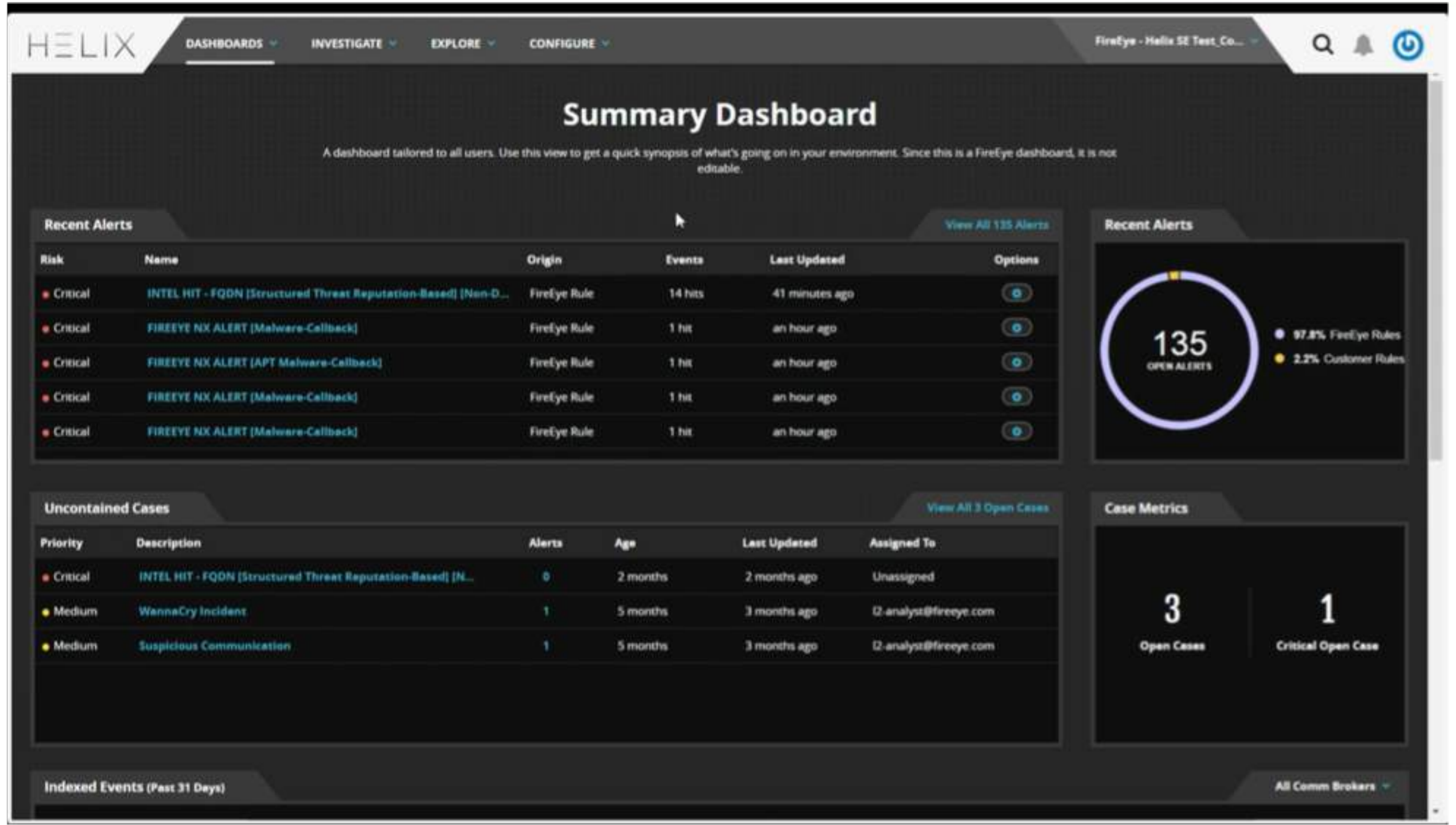
- FINANCIAL SERVICES
- MANUFACTURING
- RETAIL
- MINING
- CONSUMER GOODS
- OIL & GAS
- GOVERNMENT
- HOSPITALITY
- LEGAL
- HEALTH CARE
- TECHNOLOGY

FireEye

HELIX DEMO

Helix Summary Dashboard

- Homepage showing alerts, cases, metrics



Summary Dashboard

A dashboard tailored to all users. Use this view to get a quick synopsis of what's going on in your environment. Since this is a FireEye dashboard, it is not editable.

Recent Alerts — View All 135 Alerts

Risk	Name	Origin	Events	Last Updated	Options
● Critical	INTEL HIT - FQDN [Structured Threat Reputation-Based] [Non-D...	FireEye Rule	14 hits	41 minutes ago	
● Critical	FIREEYE NX ALERT [Malware-Callback]	FireEye Rule	1 hit	an hour ago	
● Critical	FIREEYE NX ALERT [APT Malware-Callback]	FireEye Rule	1 hit	an hour ago	
● Critical	FIREEYE NX ALERT [Malware-Callback]	FireEye Rule	1 hit	an hour ago	
● Critical	FIREEYE NX ALERT [Malware-Callback]	FireEye Rule	1 hit	an hour ago	

Recent Alerts

135 OPEN ALERTS

- ● 97.8% FireEye Rules
- ● 2.2% Customer Rules

Uncontained Cases — View All 3 Open Cases

Priority	Description	Alerts	Age	Last Updated	Assigned To
● Critical	INTEL HIT - FQDN [Structured Threat Reputation-Based] [N...	0	2 months	2 months ago	Unassigned
● Medium	WannaCry Incident	1	5 months	3 months ago	l2-analyst@fireeye.com
● Medium	Suspicious Communication	1	5 months	3 months ago	l2-analyst@fireeye.com

Case Metrics

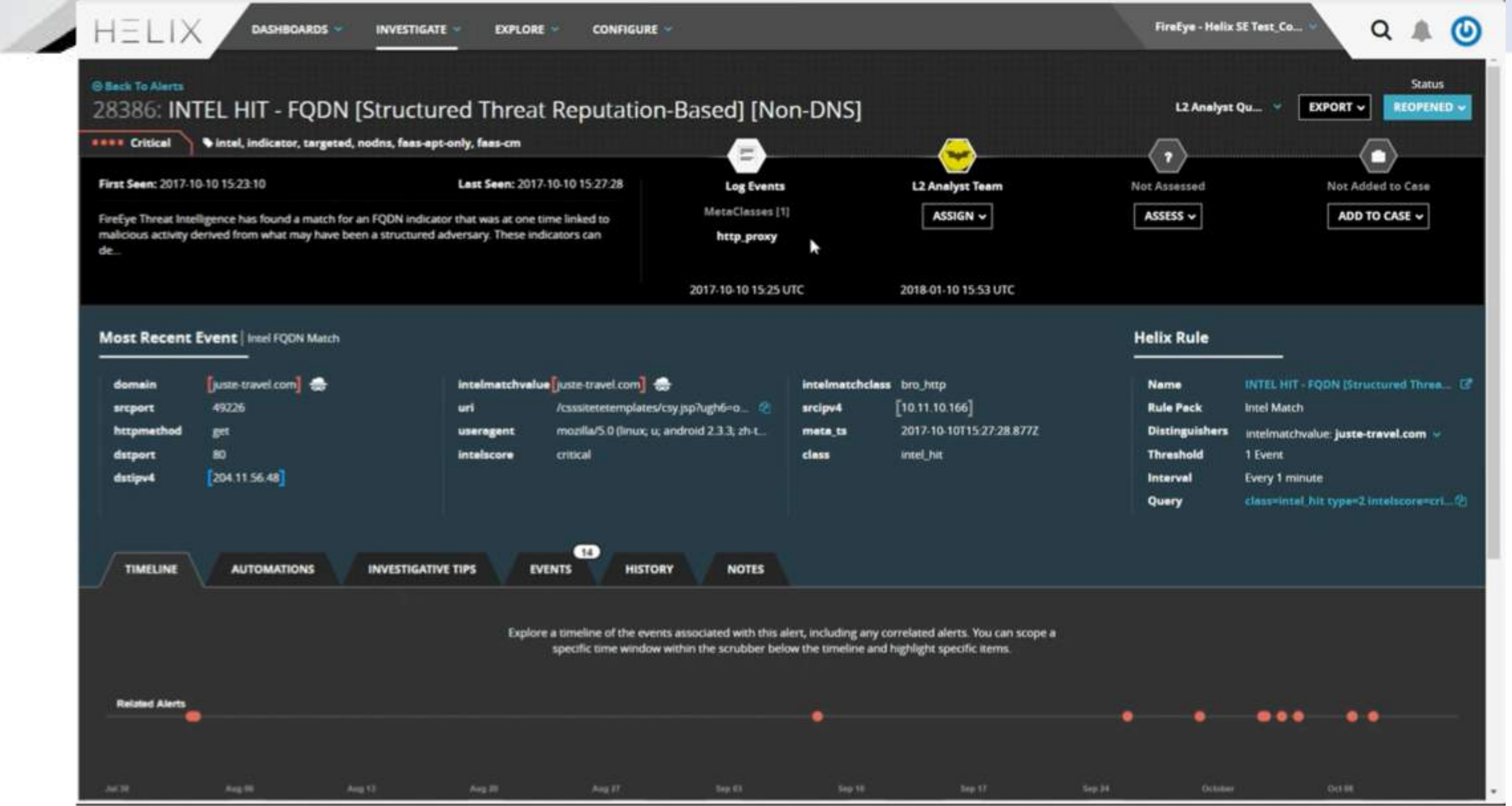
3 Open Cases

1 Critical Open Case

Indexed Events (Past 31 Days) — All Comm Brokers

Alert Detail

- Designed by incident responders to show the most important data for 30+ categories of alerts
- One-click access view gain intelligence, pivot, or get extra help



28386: INTEL HIT - FQDN [Structured Threat Reputation-Based] [Non-DNS]

**** Critical | intel, indicator, targeted, nodns, faas-apt-only, faas-cm

First Seen: 2017-10-10 15:23:10 **Last Seen:** 2017-10-10 15:27:28

FireEye Threat Intelligence has found a match for an FQDN indicator that was at one time linked to malicious activity derived from what may have been a structured adversary. These indicators can de...

Log Events	L2 Analyst Team	Not Assessed	Not Added to Case
MetaClasses [1] http_proxy	ASSIGN	ASSESS	ADD TO CASE
2017-10-10 15:25 UTC	2018-01-10 15:53 UTC		

Most Recent Event | Intel FQDN Match

domain	[juste-travel.com]	intelmatchvalue	[juste-travel.com]	intelmatchclass	bro_http
srcport	49226	uri	/csssitetetemplates/csy.jsp?ugh6=o...	srcipv4	[10.11.10.166]
httpmethod	get	useragent	mozilla/5.0 (linux; u; android 2.3.3; zh-t...	meta_ts	2017-10-10T15:27:28.877Z
dstport	80	intelscore	critical	class	intel_hit
dstipv4	[204.11.56.48]				

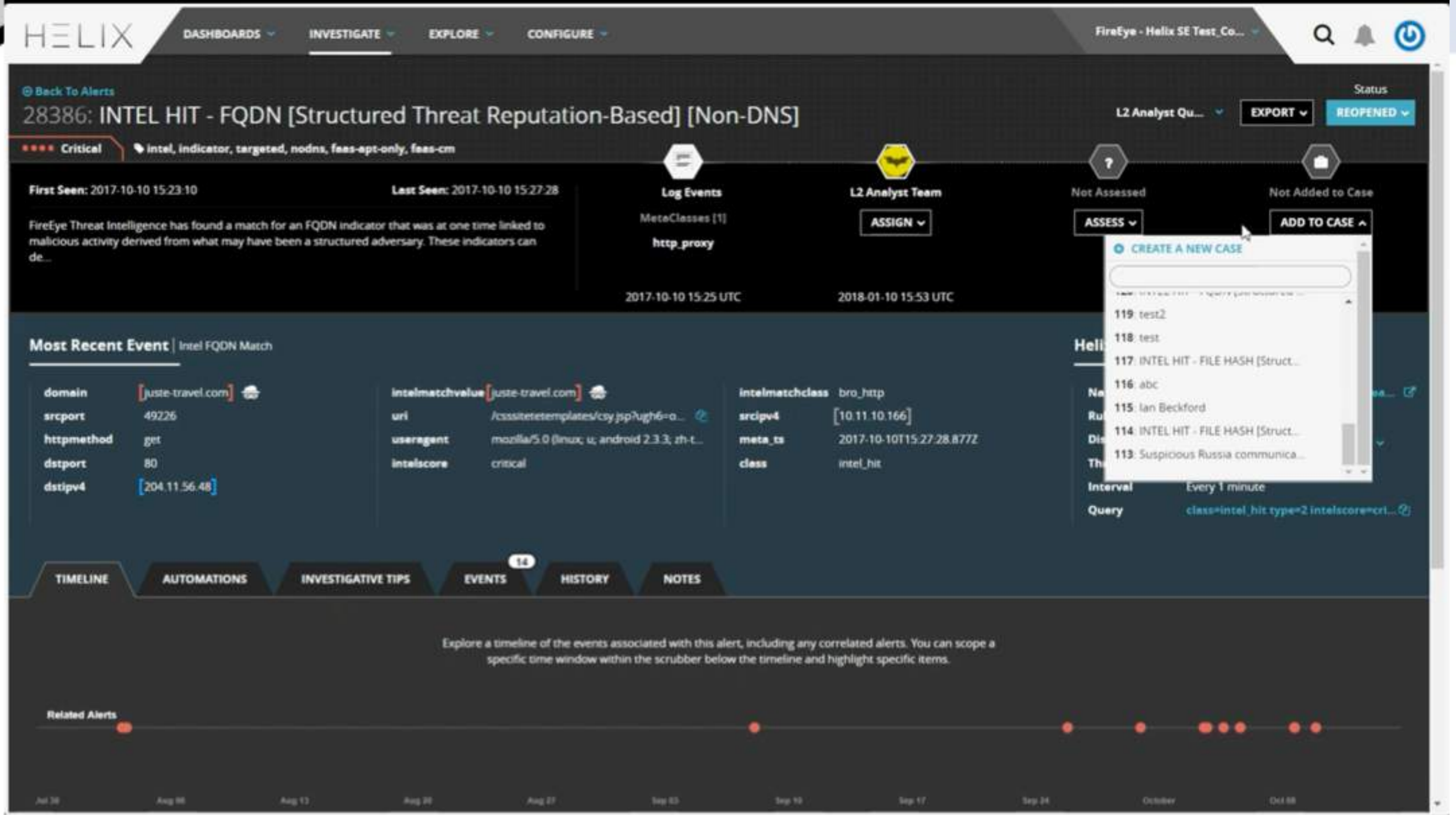
Helix Rule

Name	INTEL HIT - FQDN [Structured Threa...
Rule Pack	Intel Match
Distinguishers	intelmatchvalue: **juste-travel.com**
Threshold	1 Event
Interval	Every 1 minute
Query	class=intel_hit type=2 intelscore=cri...

Explore a timeline of the events associated with this alert, including any correlated alerts. You can scope a specific time window within the scrubber below the timeline and highlight specific items.

Case Assignment

- Integration with case management to quickly assign work



28386: INTEL HIT - FQDN [Structured Threat Reputation-Based] [Non-DNS]

intel, indicator, targeted, nodns, faas-apt-only, faas-cm

First Seen: 2017-10-10 15:23:10 **Last Seen:** 2017-10-10 15:27:28

FireEye Threat Intelligence has found a match for an FQDN indicator that was at one time linked to malicious activity derived from what may have been a structured adversary. These indicators can de...

MetaClasses [1]
http_proxy
2017-10-10 15:25 UTC

2018-01-10 15:53 UTC

119: test2
118: test
117: INTEL HIT - FILE HASH [Struct...
116: abc
115: Ian Beckford
114: INTEL HIT - FILE HASH [Struct...
113: Suspicious Russia communica...

Most Recent Event | Intel FQDN Match

domain	[juste-travel.com]	intelmatchvalue	[juste-travel.com]	intelmatchclass	bro_http
srcport	49226	uri	/csssitetetemplates/csy.jsp?ugh6=o...	srcipv4	[10.11.10.166]
httpmethod	get	useragent	mozilla/5.0 (linux; u; android 2.3.3; zh-t...	meta_ts	2017-10-10T15:27:28.877Z
dstport	80	intelscore	critical	class	intel_hit
dstipv4	[204.11.56.48]				

Heli

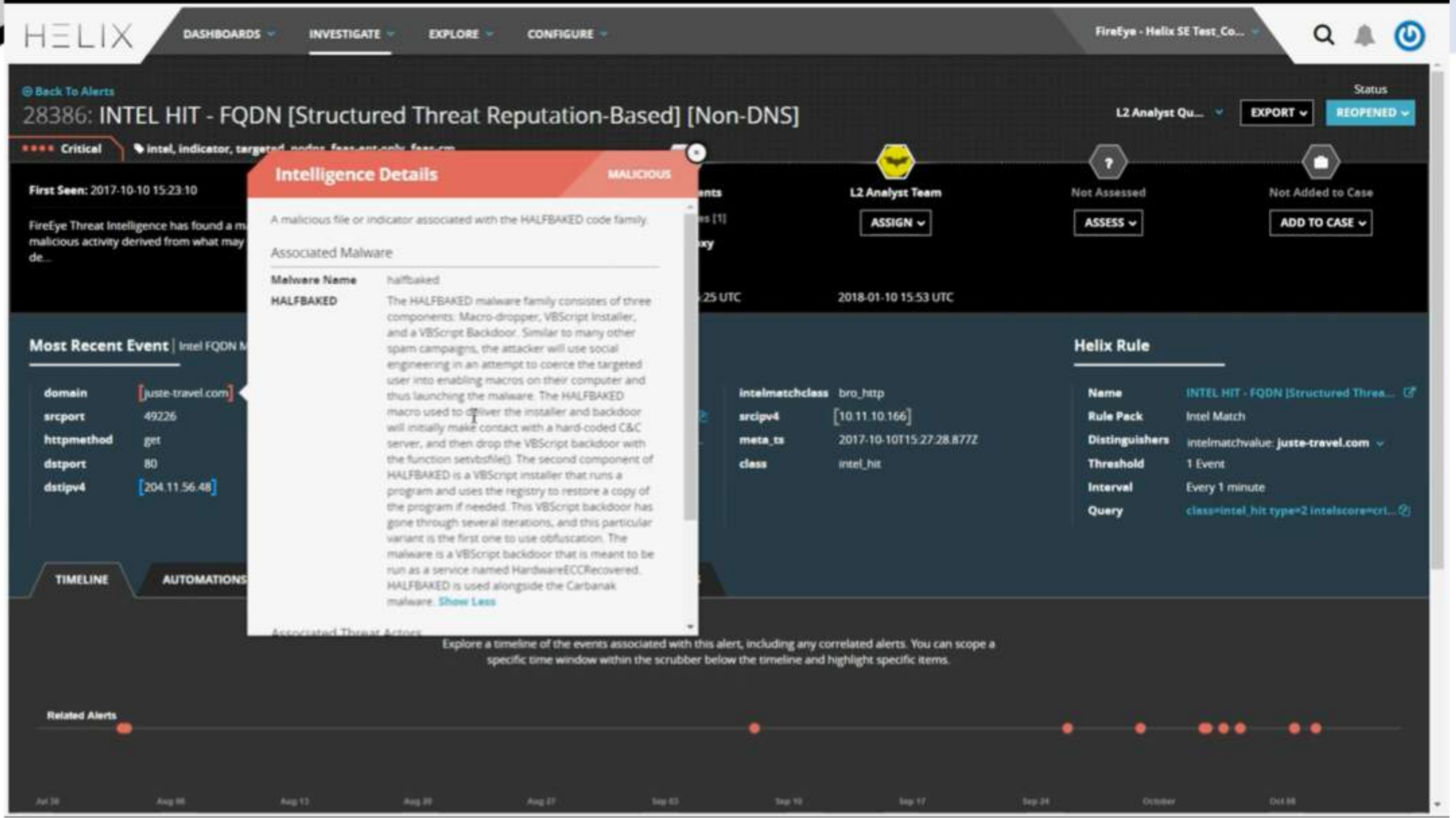
Interval Every 1 minute

Query class=intel_hit type=2 intelscore=cri...

