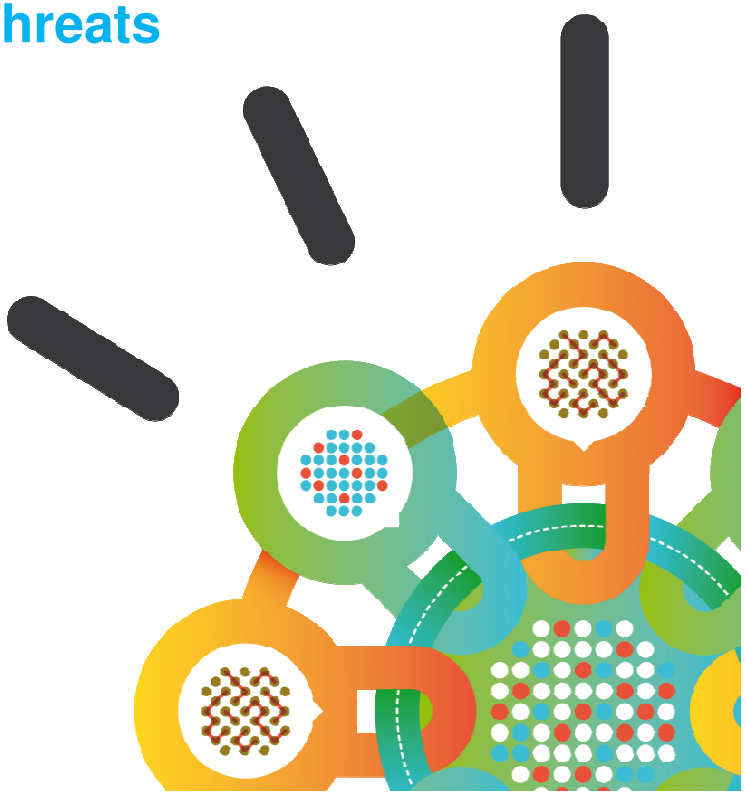
Security Intelligence.
Think Integrated.

Trusteer Apex

IBM Advanced Protection for Advanced Threats

Alexander Schmidt
alex.schmidt@de.ibm.com
+49-(0)172-6837141



© 2014 IBM Corporation

Zielgerichtete Angriffe, Mythos oder Realität?

- Dienstag, 08.04.2014, 18:13 Cyber-Attacken fast verdoppelt, Hacker haben es auf unsere Autoindustrie abgesehen. Die Zahl von Cyber-Angriffen hat sich 2013 fast verdoppelt. Insbesondere die Autoindustrie war Ziel der Attacken. Der Anstieg habe weltweit bei 91 Prozent gelegen, teilte die auf Informationssicherheit spezialisierte US-Firma Symantec am Dienstag mit. Haupt-Ursprungsländer waren demnach die USA und China. In Deutschland war den Angaben zufolge die Automobil-Industrie das attraktivste Ziel für Hacker-Angriffe. Gezielte Cyber-Angriffe waren 2011 und 2012 noch um 42 Prozent angestiegen. Die „große Veränderung“ der vergangenen Jahre sei der Übergang von breiten Cyber-Attacken gegen Millionen Computer auf gezielte Angriffe, sagte Laurent Heslault von Symantec. Die Cyber-Kriminellen nehmen Symantec zufolge vor allem zwei Berufsgruppen ins Visier: Persönliche Assistenten und PR-Mitarbeiter, „um sich Zugang zu Daten von Personen mit interessanterem Profil“ zu verschaffen - Unternehmenschefs oder berühmte Persönlichkeiten. Mittelständische Unternehmen mit 250 bis 500 Angestellten und Firmen mit mehr als 2500 Mitarbeitern standen im Zentrum.

