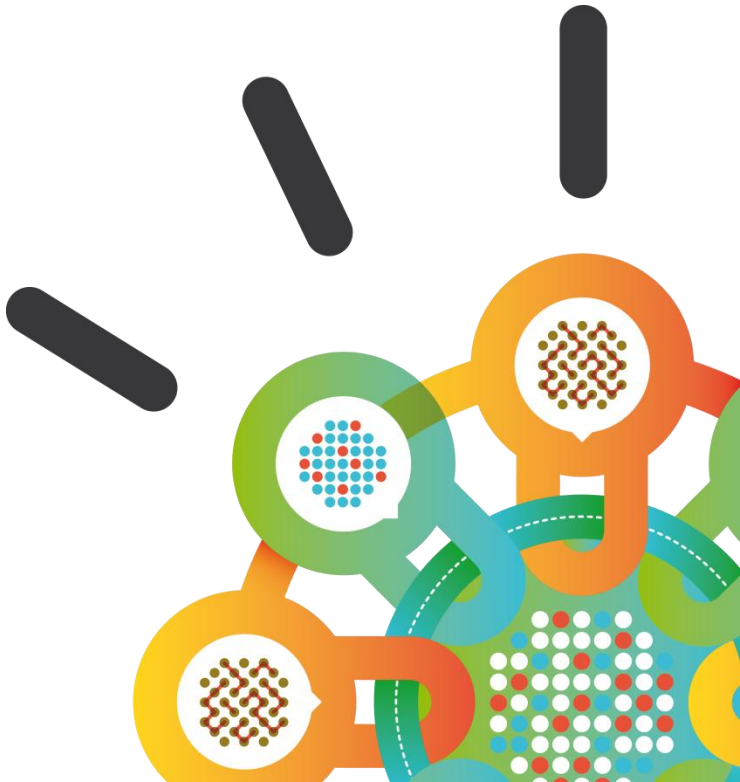
Security Intelligence.
Think Integrated.

Protecting Enterprise Endpoints against Advanced Malware
with Trusteer Apex

Dana Tamir
Director of Enterprise Security

Trusteer, an IBM Company



About Trusteer

Company	Global leader in Advanced Threat Protection
Intelligence	Analysis of events from millions of protected endpoints
Technology	Proven and trusted agent-based technology

Trusteer Apex

Stopping advanced malware and APTs by preventing malicious downloads and data exfiltration

APTs and Targeted Attacks

The Tool of Choice: Exploits and Advanced Malware

- **The Entry Point:**
  - –Vulnerable User Endpoints
- **The Means:**
  - –Exploits, Drive-by Download
  - –Advanced Malware
  - –Compromised Credentials

Vulnerability disclosures leveled out in 2013, but attackers have

plenty of older, unpatched systems to exploit.

60% of the exploits target vulnerabilities that have been publicly known for over 12 months!!!