Explore a timeline of the events associated with this alert, including any correlated alerts. You can scope a specific time window within the scrubber below the timeline and highlight specific items.

Intelligence Context

- iSIGHT Intelligence on FireEye and 3rd party alerts



28386: INTEL HIT - FQDN [Structured Threat Reputation-Based] [Non-DNS]

intel, indicator, targeted, nodns, fees-ent-only, fees-cm

First Seen: 2017-10-10 15:23:10

FireEye Threat Intelligence has found a m... malicious activity derived from what may ... de...

2018-01-10 15:53 UTC

Intelligence Details MALICIOUS

A malicious file or indicator associated with the HALFBAKED code family.

Associated Malware

Malware Name	halfbaked
HALFBAKED	The HALFBAKED malware family consistes of three components: Macro-dropper, VBScript Installer, and a VBScript Backdoor. Similar to many other spam campaigns, the attacker will use social engineering in an attempt to coerce the targeted user into enabling macros on their computer and thus launching the malware. The HALFBAKED macro used to deliver the installer and backdoor will initially make contact with a hard-coded C&C server, and then drop the VBScript backdoor with the function setvbsfile(). The second component of HALFBAKED is a VBScript installer that runs a program and uses the registry to restore a copy of the program if needed. This VBScript backdoor has gone through several iterations, and this particular variant is the first one to use obfuscation. The malware is a VBScript backdoor that is meant to be run as a service named HardwareECCRecovered. HALFBAKED is used alongside the Carbanak malware. Show Less

Associated Threat Actors

Most Recent Event | Intel FQDN M...

domain	[juste-travel.com]
srcport	49226
httpmethod	get
dstport	80
dstipv4	[204.11.56.48]

intelmatchclass	bro_http
srcipv4	[10.11.10.166]
meta_ts	2017-10-10T15:27:28.877Z
class	intel_hit

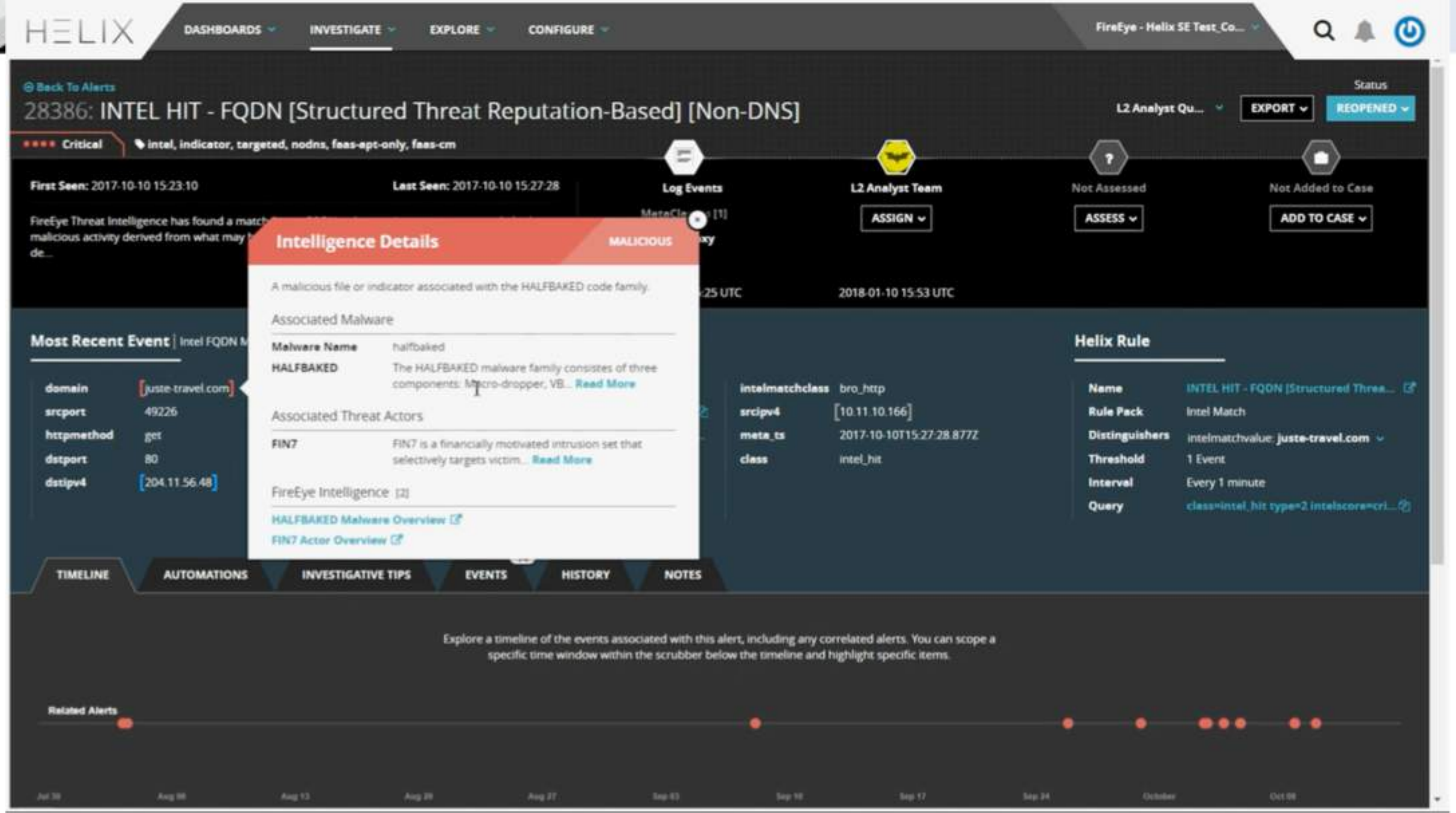
Helix Rule

Name	INTEL HIT - FQDN [Structured Threa...
Rule Pack	Intel Match
Distinguishers	intelmatchvalue: juste-travel.com
Threshold	1 Event
Interval	Every 1 minute
Query	class=intel_hit type=2 intelscore=cri...

Explore a timeline of the events associated with this alert, including any correlated alerts. You can scope a specific time window within the scrubber below the timeline and highlight specific items.

Intelligence Context

- iSIGHT Intelligence on FireEye and 3rd party alerts



28386: INTEL HIT - FQDN [Structured Threat Reputation-Based] [Non-DNS]

Critical · intel, indicator, targeted, nodns, faas-apt-only, faas-cm

First Seen: 2017-10-10 15:23:10 **Last Seen:** 2017-10-10 15:27:28

FireEye Threat Intelligence has found a match ... malicious activity derived from what may ... de...

...25 UTC 2018-01-10 15:53 UTC

Intelligence Details

A malicious file or indicator associated with the HALFBAKED code family.

Associated Malware

Malware Name	halfbaked
HALFBAKED	The HALFBAKED malware family consistes of three components: Macro-dropper, VB... Read More

Associated Threat Actors

FIN7	FIN7 is a financially motivated intrusion set that selectively targets victim... Read More

FireEye Intelligence [2]

HALFBAKED Malware Overview

FIN7 Actor Overview

Most Recent Event | Intel FQDN M...

domain	[juste-travel.com]
srcport	49226
httpmethod	get
dstport	80
dstipv4	[204.11.56.48]

intelmatchclass	bro_http
srcipv4	[10.11.10.166]
meta_ts	2017-10-10T15:27:28.877Z
class	intel_hit

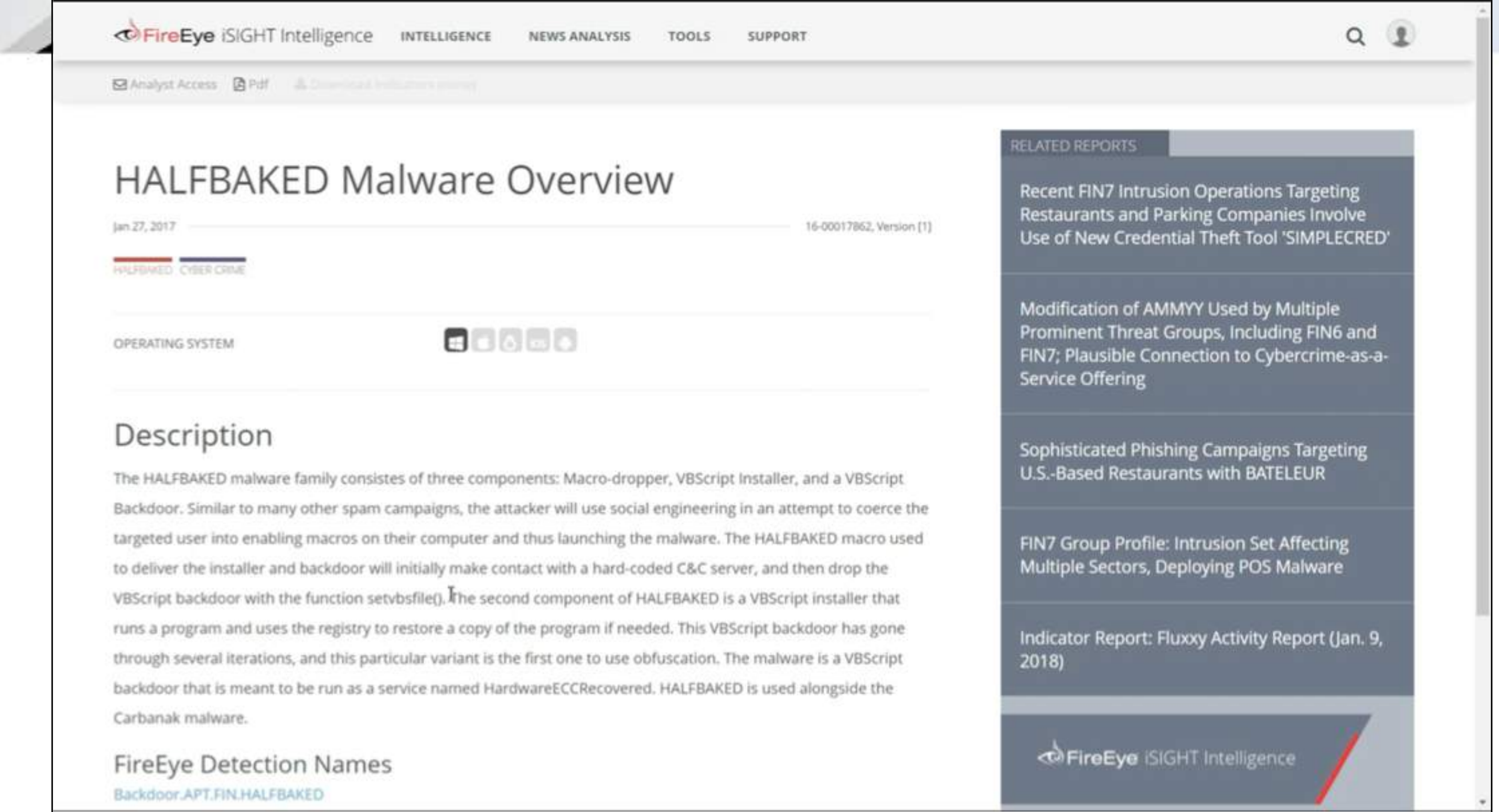
Helix Rule

Name	INTEL HIT - FQDN [Structured Threa...
Rule Pack	Intel Match
Distinguishers	intelmatchvalue: **juste-travel.com**
Threshold	1 Event
Interval	Every 1 minute
Query	class=intel_hit type=2 intelscore=cri...

Explore a timeline of the events associated with this alert, including any correlated alerts. You can scope a specific time window within the scrubber below the timeline and highlight specific items.

iSight Intelligence Portal

- Access to malware family overviews and additional information in the iSIGHT portal
- Basics provided as part of Helix, but upsell opportunities for executive intelligence, long-form finished reports, raw indicators



HALFBAKED Malware Overview

Jan 27, 2017 — 16-00017862, Version [1]

HALFBAKED CYBER CRIME

OPERATING SYSTEM

Description

The HALFBAKED malware family consistes of three components: Macro-dropper, VBScript Installer, and a VBScript Backdoor. Similar to many other spam campaigns, the attacker will use social engineering in an attempt to coerce the targeted user into enabling macros on their computer and thus launching the malware. The HALFBAKED macro used to deliver the installer and backdoor will initially make contact with a hard-coded C&C server, and then drop the VBScript backdoor with the function setvbsfile(). The second component of HALFBAKED is a VBScript installer that runs a program and uses the registry to restore a copy of the program if needed. This VBScript backdoor has gone through several iterations, and this particular variant is the first one to use obfuscation. The malware is a VBScript backdoor that is meant to be run as a service named HardwareECCRecovered. HALFBAKED is used alongside the Carbanak malware.

FireEye Detection Names

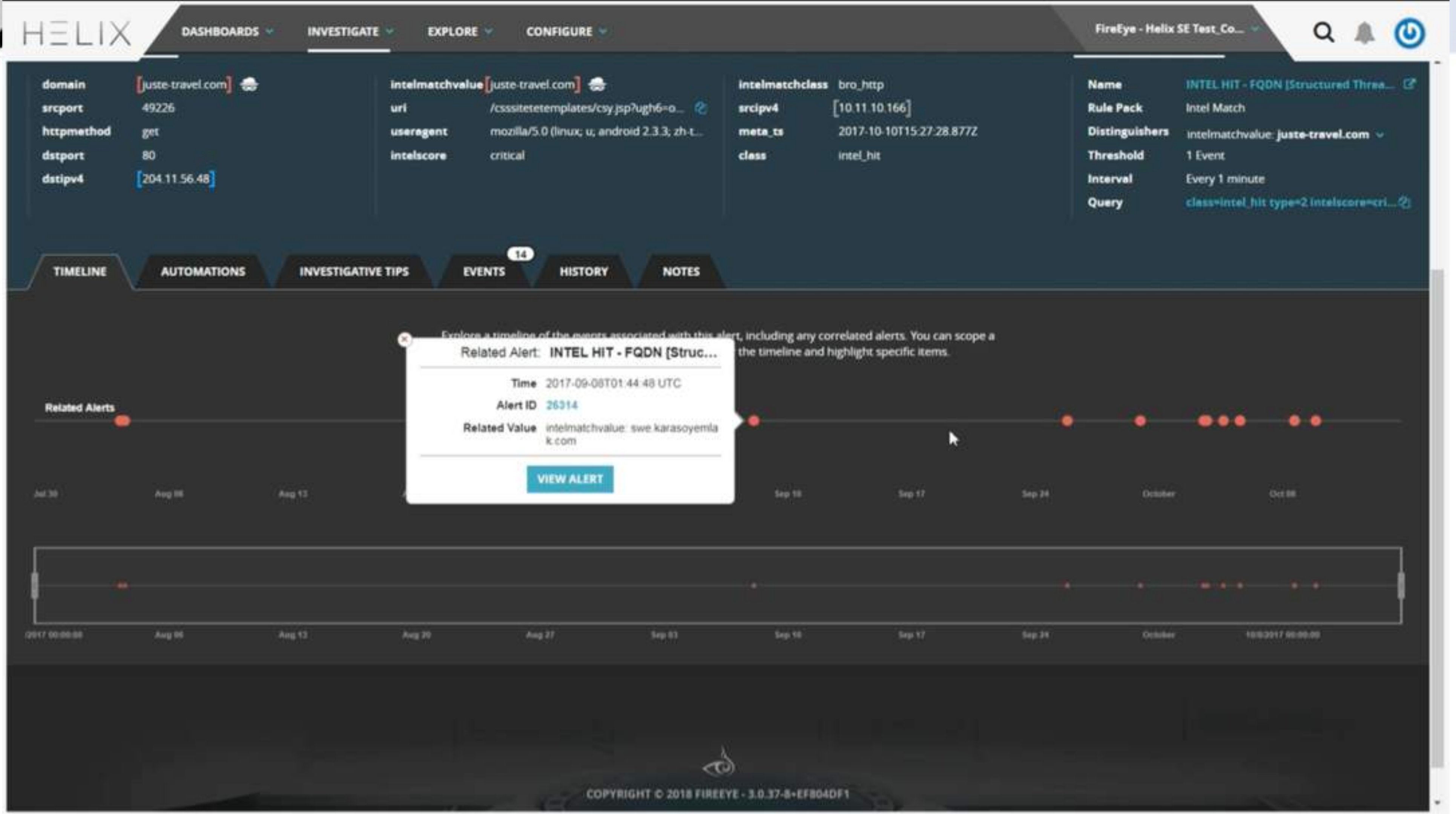
Backdoor.APT.FIN.HALFBAKED

RELATED REPORTS

- Recent FIN7 Intrusion Operations Targeting Restaurants and Parking Companies Involve Use of New Credential Theft Tool 'SIMPLECRED'
- Modification of AMMYY Used by Multiple Prominent Threat Groups, Including FIN6 and FIN7; Plausible Connection to Cybercrime-as-a-Service Offering
- Sophisticated Phishing Campaigns Targeting U.S.-Based Restaurants with BATELEUR
- FIN7 Group Profile: Intrusion Set Affecting Multiple Sectors, Deploying POS Malware
- Indicator Report: Fluxxy Activity Report (Jan. 9, 2018)

Timeline

- Timeline displays related events chronologically for rapid context



domain [juste-travel.com]
srcport 49226
httpmethod get
dstport 80
dstipv4 [204.11.56.48]

intelmatchvalue [juste-travel.com]
uri /csssitetetemplates/csy.jsp?ugh6=o...
useragent mozilla/5.0 (linux; u; android 2.3.3; zh-t...
intelscore critical

intelmatchclass bro_http
srcipv4 [10.11.10.166]
meta_ts 2017-10-10T15:27:28.877Z
class intel_hit

Name INTEL HIT - FQDN [Structured Threa...
Rule Pack Intel Match
Distinguishers intelmatchvalue: juste-travel.com
Threshold 1 Event
Interval Every 1 minute
Query class=intel_hit type=2 intelscore=cri...

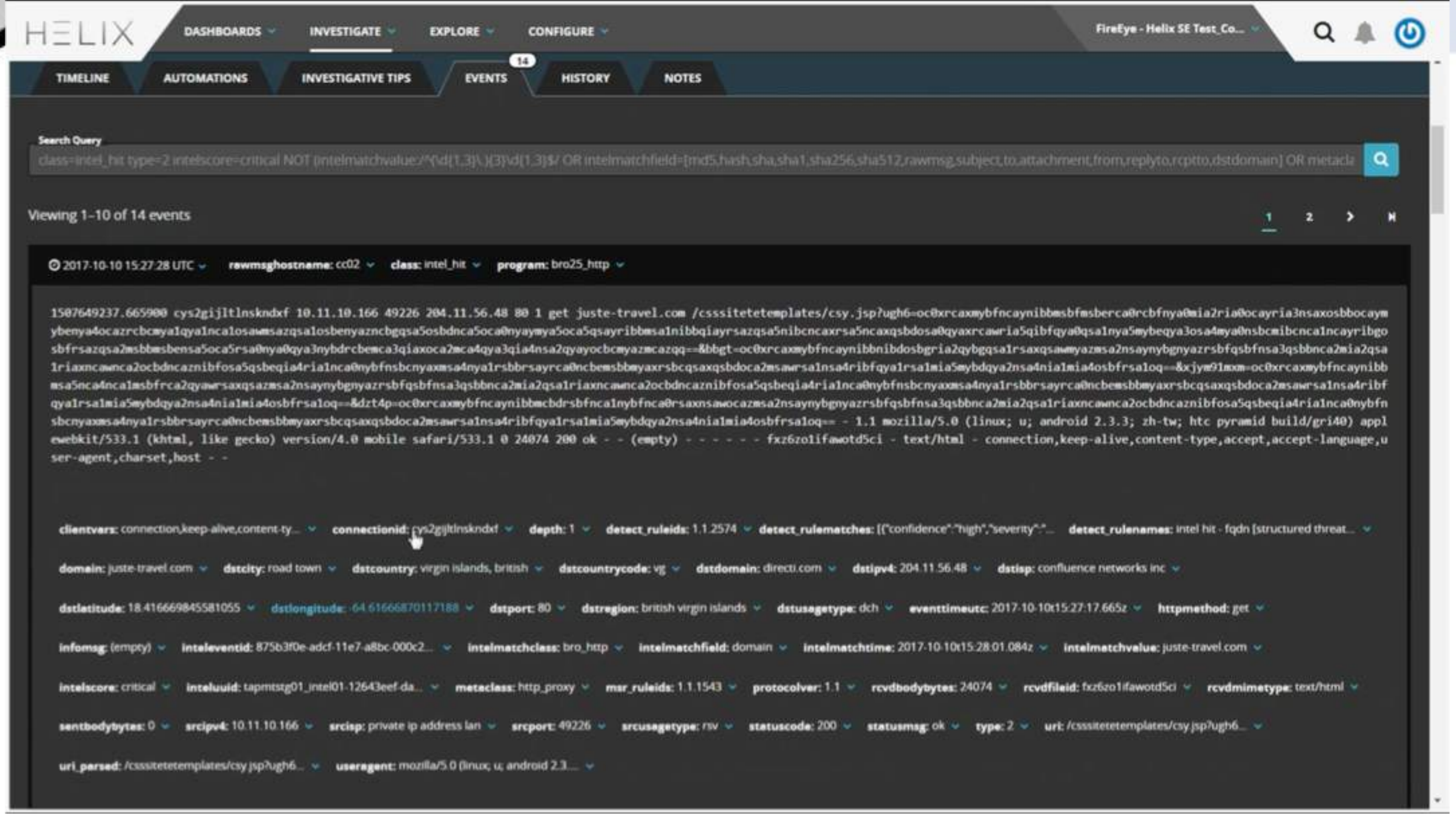
Explore a timeline of the events associated with this alert, including any correlated alerts. You can scope a ... the timeline and highlight specific items.

