BUILDING INNOVATIVE APT STRATEGIES TO PROTECT ORGANIZATIONS

Mr. Koh Ssu Han,
Solutions & Engineering Lead, Intel Security South East Asia

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

Source: McAfee Labs, Q4 2015

Threat Statistics – Q4 2015

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

Malware

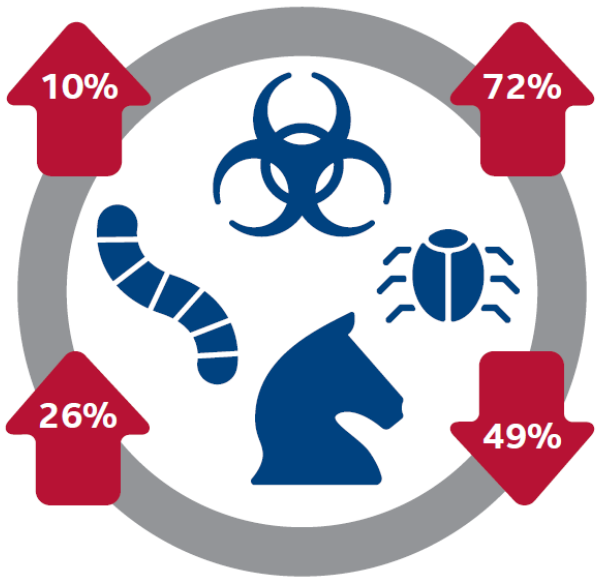
After three quarters of decline, **new malware grew 10% in Q4** with 42 million samples, the second highest on record.

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.



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.

Rootkits

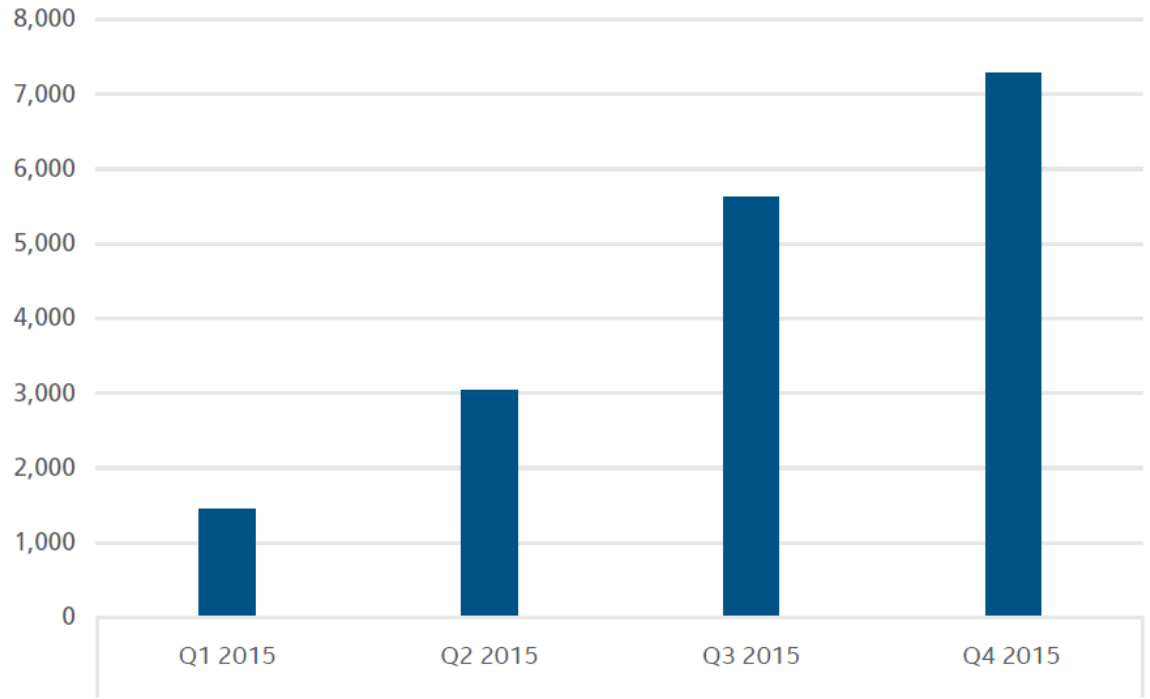
Samples dropped by 49% in Q4.

