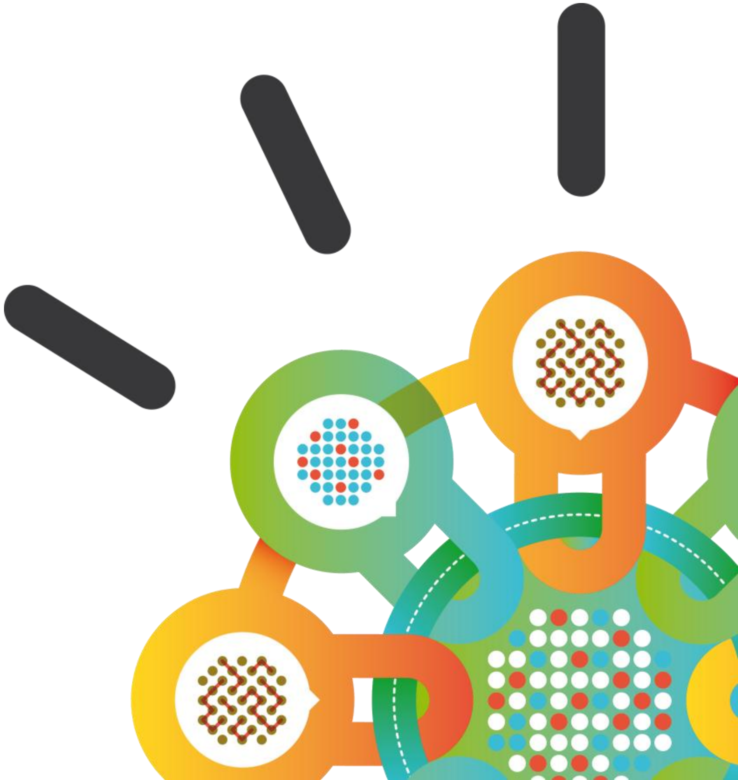
Security Intelligence.
Think Integrated.

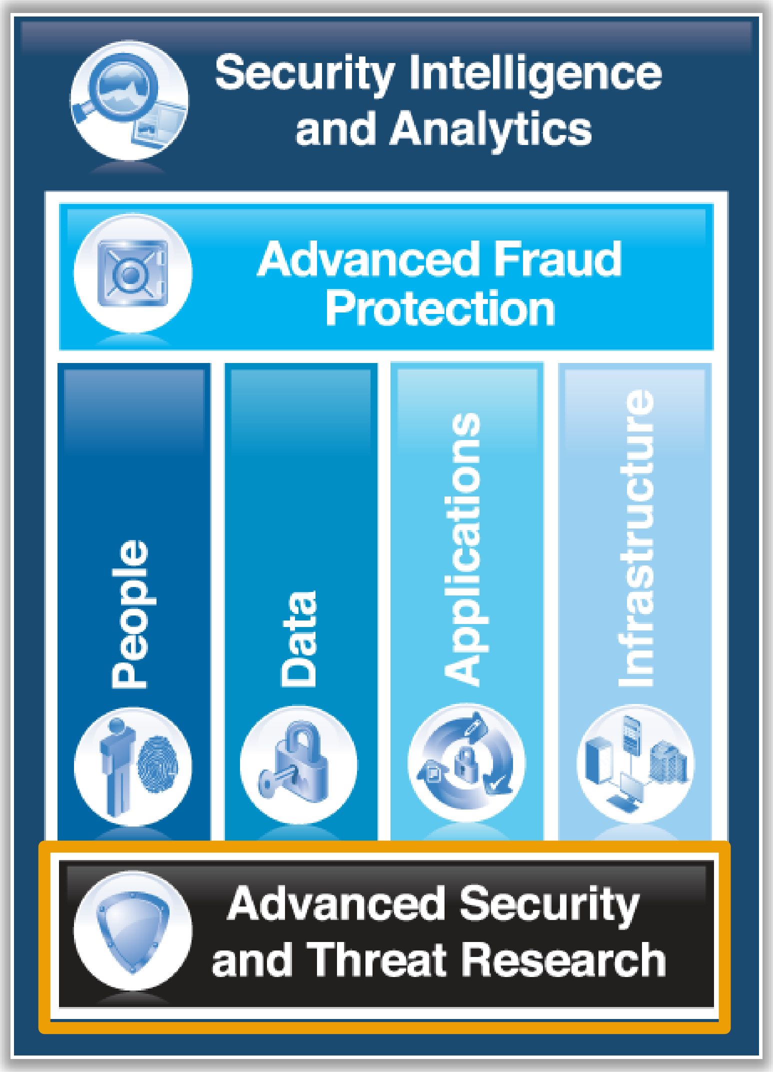
IBM X-Force: The Emerging Threat Landscape

October, 2014

Paul Griswold
Program Director, Strategy & Product Management
Infrastructure Security
IBM Security Systems