Related Alert: INTEL HIT - FQDN [Struc...

Time 2017-09-08T01:44:48 UTC
Alert ID 26314
Related Value intelmatchvalue: swe.karasoyemlak.com

Raw Data

- Raw event and alert data available for further analysis and archive



Search Query
class=intel_hit type=2 intelscore=critical NOT (intelmatchvalue:/^(\d{1,3}\.){3}\d{1,3}$/ OR intelmatchfield=[md5,hash,sha,sha1,sha256,sha512,rawmsg,subject,to,attachment,from,replyto,rcptto,dstdomain] OR metacla

Viewing 1-10 of 14 events

1 2

2017-10-10 15:27:28 UTC **rawmsghostname:** cc02 **class:** intel_hit **program:** bro25_http

```
1507649237.665900 cys2gijltlnskndxf 10.11.10.166 49226 204.11.56.48 80 1 get juste-travel.com /csssitetetemplates/csy.jsp?ugh6=oc0xrcaxmybfncaynibbmsbfmsberca0rcbfnya0mia2ria0ocayria3nsaxosbbocaym
ybenya4ocazrcbcmya1qya1nca1osawmsazqsa1osbenyazncbgqsa5osbdnca5oca0nyaymya5oca5qsayribbmsa1nibbqiayrsazqsa5nibcncaxrsa5ncaxqsbdosa0qyaxrcawria5qibfqya0qsa1nya5mybeqya3osa4mya0nsbcmibcnca1ncayribgo
sbfrsazqsa2msbbmsbensa5oca5rsa0nya0qya3nybdrcbemca3qiaxoca2mca4qya3qia4nsa2qyayocbcmyazmcazqq==&bbgt=oc0xrcaxmybfncaynibbnibdosbgria2qybgqsa1rsaxqsawmyazmsa2nsaynybgnyazrsbfqsbfnsa3qsbbnca2mia2qsa
1riaxncawnca2ocbdncaznibfosa5qsbeqia4ria1nca0nybfnsbcnyaxmsa4nya1rsbbrsayrca0ncbemsbbmyaxrsbcqsaxqsbdoca2msawrsa1nsa4ribfqya1rsa1mia5mybdqya2nsa4nia1mia4osbfrsa1oq==&xjym91mxm=oc0xrcaxmybfncaynibb
msa5nca4nca1msbfrca2qyawrsaxqsazmsa2nsaynybgnyazrsbfqsbfnsa3qsbbnca2mia2qsa1riaxncawnca2ocbdncaznibfosa5qsbeqia4ria1nca0nybfnsbcnyaxmsa4nya1rsbbrsayrca0ncbemsbbmyaxrsbcqsaxqsbdoca2msawrsa1nsa4ribf
qya1rsa1mia5mybdqya2nsa4nia1mia4osbfrsa1oq==&dzt4p=oc0xrcaxmybfncaynibbmcbdrsbfnca1nybfnca0rsaxnsawocazmsa2nsaynybgnyazrsbfqsbfnsa3qsbbnca2mia2qsa1riaxncawnca2ocbdncaznibfosa5qsbeqia4ria1nca0nybfn
sbcnyaxmsa4nya1rsbbrsayrca0ncbemsbbmyaxrsbcqsaxqsbdoca2msawrsa1nsa4ribfqya1rsa1mia5mybdqya2nsa4nia1mia4osbfrsa1oq== - 1.1 mozilla/5.0 (linux; u; android 2.3.3; zh-tw; htc pyramid build/gri40) appl
ewebkit/533.1 (khtml, like gecko) version/4.0 mobile safari/533.1 0 24074 200 ok - - (empty) - - - - - - fxz6zo1ifawotd5ci - text/html - connection,keep-alive,content-type,accept,accept-language,u
ser-agent,charset,host - -
```

clientvars: connection,keep-alive,content-ty... **connectionid:** cys2gijltlnskndxf **depth:** 1 **detect_ruleids:** 1.1.2574 **detect_rulematches:** [{"confidence":"high","severity":"... **detect_rulenames:** intel hit - fqdn [structured threat...

domain: juste-travel.com **dstcity:** road town **dstcountry:** virgin islands, british **dstcountrycode:** vg **dstdomain:** directi.com **dstipv4:** 204.11.56.48 **dstisp:** confluence networks inc

dstlatitude: 18.416669845581055 **dstlongitude:** -64.61666870117188 **dstport:** 80 **dstregion:** british virgin islands **dstusagetype:** dch **eventtimeutc:** 2017-10-10t15:27:17.665z **httpmethod:** get

infomsg: (empty) **inteleventid:** 875b3f0e-adcf-11e7-a8bc-000c2... **intelmatchclass:** bro_http **intelmatchfield:** domain **intelmatchtime:** 2017-10-10t15:28:01.084z **intelmatchvalue:** juste-travel.com

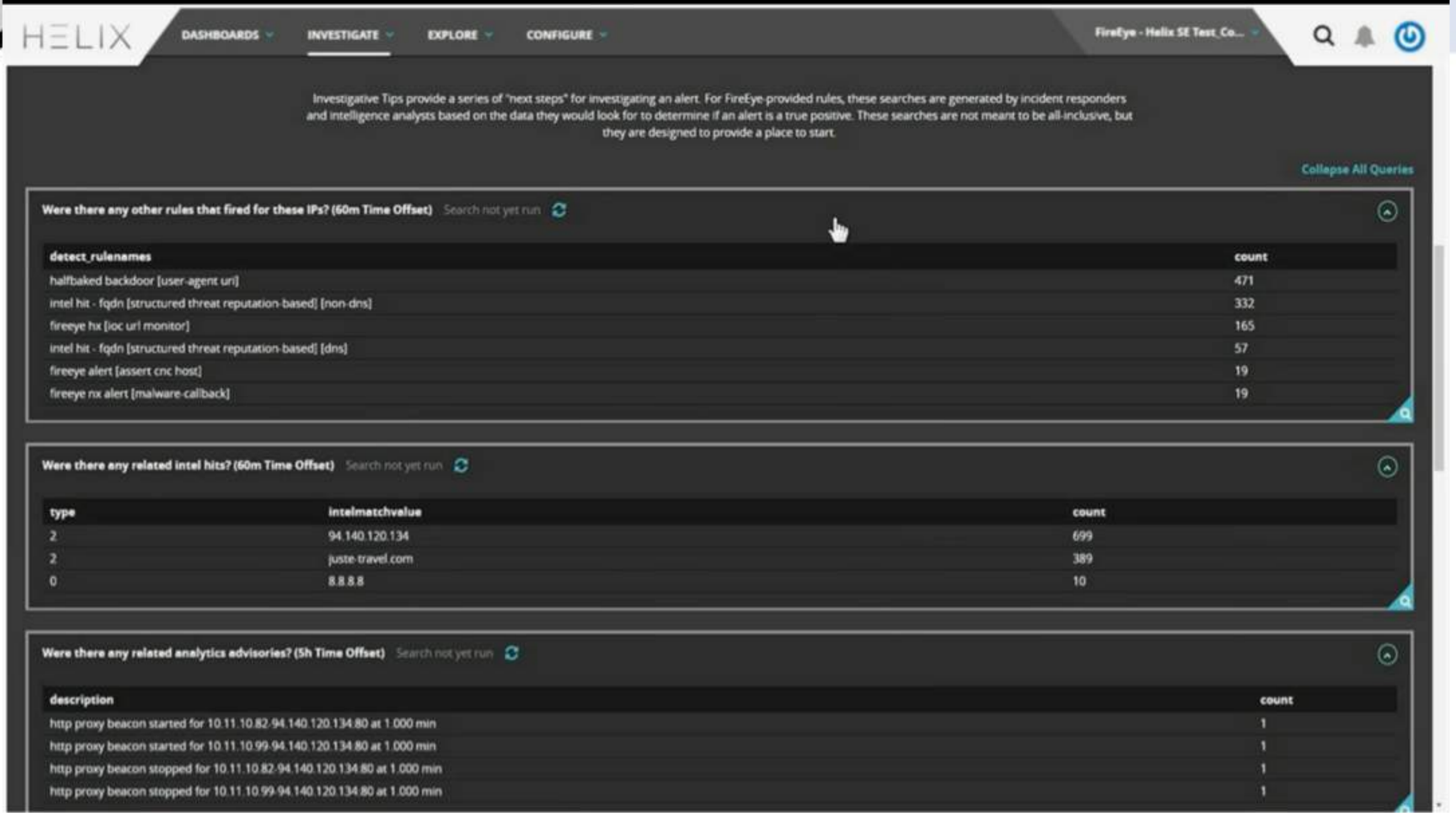
intelscore: critical **inteluuid:** tapmtstg01_intel01-12643eef-da... **metaclass:** http_proxy **msr_ruleids:** 1.1.1543 **protocolver:** 1.1 **rcvdbodybytes:** 24074 **rcvdfileid:** fxz6zo1ifawotd5ci **rcvdmimetype:** text/html

sentbodybytes: 0 **srcipv4:** 10.11.10.166 **srcisp:** private ip address lan **srcport:** 49226 **srcusagetype:** rsv **statuscode:** 200 **statusmsg:** ok **type:** 2 **uri:** /csssitetetemplates/csy.jsp?ugh6...

uri_parsed: /csssitetetemplates/csy.jsp?ugh6... **useragent:** mozilla/5.0 (linux; u; android 2.3....

Guided Investigations

- Investigative tips and next steps for less experienced investigators



Investigative Tips provide a series of "next steps" for investigating an alert. For FireEye-provided rules, these searches are generated by incident responders and intelligence analysts based on the data they would look for to determine if an alert is a true positive. These searches are not meant to be all-inclusive, but they are designed to provide a place to start.

Were there any other rules that fired for these IPs? (60m Time Offset) Search not yet run

detect_rulenames	count
halfbaked backdoor [user-agent uri]	471
intel hit - fqdn [structured threat reputation-based] [non-dns]	332
fireeye hx [ioc url monitor]	165
intel hit - fqdn [structured threat reputation-based] [dns]	57
fireeye alert [assert cnc host]	19
fireeye nx alert [malware-callback]	19

Were there any related intel hits? (60m Time Offset) Search not yet run

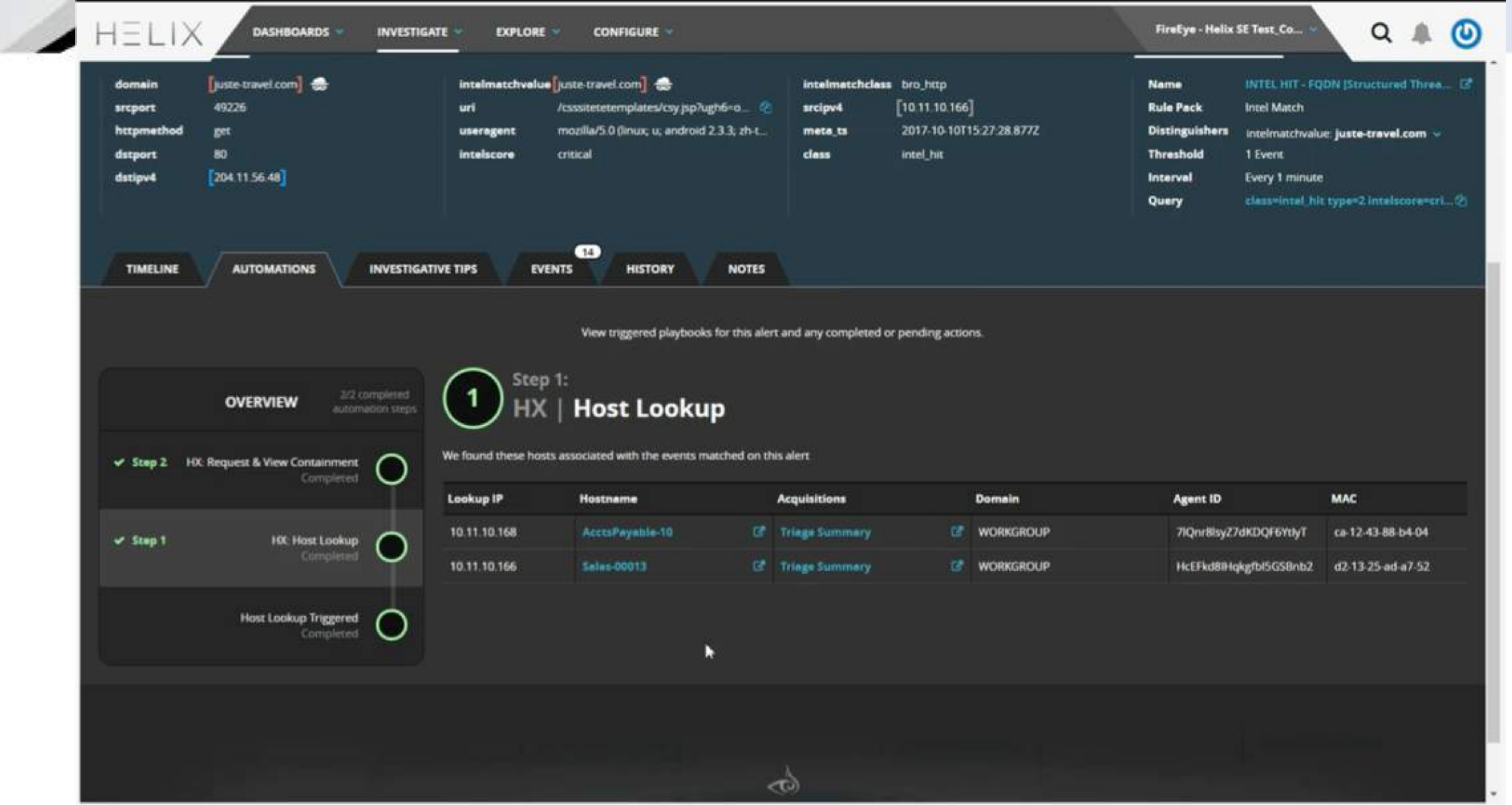
type	intelmatchvalue	count
2	94.140.120.134	699
2	juste-travel.com	389
0	8.8.8.8	10

Were there any related analytics advisories? (5h Time Offset) Search not yet run

description	count
http proxy beacon started for 10.11.10.82-94.140.120.134:80 at 1.000 min	1
http proxy beacon started for 10.11.10.99-94.140.120.134:80 at 1.000 min	1
http proxy beacon stopped for 10.11.10.82-94.140.120.134:80 at 1.000 min	1
http proxy beacon stopped for 10.11.10.99-94.140.120.134:80 at 1.000 min	1

Automation: Host Containment Phase 1

- Host lookup to retrieve additional data on host
- Lookup can be triggered by any alert: FireEye or 3rd party



domain	[juste-travel.com]	intelmatchvalue	[juste-travel.com]	intelmatchclass	bro_http	Name	INTEL HIT - FQDN [Structured Threa...
srcport	49226	uri	/csssitetetemplates/csy.jsp?ugh6=o...	srcipv4	[10.11.10.166]	Rule Pack	Intel Match
httpmethod	get	useragent	mozilla/5.0 (linux; u; android 2.3.3; zh-t...	meta_ts	2017-10-10T15:27:28.877Z	Distinguishers	intelmatchvalue: **juste-travel.com**
dstport	80	intelscore	critical	class	intel_hit	Threshold	1 Event
dstipv4	[204.11.56.48]					Interval	Every 1 minute
						Query	class=intel_hit type=2 intelscore=cri...

View triggered playbooks for this alert and any completed or pending actions.

OVERVIEW 2/2 completed automation steps

✓ Step 2 HX: Request & View Containment Completed

✓ Step 1 HX: Host Lookup Completed

Host Lookup Triggered Completed

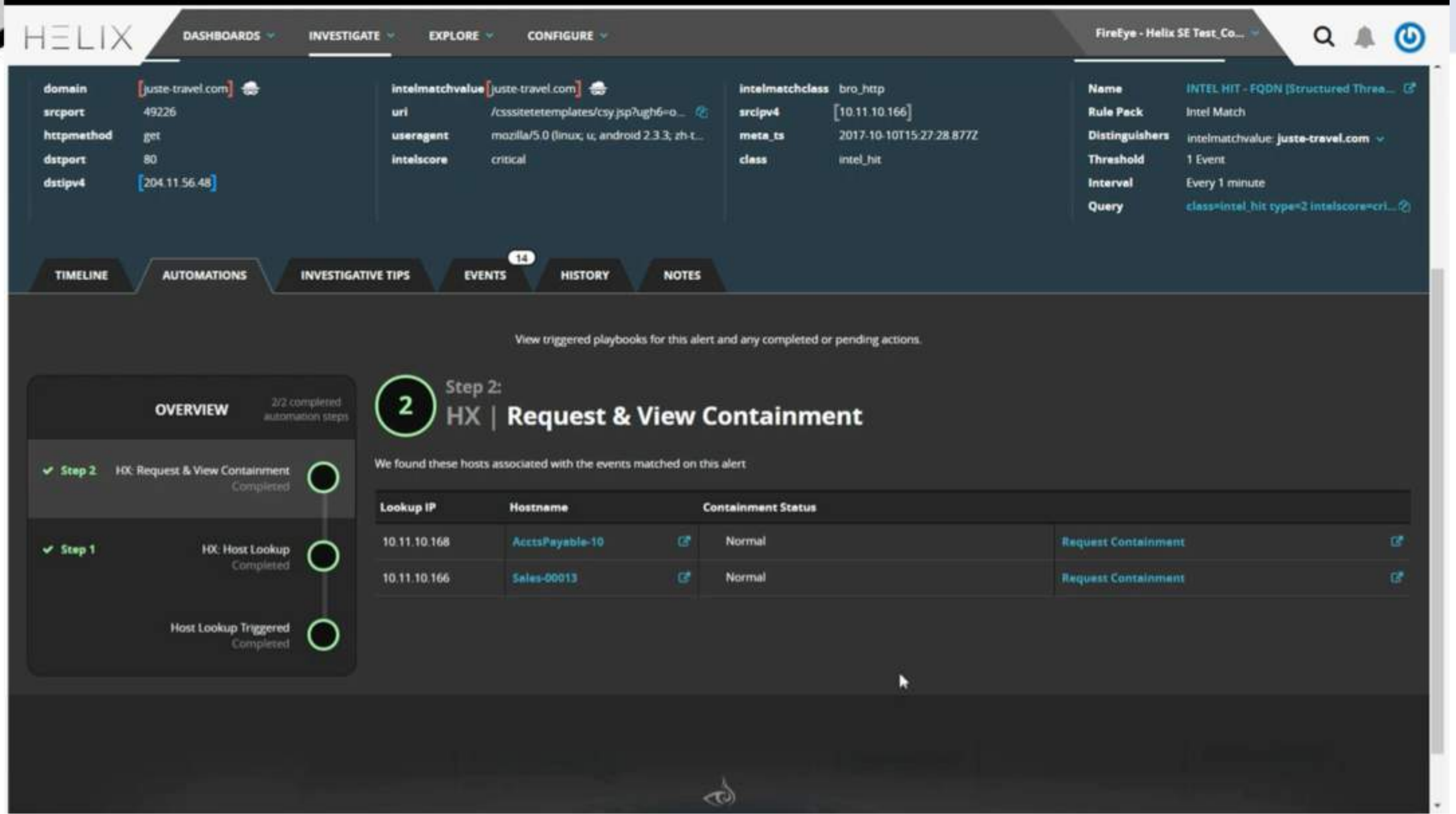
Step 1:
HX | Host Lookup

We found these hosts associated with the events matched on this alert

Lookup IP	Hostname	Acquisitions	Domain	Agent ID	MAC
10.11.10.168	AcctsPayable-10	Triage Summary	WORKGROUP	7lQnr8lsyZ7dKDQF6YtlyT	ca-12-43-88-b4-04
10.11.10.166	Sales-00013	Triage Summary	WORKGROUP	HcEFkd8lHqkgfbl5GSBnb2	d2-13-25-ad-a7-52

Automation: Host Containment Phase 2

- Request containment to neutralize impacted hosts



domain	[juste-travel.com]
srcport	49226
httpmethod	get
dstport	80
dstipv4	[204.11.56.48]

intelmatchvalue	[juste-travel.com]
uri	/csssitetetemplates/csy.jsp?ugh6=o...
useragent	mozilla/5.0 (linux; u; android 2.3.3; zh-t...
intelscore	critical

intelmatchclass	bro_http
srcipv4	[10.11.10.166]
meta_ts	2017-10-10T15:27:28.877Z
class	intel_hit

Name	INTEL HIT - FQDN [Structured Threa...
Rule Pack	Intel Match
Distinguishers	intelmatchvalue: **juste-travel.com**
Threshold	1 Event
Interval	Every 1 minute
Query	class=intel_hit type=2 intelscore=cri...

