BusinessConnect
A New Era of Smart
June 12 2014

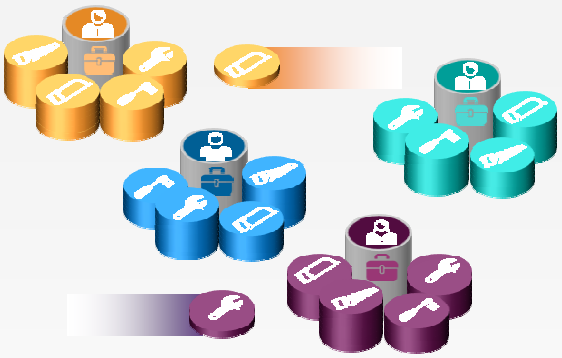
Trusteer Apex

Re-defining endpoint protection for the advanced threat landscape

Tamar Shafler
Sr. Product Manager, Trusteer Apex

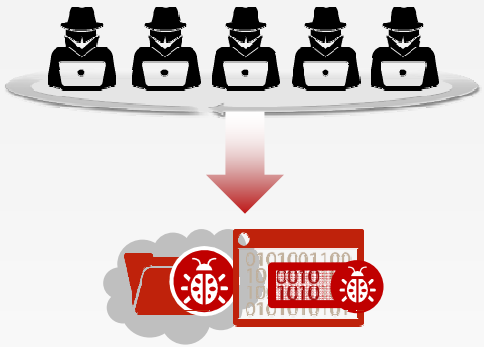
Key challenges in advanced endpoint threat solutions

Fragmented market with point products



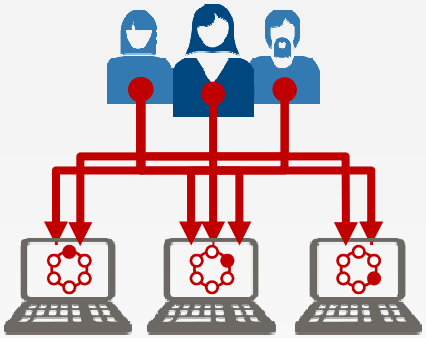
- Endpoint protection market is highly fragmented with many point solutions
  - e.g., Sandboxing, application control, whitelisting

Major control gaps



- Existing products offer no controls for major attack vectors, eg
  - Zero-day exploits (recent IE vulnerability)
  - 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

