The New Defense Strategy: Protect, Detect and Correct

Andrea Rossini | Sales Engineer

April 2016

NEW.NEXT.
SECURITY IN FOCUS.

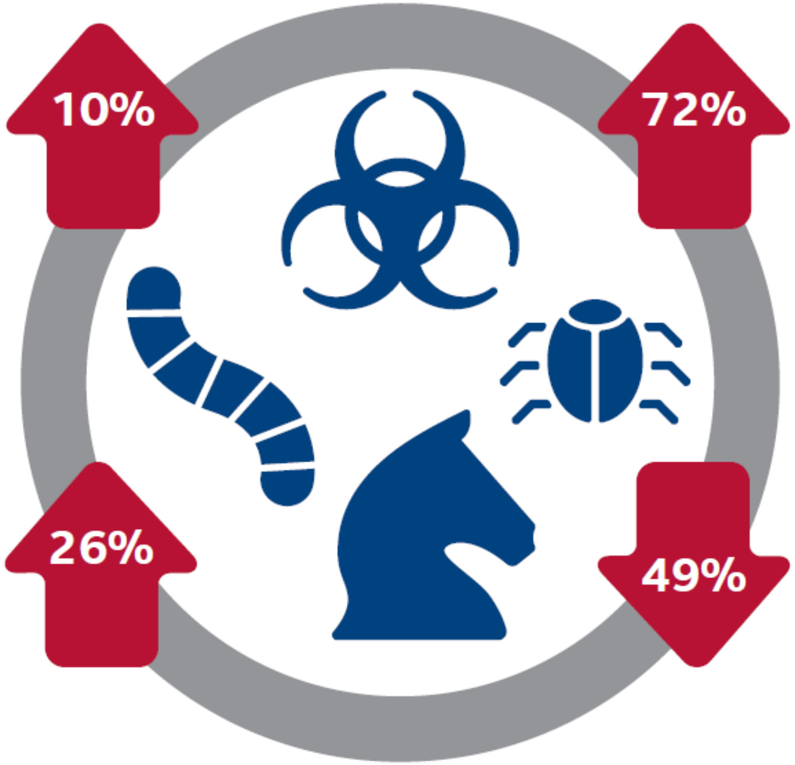
Threat Trends – Q4 2015

Malware continues to grow and get more sophisticated…

There are 316 new threats every minute, or more than 5 every second.

Malware

After three quarters of decline, **new malware grew 10% in Q4** with 42 million samples, the second highest on record.



Mobile Malware

72% more new mobile malware samples in Q4.

Google's monthly updates to Android may have forced attackers to develop malware more frequently.

Ransomware

26% more new ransomware samples in Q4.

Open-source ransomware code and ransomware-as-a-service make attacks simpler.

Attacks are financially lucrative with little chance of arrest.

Rootkits

Samples dropped by 49% in Q4.

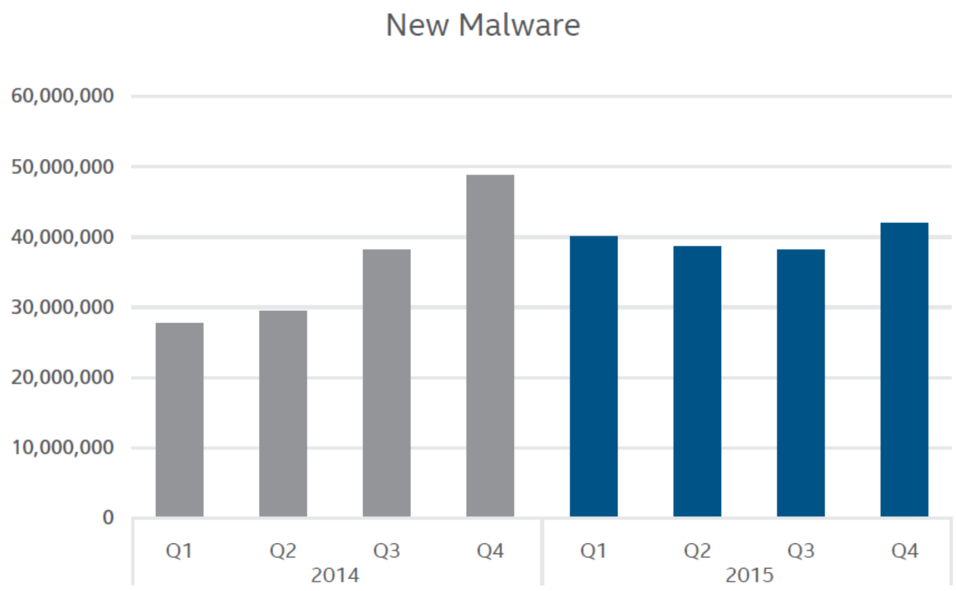
Long-term downward trend driven by 64-bit Intel CPUs and 64-bit Windows.