View triggered playbooks for this alert and any completed or pending actions.

OVERVIEW 2/2 completed automation steps

- ✓ Step 2 HX: Request & View Containment Completed
- ✓ Step 1 HX: Host Lookup Completed
- Host Lookup Triggered Completed

2 Step 2:

HX | Request & View Containment

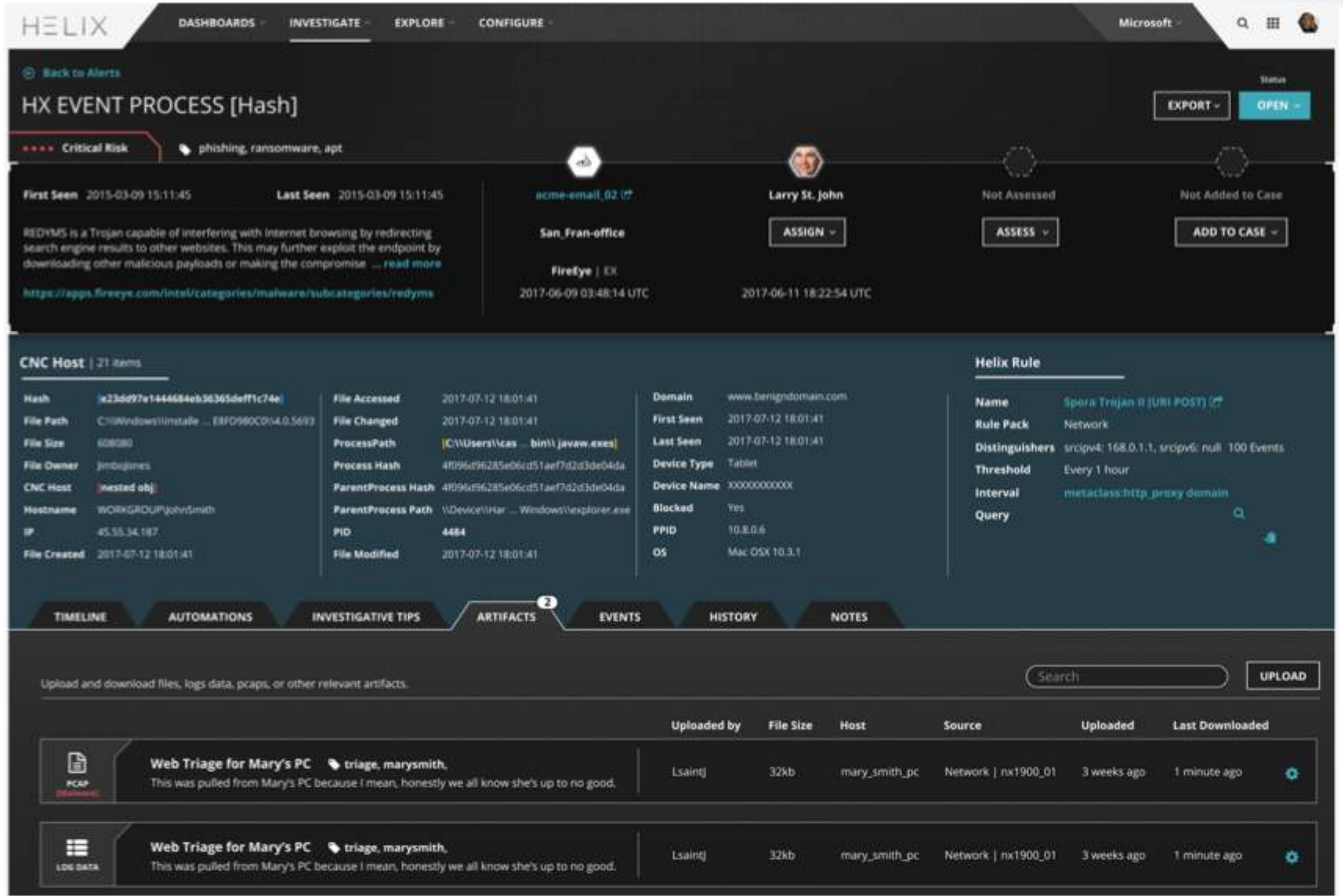
We found these hosts associated with the events matched on this alert

Lookup IP	Hostname	Containment Status	
10.11.10.168	AcctsPayable-10	Normal	Request Containment
10.11.10.166	Sales-00013	Normal	Request Containment

COMING SOON:

Artifact Collection & Management for FireEye Devices

- Adding a new ”Artifacts” tab in the alert details page to enable collection from FireEye devices.
- Combination of auto-collected artifacts and manual acquisitions as needed



HX EVENT PROCESS [Hash]

•••• Critical Risk

phishing, ransomware, apt

First Seen 2015-03-09 15:11:45 Last Seen 2015-03-09 15:11:45

REDYMS is a Trojan capable of interfering with Internet browsing by redirecting search engine results to other websites. This may further exploit the endpoint by downloading other malicious payloads or making the compromise ... read more

https://apps.fireeye.com/intel/categories/malware/subcategories/redyms

acme-email_02
San_Fran-office
FireEye | EX
2017-06-09 03:48:14 UTC

Larry St. John
2017-06-11 18:22:54 UTC

Not Assessed

Not Added to Case

CNC Host | 21 items

Hash	e23dd97e1444684eb36365deff1c74e	File Accessed	2017-07-12 18:01:41	Domain	www.benigndomain.com
File Path	C:\\Windows\\Installe ... E8FO980C0\\4.0.5693	File Changed	2017-07-12 18:01:41	First Seen	2017-07-12 18:01:41
File Size	608080	ProcessPath	C:\\Users\\cas ... bin\\ javaw.exes	Last Seen	2017-07-12 18:01:41
File Owner	Jimbojones	Process Hash	4f096d96285e06cd51aef7d2d3de04da	Device Type	Tablet
CNC Host	nested obj	ParentProcess Hash	4f096d96285e06cd51aef7d2d3de04da	Device Name	XXXXXXXXXXX
Hostname	WORKGROUP\johnSmith	ParentProcess Path	\\Device\\Har ... Windows\\explorer.exe	Blocked	Yes
IP	45.55.34.187	PID	4484	PPID	10.8.0.6
File Created	2017-07-12 18:01:41	File Modified	2017-07-12 18:01:41	OS	Mac OSX 10.3.1

Helix Rule

Name	Spora Trojan II (URI POST)
Rule Pack	Network
Distinguishers	srcipv4: 168.0.1.1, srcipv6: null 100 Events
Threshold	Every 1 hour
Interval	metaclass:http_proxy domain
Query	

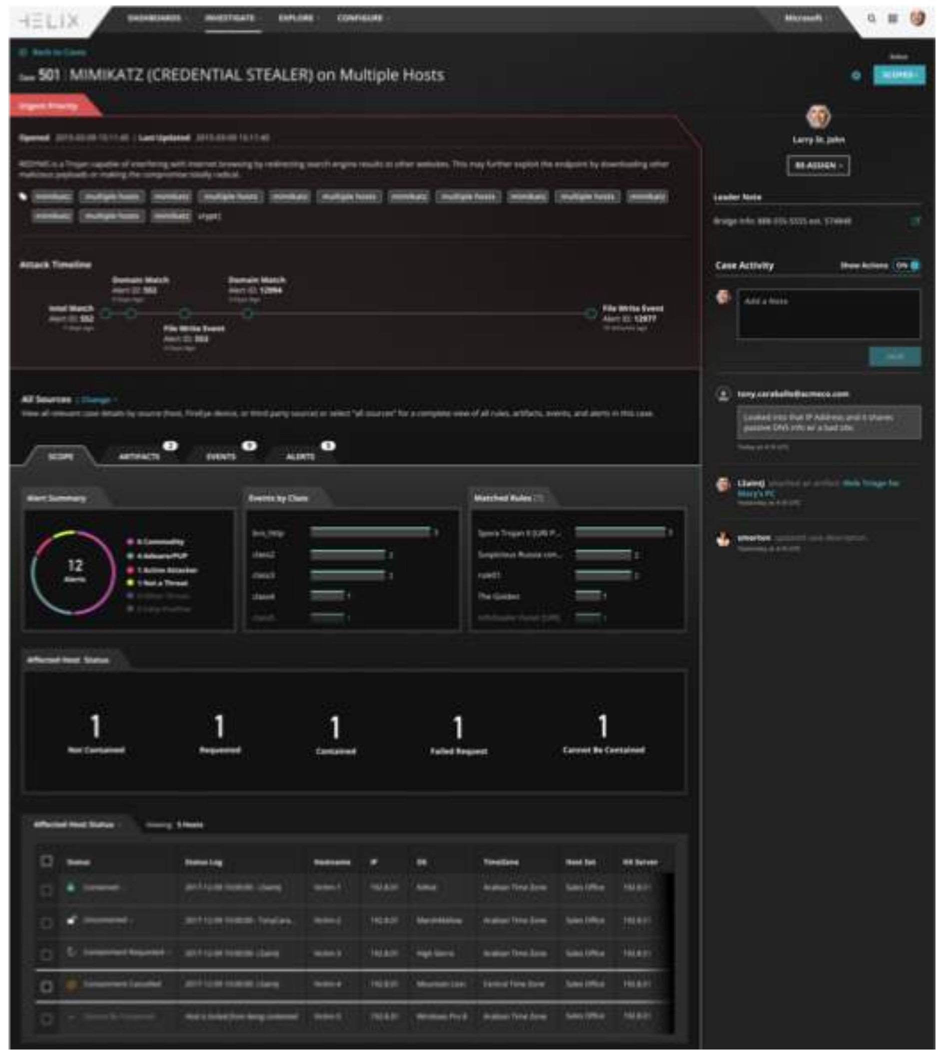
Upload and download files, logs data, pcaps, or other relevant artifacts.

	Uploaded by	File Size	Host	Source	Uploaded	Last Downloaded
Web Triage for Mary's PC triage, marysmith, This was pulled from Mary's PC because I mean, honestly we all know she's up to no good.	Lsaintj	32kb	mary_smith_pc	Network | nx1900_01	3 weeks ago	1 minute ago
Web Triage for Mary's PC triage, marysmith, This was pulled from Mary's PC because I mean, honestly we all know she's up to no good.	Lsaintj	32kb	mary_smith_pc	Network | nx1900_01	3 weeks ago	1 minute ago

COMING SOON:

Advanced Case Management

- Complete refresh of case management in Helix
- Focus on better summarizing the overall impact and scope of a case through attached alerts, artifacts, and events.
- New collaboration and status tracking capabilities
- Future iterations will focus on improved collaboration and task management coupled with improved incident storytelling and response tools



FireEye

BUILT TO INNOVATE

GRADY SUMMERS CTO

Break

FireEye Customers

FireEye

BUILT TO PROTECT

KEVIN MANDIA CEO

We Made Great Progress in

2017

2017 We Did What We Said We Would Do…

ON-PREMISE → CLOUD/HYBRID

HARDWARE → SOFTWARE / VIRTUAL

APT → ALL THREATS

CLOSED → OPEN

LARGE ENTERPRISE → ALL SIZE

U.S. → GLOBAL

SANDBOX → SECURITY

UNPROFITABLE → PROFITABLE GROWTH

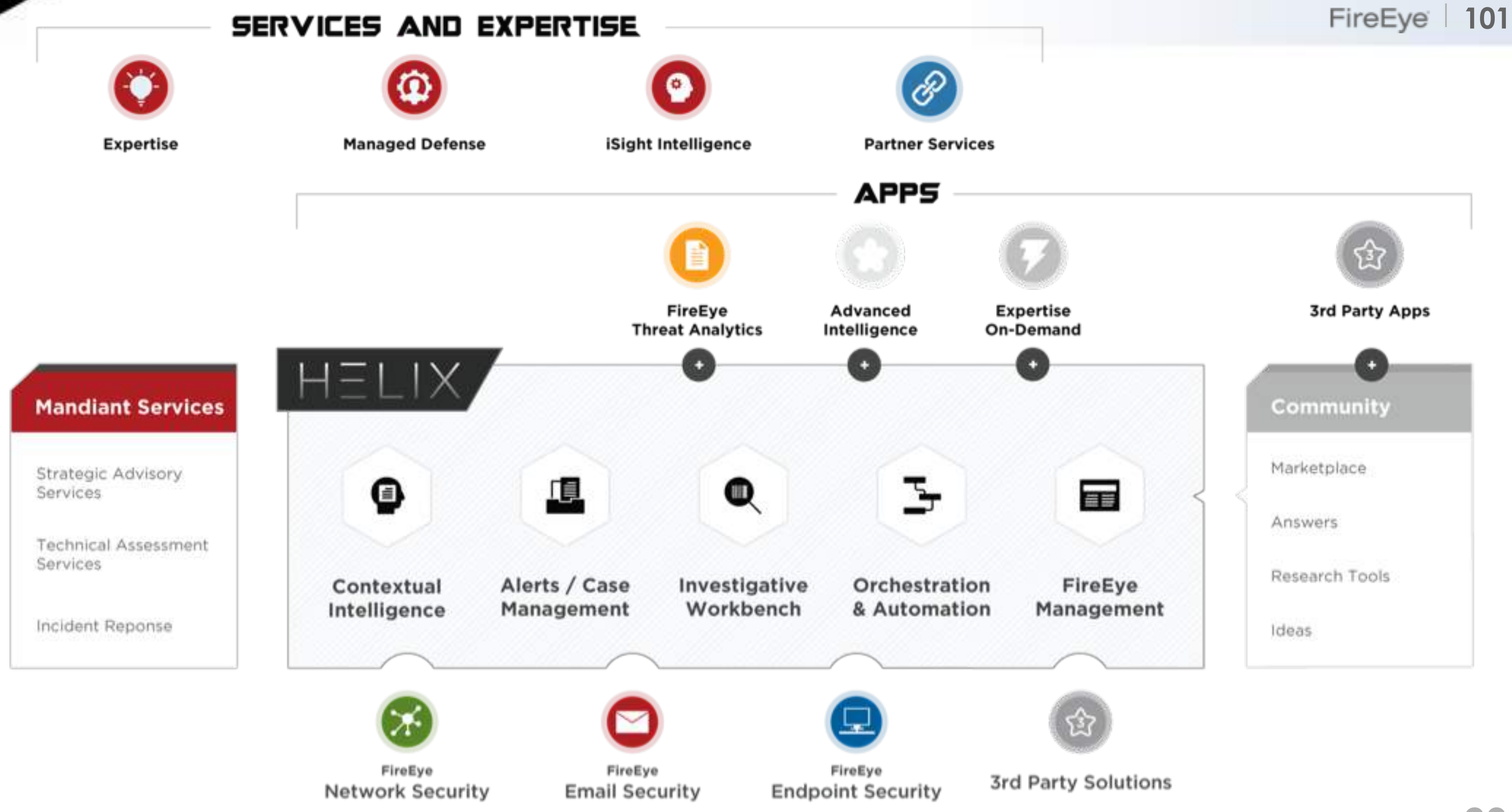
We Will Continue to Build in 2018

1. Innovation
2. Simplify GTM
3. Thought Leadership
4. Elevate
5. Profitable Growth

1

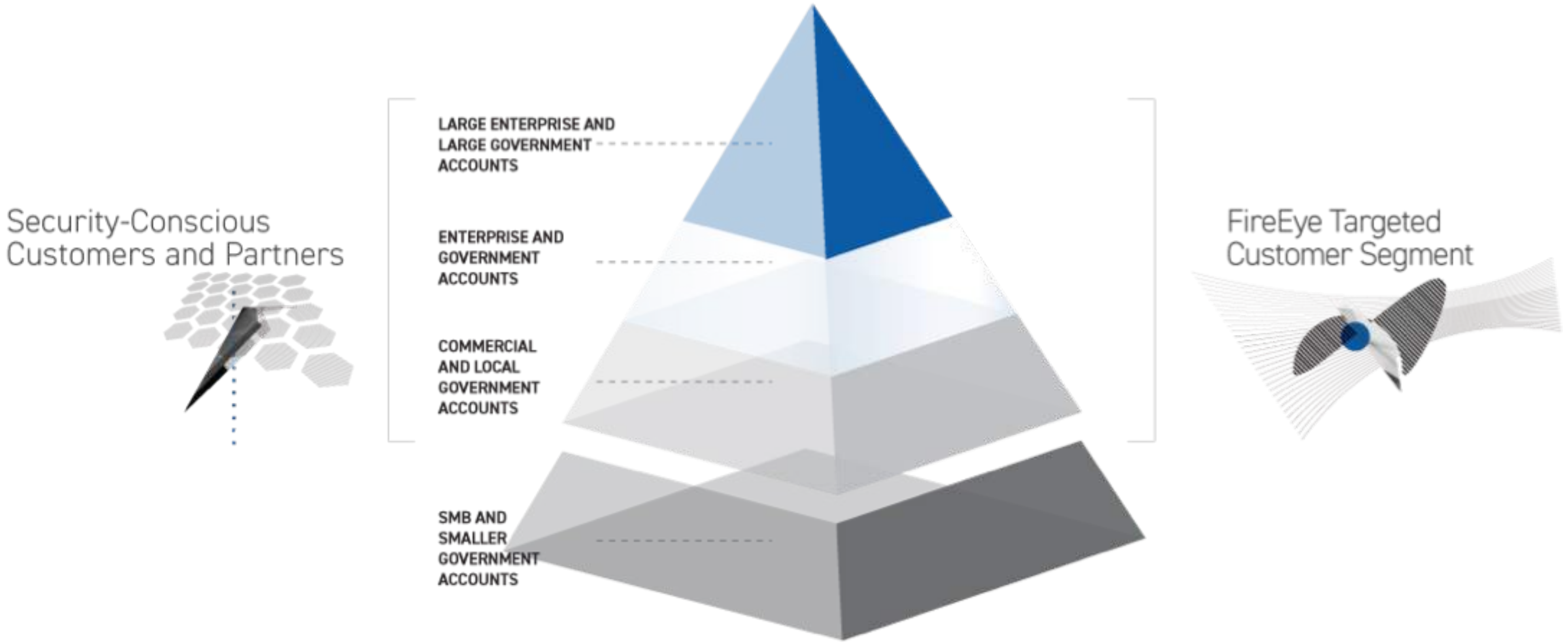
INNOVATION

When our technology can prevent the impact and consequences of all the cyber threats we are aware of, then **we are well on our way to accomplishing our mission.**