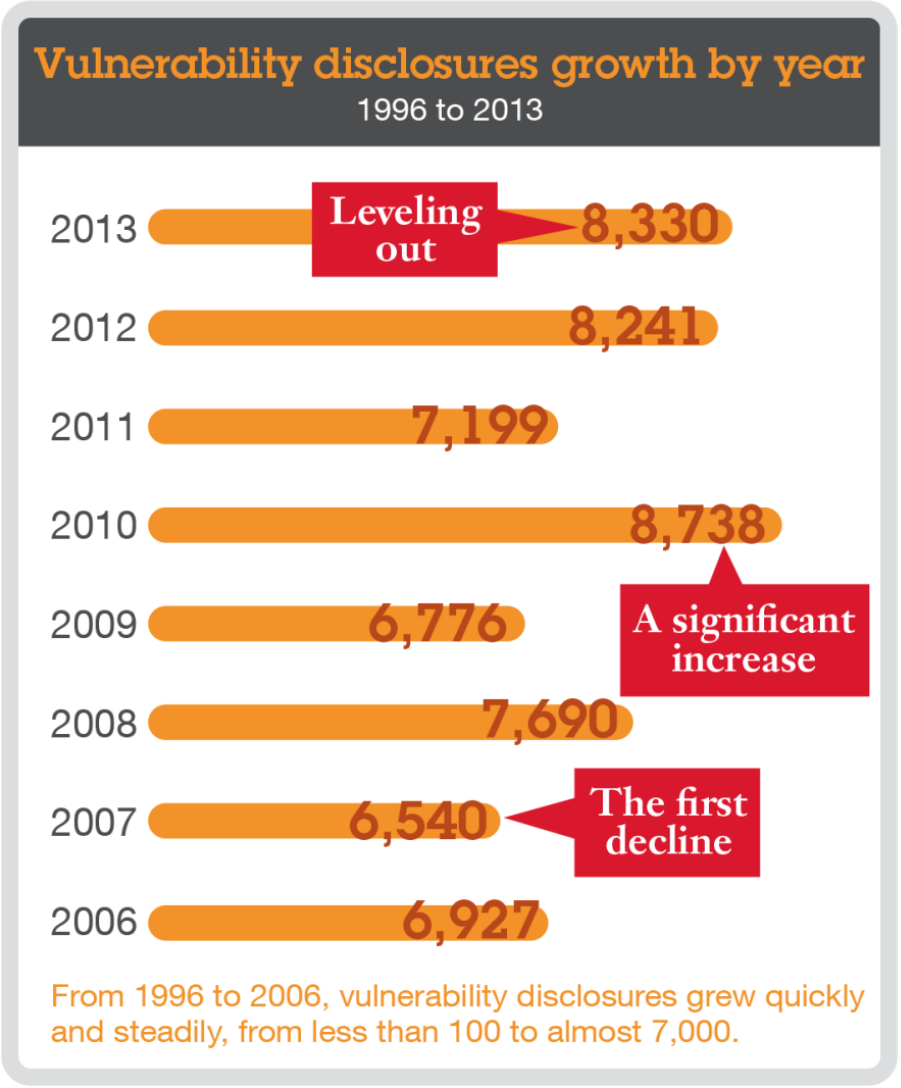
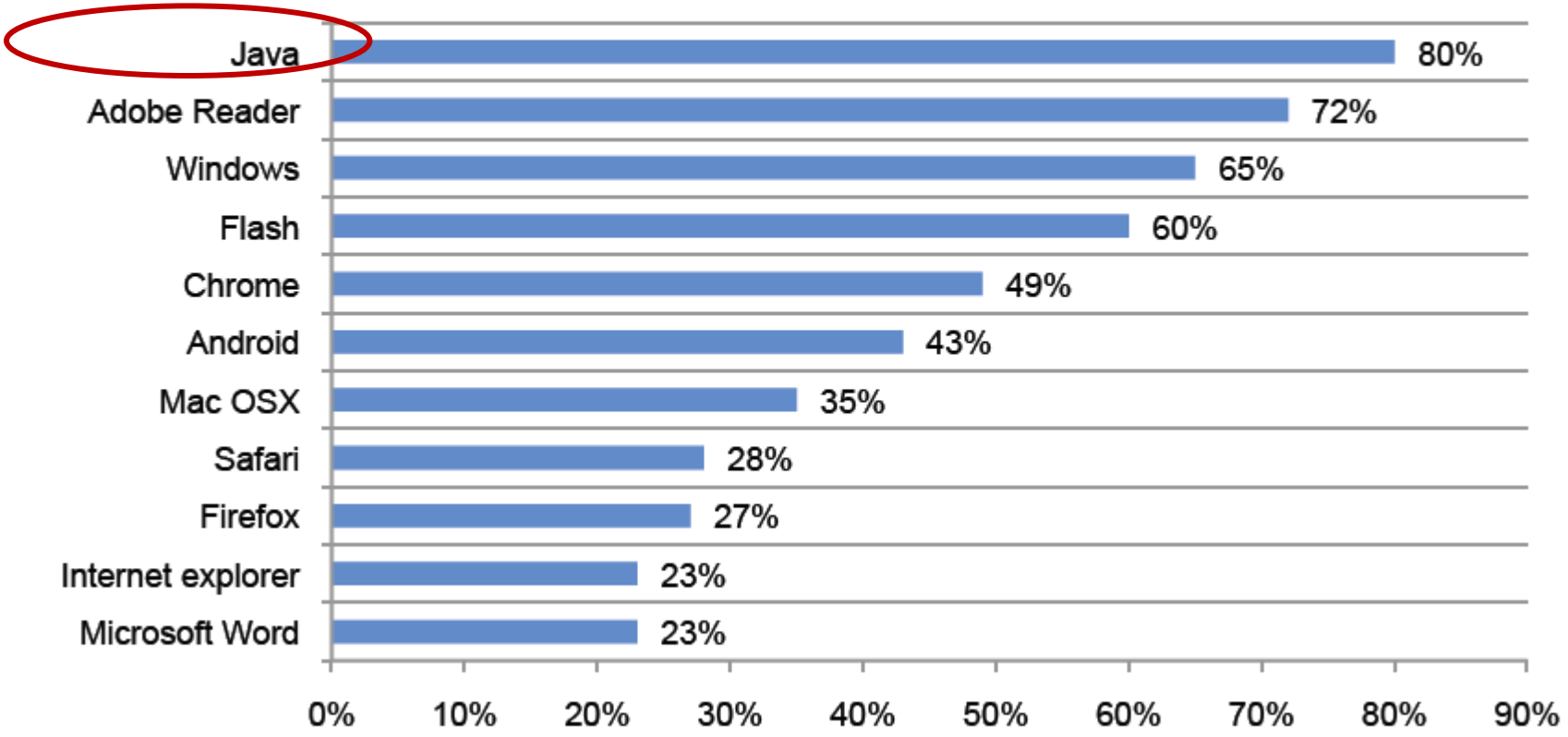


Figure 8. Vulnerability disclosures growth by year, 1996 to 2013

Source: IBM X-Force® Research and Development

Do you patch applications?