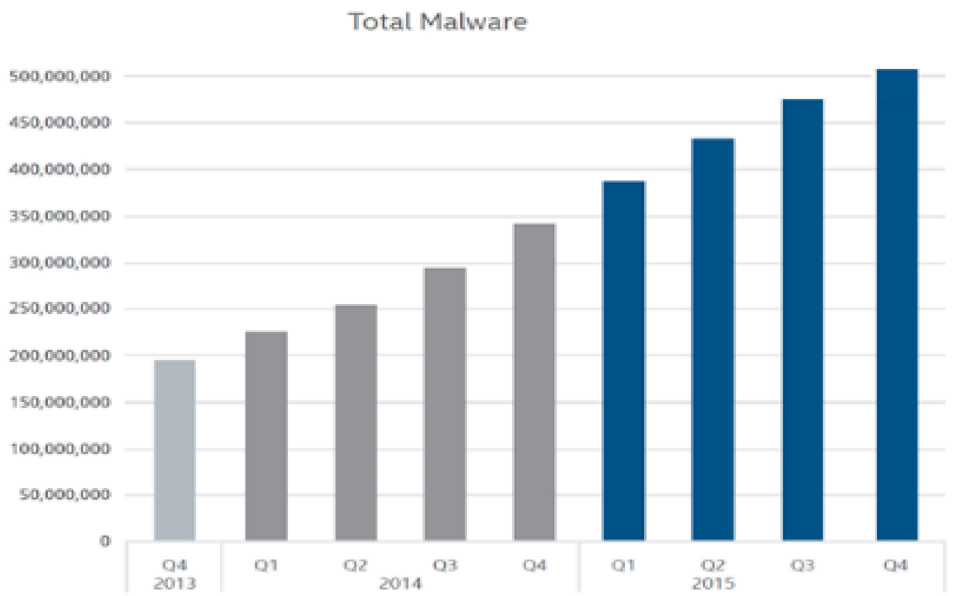
Source: McAfee Labs

Malware

New record for new malware samples

December 31, 2015: we reach 516 million samples (~ 480k new and unique malicious binaries classified daily)





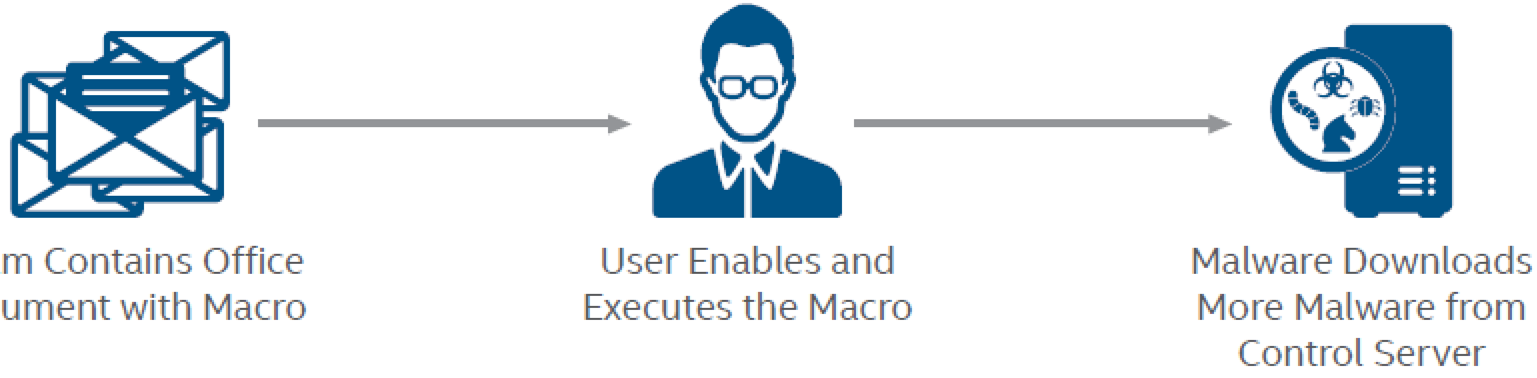
After three quarters of decline, the number of new malware samples resumed its ascent in Q4, with 42 million new malicious hashes discovered, 10% more than in Q3 and the second highest on record. The growth in Q4 was driven, in part, by 2.3 million new mobile threats, 1 million more than in Q3.