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

Apex multi-layered defense architecture

Threat and Risk Reporting NEW

Threat central for vulnerability mapping and critical event reporting

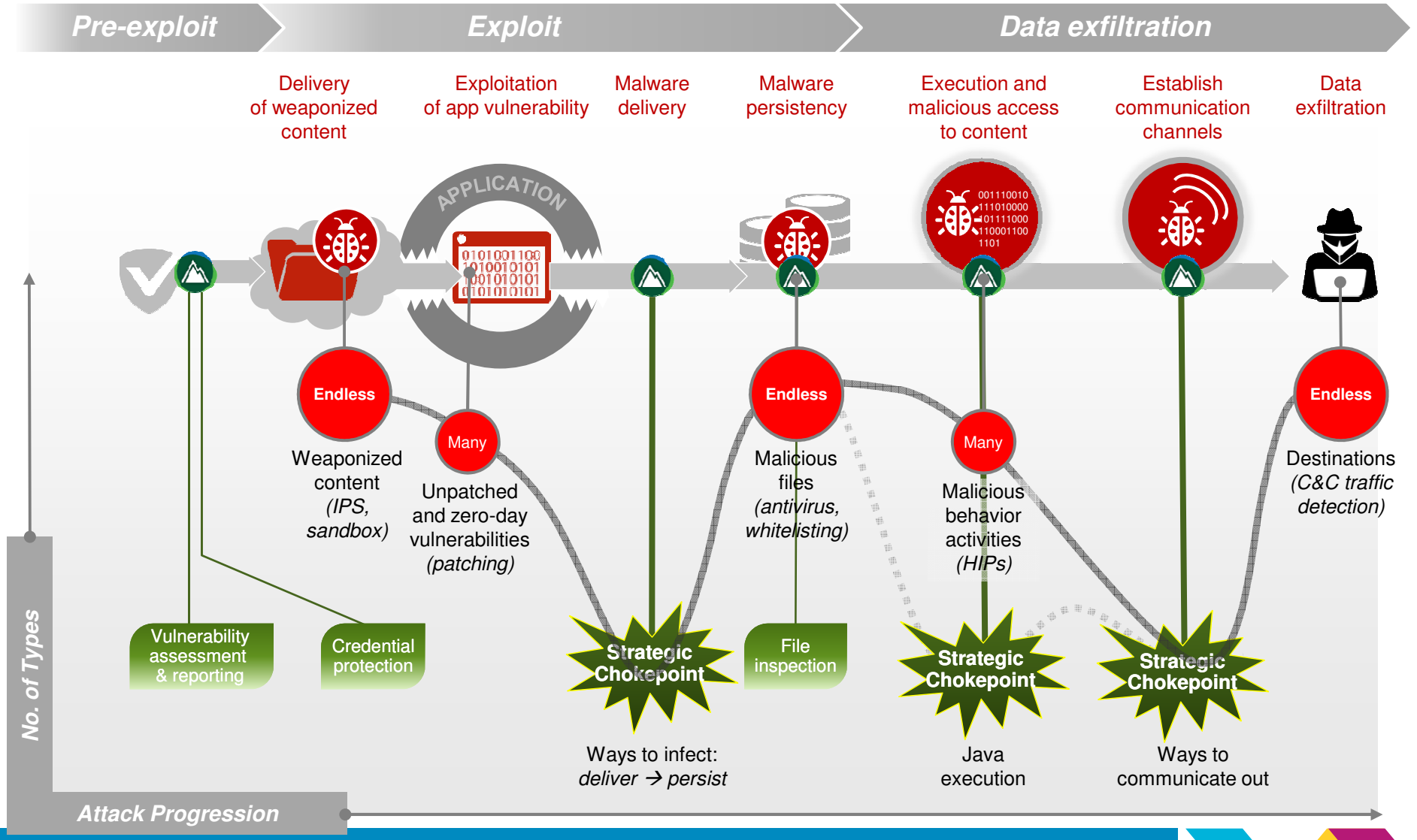
Advanced Threat Analysis and Turnkey Service

Credential Protection	Exploit Chain Disruption	Cloud Based File Inspection NEW	Lockdown for Java NEW	Malicious Communication Prevention
• Alert and prevent phishing and reuse on non-corporate sites	• Prevent infections via exploits • Zero-day defense by controlling exploit-chain choke point	• Legacy protection against known viruses • Consolidates over 20 AV engines for maximal efficacy and operational simplicity	• Prevent high-risk actions by malicious Java applications	• Block malware communication - Disrupt C&C control - Prevent data exfiltration