2

SIMPLIFY OUR CUSTOMER & GO-TO-MARKET STRATEGY



Security-Conscious Customers and Partners

LARGE ENTERPRISE AND LARGE GOVERNMENT ACCOUNTS

ENTERPRISE AND GOVERNMENT ACCOUNTS

COMMERCIAL AND LOCAL GOVERNMENT ACCOUNTS

SMB AND SMALLER GOVERNMENT ACCOUNTS

FireEye Targeted Customer Segment

3 THOUGHT LEADERSHIP

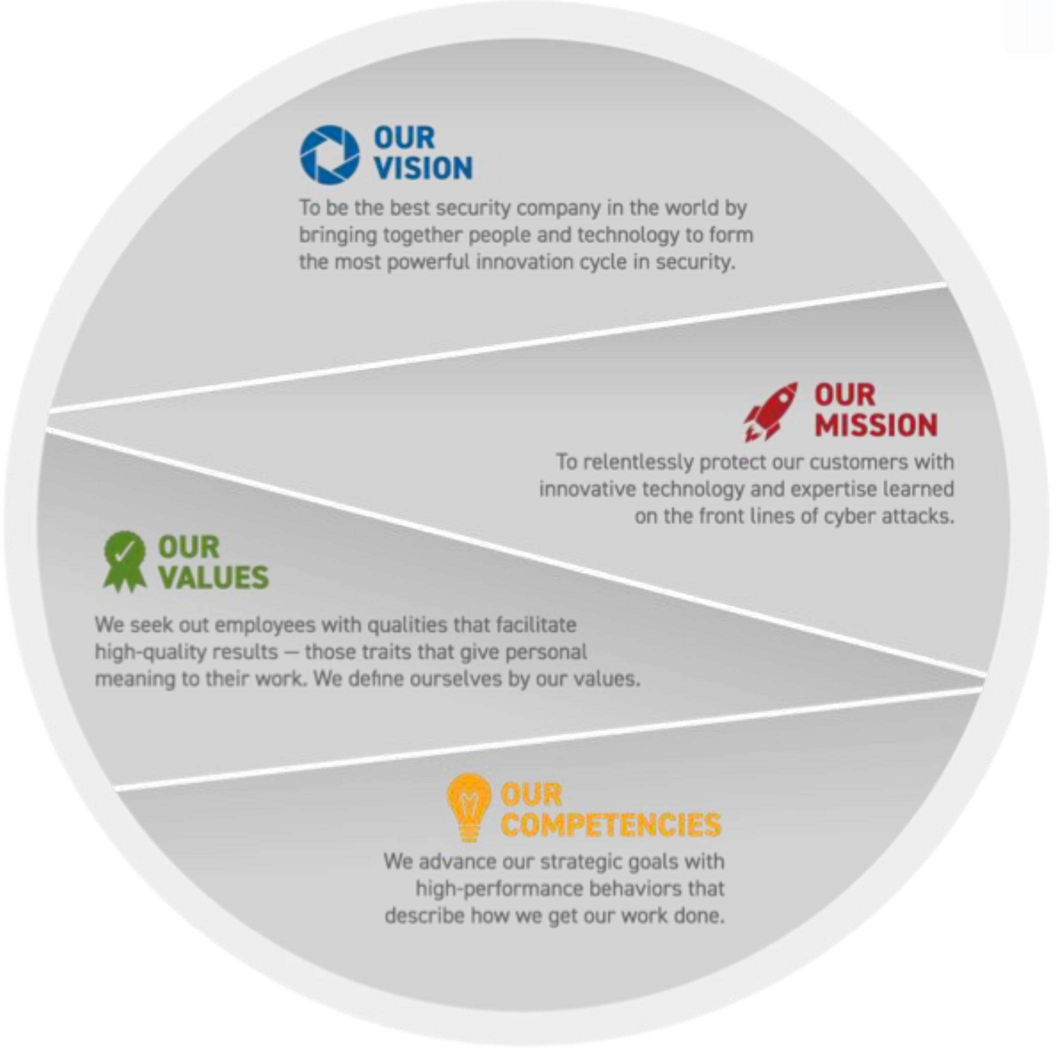
We ought to ask ourselves – how many security technology companies have this type of security DNA? **We have the ability to create a differentiated brand, based on our thought leadership.**

We routinely **influence national-level** policy

We have **developed formal training** to help build cyber security workforces around the globe

We have testified as **subject matter experts** in the U.S. Congress

4 ELEVATE ONE TEAM



OUR VISION

To be the best security company in the world by bringing together people and technology to form the most powerful innovation cycle in security.

OUR MISSION

To relentlessly protect our customers with innovative technology and expertise learned on the front lines of cyber attacks.

OUR VALUES

We seek out employees with qualities that facilitate high-quality results — those traits that give personal meaning to their work. We define ourselves by our values.

OUR COMPETENCIES

We advance our strategic goals with high-performance behaviors that describe how we get our work done.

5

PROFITABLE GROWTH

Accelerating into the Future

We have great **innovation**

AND

we need to **simplify our go to market.**

CMS

Support NX VMs

HX DTI AX

COMPLEXITY

PX

MVX Attach URL EX Appliances IA

FX ETP VX

CMS NX VMs Support HX DTI AX PX MVX Attach URL EX Appliances IA FX ETP VX

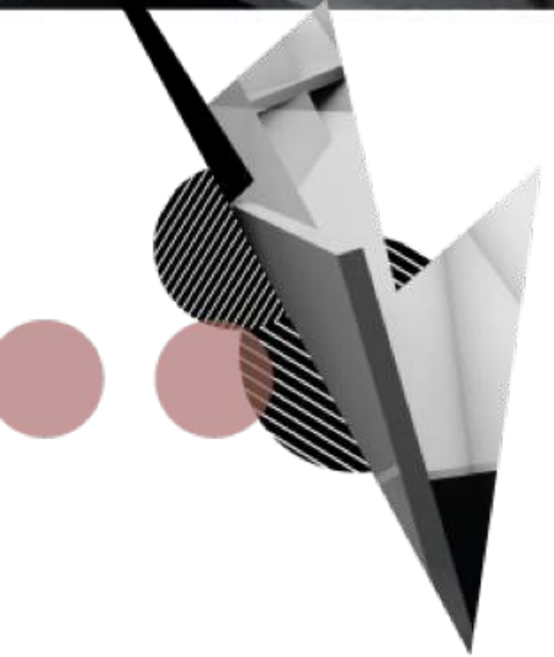
Simplify to

SELL MORE

Packaging

Pricing

Naming

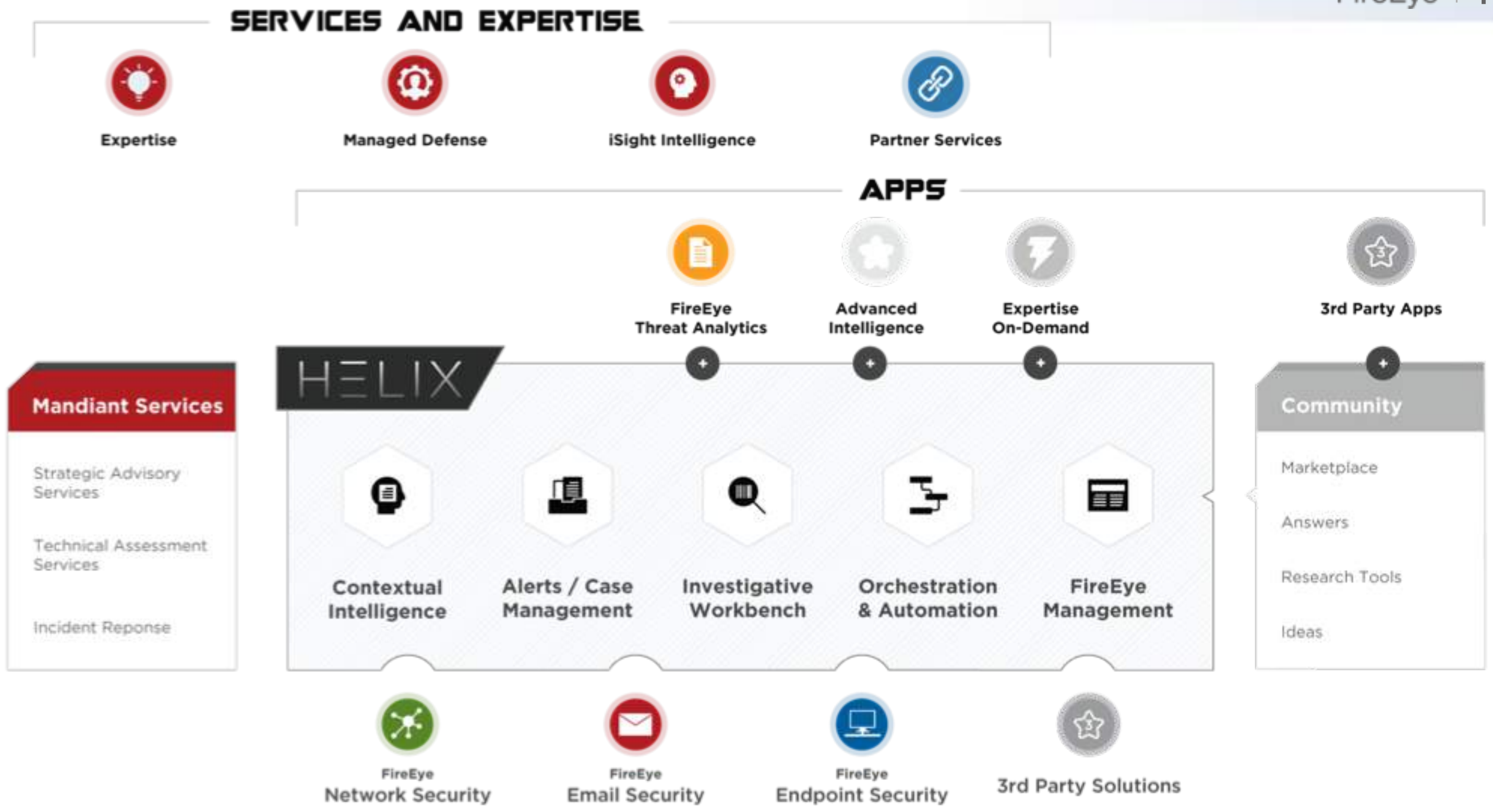


CREATE SOLUTIONS

Security Product Lines

CREATE SOLUTIONS

Security Product Lines



SERVICES AND EXPERTISE

Expertise

Managed Defense

iSight Intelligence

Partner Services

APPS

FireEye Threat Analytics

Advanced Intelligence

Expertise On-Demand

3rd Party Apps

Mandiant Services

Strategic Advisory Services

Technical Assessment Services

Incident Reponse

HELIX

Contextual Intelligence

Alerts / Case Management

Investigative Workbench

Orchestration & Automation

FireEye Management

Community

Marketplace

Answers

Research Tools

Ideas

FireEye Network Security

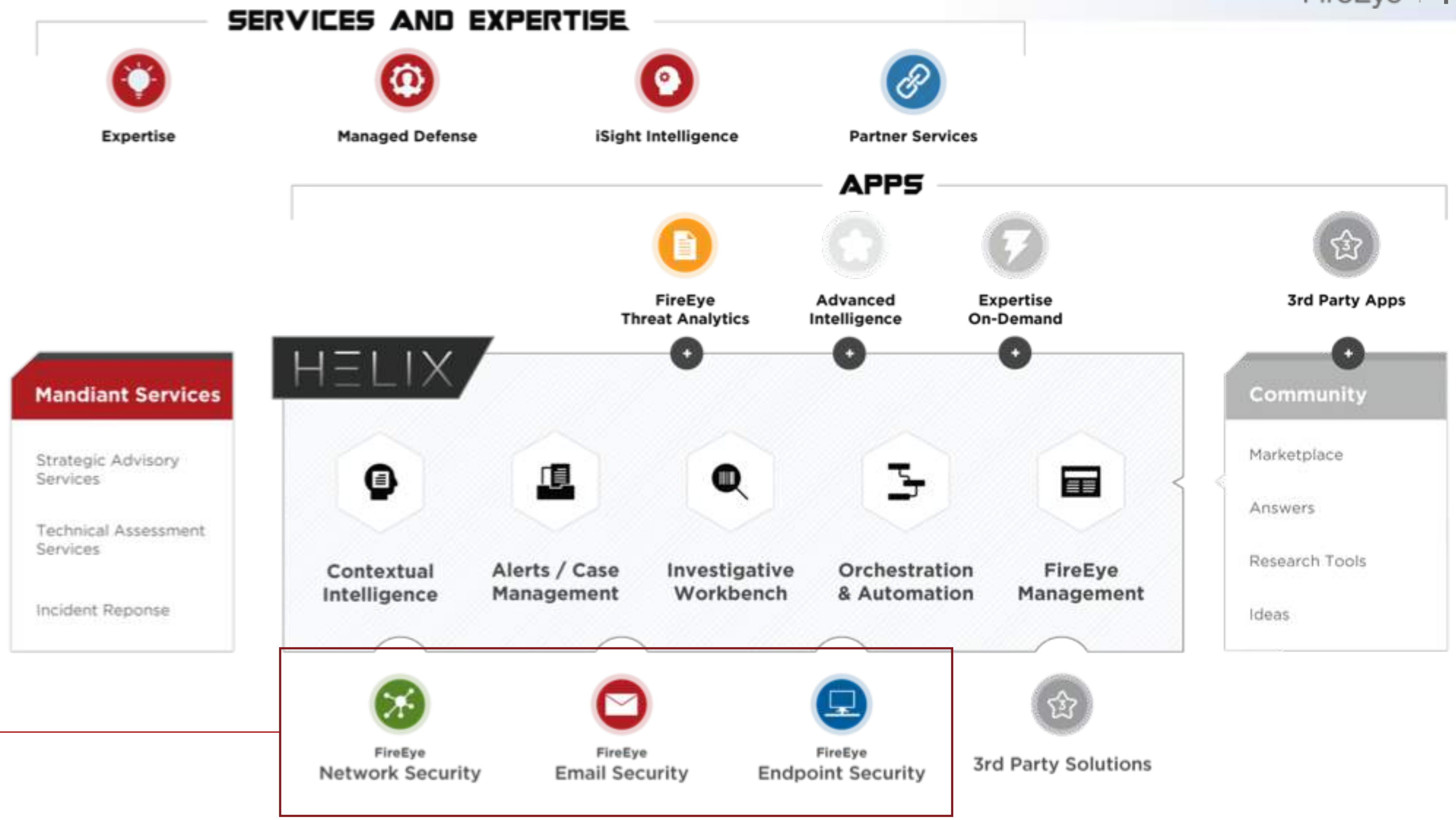
FireEye Email Security

FireEye Endpoint Security

3rd Party Solutions

CREATE SOLUTIONS

Security Product Lines



SERVICES AND EXPERTISE

Expertise

Managed Defense

iSight Intelligence

Partner Services

APPS

FireEye Threat Analytics

Advanced Intelligence

Expertise On-Demand

3rd Party Apps

Mandiant Services

Strategic Advisory Services

Technical Assessment Services

Incident Reponse

HELIX

Contextual Intelligence

Alerts / Case Management

Investigative Workbench

Orchestration & Automation

FireEye Management

Community

Marketplace

Answers

Research Tools

Ideas

FireEye Network Security

FireEye Email Security

FireEye Endpoint Security

3rd Party Solutions

3 KEY SOLUTIONS

CREATE SOLUTIONS

NETWORK SECURITY

ENDPOINT SECURITY

EMAIL SECURITY

New Enterprise Packaging

FireEye Network Security

$/Mbps

Includes:

- Helix
- Network Security – NX or SmartVision
- Cloud MVX for virtual deployments
- DTI
- Platinum Support

Optional add-ons:

- Service – PPP or GPP
- Intel Sharing – 1-way or Offline

FireEye Email Security

$/Mailbox

Includes:

- Helix
- Email Security – Cloud or Server
- DTI
- URL attach
- Platinum Support

Optional add-ons:

- Service – PPP or GPP
- Intel Sharing – 1-way or Offline (EX)
- Antivirus / Anti-Spam (Cloud Only)

FireEye Endpoint Security

$/Endpoint

Includes:

- Helix
- Endpoint Security – Essentials or Power
- DTI
- Platinum Support

Optional add-ons:

- Service – PPP or GPP
- Intel Sharing – 1-way or Offline

Simplify Selling **FireEye Network Security**

OLD MODEL – Per appliance throughput

NX2550	**NX2550**	**NX3500**
(100mbps)	(100mbps)	(250mbps)

EXAMPLE CUSTOMER

3 Egress Points

INTERNET

70 Mbps	90 Mbps	240 Mbps

NEW MODEL

400Mbps

Subscription

FireEye
Network Security

NX software
Cloud MVX
DTI
Platinum Support
VMs

+ Options
+ Hardware

FireEye

Network Security

NX Edition

Protects internet traffic

New

SmartVision Edition

Analyzes intranet traffic

Growing Business

IN THE MID-MARKET

Channel Friendly

Bundles

Specific Pricing

Per User Pricing

Mid-market

UP TO **2000** USERS

NOW

FireEye
Network Security

NOW

FireEye
Email Security

NOW

FireEye
Endpoint Security

One Subscription SKU

+

Solution Options

+

Á la carte Hardware

FireEye Complete Security for the Mid-market

NOW

FireEye Security Suite

Complete Security Solution

FireEye
Network Security

FireEye
Endpoint Security

FireEye
Email Security

FireEye
Helix

One Subscription SKU

+

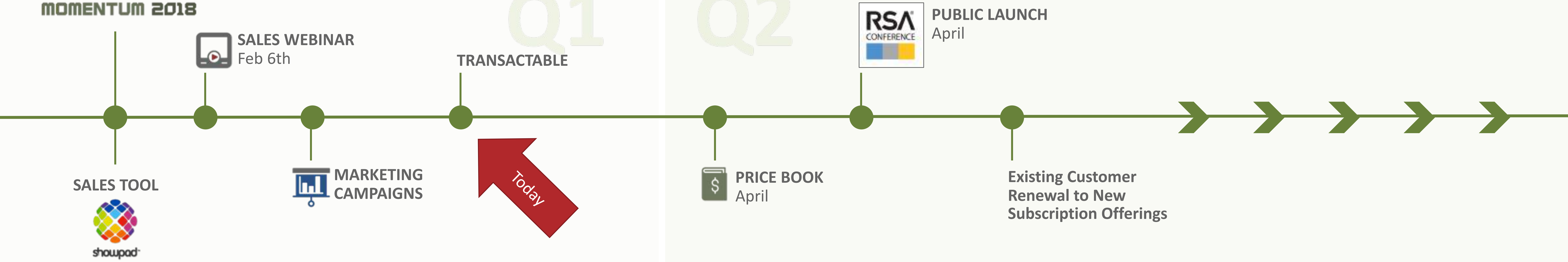
Solution Options

+

Á la carte Hardware

UP TO **2000** USERS

FireEye
MOMENTUM 2018



SALES TOOL

SALES WEBINAR
Feb 6th

MARKETING
CAMPAIGNS

TRANSACTABLE

PRICE BOOK
April

PUBLIC LAUNCH
April

Existing Customer
Renewal to New
Subscription Offerings

Enterprise

FireEye Network Security

$ Per Mbps

FireEye Email Security

$ Per Mailbox

FireEye Endpoint Security

$ Per Endpoint

Mid-market

FireEye Network Security

$ Per User

FireEye Email Security

$ Per User

FireEye Endpoint Security

$ Per User

Enterprise

FireEye
Network Security

$ Per Mbps

FireEye
Email Security

$ Per Mailbox

FireEye
Endpoint Security

$ Per Endpoint

Mid-market

FireEye
Network Security

$ Per User

FireEye
Email Security

$ Per User

FireEye
Endpoint Security

$ Per User

FireEye
Security Suite
FOR UP TO 2000 USERS

FireEye

BUILT TO PROTECT

KEVIN MANDIA CEO

FireEye

BUILT TO WIN

BILL ROBBINS EVP WORLDWIDE SALES

Agenda / Key Messages

Expanding Market Opportunity

Sales Transformation Centered Around Simplifying GTM Strategy

Leading Indicators of Success

2017 Highlights

EXECUTION, EXECUTION, EXECUTION

1 **Met or Exceeded Top-line Guidance Ranges in All Four Quarters**

2 **Strong Q4'17 Finish**

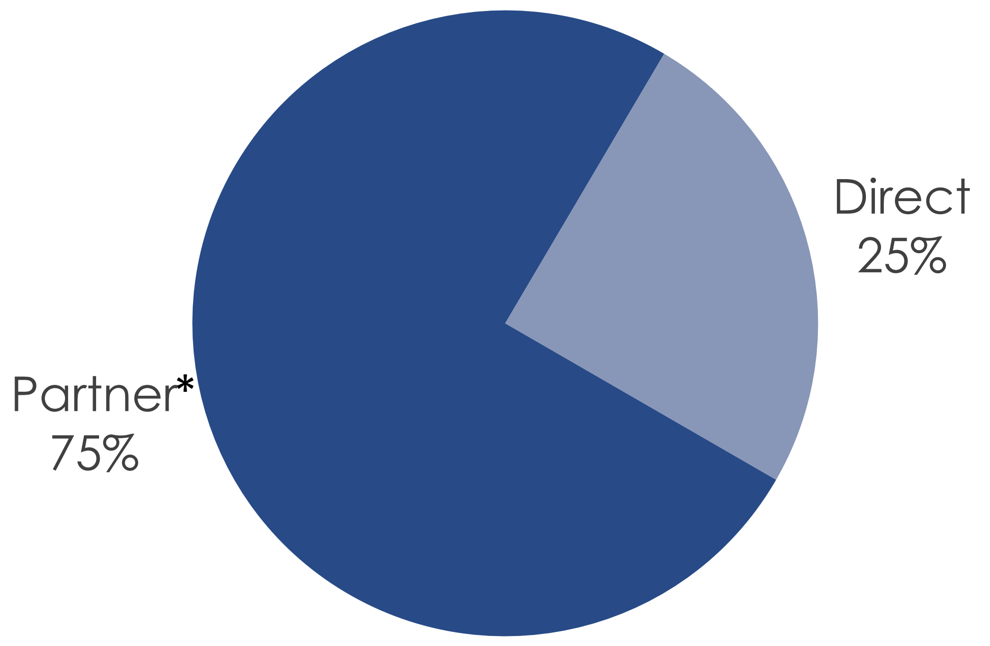
- 9% Billings Growth
- Y/Y & Sequential Growth in Every Major Product Family & Geographic Region
- Record Transactions >$1M