Source: McAfee Labs

The Return of Macro Malware

Microsoft Office macro threats are at their highest level in six years.

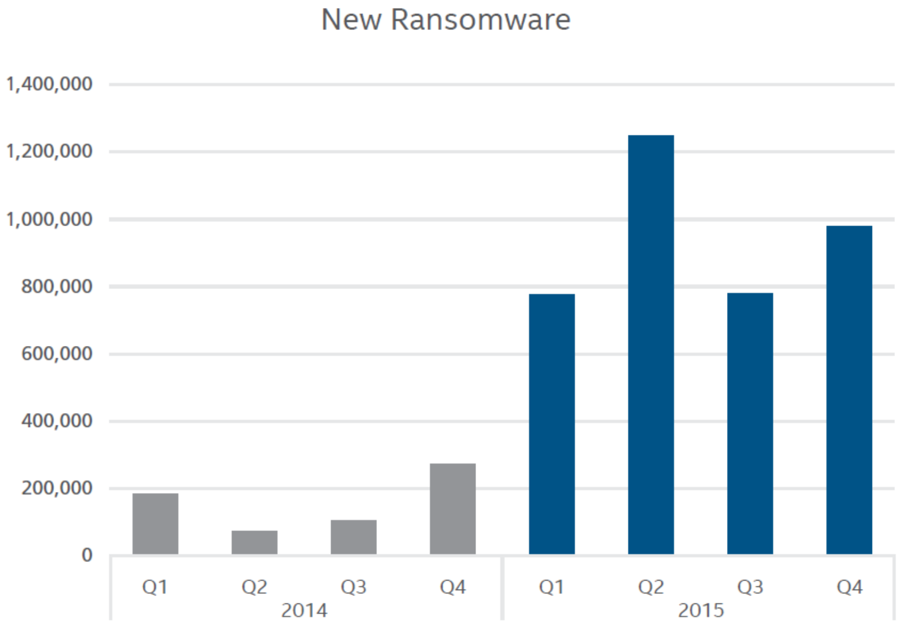
Macro Malware Infection Chain

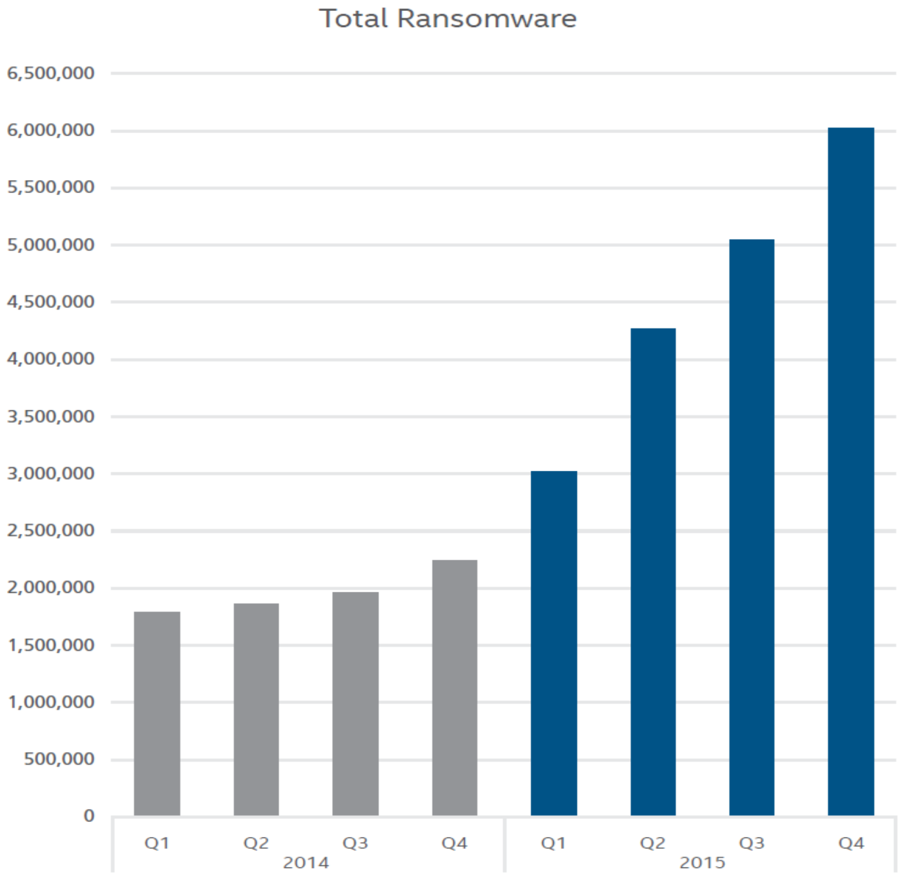

Spam Contains Office Document with Macro
User Enables and Executes the Macro
Malware Downloads More Malware from Control Server

Successful campaigns deliver clever new macro malware through documents attached to sophisticated spam (Most of them are Microsoft OFFICE). The malicious macros remain hidden even after they have downloaded their payloads.