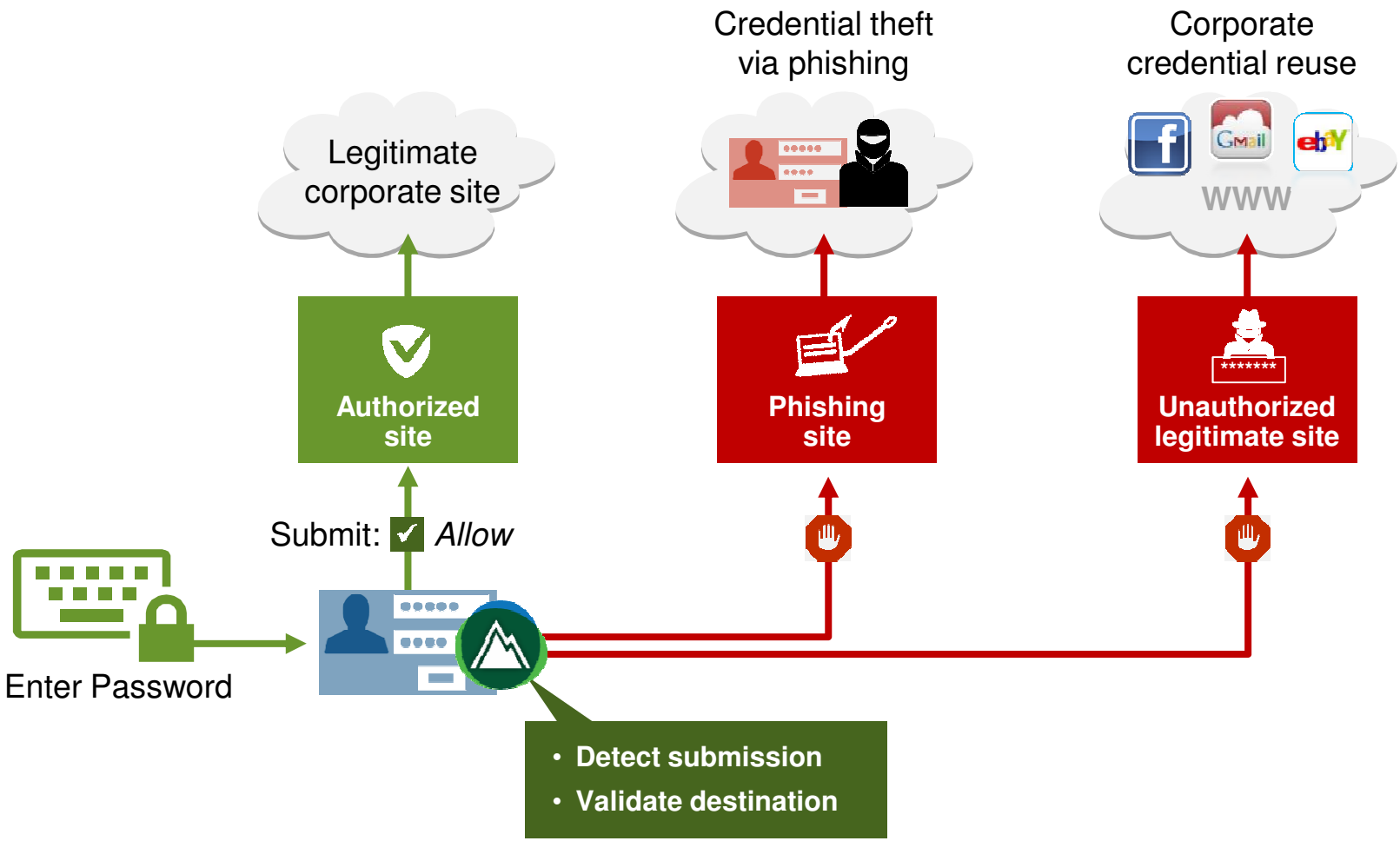
Global Threat Research and Intelligence

Global threat intelligence delivered in near-real time from the cloud

Controlling exploit-chain chokepoints

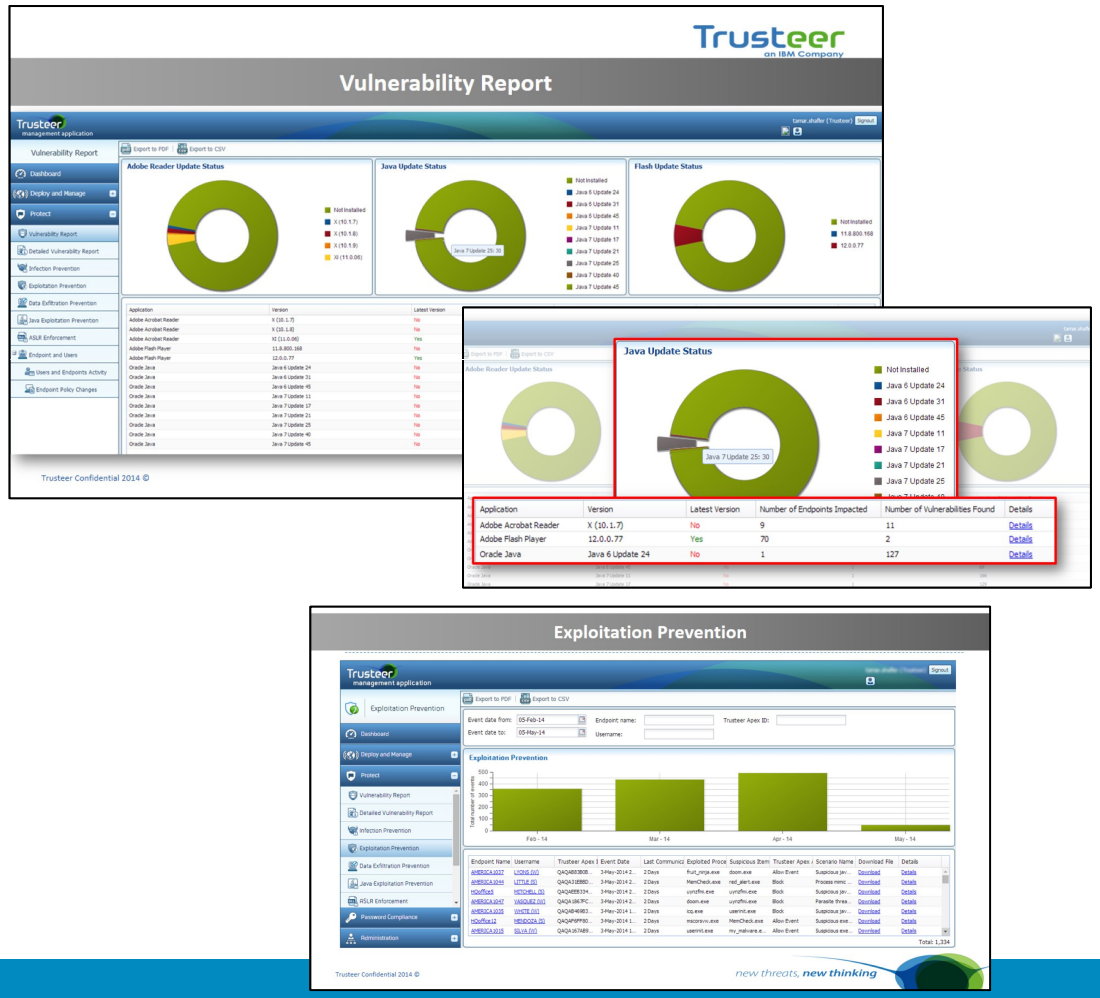


Corporate credentials protection