© 2014 IBM Corporation

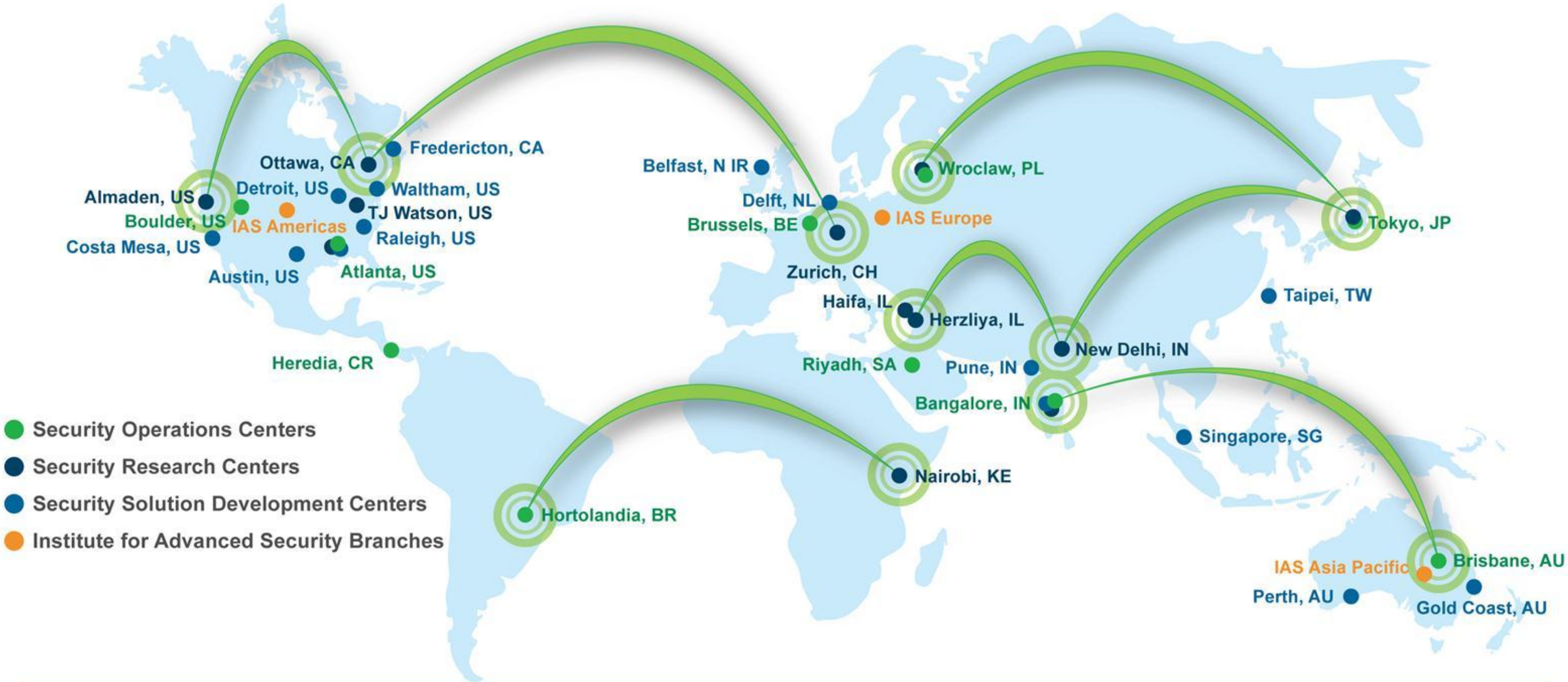

Security Intelligence and Analytics
Advanced Fraud Protection
People
Data
Applications
Infrastructure
Advanced Security and Threat Research

IBM X-Force

is the foundation for advanced security and threat research across the IBM Security Framework.

© 2014 IBM Corporation

IBM Security has global reach



IBM Security by the Numbers

133 + monitored countries (MSS)

3300 + service delivery experts

20000 + devices under contract

270000000 + endpoints protected

15000000000 + events managed per day

© 2014 IBM Corporation

IBM X-Force® delivers expert analysis and threat intelligence

- Backdoors
- Botnets
- Buffer Overflow Attacks
- Client Side Attacks
- Cross-site Scripting (XSS)
- Distributed Denial of Service (DDoS)
- Exploit Toolkits
- Malicious Content
- Peer-to-Peer Networks
- Protocol Tunneling
- Reconnaissance
- SQL Injection
- Trojans
- Worms

Sharing real-time and anonymized threat intelligence

IBM Security Operations Centers and Security Products

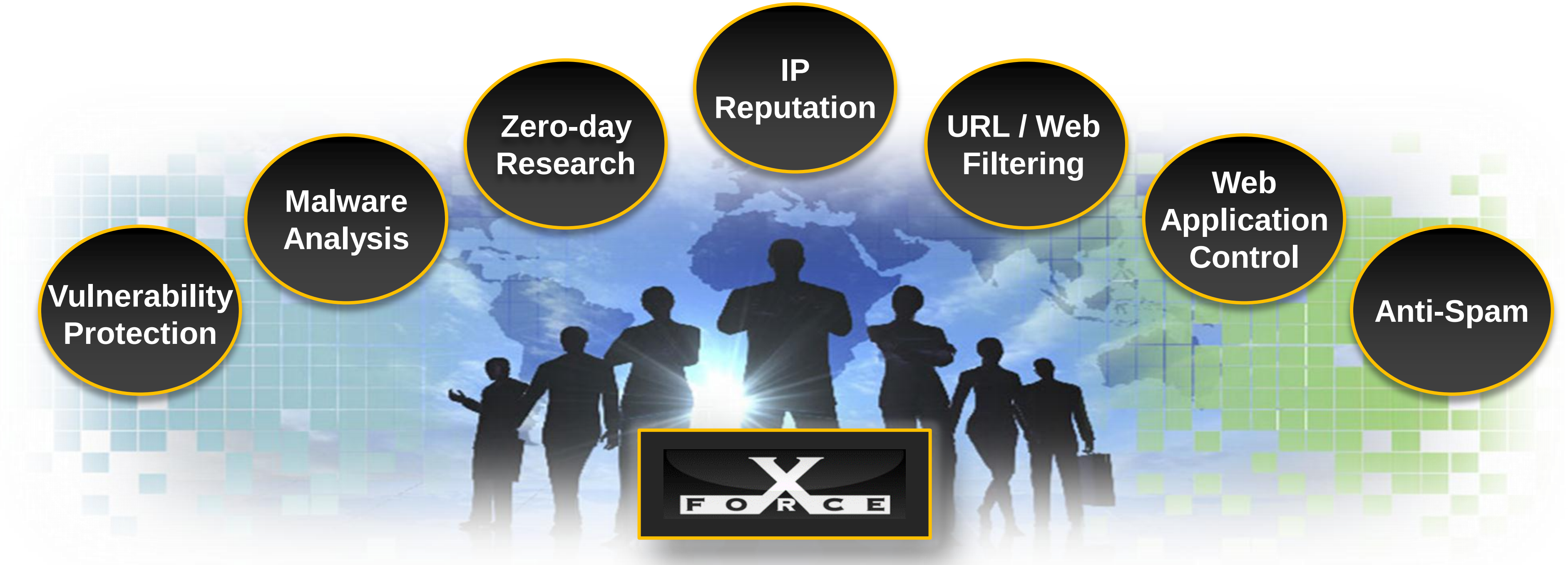
X-Force Helps Keep Customers Ahead of the Threat