Ransomware

26% growth in Q4 2015



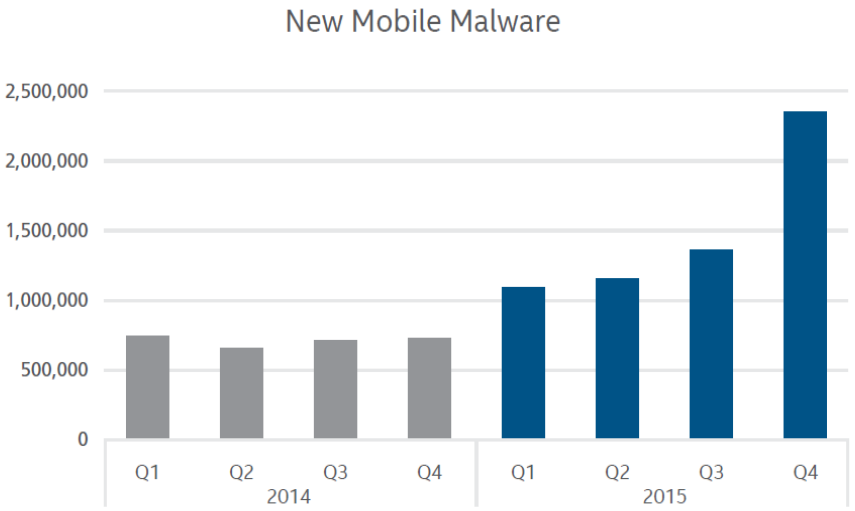


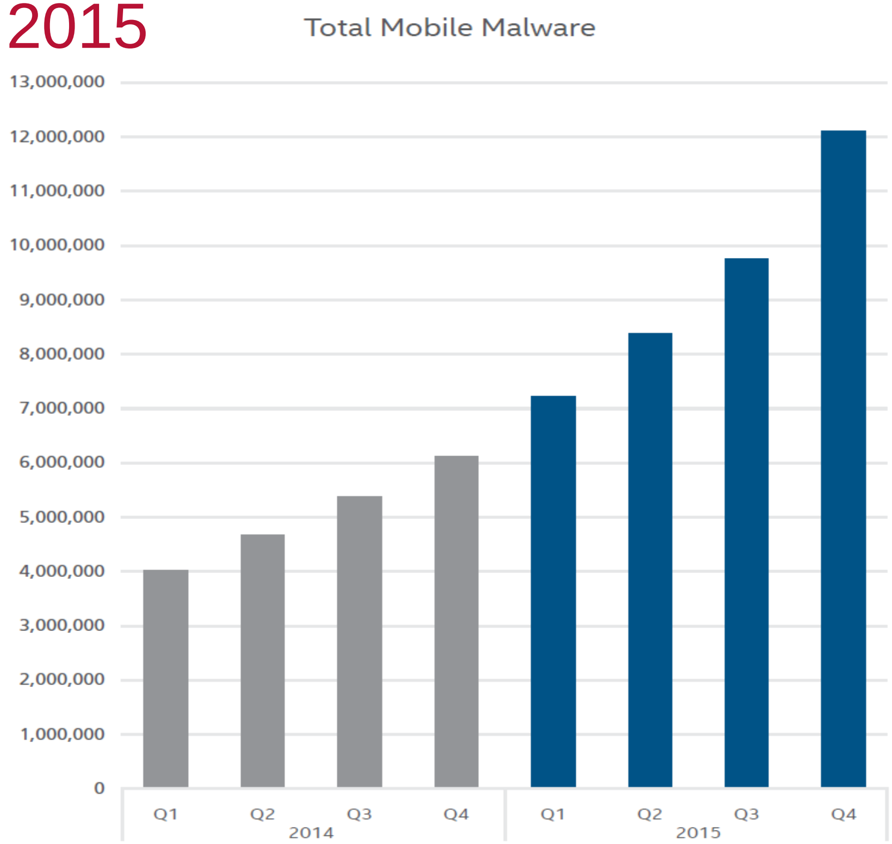
Open source ransomware code (for example, Hidden Tear, EDA2)
Ransomware-as-a-service (Ransom32, Encryptor)
TeslaCrypt and CryptoWall 3 campaigns also continue