Threat and risk reporting: Vulnerability mapping and critical event reporting

Identify risks from vulnerabilities and user behavior, help ensure compliance



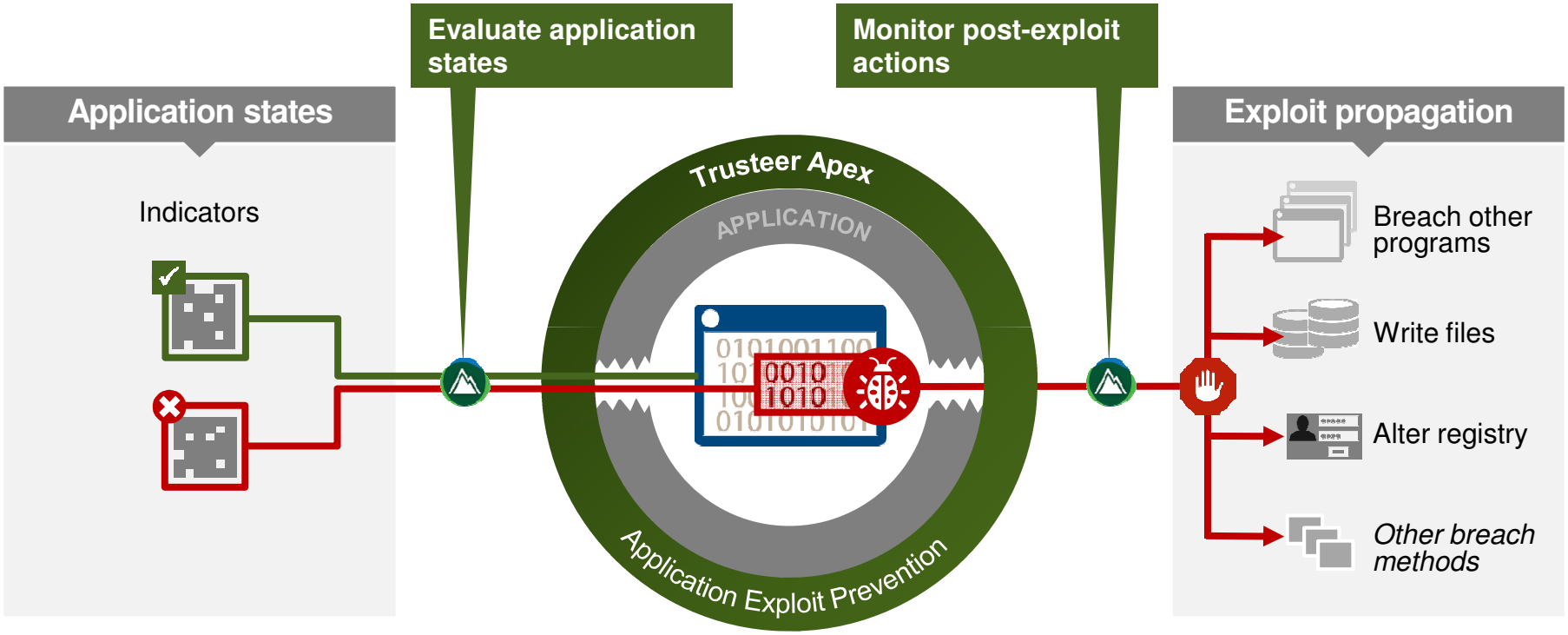
Vulnerability reports
Detailed reporting to visualize and understand which endpoints and apps are vulnerable to exploits