- Cataloging, analyzing and researching vulnerabilities since 1997
- Providing zero-day threat alerts and exploit triage to IBM customers worldwide
- Building threat intelligence from collaborative data sharing across thousands of clients
- Analyzing malware and fraud activity from 270M+ Trusteer-protected endpoints

© 2014 IBM Corporation

IBM X-Force® Research and Development

Expert analysis and data sharing on the global threat landscape



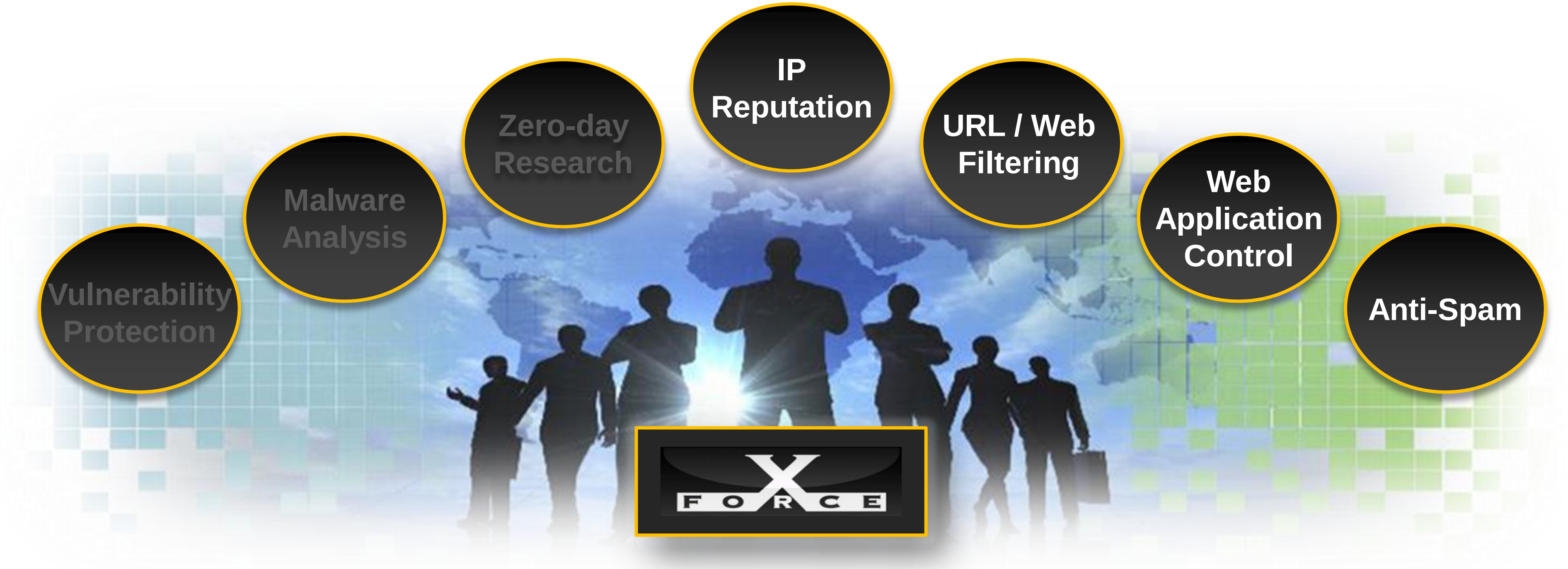
The IBM X-Force Mission

- **Monitor** and evaluate the rapidly changing threat landscape
- **Research** new attack techniques and develop protection for tomorrow's security challenges
- **Educate** our customers and the general public
- **Integrate** and distribute Threat Protection and Intelligence to make IBM solutions smarter