3 **Added 990 New Logos**

4 **Increased Partner Contribution**

5 **Steady Improvement in Sales Productivity**

2017 Non-Services Billings



* Includes Partner-led and Partner fulfilled

Defining the Win

2018 SALES & MARKETING GOALS

>1,000

NEW CUSTOMER LOGOS

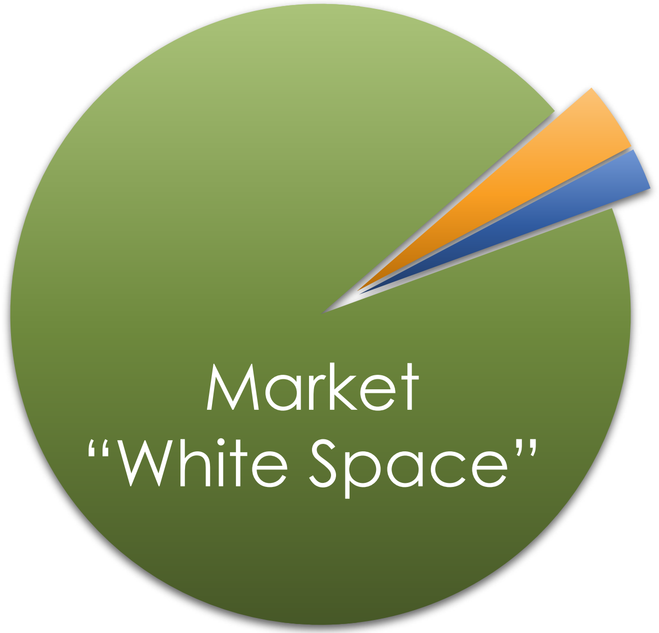
>$830M

2018 BILLINGS
EXCEED HIGH END
OF GUIDANCE RANGE

33%

**PARTNER-LED
BUSINESS**

Significant "White Space" Opportunity Worldwide



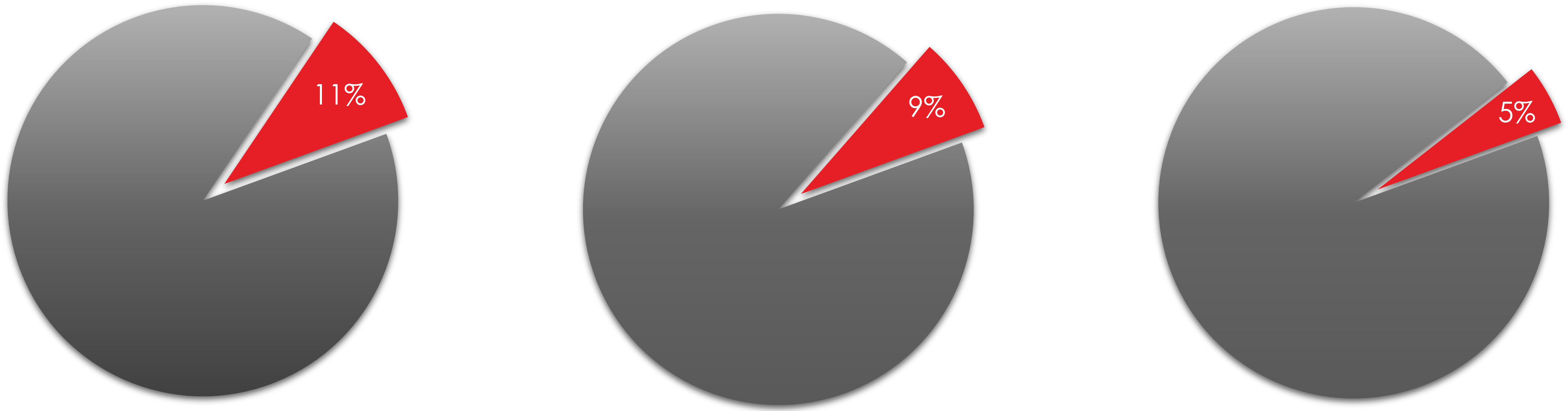
1-2 FireEye Products

3 or More FireEye Products

…In Every Market Segment

🟥 FireEye customers

⬛ Non-FireEye customers

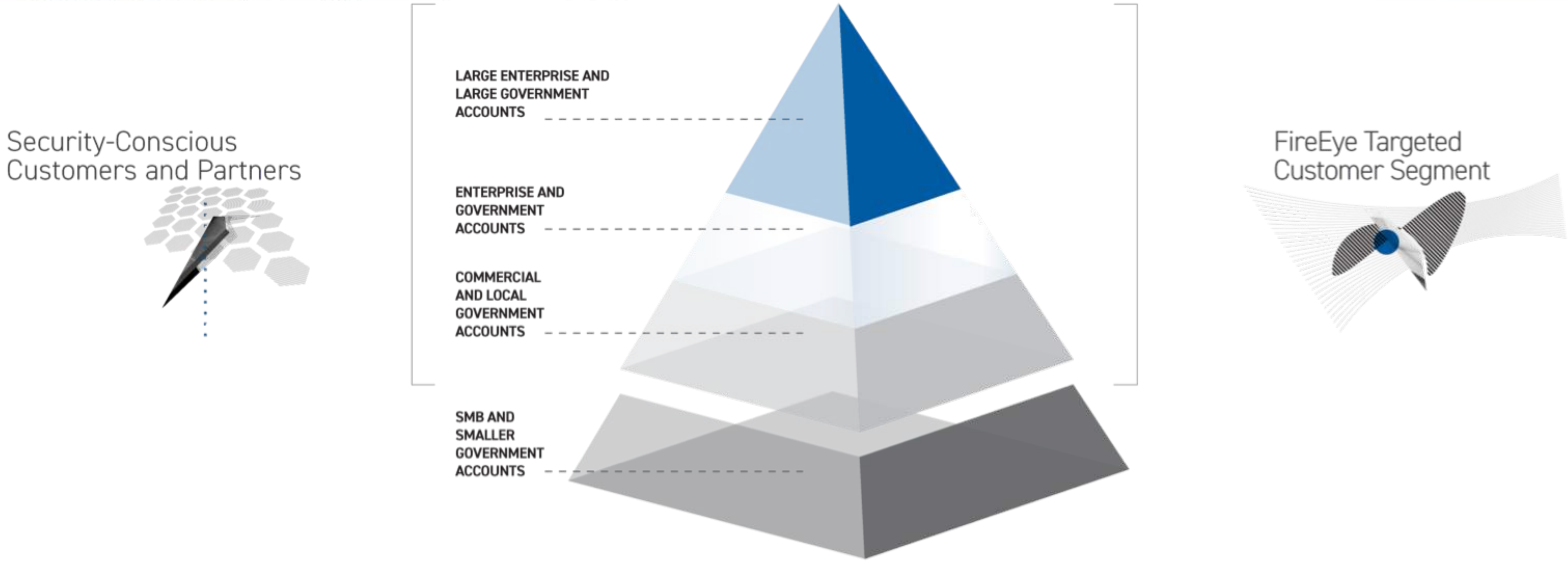


	>20,000 EMPLOYEES	5,000 – 19,999 EMPLOYEES	< 5,000 EMPLOYEES
WW Accounts [1]	~7,200	~8,200	>63,000
Potential $ per 1% [2]	~$25M	~$20M	~$60M

1. FireEye Proprietary and FireEye estimates.
2. Based on average transaction size and # of transactions per year of current installed base of FireEye customers.

Organized to Succeed

DATA DRIVEN MARKET SEGMENTATION



Security-Conscious Customers and Partners

LARGE ENTERPRISE AND LARGE GOVERNMENT ACCOUNTS

ENTERPRISE AND GOVERNMENT ACCOUNTS

COMMERCIAL AND LOCAL GOVERNMENT ACCOUNTS

SMB AND SMALLER GOVERNMENT ACCOUNTS

FireEye Targeted Customer Segment

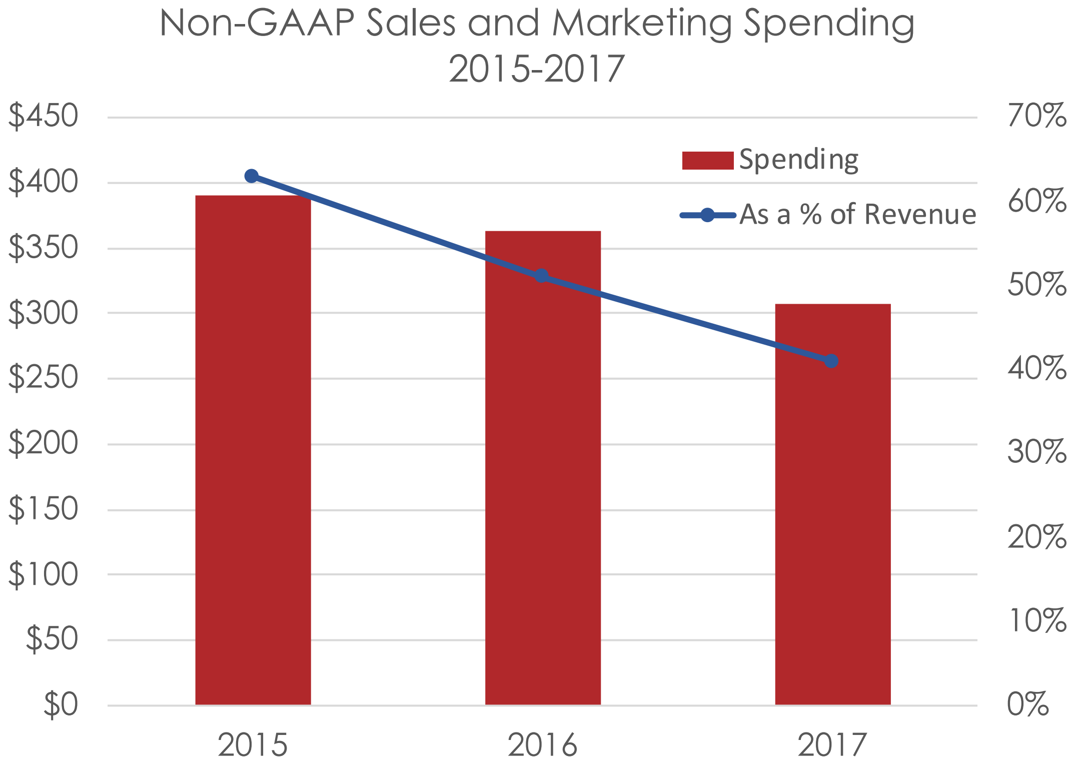
Organized to Succeed

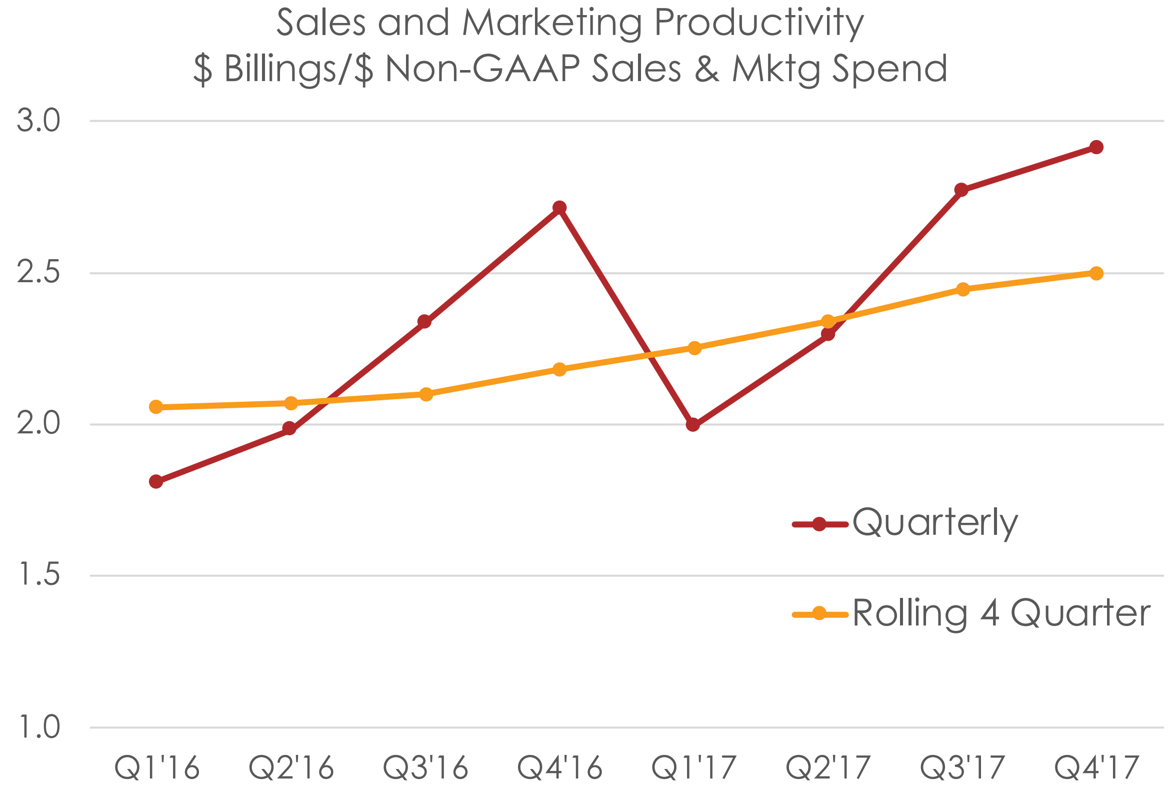
INVESTING IN TENURED LEADERSHIP, COMMITTED REPS

Sales Management Positions Filled

- EMEA in Q1'17
- Japan in Q2'17
- GSI in Q2'17
- Americas in Q3'17
- Public Sector in Q3'17

Sales Force Stabilized, Attrition At/Below Industry Averages


Non-GAAP Sales and Marketing Spending 2015-2017


Sales and Marketing Productivity
$ Billings/$ Non-GAAP Sales & Mktg Spend

Organized to Succeed

CHANNEL STRATEGY GUIDING PRINCIPLES

1. Accelerate Mutual Growth & Profitability
2. Help Build Partner FireEye Business
3. Consistent Implementation of Strategies Programs, Processes
4. Partner with Integrity & Respect for Partner Value Add

Reseller Channel Enablement

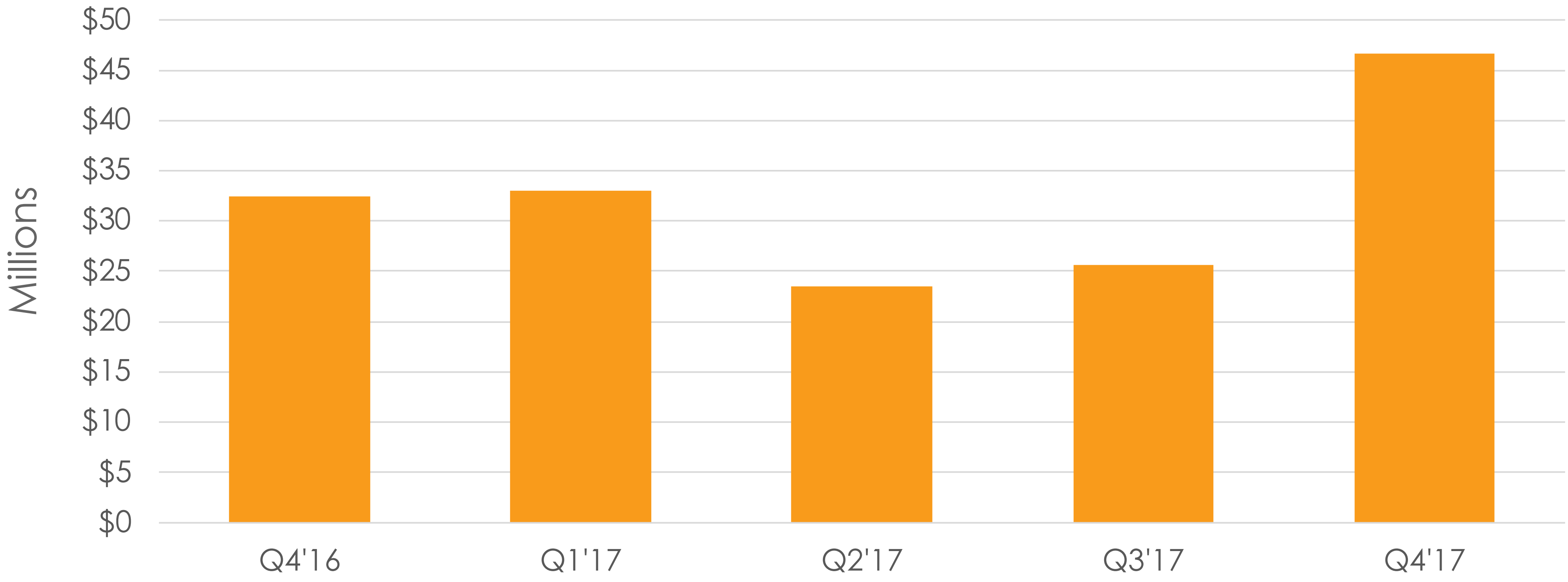
PAST, PRESENT & FUTURE

PAST	2017 ACTIONS	FUTURE
PRODUCT Appliance-based APT Detection	**PRODUCT** Endpoint A/V, Cloud/Virtual Products, Helix	**PRODUCT** Channel-ready Product/Solution Development
PRICING High / Appliance-based	**PRICING** More Competitive	**PRICING** Competitive, Usage-based Subscriptions
PROCESS Complex, Multi-step	**PROCESS** Fewer Steps, Easier Solution Deployment	**PROCESS** Simplified, Channel-enabled
RESULTS Perceived Conflict, Declining Engagement	**RESULTS** Improving	**RESULTS** Engaged & Committed to Mutual Growth, Profitability