Corporate credential reports
Reporting on which users are re-using credentials, out of policy guidelines

Incident reports
Reporting on security incidents – exploits, suspicious communication, infections

Exploit chain disruption

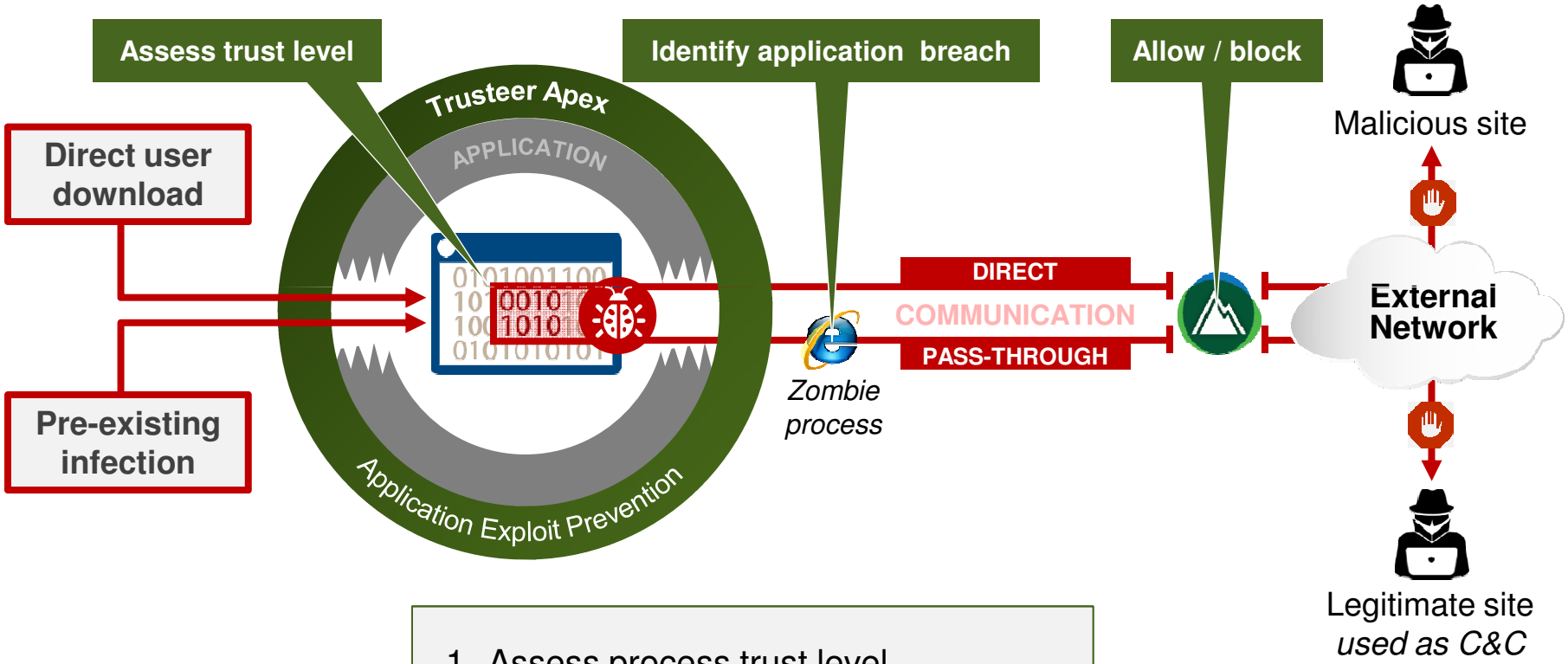
Block zero day attacks without prior knowledge of the exploit or vulnerability