Source: McAfee Labs

Mobile Malware

72% new mobile malware samples in Q4 2015

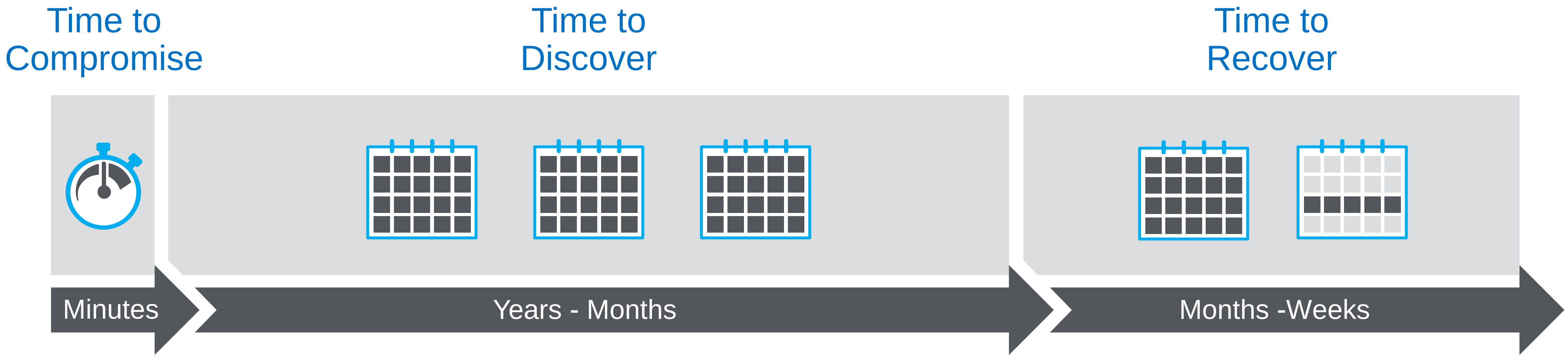




Authors to develop new malware more frequently in response to the enhanced security by Google updates, in each monthly release of the operating system. The detection of newly developed mobile malware is reflected in our Q4 statistics.