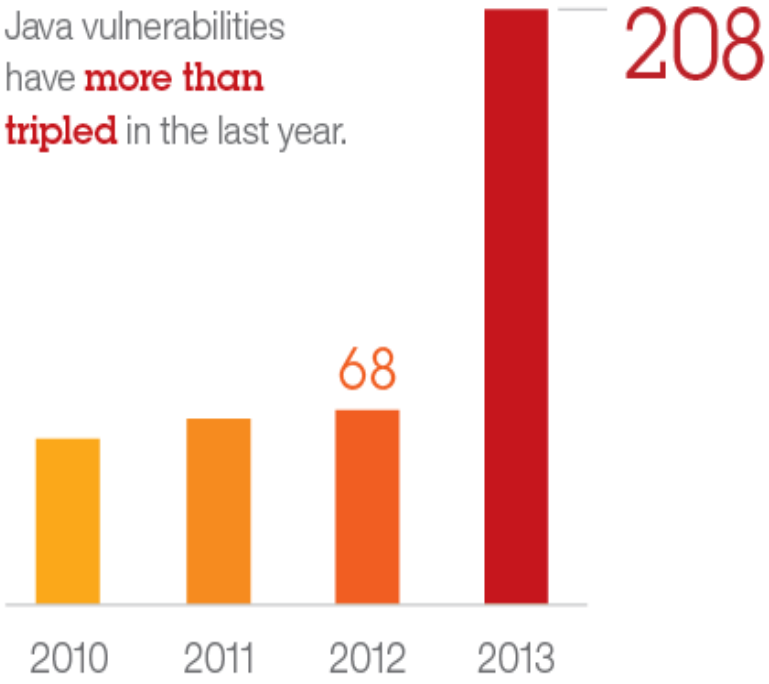
© 2014 IBM Corporation

Die Rolle der Applikation

Attackers are targeting Java vulnerabilities over others to exploit end-user applications and infiltrate organizations

Oracle Java is a **top target** for exploits, exposing organizations to attacks.

Java vulnerabilities have **more than tripled** in the last year.



Source: IBM X-Force Threat Intelligence Quarterly - 1Q 2014

© 2014 IBM Corporation

Introducing IBM Trusteer Apex

Re-defining endpoint protection for the advanced threat landscape

Trusteer Fast Facts:

Acquired by IBM August 2013
Adds endpoint protection capabilities to the IBM Security Portfolio

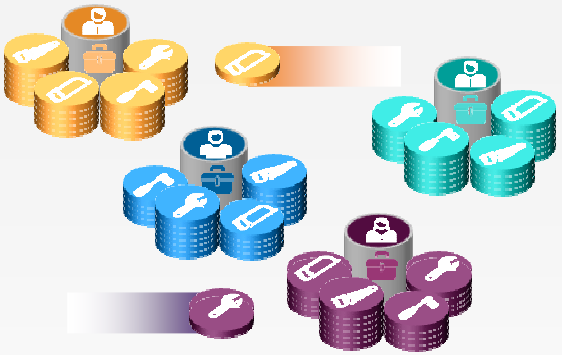
Advanced Threat Defense Leaders
Analyzing and preventing APT's for the last 8 years

Unique Integrations
Integrated into IBM Threat Protection System

© 2014 IBM Corporation

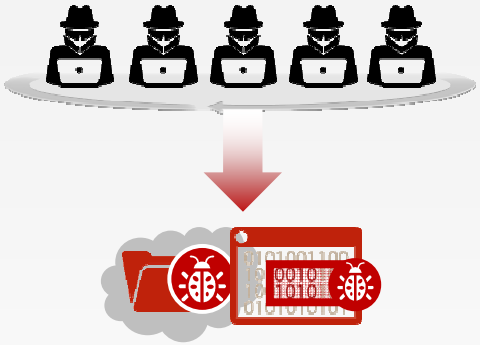
Do you have the right weapons?

Fragmented market with point products



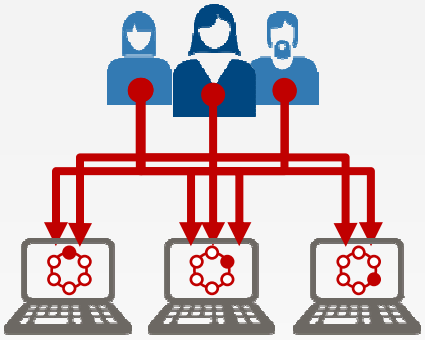
- Endpoint protection market is highly fragmented with many point solutions
  - e.g., Sandboxing, application control, whitelisting

Major security control gaps



- Existing products offer no controls for major attack vectors
  - e.g., Zero-day exploits, applicative Java attacks

Challenging manageability and operations



- Advanced threat solutions are difficult and costly to operate
- Difficult to scale manual remediation processes to thousands of enterprise endpoints
- High false positive rates
- Whitelisting processes on endpoints non-manageable