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

Malicious communication blocking

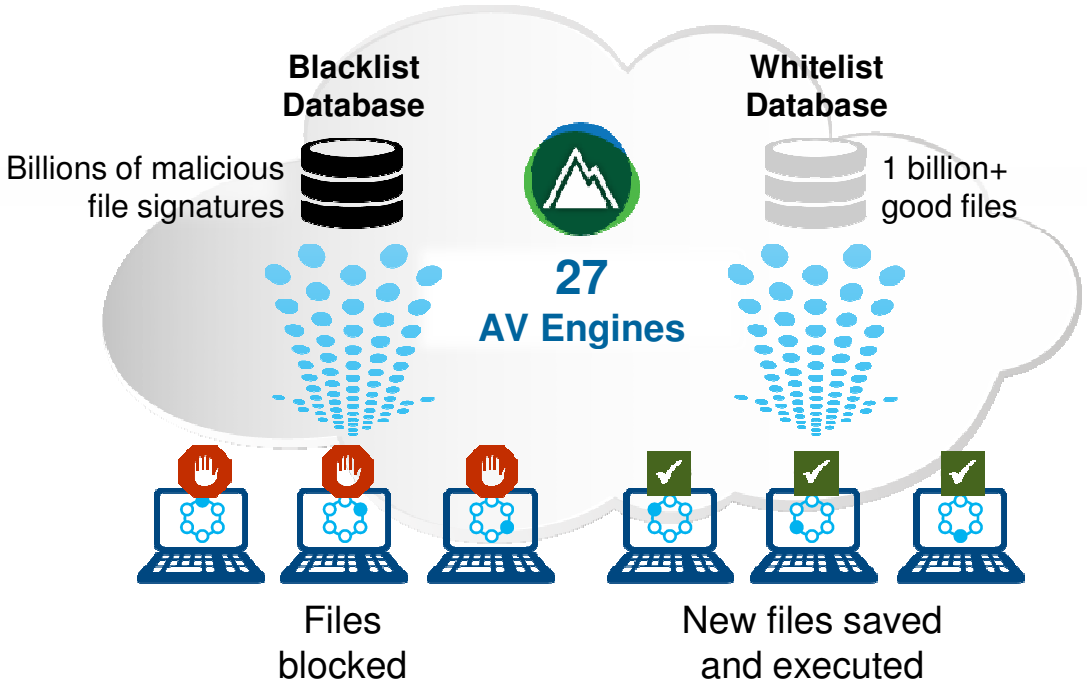
Block suspicious executables that attempt to compromise other applications or open malicious communication channels



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

Cloud-based file inspection

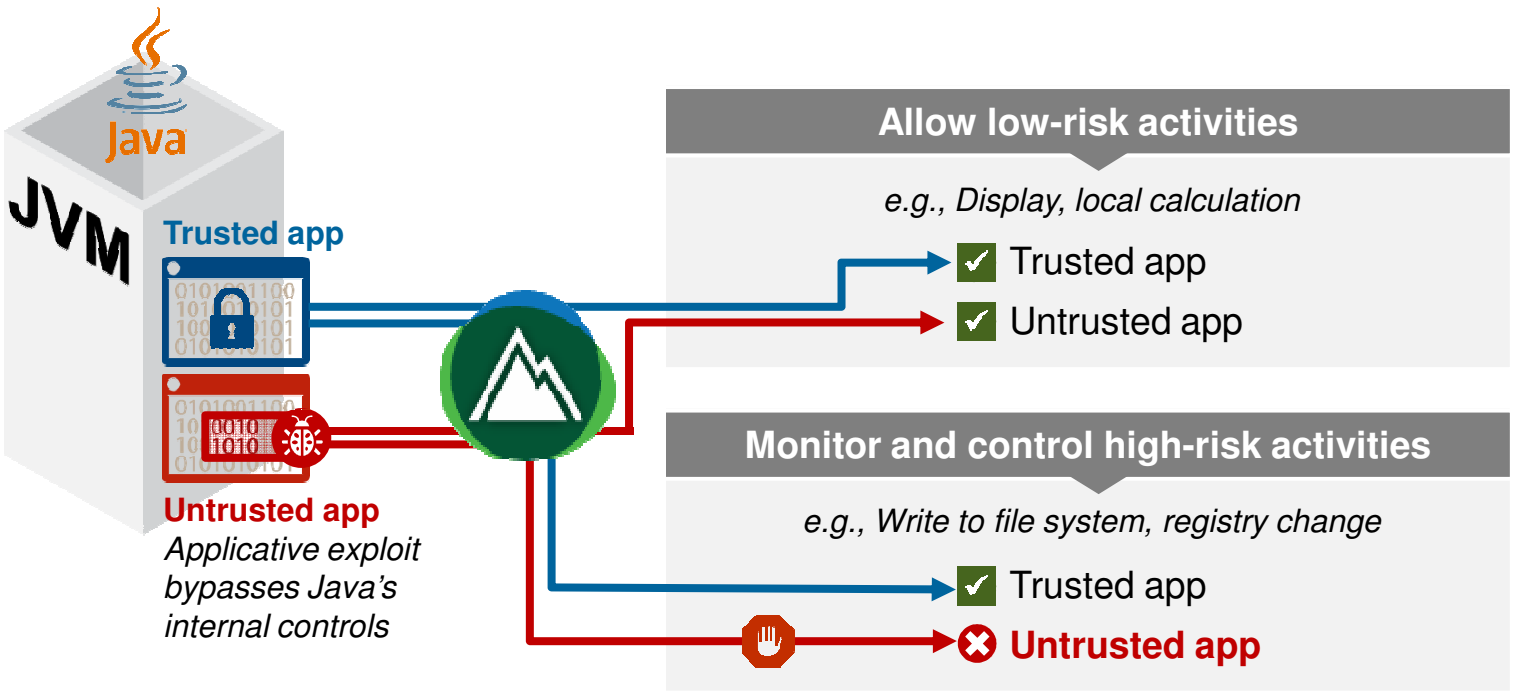
Legacy threat protection with improved operability



