FireEye

CYBER DEFENSE LIVE

Hong Kong 2018

Extend Your Security Operation with Frontline Intelligence and Expertise

Anthony Ng

Sr. Director, Systems Engineering

How Quickly Are You Able To Detect And Respond?

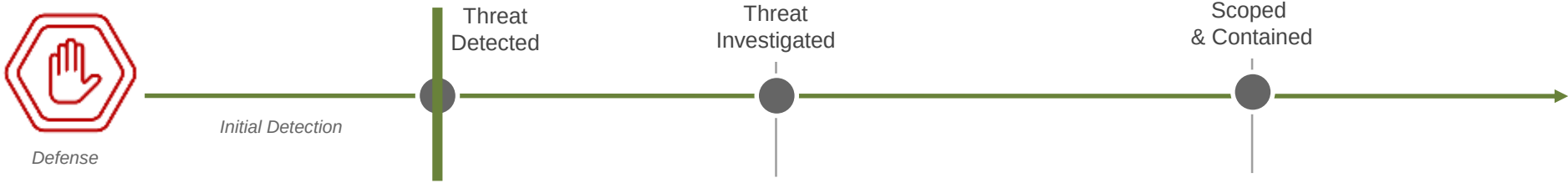
Am I targeted? Am I compromised? Am I ready to respond?

498 Days

Average days before a breach was detected*

$3.62M

Average cost of a breach**



Faster detection and response reduces business risk.

* 2018 FireEye Mtrends Report
**2017 Ponemon Cost of a Data Breach Study

What Keeps You From Confidently Answering Those Questions?

Security budgets are flat or falling

Scarcity of Security Expertise

Increasing Financial Consequences

Limited visibility into emerging campaigns

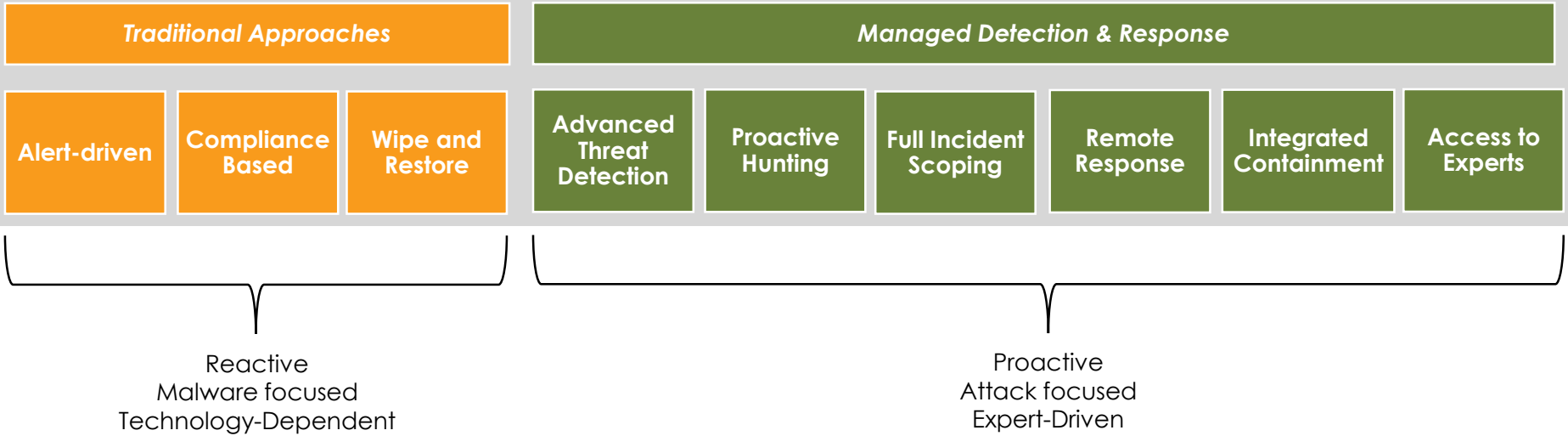
Lack of intelligence context

Sophisticated Attackers Continually Evolve

Gartner: Market Shift to MDR

Managed detection and response improves threat detection and incident response capabilities via a turnkey approach to detecting threats that have bypassed traditional security measures.

By 2020, 80% of worldwide managed security service providers (MSSPs) will offer MDR-type services. Gartner, Market Guide for MDR 2017



Introducing FireEye Managed Defense

FireEye Managed Defense is a managed detection and response (MDR) service that combines **industry recognized cyber security expertise**, **FireEye technology** and **unparalleled knowledge of attackers** to identify threats early and **reduce the consequences of a breach**.

FireEye Managed Defense: How it Works

Knowledge Center - Intelligence & Front Line Experience

- Product Telemetry
- Victim Intelligence
- Research & Development
- Adversary Intelligence
- Campaign Intelligence

Technology-Driven Detection & Visibility Across All Vectors

HELIX

- Network Security
- Email Security
- Endpoint Security
- Threat Analytics

	Key Features	Customer Benefits
Intelligence-Led Detection	▪ Pro-active Hunting ▪ Campaign Response ▪ Identify the Threats That Matter	**Identify threats early to help prevent a security incident.**
Experience-Driven Response	▪ Incident Scoping ▪ Rapid Response ▪ Remediation & Containment	**Disrupt the attack chain and act to mitigate damage and reduce the impact of an incident**
Guidance and Insight	▪ Access to Intelligence ▪ Access to Expertise	**Improve efficiency of your resources and augment with ours.**

Intelligence-Led Detection

Identify intrusions that have evaded other controls to avoid security incidents

Proactive Hunting

Mitigate the risk of an attacker going undetected for an extended period of time, exposing intellectual property, sensitive customer data, or financial resources.