© 2014 IBM Corporation

IBM X-Force® Research and Development

Expert analysis and data sharing on the global threat landscape



Vulnerability Protection

Malware Analysis

Zero-day Research

IP Reputation

URL / Web Filtering

Web Application Control

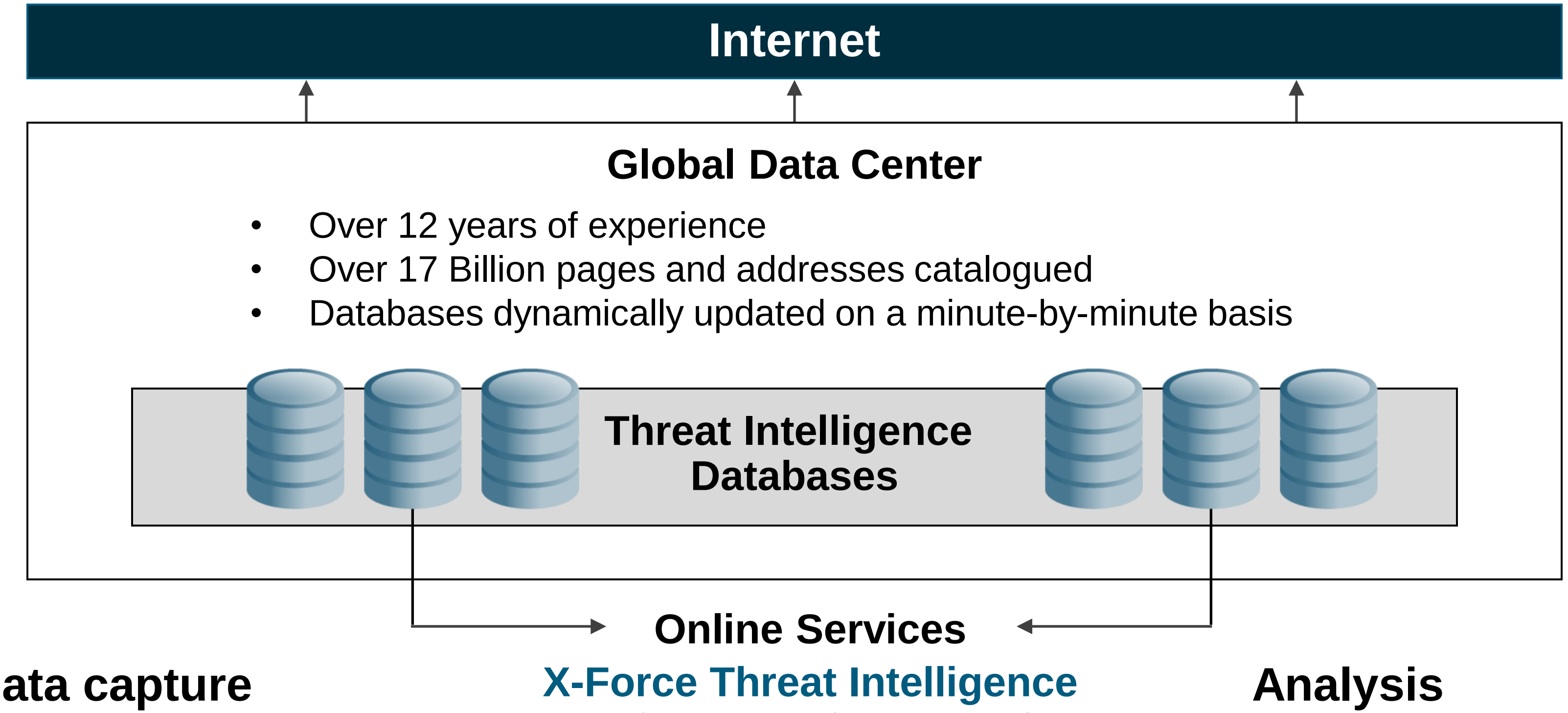
Anti-Spam

The IBM X-Force Mission

- **Monitor** and evaluate the rapidly changing threat landscape
- **Research** new attack techniques and develop protection for tomorrow’s security challenges
- **Educate** our customers and the general public
- **Integrate** and distribute Threat Protection and Intelligence to make IBM solutions smarter

© 2014 IBM Corporation

Monitor - X-Force has the skills and infrastructure for collecting and analyzing changing threats



Internet

Global Data Center

- Over 12 years of experience
- Over 17 Billion pages and addresses catalogued
- Databases dynamically updated on a minute-by-minute basis

Threat Intelligence Databases

Online Services

X-Force Threat Intelligence

Data capture

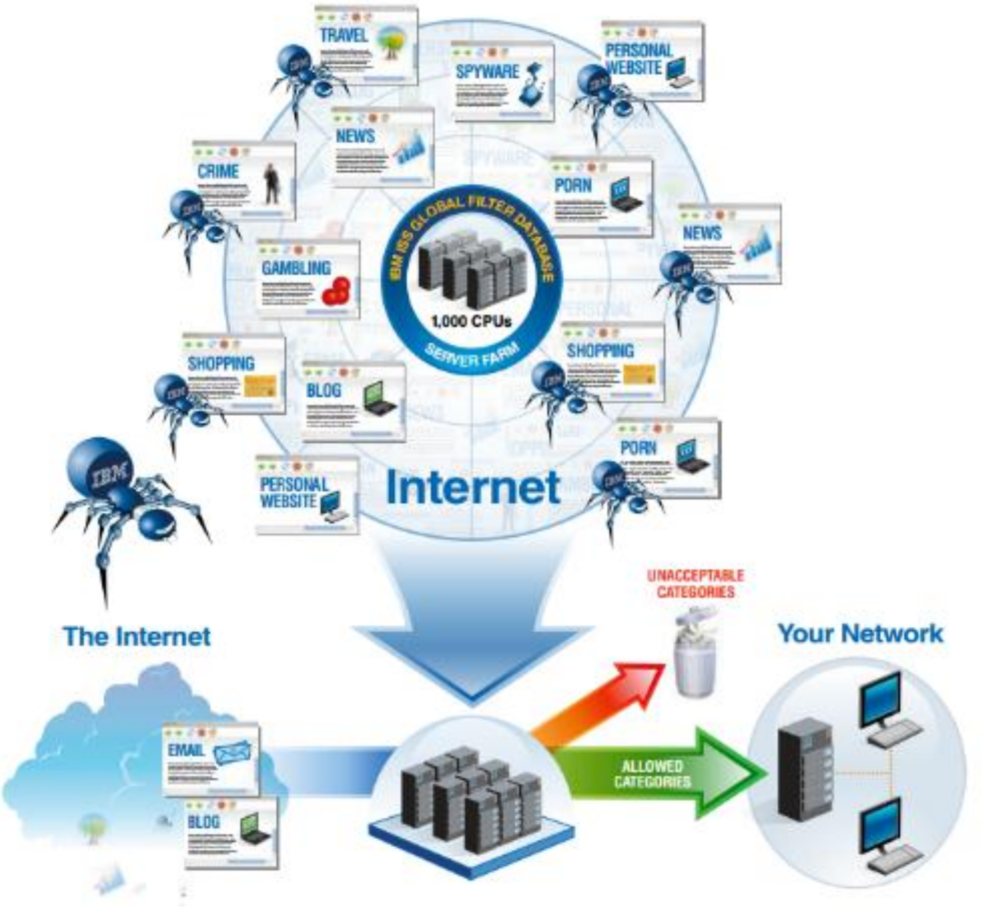
- Crawler robots search the web in parallel
- Honeypots & darknets capture information
- Spamtraps obtain Spam IPs and samples