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

Lockdown for Java

Monitor and control high risk Java application actions

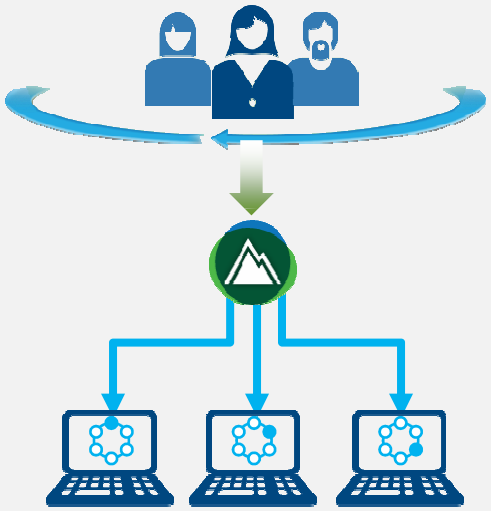


- Malicious code is blocked while legitimate Java applications are allowed
- Trust is granted by Trusteer / IT administrator

Low operational impact

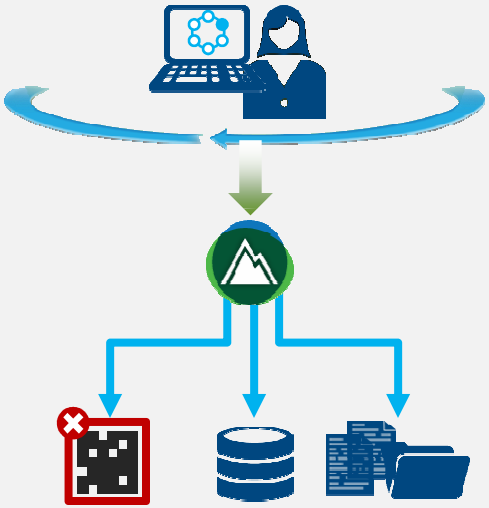
Advanced threat analysis and turnkey service

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 support endpoint users

Client example: Major heavy equipment manufacturer

Protecting endpoints against advanced threats and malware

Advanced fraud protection

Discovered

32 threats

and

100 suspicious activities

within weeks of deployment

Business challenge

- Needed to protect 10,000 endpoints in multiple international locations

IBM Security Solution (Trusteer Apex)

Trusteer Apex provides exploit chain disruption, malicious communication blocking, and cloud-based threat intelligence. The Trusteer threat intelligence and research team provided turnkey analysis of all suspected threats and provided protections when appropriate.

Client example: Major health care provider

Protecting sensitive patient data

Advanced fraud protection

Protected

40,000

endpoints from

high risk infections

Business challenge

- Protect sensitive patient data across 40,000 endpoints
- Stop attackers from taking control of machines remotely in order to gain access to sensitive patient data

IBM Security Solution (Trusteer Apex)

Sensitive patient data protection with minimal operational impact to the IT Security team. Trusteer's turnkey service provides analysis of alerts, whitelisting of exceptions, and attack analysis.

Thank You