Source: McAfee Labs

Current ThreatScape Realities



Time to Compromise

Time to Discover

Time to Recover

Minutes

Years - Months

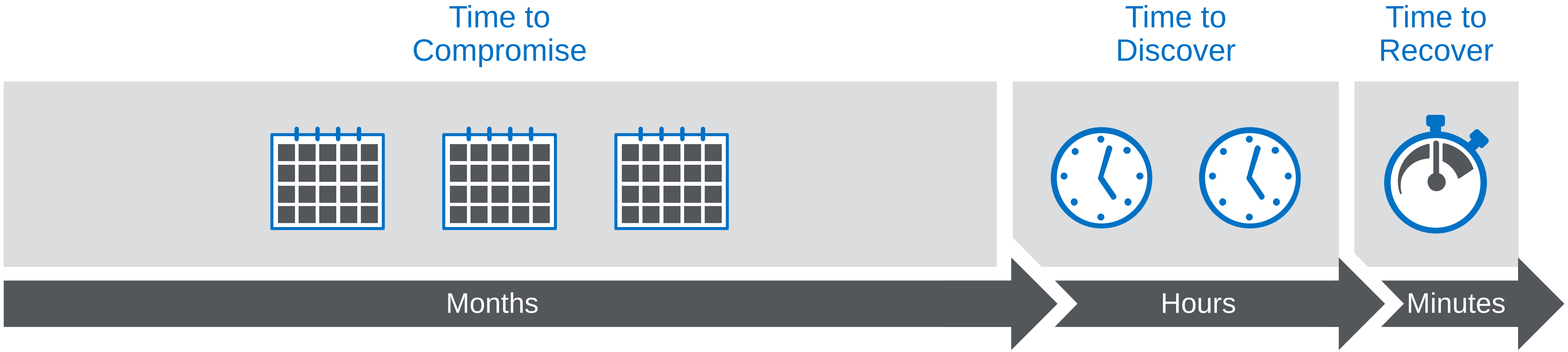
Months -Weeks

Minimal Adversarial Effort

Overwhelmed Security Teams

$$$ Catastrophic Impact $$$

Business and Security Outcomes



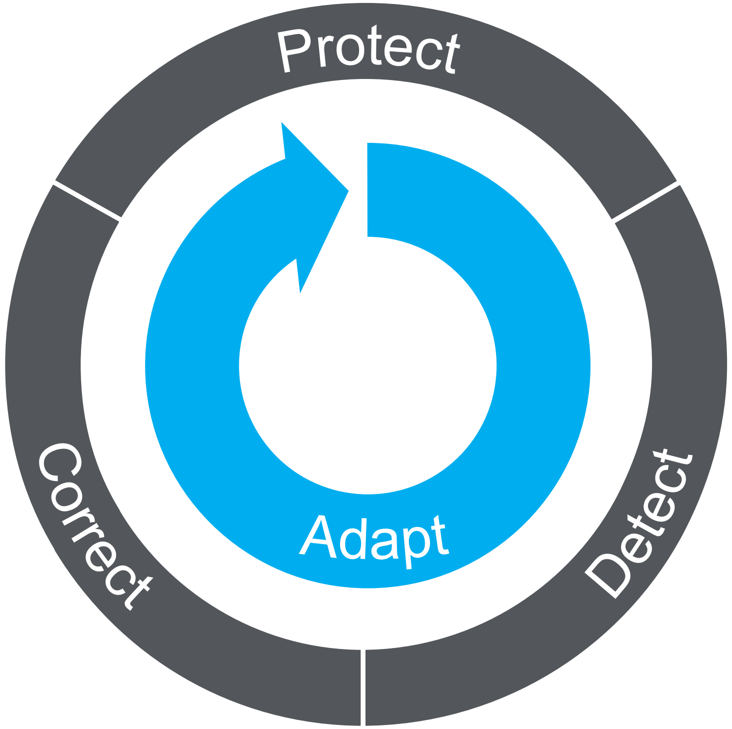
Significant
Adversarial Effort

Optimized
Security Teams

$ Minimized
Impact $

Threat Defense Lifecycle's Value

Continuous, Automated, and Shared Threat Intelligence



Protect – Stop pervasive attack vectors while also disrupting never-before-seen techniques and payloads.

Detect – Illuminate low-threshold maneuvering through advanced intelligence and analytics.

Correct – Improve triage and prioritize response as part of a fluid investigation.

Adapt – Apply insights immediately throughout an integrated security system.

Threat Defense Platform: Protect, Detect, Correct

Endpoint Security

Threat Intelligence Exchange

Data Protection

Network Security Platform

McAfee Web Gateway

McAfee ePO

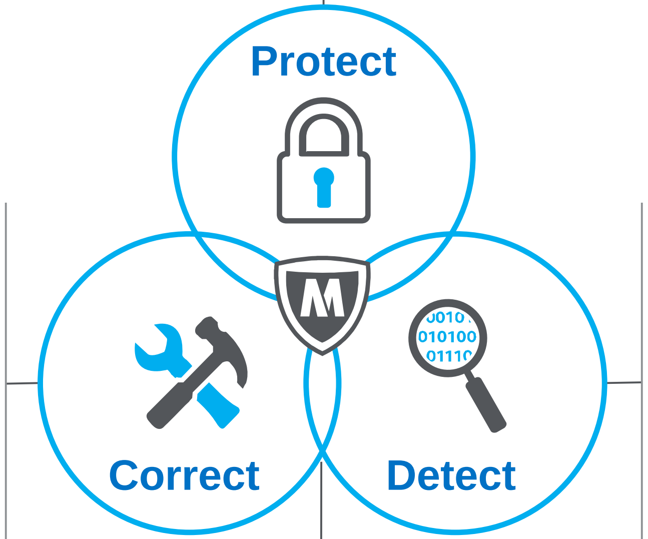
McAfee Enterprise Security Manager (SIEM)

McAfee Threat Intelligence Exchange/Data Exchange Layer

McAfee Advanced Threat Defense

McAfee Active Response

McAfee ePO



McAfee Advanced Threat Defense

McAfee Enterprise Security Manager (SIEM)