Analysis

- Server clusters analyze the data acquired
- Insights for different threats are gleaned from the data and stored in an efficient manner

© 2014 IBM Corporation

Monitor - Intelligence integrated into products for better accuracy



Web Crawler

- Crawlers collect image and text data from the Internet 24x7x365
- Every day, hundreds of thousands of changes to customers
- Indexed into 80+ categories
- Extended to Application Control

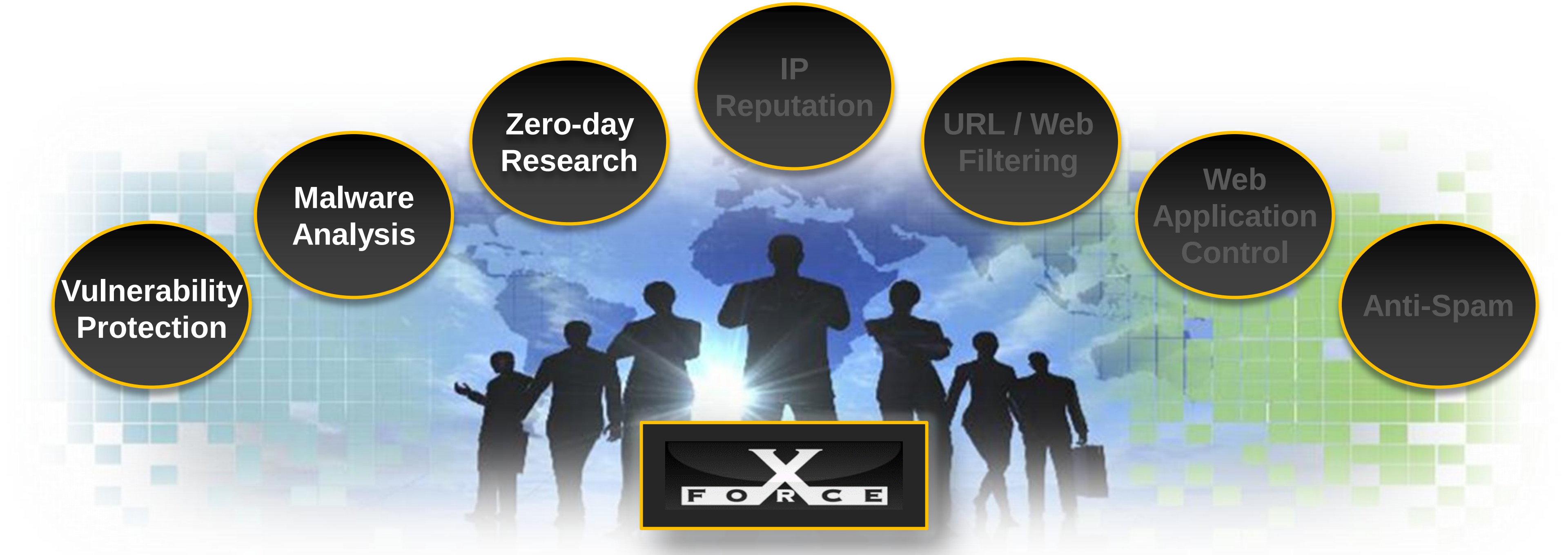
IP Reputation

- Malicious IPs
- Malware hosts
- SPAM sources
- Dynamic IPs
- Anonymous Proxies
- and more…

© 2014 IBM Corporation

IBM X-Force® Research and Development

Expert analysis and data sharing on the global threat landscape



The IBM X-Force Mission

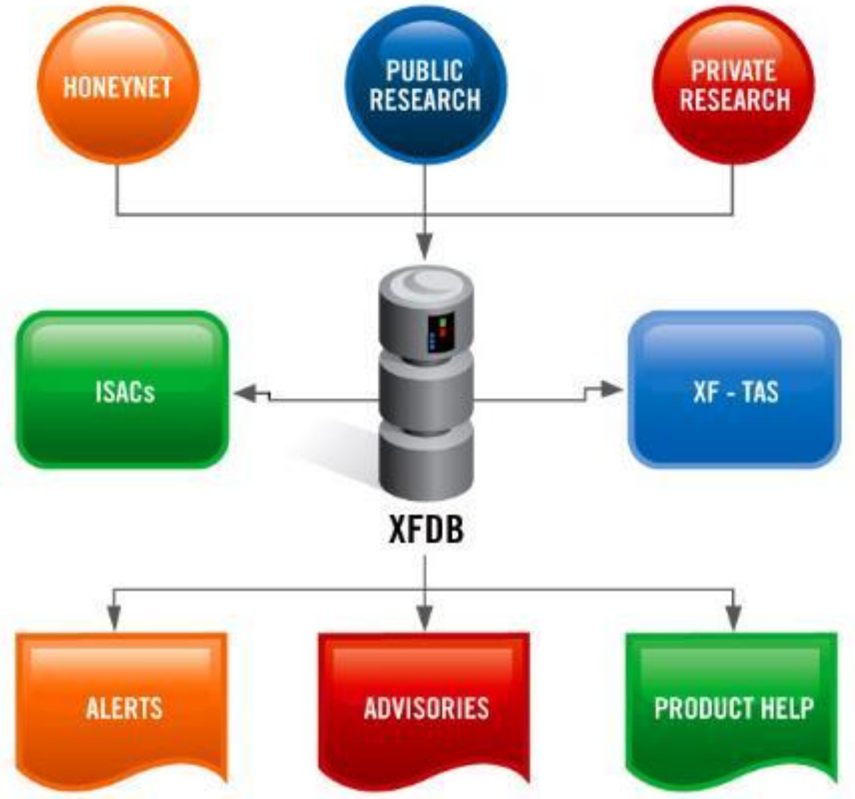
- **Monitor** and evaluate the rapidly changing threat landscape
- **Research** new attack techniques and develop protection for tomorrow's security challenges
- **Educate** our customers and the general public
- **Integrate** and distribute Threat Protection and Intelligence to make IBM solutions smarter