© 2014 IBM Corporation

Trusteer Apex

Preemptive, low-impact defense for enterprise endpoints

ADVANCED MULTI-LAYERED DEFENSE

Comprehensive endpoint defense against advanced threats

LOW OPERATIONAL IMPACT

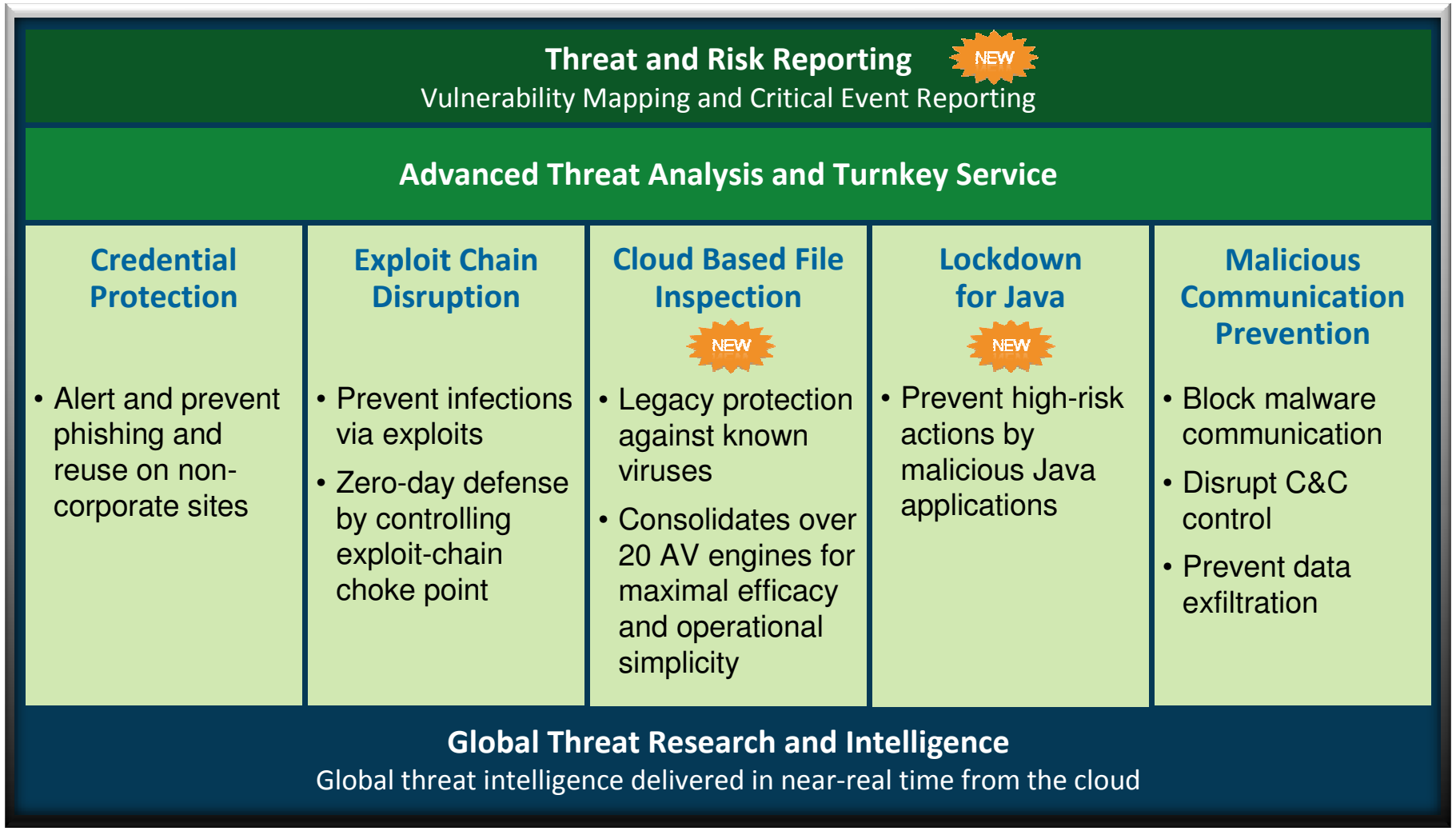
Low overhead on IT / security teams, transparent to end users