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

Source: McAfee Labs, Q4 2015

Adwind Java-based Malware

Adwind .jar file submissions to McAfee Labs

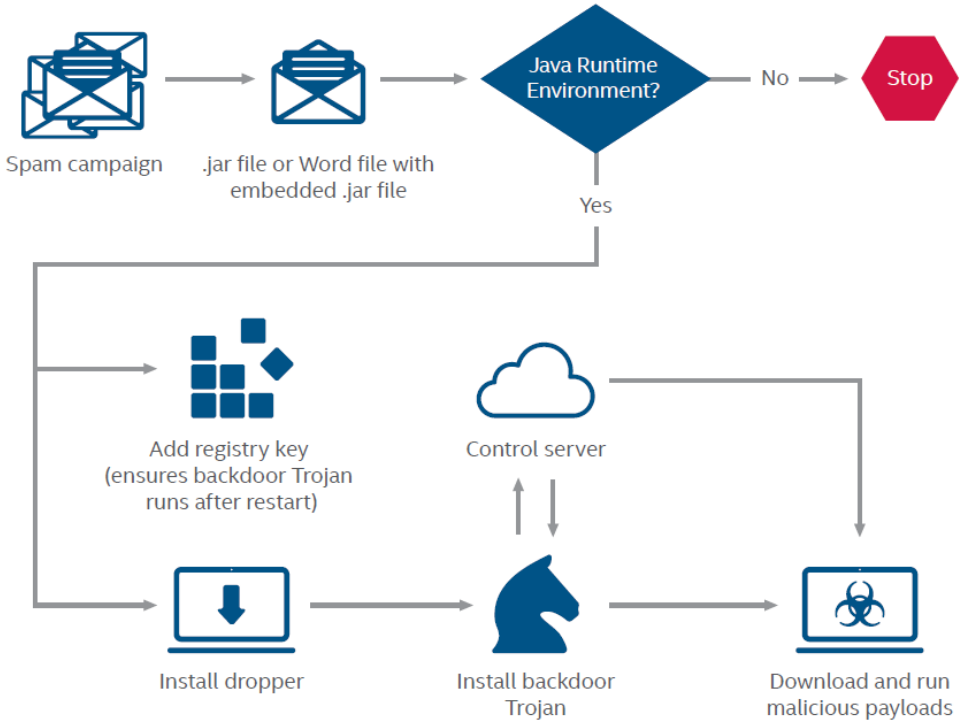


Source: McAfee Labs, 2016

Key Topic

Adwind Java-based Malware

Typical attack method for Adwind



Source: McAfee Labs, 2016

Key Topic

Adwind Java-based Malware

Post-infection attack examples

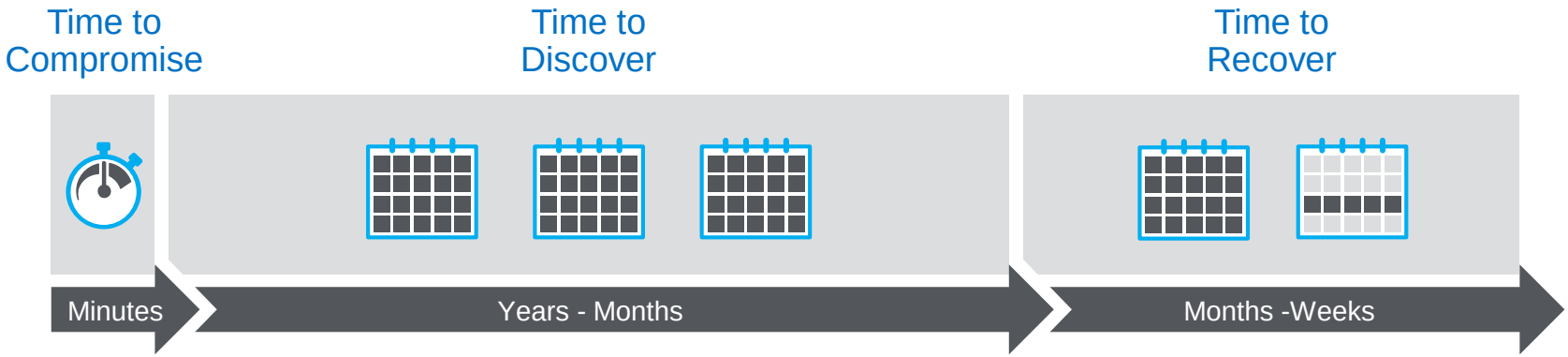
- Log keystrokes
- Modify and delete files
- Download and execute further malware
- Take screenshots
- Access the system's camera
- Take control of the mouse and keyboard
- Update itself, and more.