© 2014 IBM Corporation

Research - We analyze them all - X-Force Database (XFDB)

Most comprehensive Vulnerability Database in the world

- Updated daily by a dedicated research team
- Entries date back to the 1990's
- Over 80,000 unique vulnerabilities



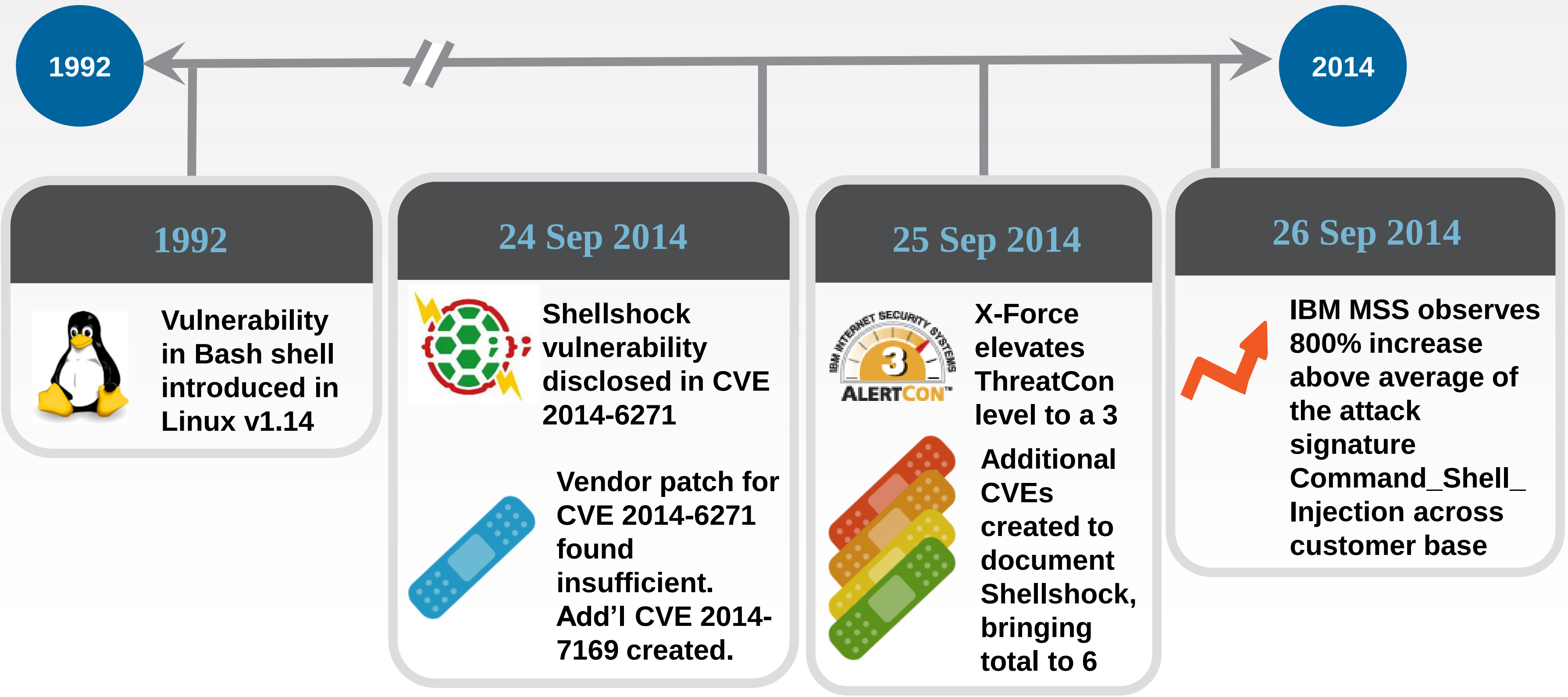
Research also turns into innovative product "engines"

- Protocol Analysis Module
- Shellcode Heuristics
- Web Injection Logic Engine
- Java and JavaScript Heuristics

© 2014 IBM Corporation

The disclosure of the Shellshock bug in September brought immediate exploit attempts.

Patching the original vulnerability was complicated by the development of additional exploit techniques, resulting in additional CVE numbers created.



1992

Vulnerability in Bash shell introduced in Linux v1.14

24 Sep 2014

Shellshock vulnerability disclosed in CVE 2014-6271

Vendor patch for CVE 2014-6271 found insufficient. Add’l CVE 2014-7169 created.