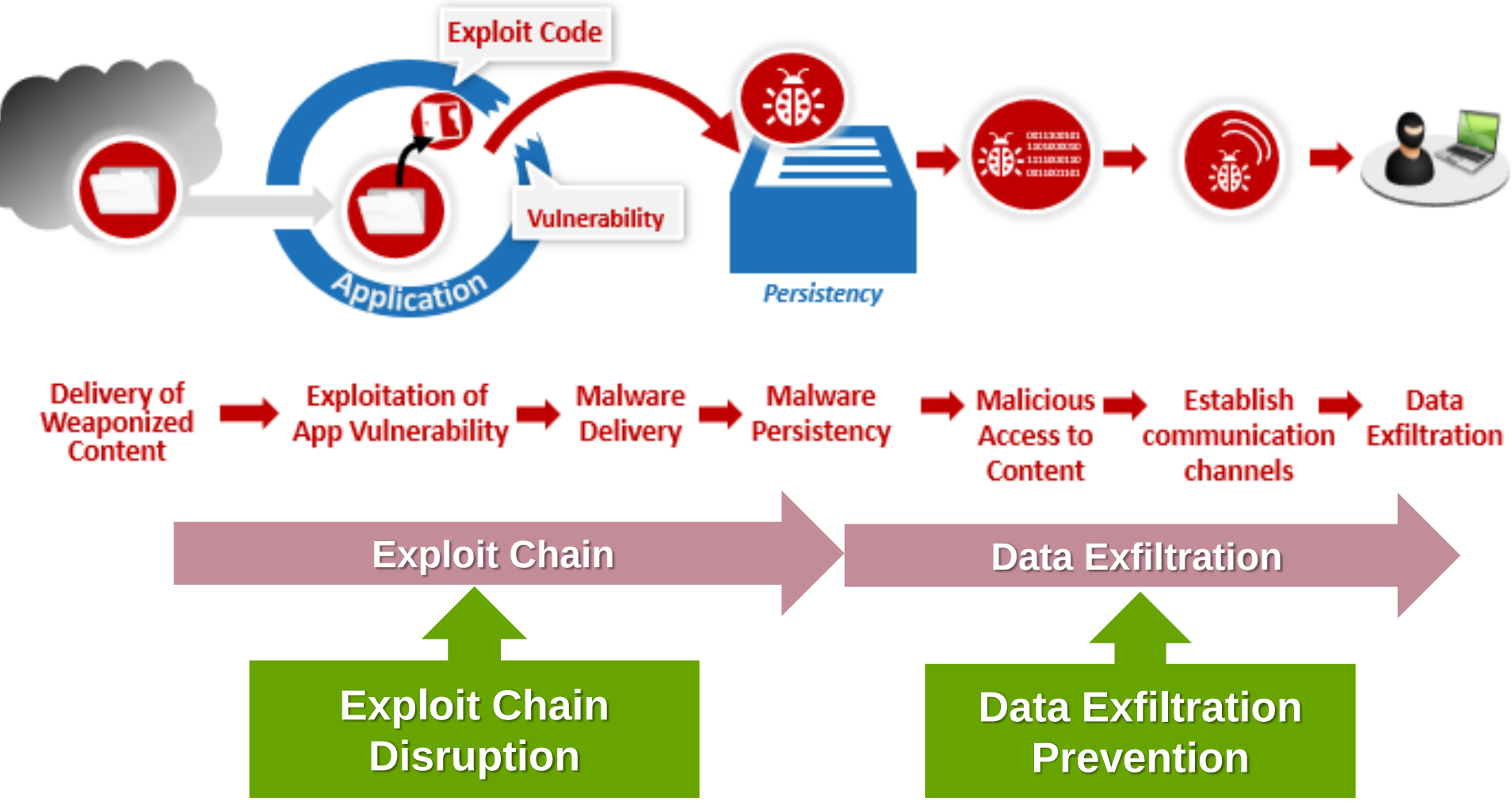
Figure 4. Which applications make it difficult to ensure all security patches have been fully implemented in a timely manner
Very difficult and difficult response combined