DYNAMIC INTELLIGENCE

Advanced threat intelligence collected from tens of millions of endpoints

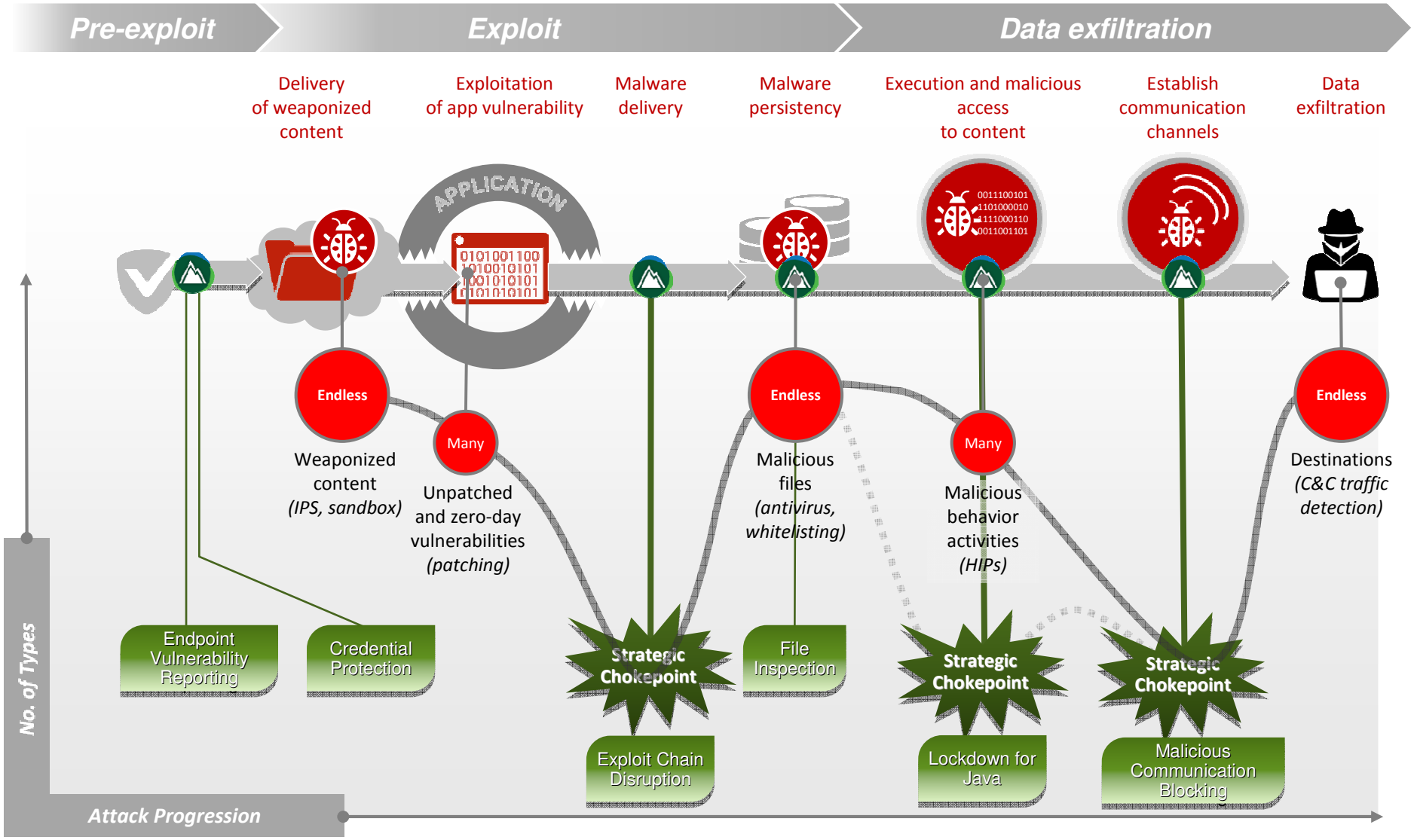
© 2014 IBM Corporation

Apex multi-layered defense architecture



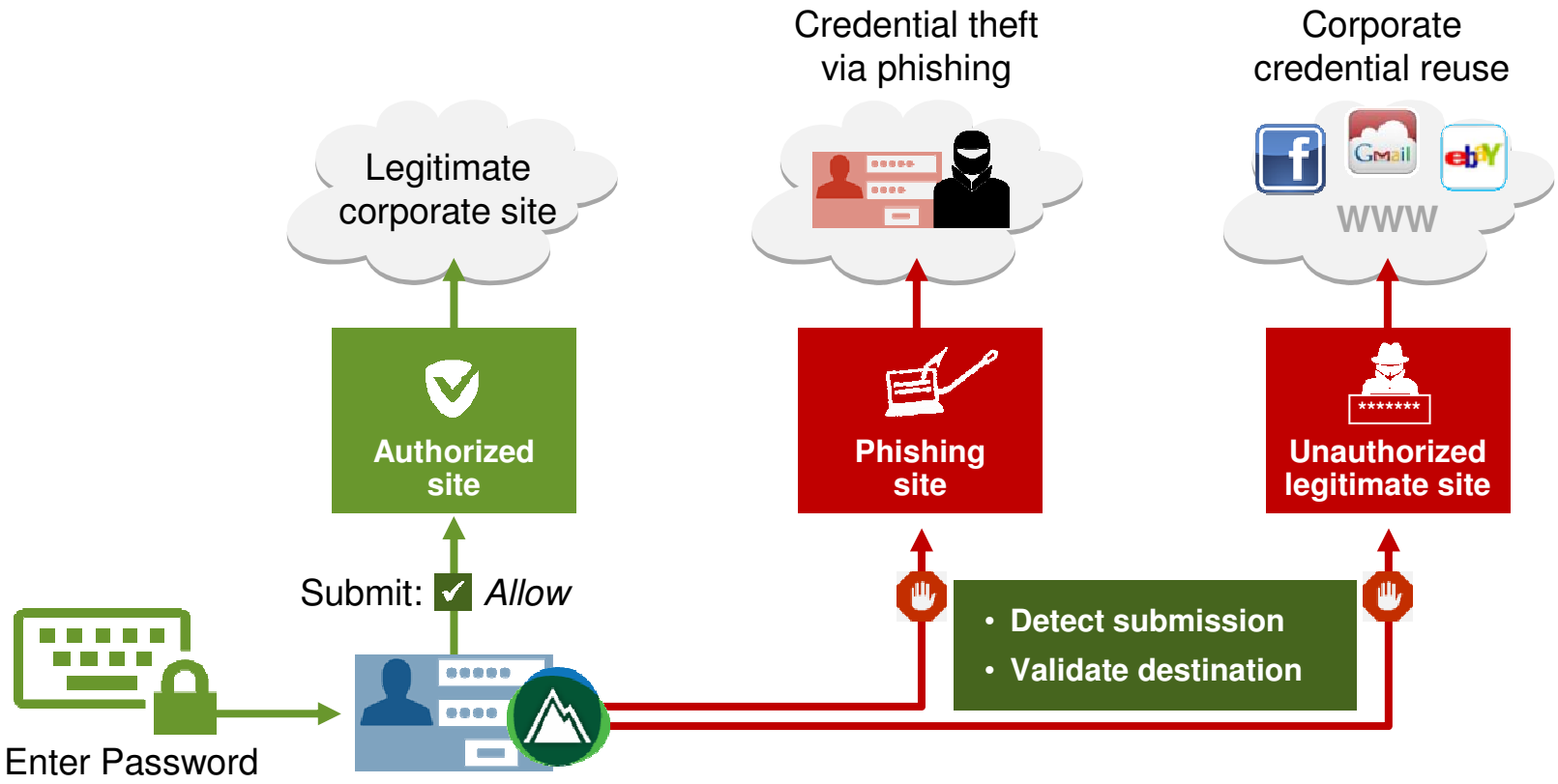