25 Sep 2014

X-Force elevates ThreatCon level to a 3

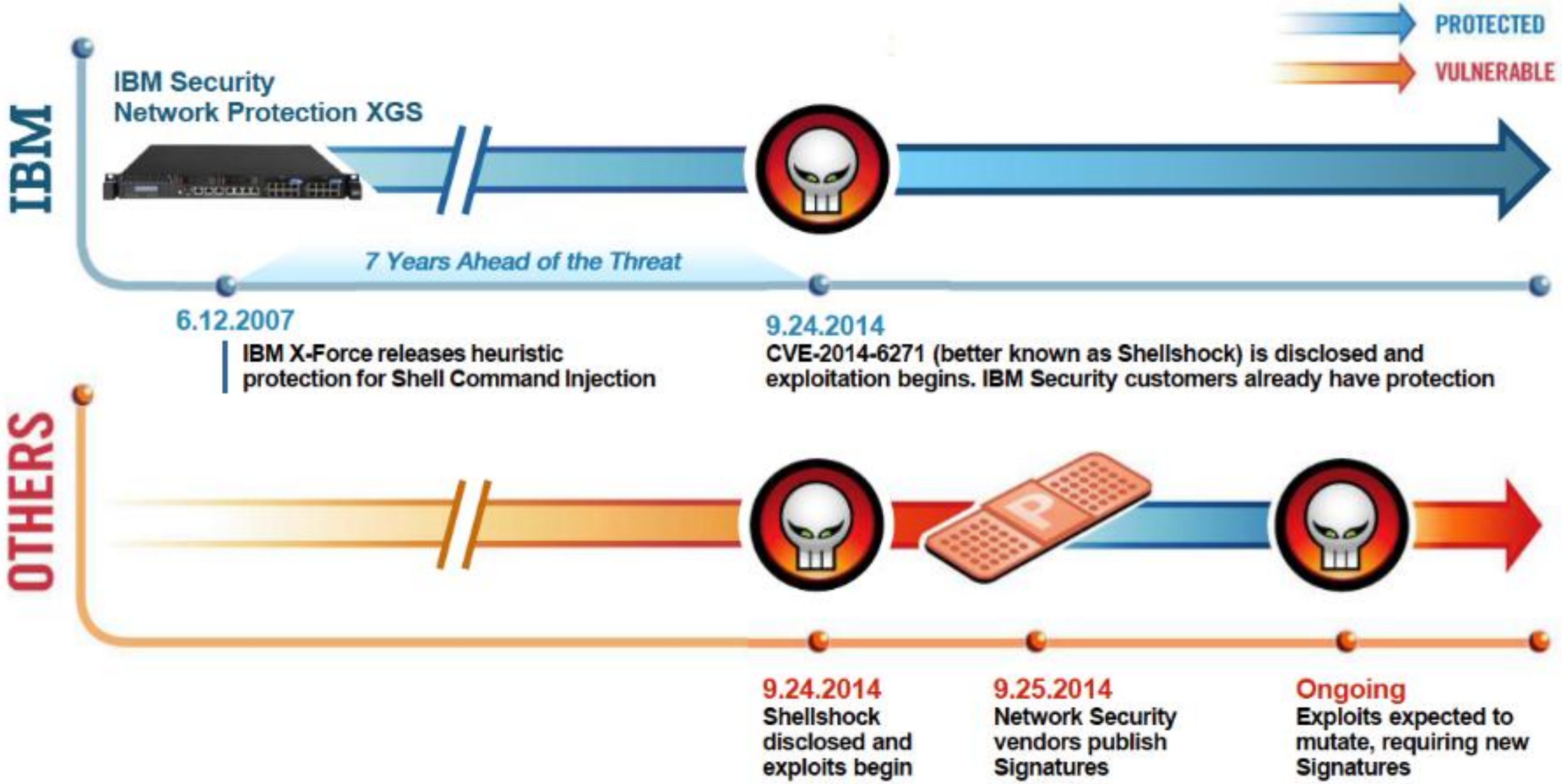
Additional CVEs created to document Shellshock, bringing total to 6

26 Sep 2014

IBM MSS observes 800% increase above average of the attack signature Command_Shell_ Injection across customer base

Avoiding the Shock

IBM's preemptive security helps protect customers against the Bash "Shellshock" vulnerability



PROTECTED

VULNERABLE

IBM

IBM Security
Network Protection XGS

7 Years Ahead of the Threat

6.12.2007
IBM X-Force releases heuristic protection for Shell Command Injection

9.24.2014
CVE-2014-6271 (better known as Shellshock) is disclosed and exploitation begins. IBM Security customers already have protection