Source: Ponemon

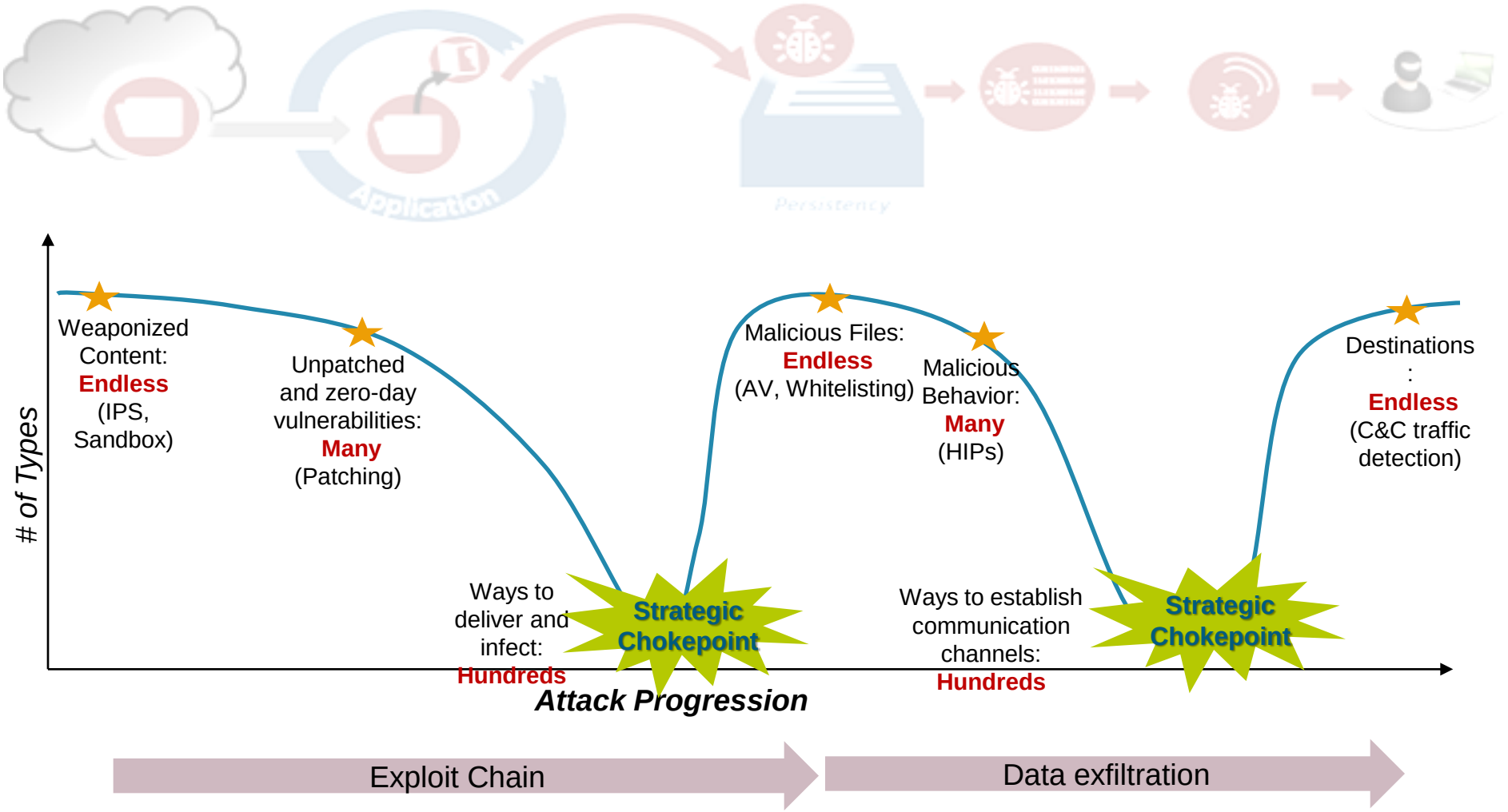
5

The Threat Lifecycle



Controlling Strategic Chokepoints

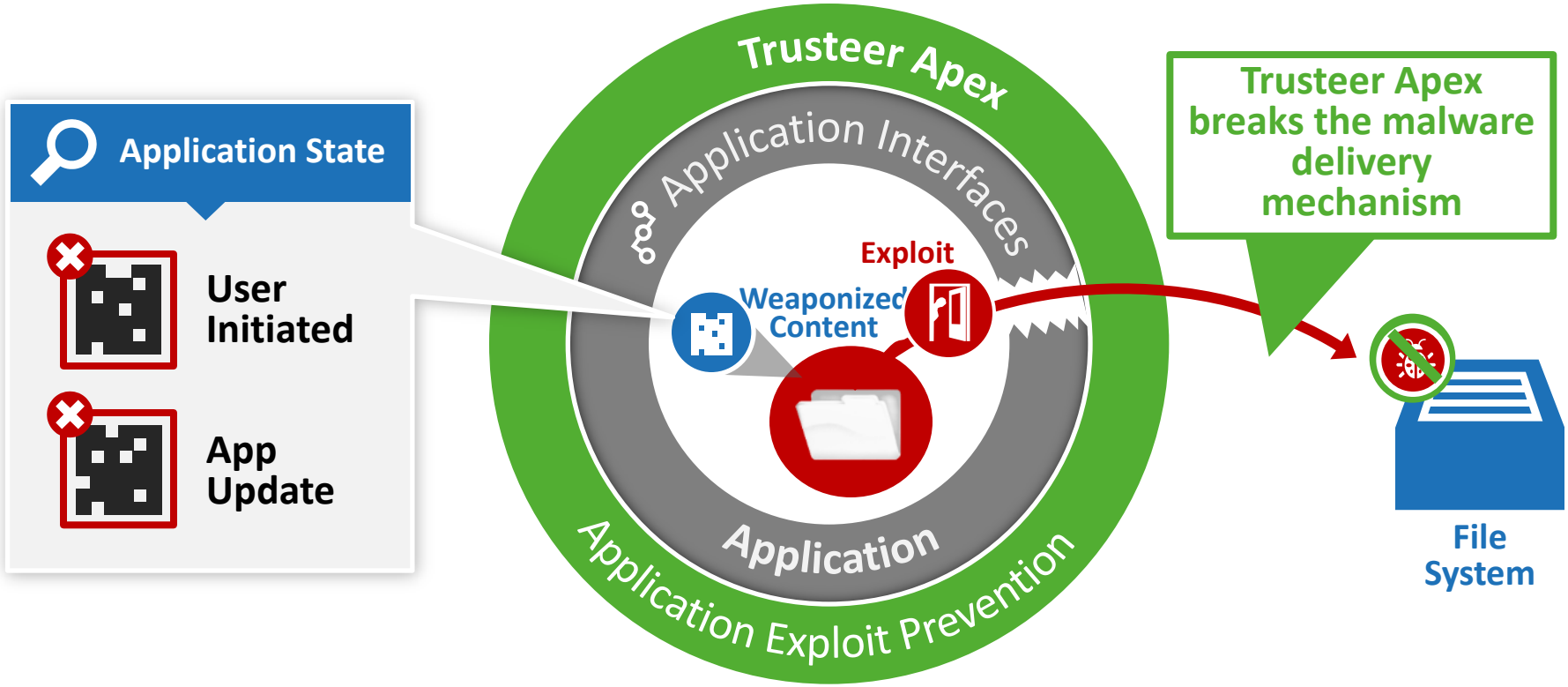
To break the threat lifecycle