Indicators of Compromise

"%AppData%\[random folder name]\[random filename].jar"

HKCU\Software\Microsoft\Windows\CurrentVersion\Run] "[random value name"="[Java Runtime Environment directory]\javaw.exe" – jar "%AppData%\[random folder name]\[random filename].jar"

Current ThreatScape Realities



Minimal Adversarial Effort

Overwhelmed Security Teams

$$$ Catastrophic Impact $$$

Current Industry Realities

Standardize integration and communication to break down operational silos

Disjointed API-Based Integrations

Result

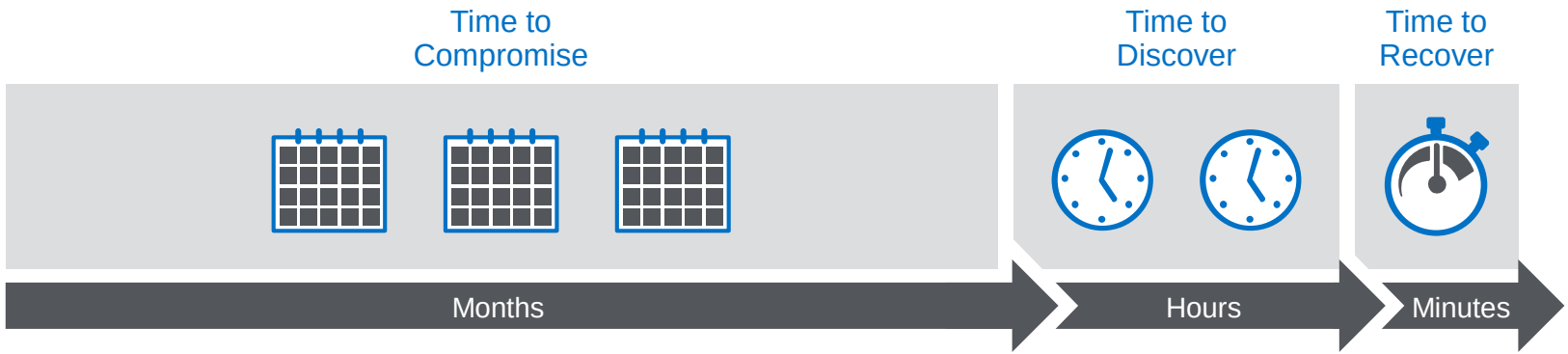
Slow, heavy, and burdensome

Complex and expensive to maintain

Limited vendor participation

Fragmented visibility

Business and Security Outcomes



Significant Adversarial Effort

Optimized Security Teams

$ Minimized Impact $

Industry Collaboration through DXL

Standardize integration and communication to break down operational silos

Disjointed API-Based Integrations

Result

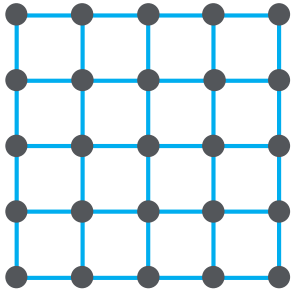
Slow, heavy, and burdensome

Complex and expensive to maintain

Limited vendor participation

Fragmented visibility

Collaborative Fabric-Based Ecosystem (DXL)



Result

Fast, lightweight, and streamlined

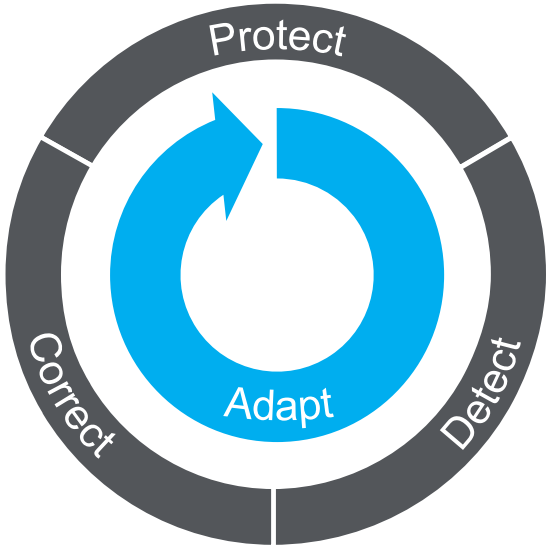
Simplified and reduced TCO

Open vendor participation

Holistic visibility

Threat Defense Lifecycle

Shift to a continuous defensive cycle



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.