© 2014 IBM Corporation

Controlling exploit-chain chokepoints



© 2014 IBM Corporation

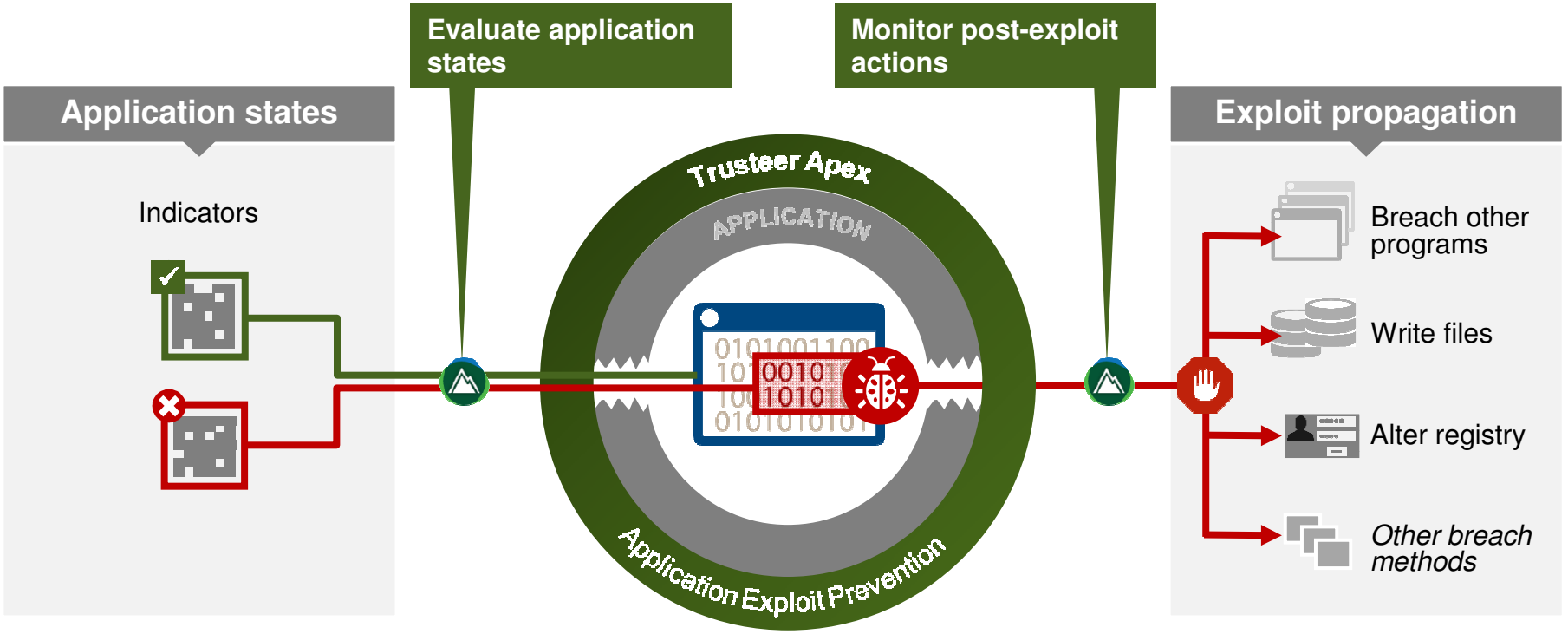
Corporate credentials protection



© 2014 IBM Corporation

Exploit chain disruption