Exploit Chain Disruption:
Stateful Application Control

Trusteer
an IBM Company

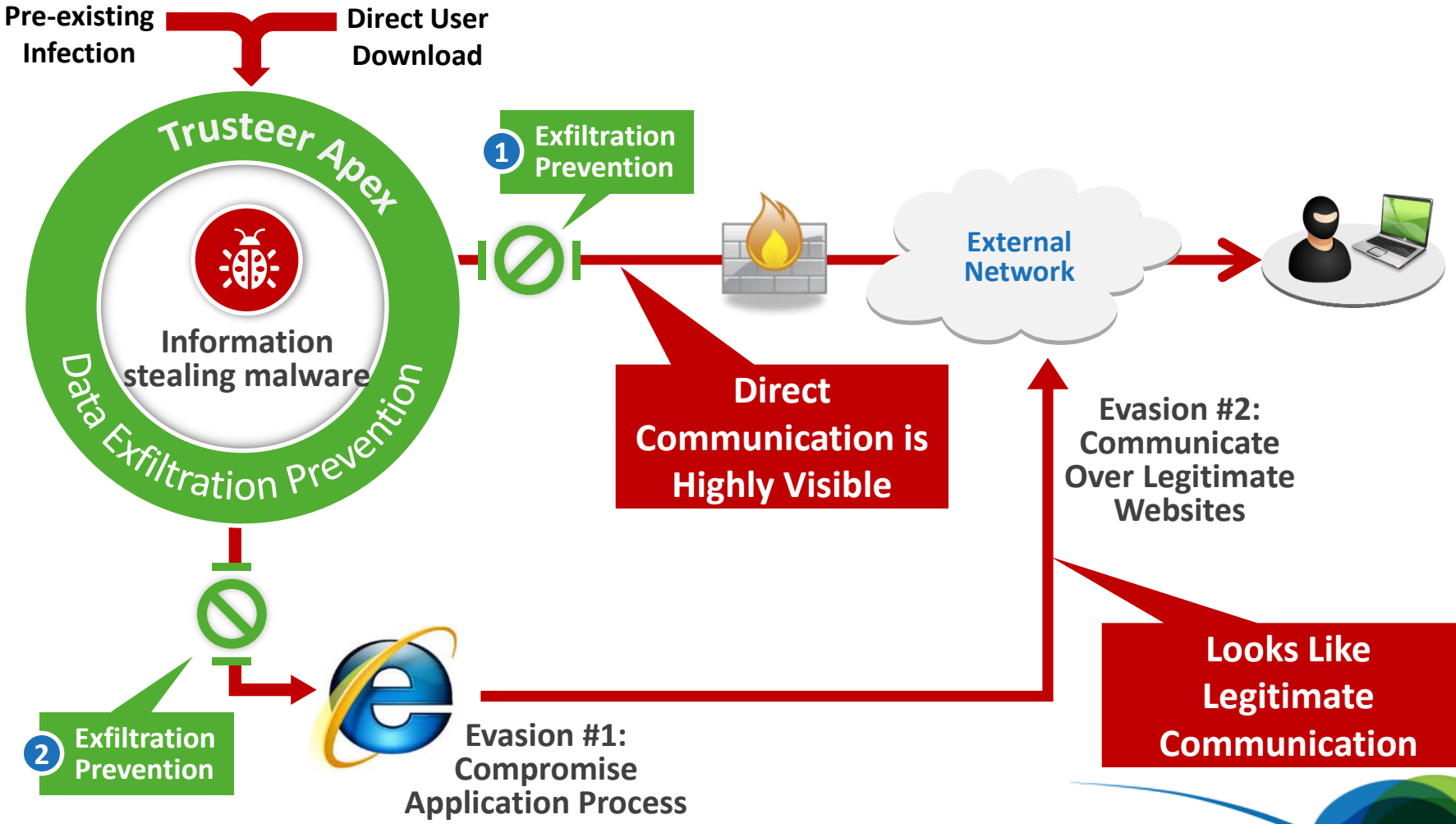
When unknown application states are created Apex stops the file delivery.