Campaign Response

Leverage FireEye's unique vantage point to identify emerging threats and campaigns which may impact customers broadly, or in a particular industry or region.

Identify the Threats that Matter

Cut through the noise of the "alert-cannon" to focus on the most impactful threats, saving your team time and effort.

Experience-Driven Response

Rapidly scope the extent and implications of a breach to reduce cost and impact

Incident Scoping

Ensure response efforts are appropriate to the situation to avoid inadvertent destruction of critical evidence or wasted cycles.

Rapid Response

In most cases, avoid the added cost of onsite IR by acting quickly to contain impact.

Remediation & Containment

Ensure thorough remediation and mitigate likelihood that attackers return or maintain access while meeting regulatory breach notification requirements.

Guidance & Insight

Make more informed decisions to apply resources where they can be most impactful

Access to Intelligence

Make better decisions about how to respond and protect your assets.

Access to Expertise

Extend your team with access to hundreds of FireEye experts.

Attacks, not Malware; Answers, not Alerts

Proactive	→	We don't wait for product alerts, we proactively hunt for evidence of attacker activity
Attack-Focused	→	We don't solely look for malware, we look for malicious attacker behaviors, regardless of motivation
Expert-Driven	→	We use our frontline expertise to continually refine our hunting and investigation methodologies
Answers, not Alerts	→	In-depth investigation reports and response recommendations so you can quickly assess risk and take action

2017 Proof Points

100M FireEye Product Detections

6M Managed Defense Alerts Ingested

120K Analyst Investigations

67 mins Median time to investigate and respond

9400 Hunting Activities Conducted

352 Customers Hunting Cases

3600 High/Medium Severity Cases

199 Rapid Response Incidents

94% Resolved without requiring Rapid Response

98% Resolved without full Incident Response

* Approximated for annual

2017 Proof Points

19

Known FIN/APT Attack Groups

45%

Customers protected through Community Protection

$3.62M*

Average Cost of a Breach

7

New Attack Groups Identified

23

Community Protection Events in 2017

56%

IR Customers Re-targeted within 1 year

* Approximated for annual

Key Benefits of Managed Defense

Experience

Leverage **+100K hours of IR experience** per year from the most impactful breaches

Intelligence

Access to **nation-state grade intel** collection supported by 150+ intel analysts

In-region Expertise

7 global SOCs; In-region technical engagement managers 24x7x365

Campaign Visibility

Visibility into and protection from **campaigns across similar industries** as they unfold

Proactive Hunting

Integrated hunting and investigation across network, logs and endpoint

Adaptive Detection

In-depth **understanding of adversary TTPs** to focus on detecting attacker methods and behaviors

700
frontline cyber security experts

99.8%
validated compromises without requiring IR

4M
endpoints monitored through managed defense

10M
threat actor personas tracked

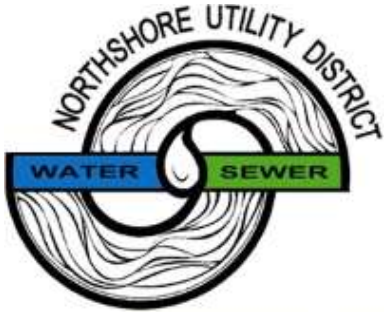
What Customers Are Saying about Managed Defense

International Global Telecom Company

- **Who:** Globe Telecom
- **Need:** Extend the capabilities of in house resources
- **Quote:** "It's really reassuring to know there is a team monitoring our environment round the clock. Managed Defense gives me validation that a potential threat is actually real and immediately follows this by looking for signs of compromise. If things start to get really active, I now don't have to worry that we won't have the necessary bandwidth to effectively respond to incidents: If I need extra feet on the ground, I get them from FireEye."

What Customers Are Saying about Managed Defense

North American Utility Company



- **Who:** Northshore Utility District
- **Need:** Adding advanced capabilities with resource constraints
- **Quote:** "Managed Defense gives us access to broader set of capabilities without having to recruit additional headcount in an already overly competitive job market. Having this caliber of expertise and technology on call when we need it most really gives us the best of both worlds."

The Value of Managed Detection and Response (MDR)

Time to Detect

498 days

Average time it takes an APAC organizations to discover a breach

+

Time to Respond

32 days

Average time it takes an organization to respond to a breach

=

Time to deal with a prevention failure

530 days

Average time it takes an organization to respond to a breach

Without FireEye Managed Defense

Equifax *said the breach happened between mid-May and July. It discovered the hack on July 29.*

Source : http://money.cnn.com/2017/09/08/technology/equifax-hack-qa/index.html

Uber *was first hacked in October 2016 and discovered the data breach the following month.*

Source : https://www.reuters.com/article/us-uber-cyberattack/ubers-messy-data-breach-collides-with-launch-of-softbank-deal-idUSKBN1DM2F9

Yahoo *three years to discover and disclose the breach, and almost four years to complete the investigation.*

Source : https://www.wired.com/story/yahoo-breach-three-billion-accounts/

VS

67 mins

Median time FE MD takes to investigate and provide response recommendations to an alert in minutes

With FireEye Managed Defense

Source : Mtrends 2018

FireEye

Thank You