Block zero day attacks without prior knowledge of the exploit or vulnerability

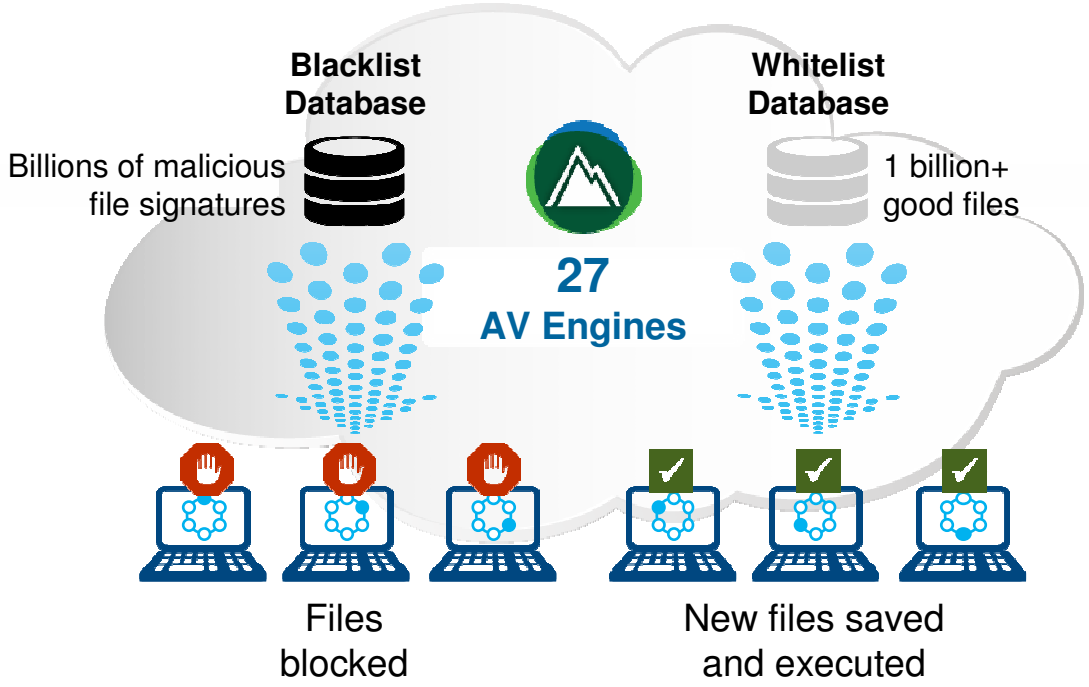


- Correlate application state with post-exploit actions
- Apply allow / block controls across the exploit chain