McAfee Threat Intelligence Exchange/Data Exchange Layer

McAfee Active Response

McAfee ePO

SIA Partners

DXL: an open layer

DATA EXCHANGE LAYER

Ultra-fast persistent bidirectional messaging fabric

OPEN ECOSYSTEM

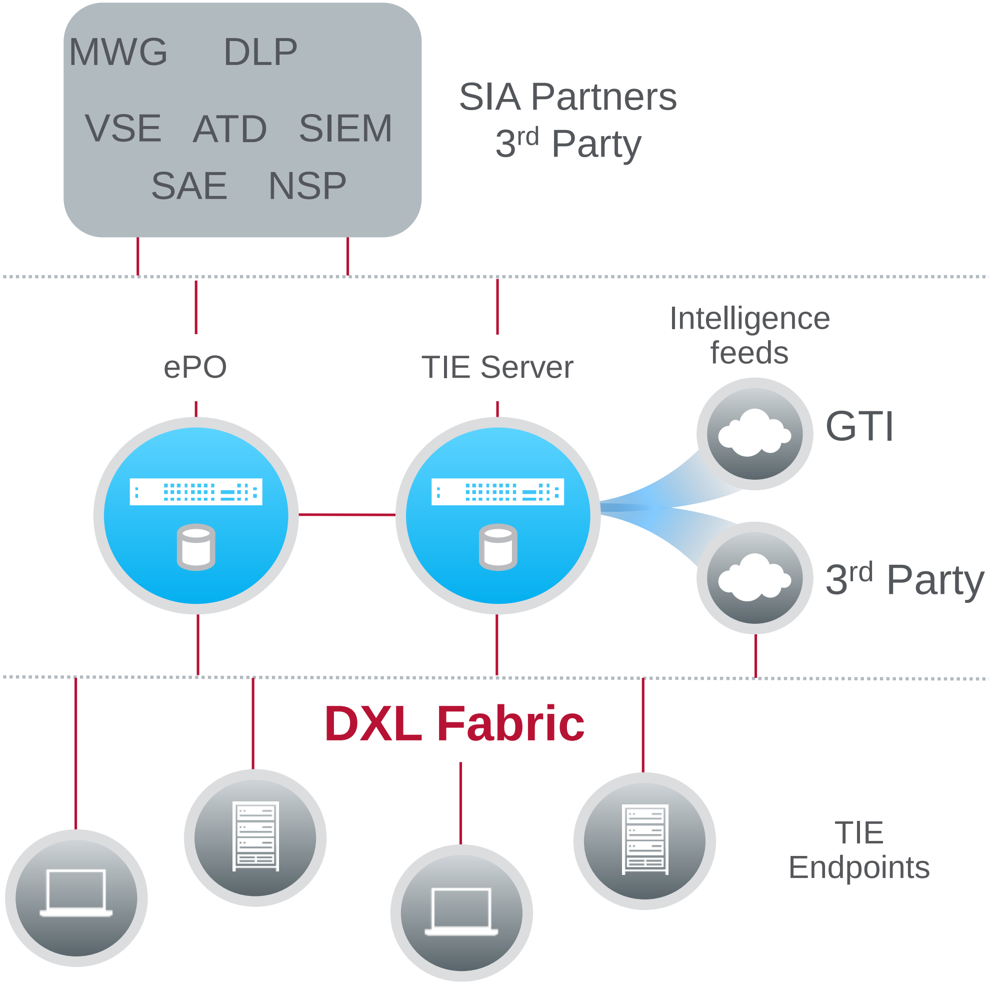
Security-Connected
IT Infrastructure

TIE SERVER

Incident Response Knowledgebase
Local Intelligence

TIE ENDPOINTS

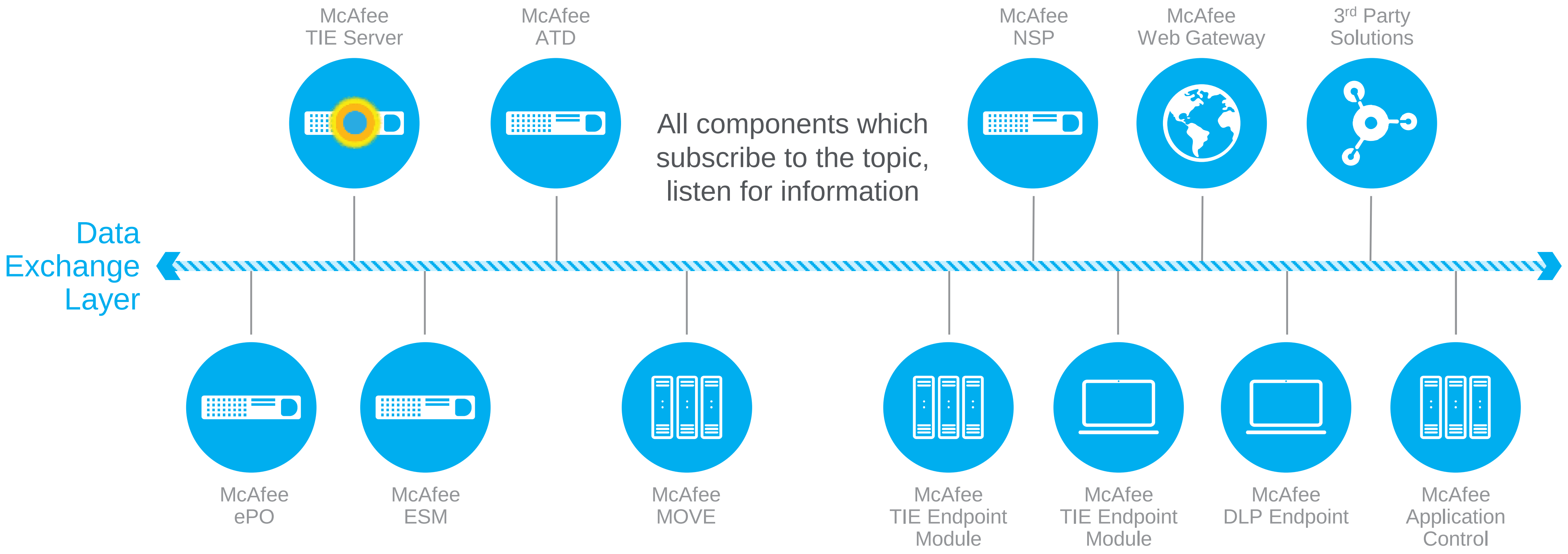
Execution-time reputation analysis & protection