Leading Indicators

CHANNEL ENGAGEMENT

Partner-Led Sales



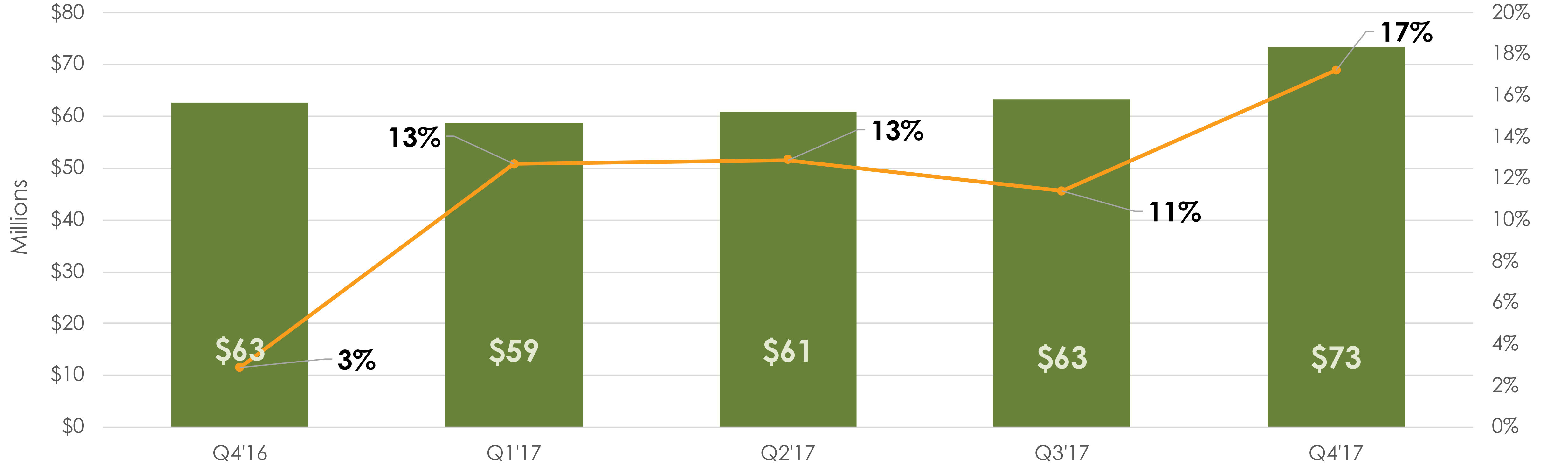
THE CHANNEL CO. CRN TECH INNOVATORS 2017

CHANNELNOMICS INNOVATION AWARDS 2017

Leading Indicators

GROWING INTERNATIONAL MOMENTUM

International Revenue



— % Year over Year

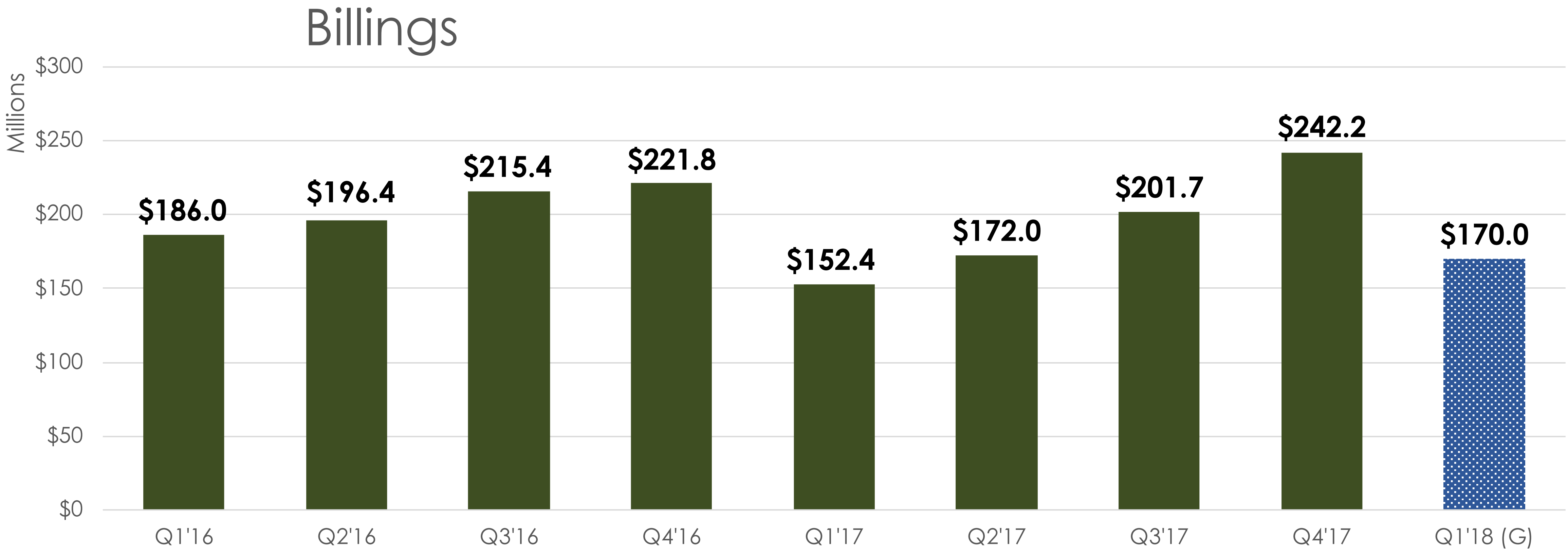
🟩 International Revenue (Millions of Dollars)

Leading Indicators

BILLINGS TREND

🟩 Billings

▨ Reflects Mid-point of Q1 2018 Guidance



Non-GAAP. Reconciliation to nearest GAAP metric in Appendix. Reconciliation not available for forward-looking metrics.

FireEye

2018 BUILT TO WIN

FireEye

BUILT TO LAST

FRANK VERDECANNA EVP AND CHIEF FINANCIAL OFFICER

FireEye

Built to Last

- 2017 Milestones and 2018 Guidance
- Long Term Model

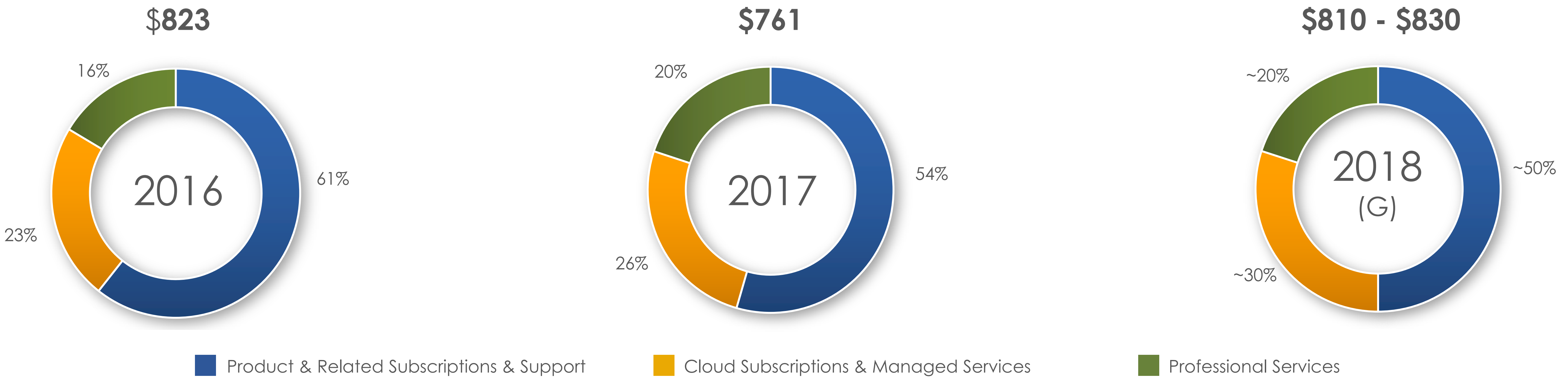
2018 Guidance Summary

	2017	2018 Guidance	YoY Growth
Billings[1]	$761M	$810M - $830M	6% – 9%
Revenue	$779M	$815M - $825M	5% – 6%
Operating Margin[1]	(0.3)%	1% to 2%	1% to 2%
Provision for Income Taxes[1]	$5M	$5M - $6M	$0 - $1M
Net Income per share[1]	$(0.06)	$0.00 - $0.04	$0.06 - $0.10
Cash Flow from Operations	$18M	$45M - $55M	$27M - $37M
Capital Expenditures	$44M	$35M - $40M	$(9M) - $(4M)

[1] Non-GAAP. Reconciliation to nearest GAAP metric in Appendix. Reconciliation not available for forward looking metrics.

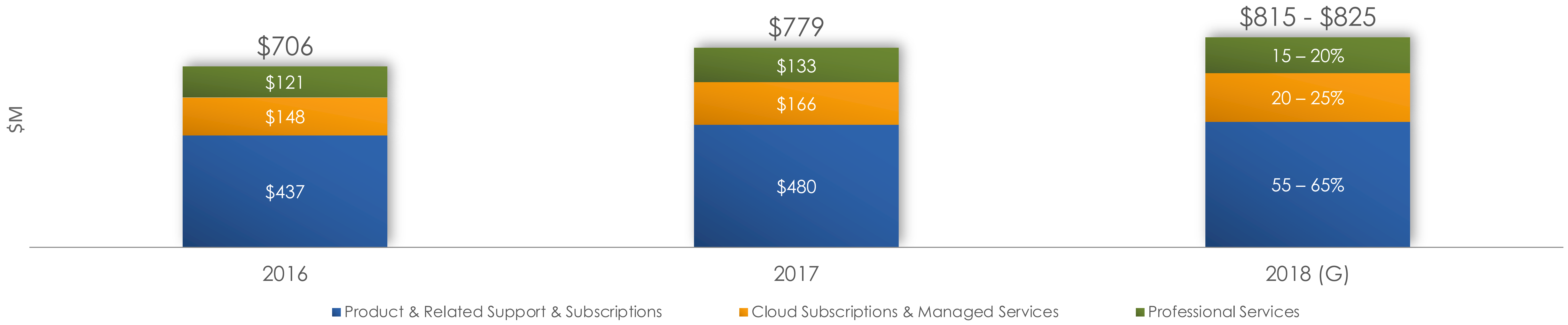
Billings[1] by Category, 2016 - 2018

$M

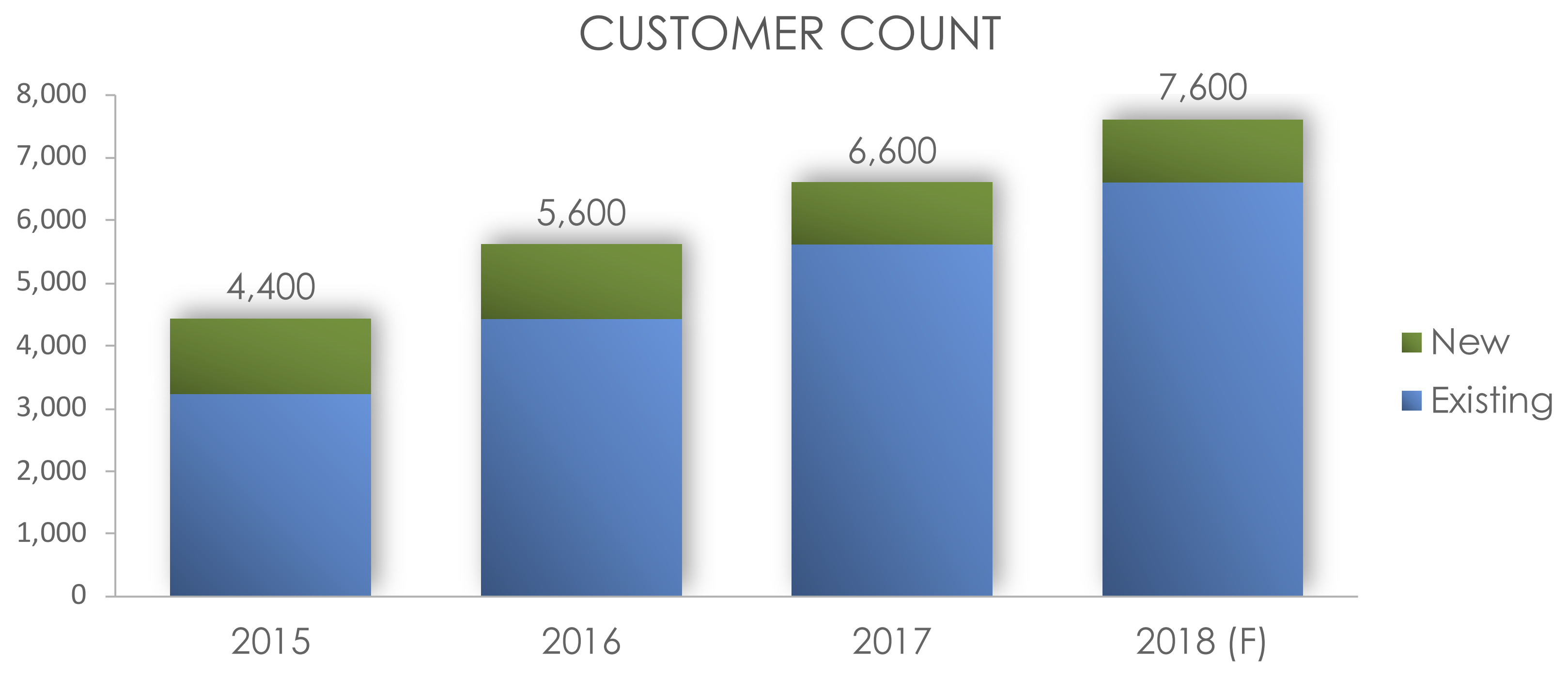


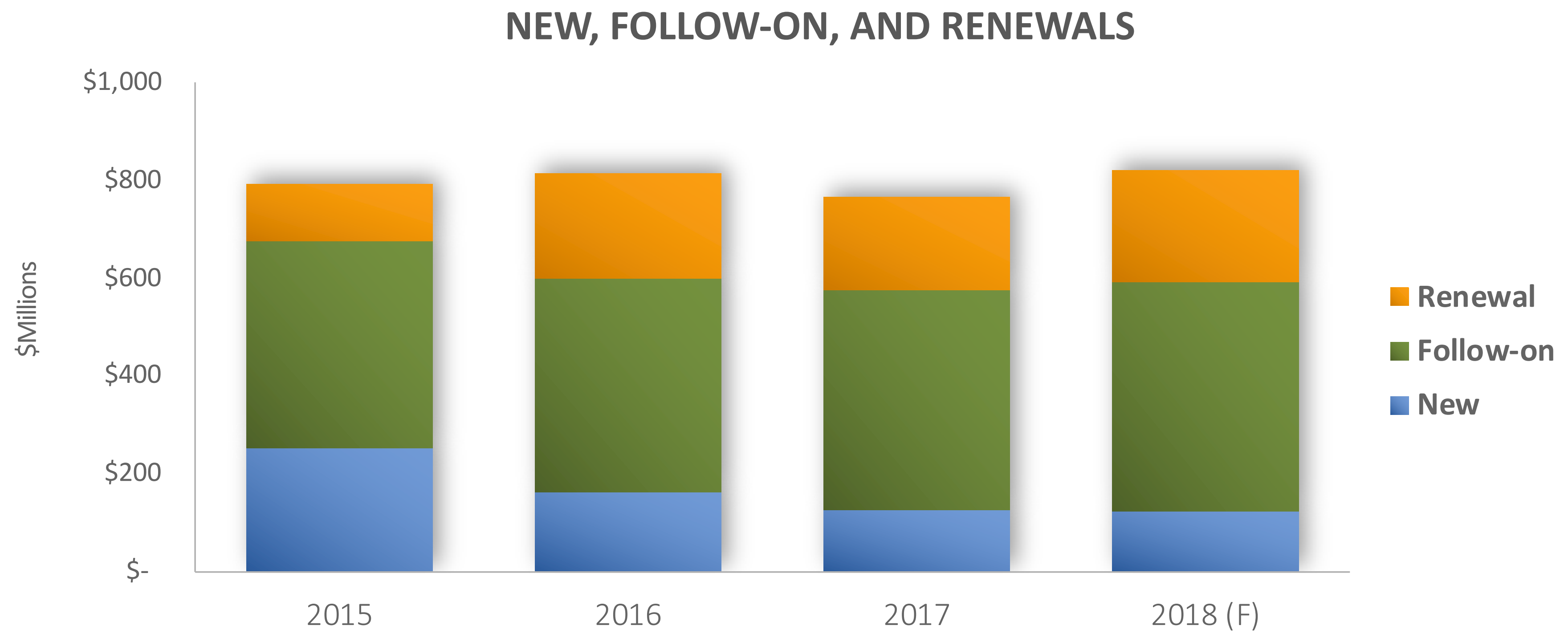
[1] Non-GAAP. Reconciliation to nearest GAAP metric in Appendix. Reconciliation not available for forward looking metrics.

Annual Revenue, 2016 - 2018

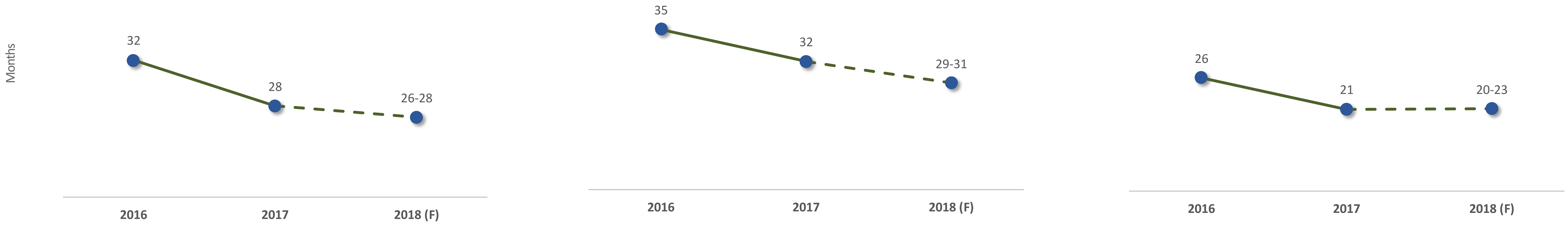


Growth Drivers – More Customers, More Products



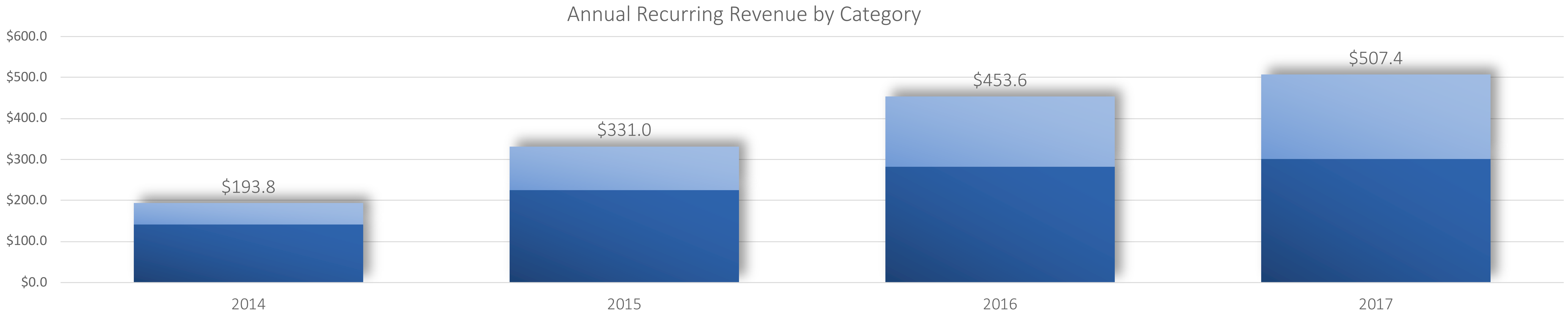


Average Contract Length[1]



[1] Product & Related Subscription and Support and Ratable Billings include amortization of appliances over 48-month period.