© 2014 IBM Corporation

Cloud-based file inspection

Legacy threat protection with improved operability

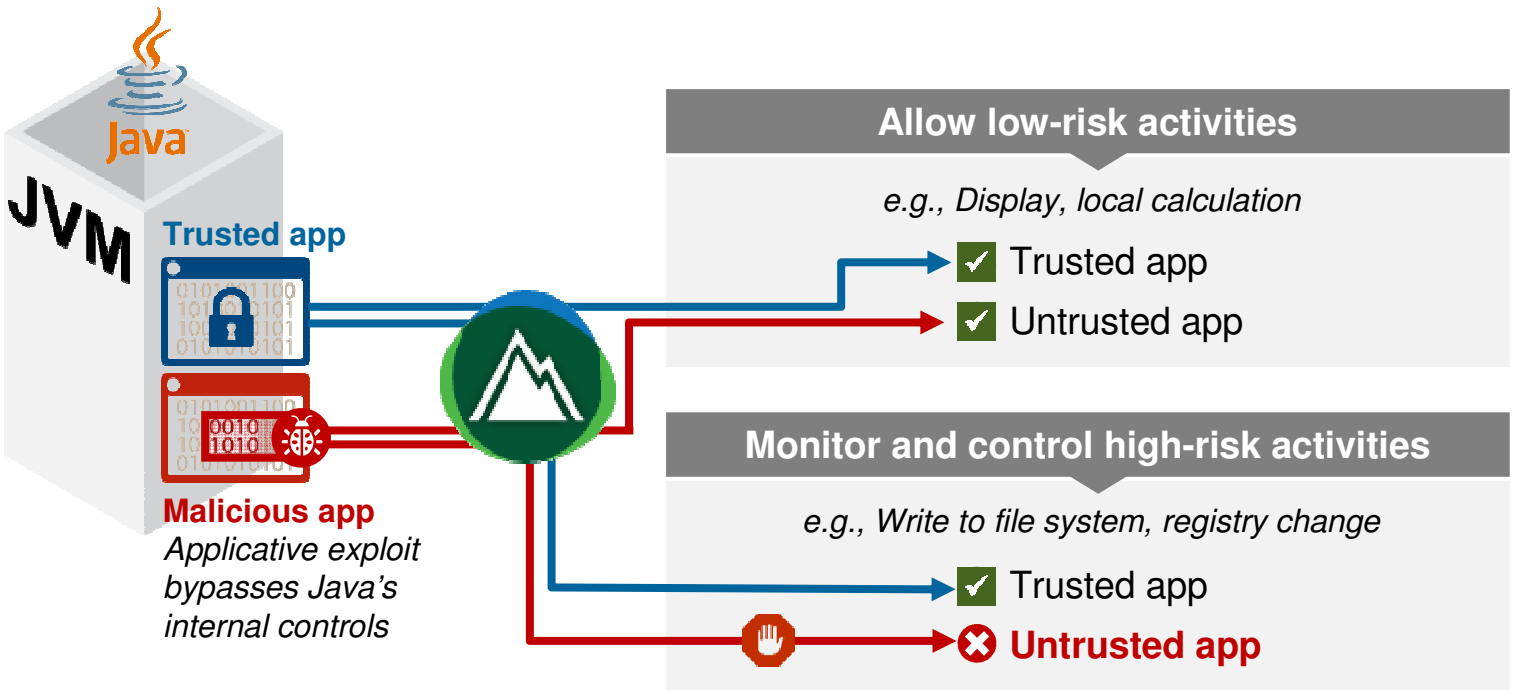


- No signature file update process to endpoints
- Combined knowledge: As good as the first AV that detects the malware