Data Exfiltration Prevention:
Block Malicious External Communication

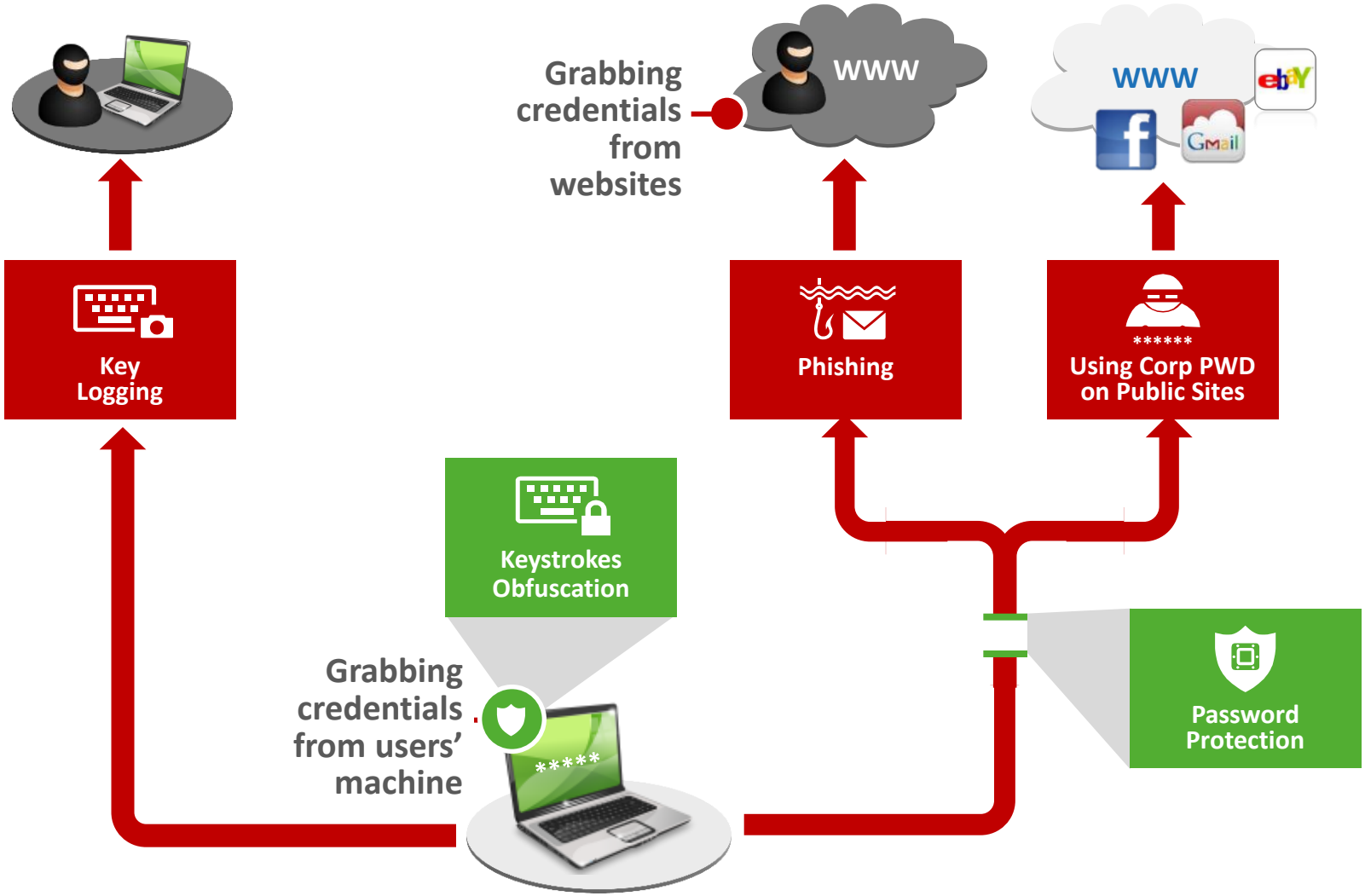
Trusteer
an IBM Company

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



Corporate Credentials Protection
Prevent Credentials Theft

Trusteer
an IBM Company



Trusteer Apex: 3 Security Layers

- Disrupts the exploit chain in multiple points
- Prevents silent malware download via exploitation
- Protects against zero-day threats

- Blocks malicious attempts to compromise applications
- Prevents attempts to establish communication channels
- Prevent information theft

- Block key-loggers
- Prevent submission on phishing sites
- Prevent reuse on public consumer sites

A few words about Java

A powerful yet dangerous application:

From laptops to datacenters, game consoles to scientific supercomputers, cell phones to the Internet, Java is everywhere!

- 1.1 billion desktops run Java
- 930 million Java Runtime Environment downloads each year
- 3 bil
- 31 ti
  com
- 100
- 1.4 b
- Java
  ATM
  mor

oid

ems,

ns, and

Did you know that…

Java is installed on ~85% of the desktop computers.

Google Analytics

explosive growth of **Java vulnerabilities**...

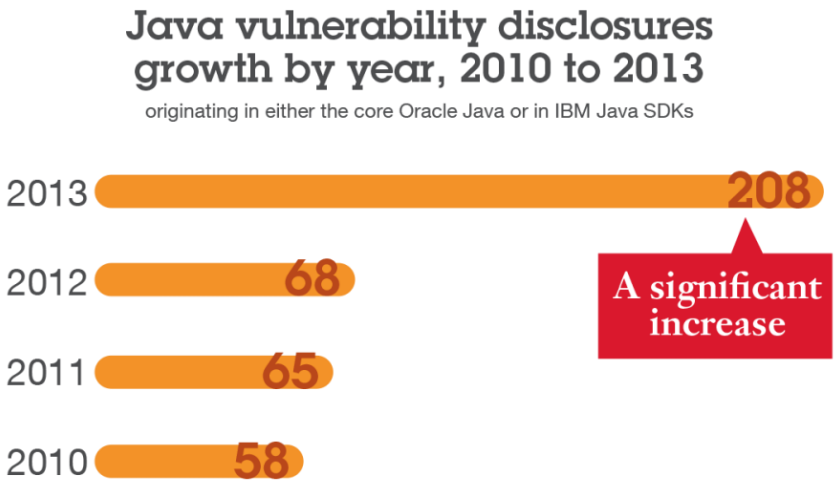


Figure 5. Java vulnerability disclosures growth by year, 2010 to 2013

Source: IBM X-Force® Research and Development

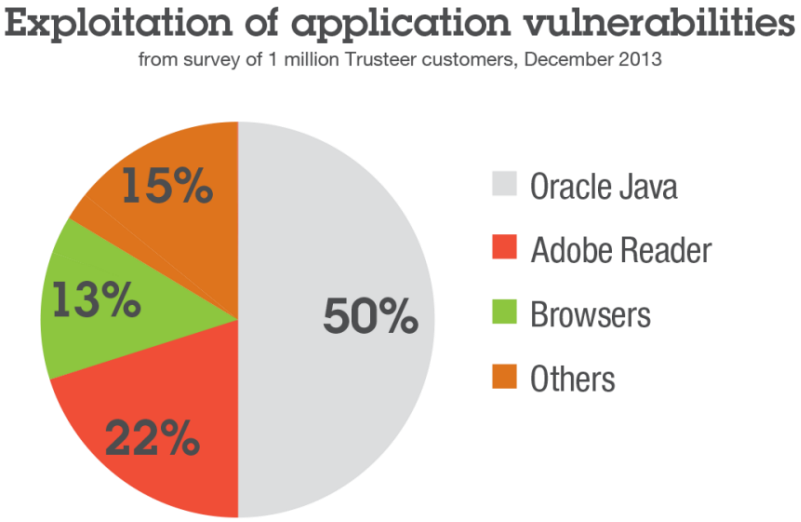


Figure 4. Exploitation of application vulnerabilities

Source: IBM X-Force® Research and Development

… combined with a presence in every enterprise makes Java the **top target** for exploits.