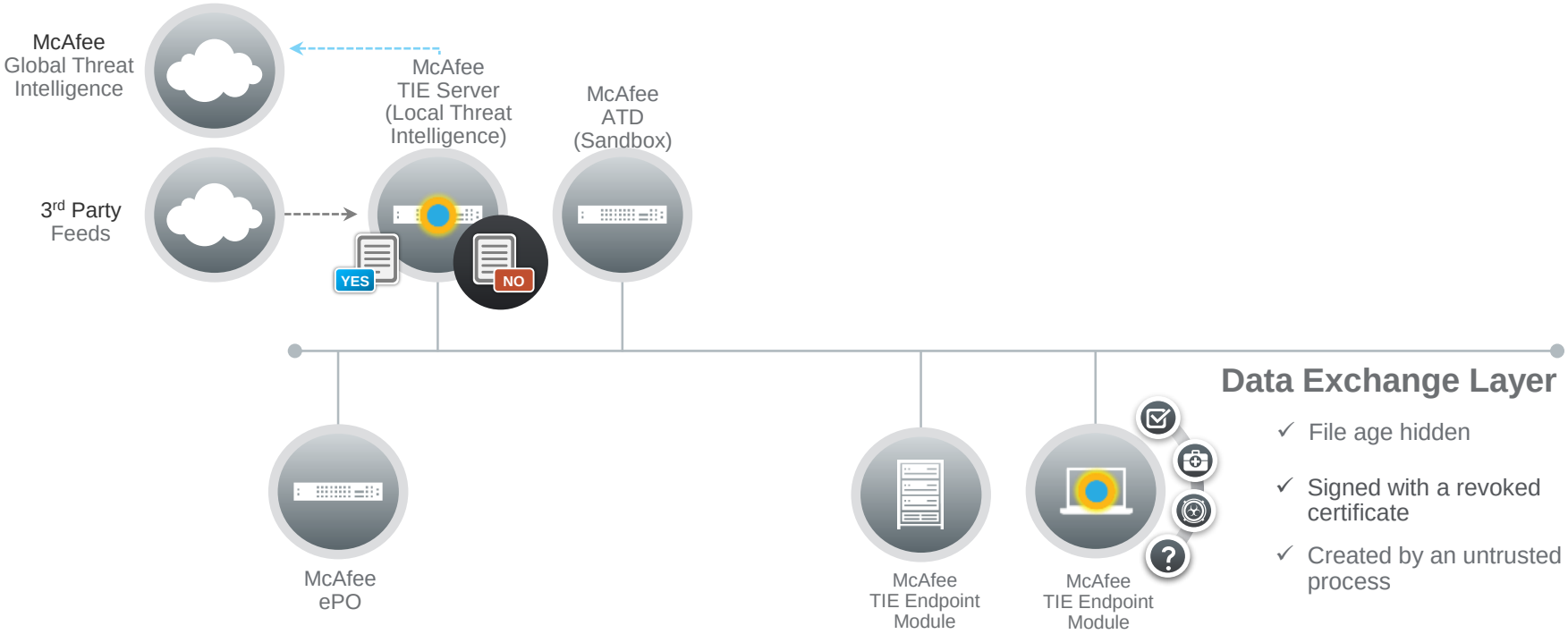
Delivering Business and Security Outcomes

Solving the industry's most acute pain points

	Complexity	Time	Constraints
Problem	Billions of connected devices and exponential growth in data and a paradigm shift to the cloud resulting in an increased number of threats.	Increased attacker sophistication and rising cost of breaches, resulting in a need to detect and respond to threats faster.	Rising security needs and growing product complexity, resulting in a shortage of qualified security talent.
Solution	Resolve more threats… Extend beyond discrete and siloed security, to a cohesive threat lifecycle defense; "Cloudify" and "mobilize" protection.	…faster… Deliver automated detection and correction; operate as a security system.	…and with fewer resources Integrate and streamline and automate processes to improve operational efficiency