Annual Recurring Revenue



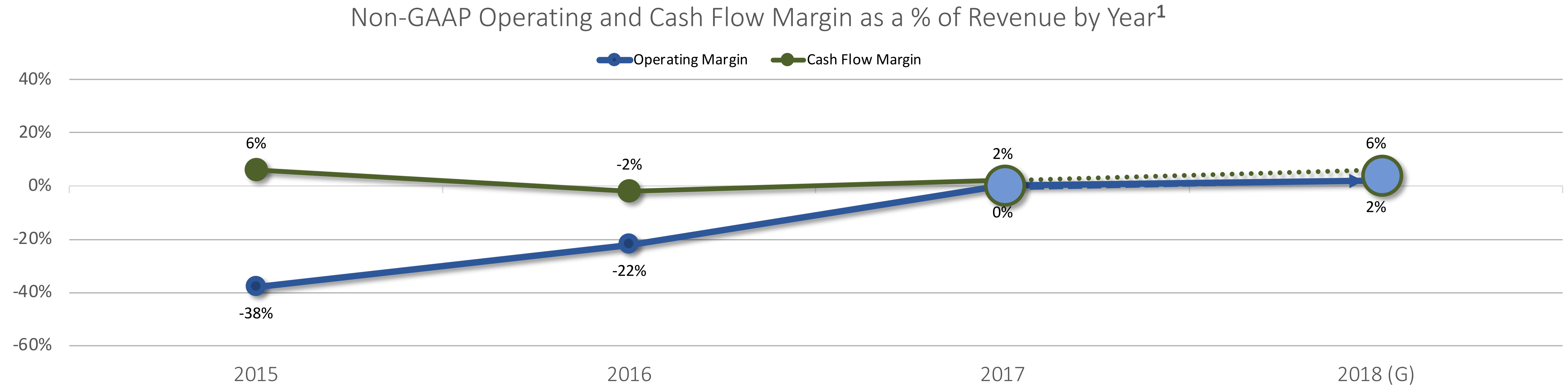
'14-17
CAGR
38%

Cloud Subs & Managed Services
58%

Product Related Subs & Support
29%

ARR Definition: We define ARR as the annualized value of all recurring revenue related contracts in place at the end of a period

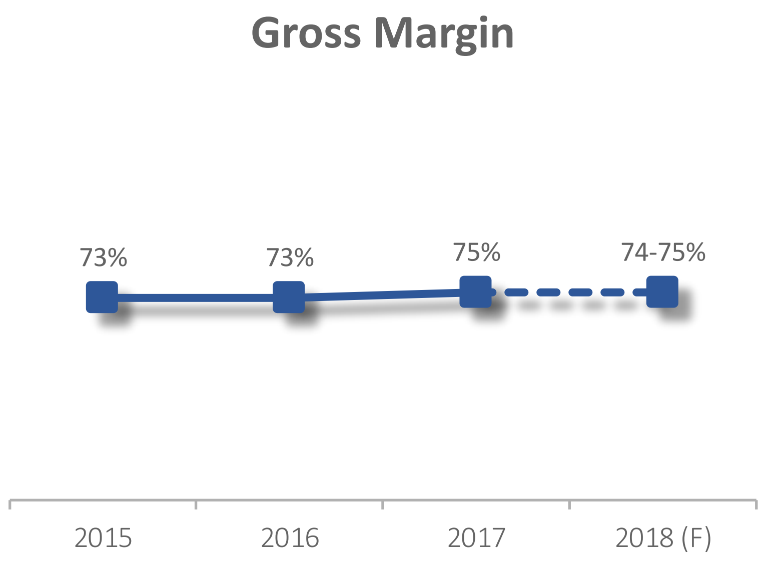
Continued Operating Leverage Improvement

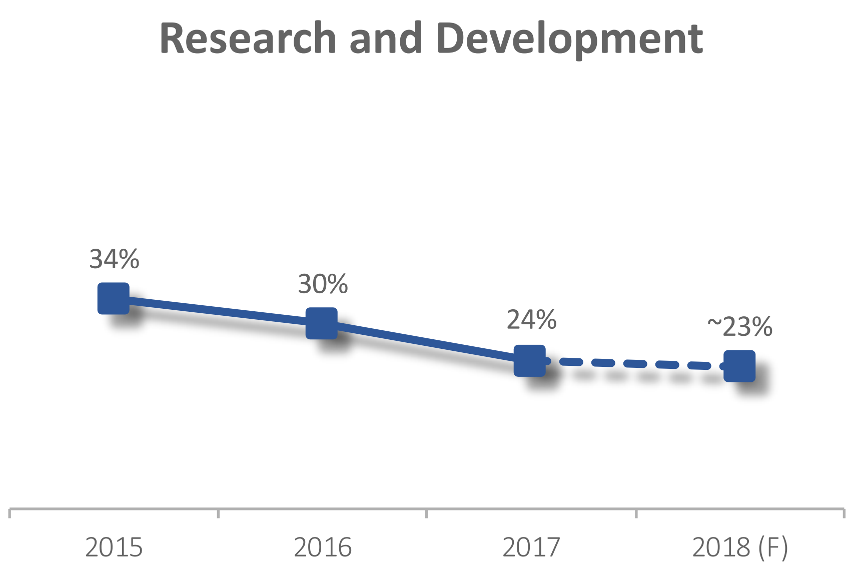


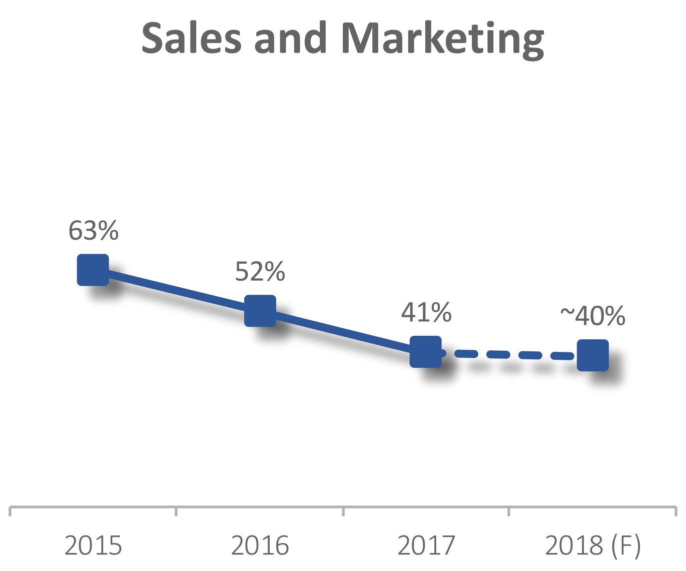
2018 guidance illustrates continued margin improvement following our profitable Q4 2017 exit.

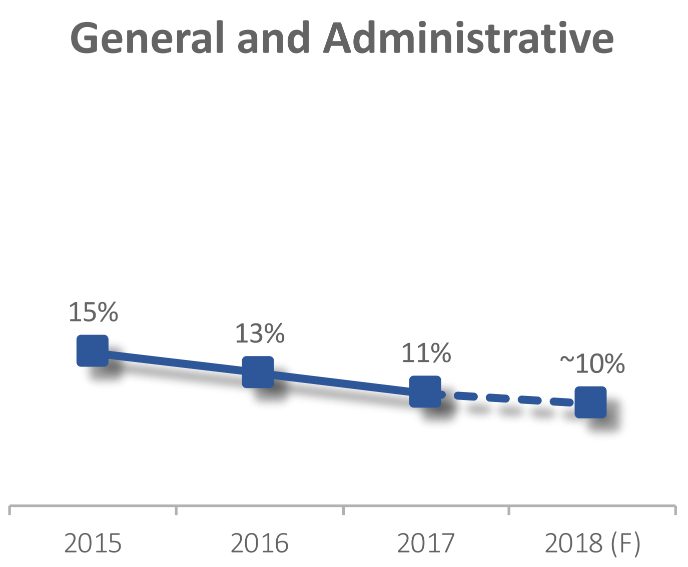
1. Non-GAAP. Reconciliation to nearest GAAP metric in Appendix. Reconciliation not available for forward looking metrics.

Continued Improvement in Operating Efficiency

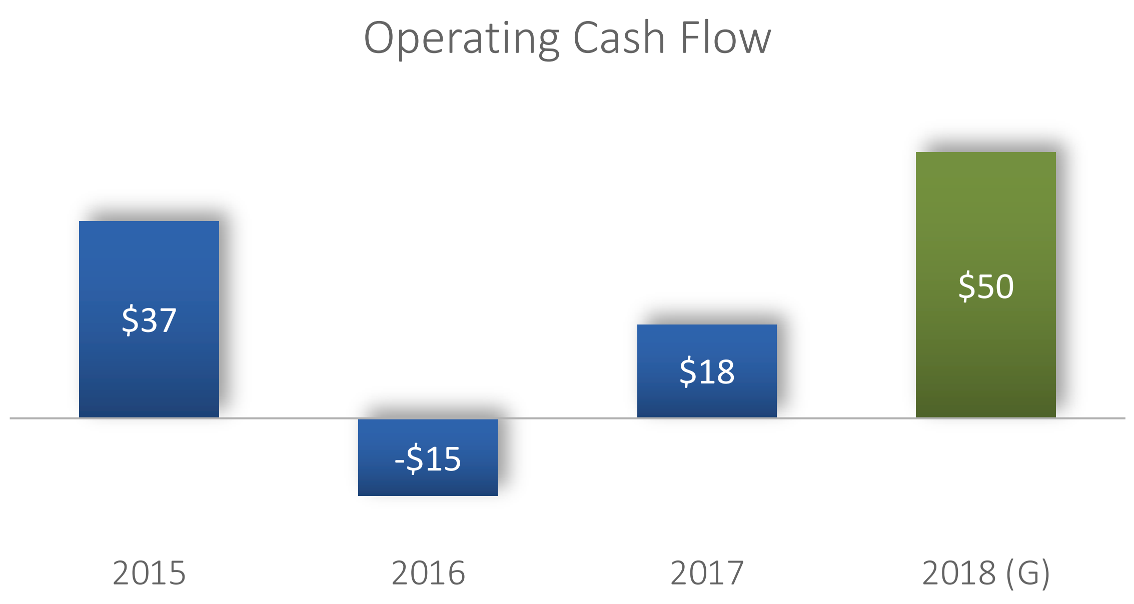


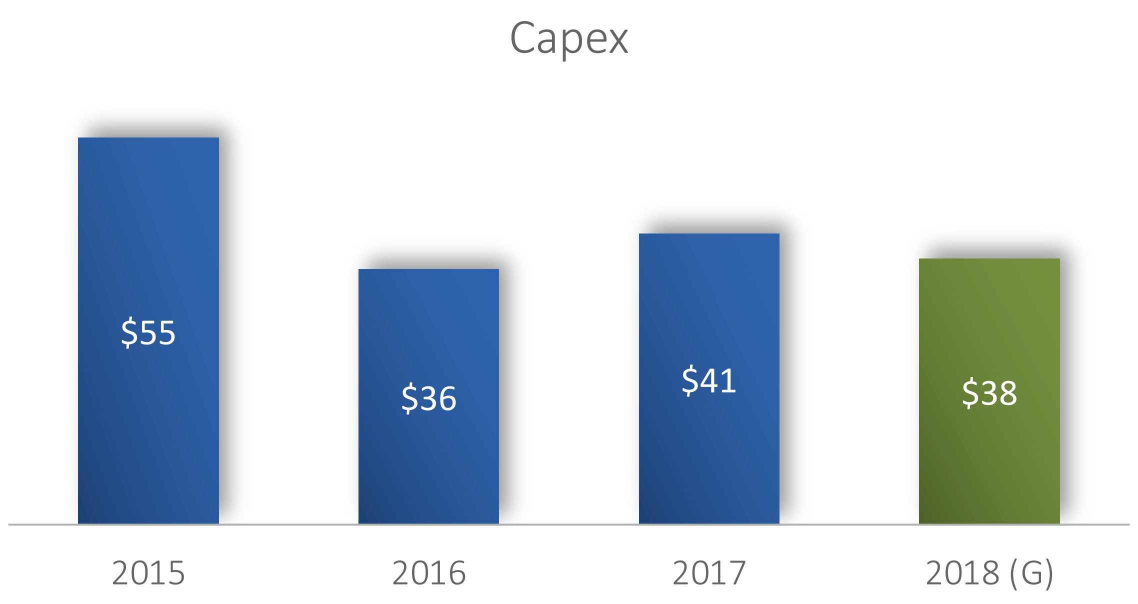


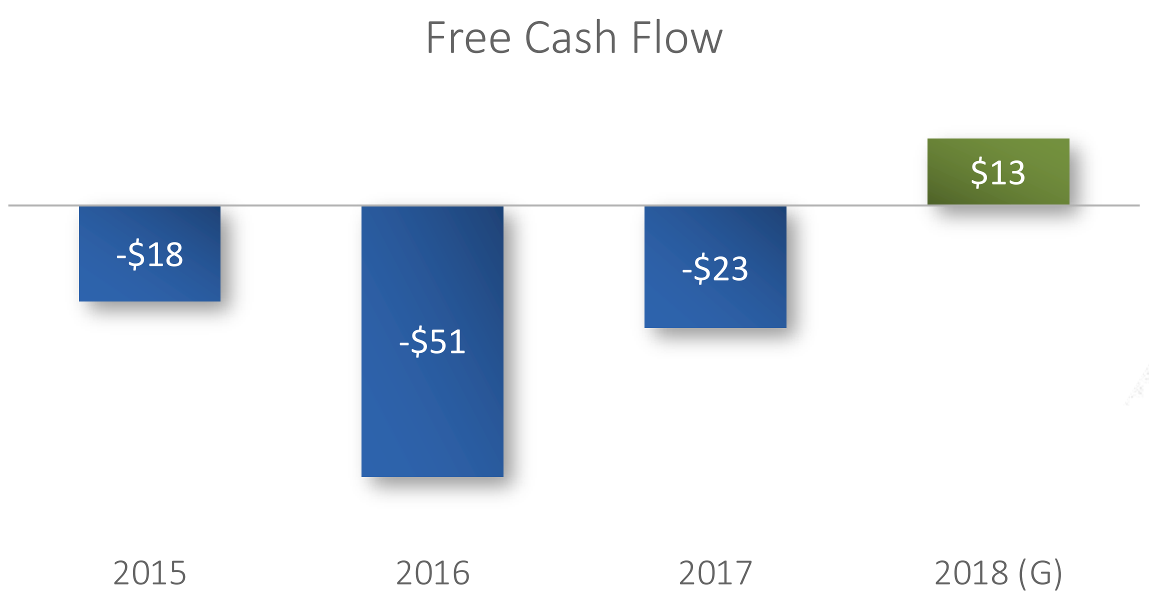




Cash Flow


Operating Cash Flow
$37
-$15
$18
$50
2015
2016
2017
2018 (G)


Capex
$55
$36
$41
$38
2015
2016
2017
2018 (G)


Free Cash Flow
-$18
-$51
-$23
$13
2015
2016
2017
2018 (G)

Summary

- Performance inflected in Q4 2017
  - Return to year-over-year billings growth
  - First quarter of non-GAAP profitability as a public company
  - Positive free cash flow

- We expect continuation of path to profitable growth in 2018

FireEye

Long Term Financial Model

Baseline Assumptions

- Following 2017, FireEye returns to consistent top-line growth
- Billings growth rate is key model driver
- Average contract length modeled to reflect small year-over-year decline
- Product sales declining at a moderate rate over time

Billings Growth Framework

Reflects Adoption of ASC 606

	2017 Actual (recast for ASC 606)		2018 Guidance Midpoint		2022 12.5% CAGR (2018-2022)	
	Mix	YoY Change	Mix	YoY Change @ midpoint	Mix	CAGR @ midpoint
Product & Related Subscriptions & Support	54%	-17%	45-55%	4%	25-30%	~1%
Cloud Subscriptions and Managed Services	26%	3%	25-35%	26%	55-60%	~30%
Services	20%	13%	15-20%	7%	15%	~5%
Total	**$761M**	**-7%**	**$820M**	**8%**	**$1,310M**	**12%**
Assumptions:						
Average Contract Length in months	28 months		26-27 months		20-24 months	

From Here to There – Long Term Operating Model

Non-GAAP[1] As a % of revenue, except Subscription & Support Billings %	2017	2018 Guidance	Long-Term Model[2]	Key Drivers
Gross Margin	75%	74% - 75%	**75% - 80%**	Subscription mix, cost of cloud operations
Research & Development	24%	23% - 24%	**14% - 18%**	Headcount Mix onshore vs. offshore
Sales & Marketing	41%	39% - 41%	**32% - 36%**	Headcount Sales productivity, channel leverage
General & Administrative	11%	9% - 11%	**7% - 8%**	Headcount efficiency
Operating Margin	0%	1% - 2%	**19% - 22%**	All of the above
Operating Cash Flow Margin (% of Revenue)	2%	5% - 6%	**25% - 30%**	Billings growth, consistent DSO, expense control

[1] Non-GAAP. Reconciliation to nearest GAAP metric in Appendix. Reconciliation not available for forward looking metrics.
[2] Targeting model achievement in 2022.

Long-term Sensitivity Analysis: Billings[1] CAGR

Billings CAGR, 2018 – 2022	10%	12.5%	15%
Non-GAAP Billings	$1,200	$1,310	$1,430
Revenue	$1,090	$1,140	$1,230
Revenue CAGR	7%	9%	11%
Non-GAAP Gross Margin	75% - 80%	75% - 80%	75% - 80%
Non-GAAP Operating Margin	16%-18%	19%-22%	19%-22%

[1] Non-GAAP. Reconciliation to nearest GAAP metric in Appendix. Reconciliation not available for forward looking metrics.

Summary

- Intelligence and expertise differentiates our solutions
- Innovation will drive long-term growth and operating leverage
- Positioned to extend profitability and cash generation into 2018 and beyond.

FireEye

BUILT TO LAST

FRANK VERDECANNA EVP AND CHIEF FINANCIAL OFFICER

FireEye

EXECUTIVE PANEL / Q&A

Executive Panel

Kevin Mandia
CHIEF EXECUTIVE OFFICER

Frank Verdecanna
EXECUTIVE VP
CHIEF FINANCIAL OFFICER
CHIEF ACCOUNTING OFFICER

Bill Robbins
EXECUTIVE VP OF
WORLDWIDE SALES

Vasu Jakkal
EXECUTIVE VP
CHIEF MARKETING OFFICER

Grady Summers
EXECUTIVE VP
CHIEF TECHNOLOGY OFFICER

Phil Montgomery
VP
PRODUCT MARKETING

FireEye

EXECUTIVE PANEL / Q&A

Thank You

For additional information about FireEye, visit www.FireEye.com

APPENDIX

Billings and Revenue Supplemental Breakout Categories

Historically ~20% of product billings and revenue

ASC 605

Product Offering	Supplemental Breakout Categories	Revenue Recognition
Term licenses (tech fees, FSO)	Product	Ratable
Management & Forensic Appliances (CMS, PX)		Up front
Detection/Protection Appliances (NX, EX, FX, AX, HX)		
Support & Maintenance	Support	Ratable over contract term
Dynamic Threat Intelligence (DTI) for NX, EX, FX, AX, HX URL/Attachment Database (EX only)	Product Subscription	
Email Threat Prevention (ETP), FireEye as a Service/Managed Defense, iSIGHT threat intelligence, Helix, Threat Analytics Platform (TAP)		
Mandiant Services	Services	As Delivered

ASC 606

Product Offering	Supplemental Breakout Categories	Revenue Recognition
Term licenses (tech fees, FSO)	Product & Related Subscriptions and Support	Up front
Management & Forensic Appliances (CMS, PX)		
Detection/Protection Appliances (NX, EX, FX, AX, HX)		Ratable (4 years)
Support & Maintenance		Ratable over contract term
Dynamic Threat Intelligence (DTI) for NX, EX, FX, AX, HX URL/Attachment Database (EX only)		
Email Threat Prevention (ETP), FireEye as a Service/Managed Defense, iSIGHT threat intelligence, Helix, Threat Analytics Platform (TAP)	Cloud Subscriptions and Managed Security Services	Ratable over contract term
Mandiant Services	Services	As Delivered

Single performance obligation

Shaded areas = Ratable revenue recognition