NEW.NEXT.
SECURITY IN FOCUS.

McAfee Data Exchange Layer (DXL)

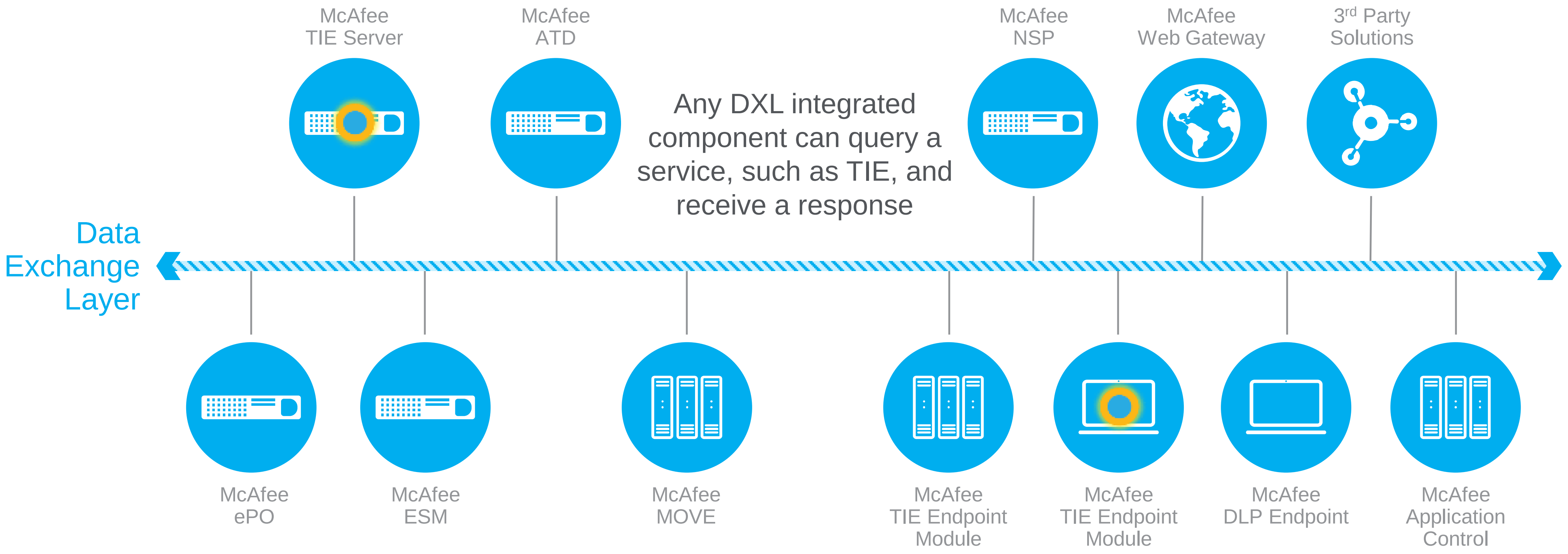
Publish/Subscribe Model



McAfee TIE Server
McAfee ATD
All components which subscribe to the topic, listen for information
McAfee NSP
McAfee Web Gateway
3rd Party Solutions
Data Exchange Layer
McAfee ePO
McAfee ESM
McAfee MOVE
McAfee TIE Endpoint Module
McAfee TIE Endpoint Module
McAfee DLP Endpoint
McAfee Application Control

McAfee Data Exchange Layer (DXL)

1:1 Query/Response Model



Any DXL integrated component can query a service, such as TIE, and receive a response intel® Security