© 2014 IBM Corporation

Lockdown for Java

Monitor and control high risk Java application actions

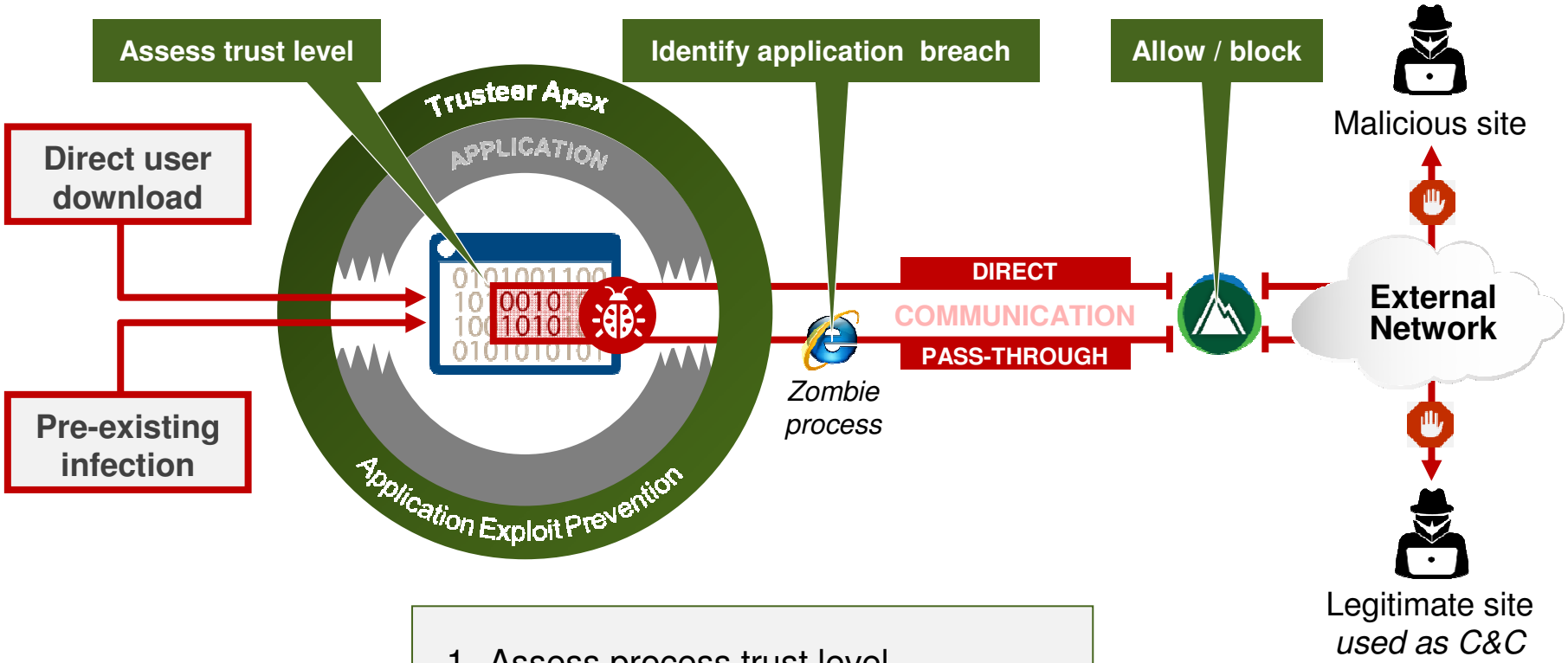


- Malicious code is blocked while legitimate Java applications are allowed
- Trust for specific Java apps is granted by Trusteer / IT administrator

© 2014 IBM Corporation

Malicious communication blocking

Block suspicious executables that attempt to compromise other applications or open malicious communication channels



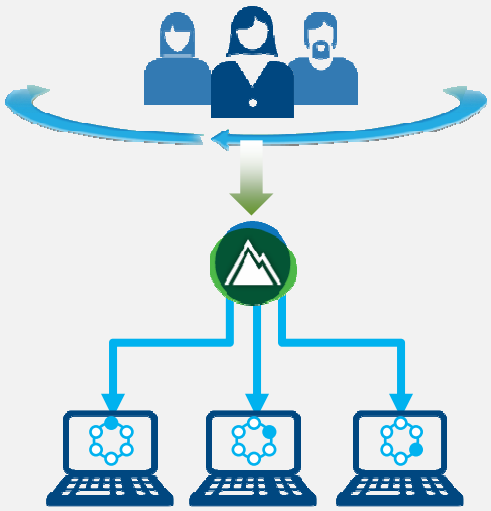
1. Assess process trust level
2. Identify process breach
3. Allow / block external communication

© 2014 IBM Corporation

Low operational impact

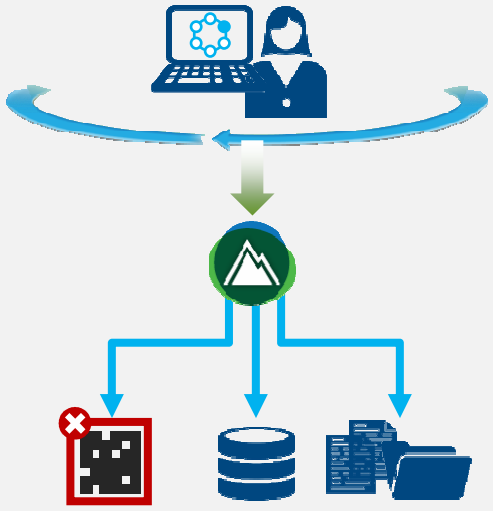
Advanced threat analysis and turnkey service

Low impact to IT security team



Eliminate the traditional security team approach (detect, notify, and manually resolve)

Low-footprint threat prevention



Minimize impact by blocking only the most sensitive actions

Exceptional turnkey service

Centralized risk assessment service

Directly update endpoint users

© 2014 IBM Corporation

Why Apex

Apex is re-defining endpoint protection for advanced threats with a holistic approach:

Advanced Multi-Layered Defense

- ✓ Credential Protections
- ✓ Exploit Chain Disruption
- ✓ Lockdown for Java
- ✓ Malicious Communication Blocking
- ✓ Cloud-Based File Inspection
- ✓ Endpoint Vulnerability Reporting

Low Operational Impact

- ✓ Low impact to IT security team
- ✓ Low-footprint threat prevention
- ✓ Exceptional turnkey service

Dynamic Intelligence

- ✓ Combines the renowned expertise of X-Force with Trusteer malware research
- ✓ >100 million endpoints collecting intelligence
- ✓ Protections dynamically updated near real-time