Most successful Java exploits are **applicative**, exploiting vulnerabilities related to the **Java security manager** and bypassing native OS-level protections.

Applicative exploits

- Difficult to defend
- Gain unrestricted privileges
- Bypass native OS-level protections

Native exploits

- Buffer Overflow
- Illegal memory use
- Use-after-free

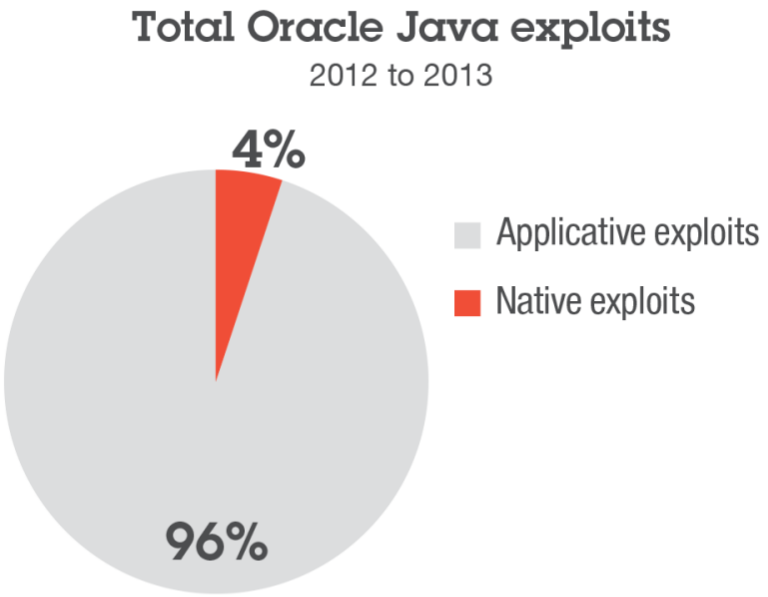


Figure 6. Total Oracle Java expoits, 2012 to 2013

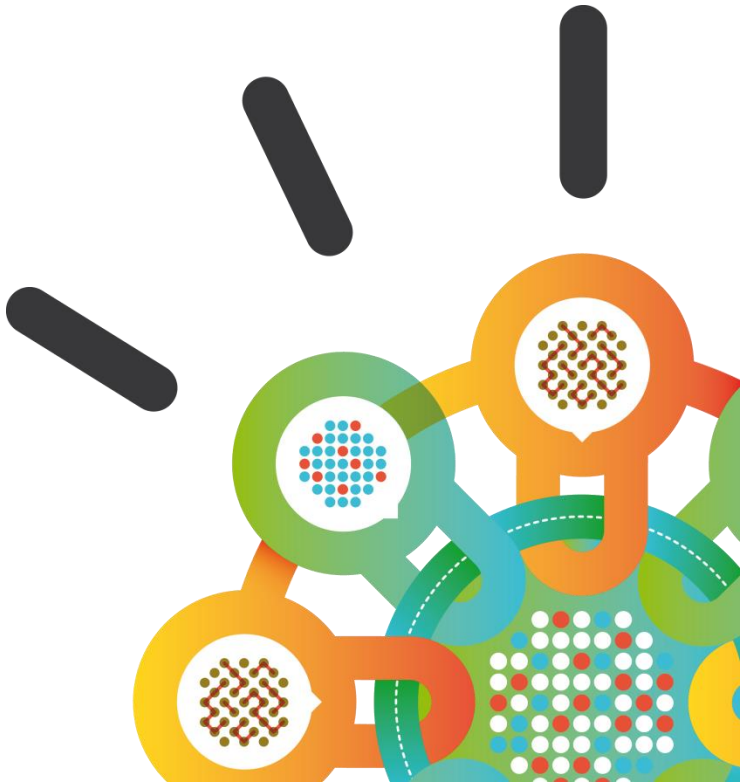
Source: IBM X-Force® Research and Development

Java Execution Should be Monitored and Controlled

- Prevent Exploitation of both Native and Applicative Vulnerabilities
- Execution of Java code on the endpoint must be restricted
  - Fine grained control is needed
- Oracle's solution: Allow execution of signed JARs
  - Not good enough

Security Intelligence.
Think Integrated.

Questions?



Connect with IBM X-Force Research & Development

Follow us at @ibmsecurity and @ibmxforce

Download IBM X-Force Threat Intelligence Reports
http://www.ibm.com/security/xforce/

X-Force Security Insights blog at www.SecurityIntelligence.com/x-force

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Thank You

www.ibm.com/security