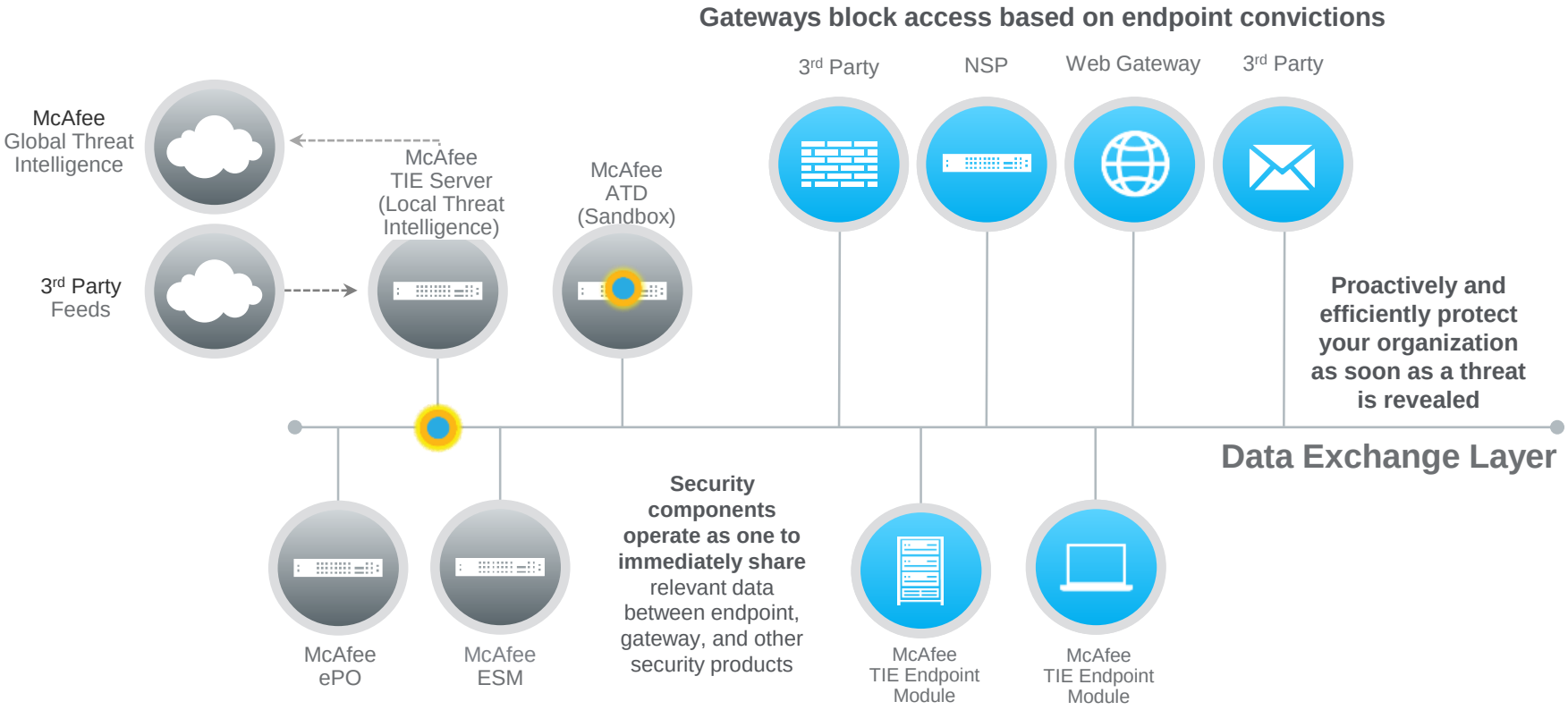
Use case 1 : Adapt and Immunize

— From Encounter to Containment in Milliseconds



Use case 1 : Adapt and Immunize

— From Encounter to Containment in Milliseconds



Integrated System Value

Requirements	Disconnected Architecture	Integrated System
Time to Respond	1455:17 min ≈24hr	6:50 min 410 sec
Time to Protect	254:02 min ≈4.2hr	1:08 min 68 sec
Capacity	6 IOC/day	210 IOC/day
Coverage Gaps	Gap in hash data sent to SIEM	0
Data Confidence	2	4
Consoles	6	2
Manual Steps	19	4

EFFICACY

- Average Time to Respond reduces dwell time to less than 7 min
- Full use of intelligence gives customer a higher confidence that security is effective

EFFICENCY

- 66% reduction in technology components reduces the cost of security
- 85% decrease in manual steps allows customer to repurpose the analysts to harder tasks
- 3500% increase in IOC handling capacity


intel
Security