OTHERS

9.24.2014
Shellshock disclosed and exploits begin

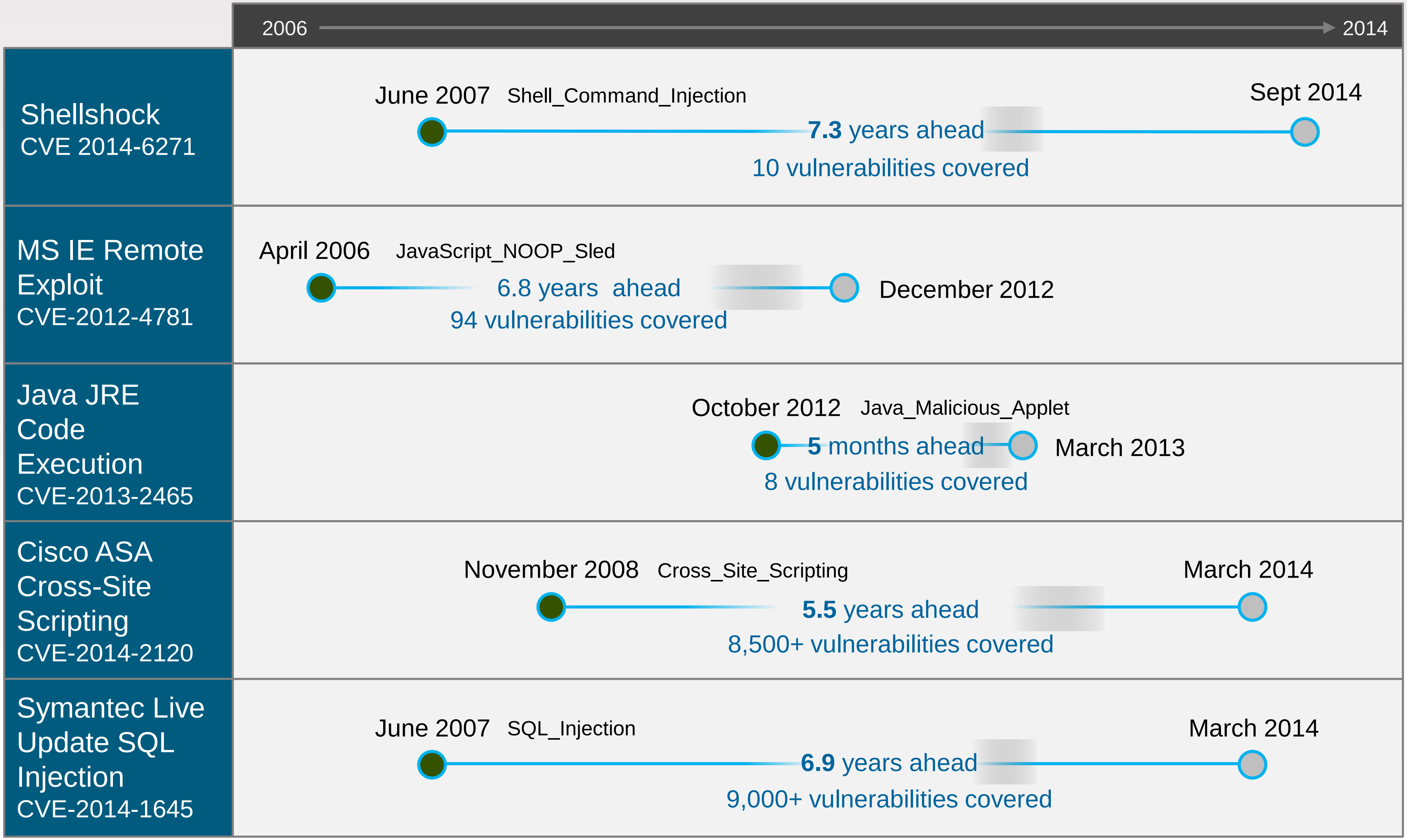
9.25.2014
Network Security vendors publish Signatures

Ongoing
Exploits expected to mutate, requiring new Signatures

IBM Security Network Protection XGS is the only network security solution to offer protection **2661 days** before impact.

Behavioral-based detection blocks attacks that have never been seen before

● IBM Protection ○ Disclosed



2006 → 2014

Shellshock
CVE 2014-6271

June 2007 Shell_Command_Injection

7.3 years ahead

10 vulnerabilities covered

Sept 2014

MS IE Remote Exploit
CVE-2012-4781

April 2006 JavaScript_NOOP_Sled

6.8 years ahead

94 vulnerabilities covered

December 2012

Java JRE Code Execution
CVE-2013-2465

October 2012 Java_Malicious_Applet

5 months ahead

8 vulnerabilities covered

March 2013

Cisco ASA Cross-Site Scripting
CVE-2014-2120

November 2008 Cross_Site_Scripting

5.5 years ahead

8,500+ vulnerabilities covered

March 2014

Symantec Live Update SQL Injection
CVE-2014-1645

June 2007 SQL_Injection

6.9 years ahead

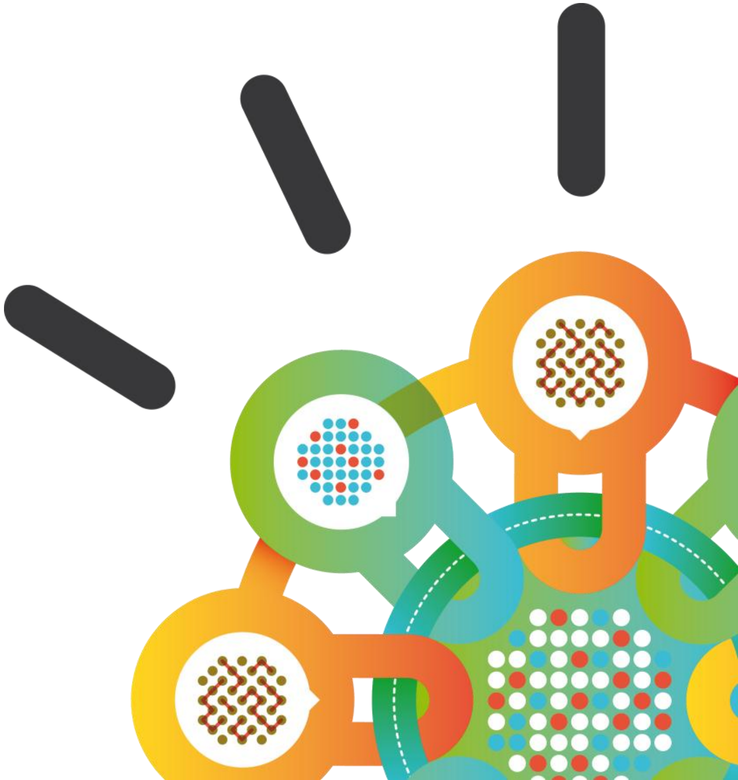
9,000+ vulnerabilities covered

March 2014

© 2014 IBM Corporation

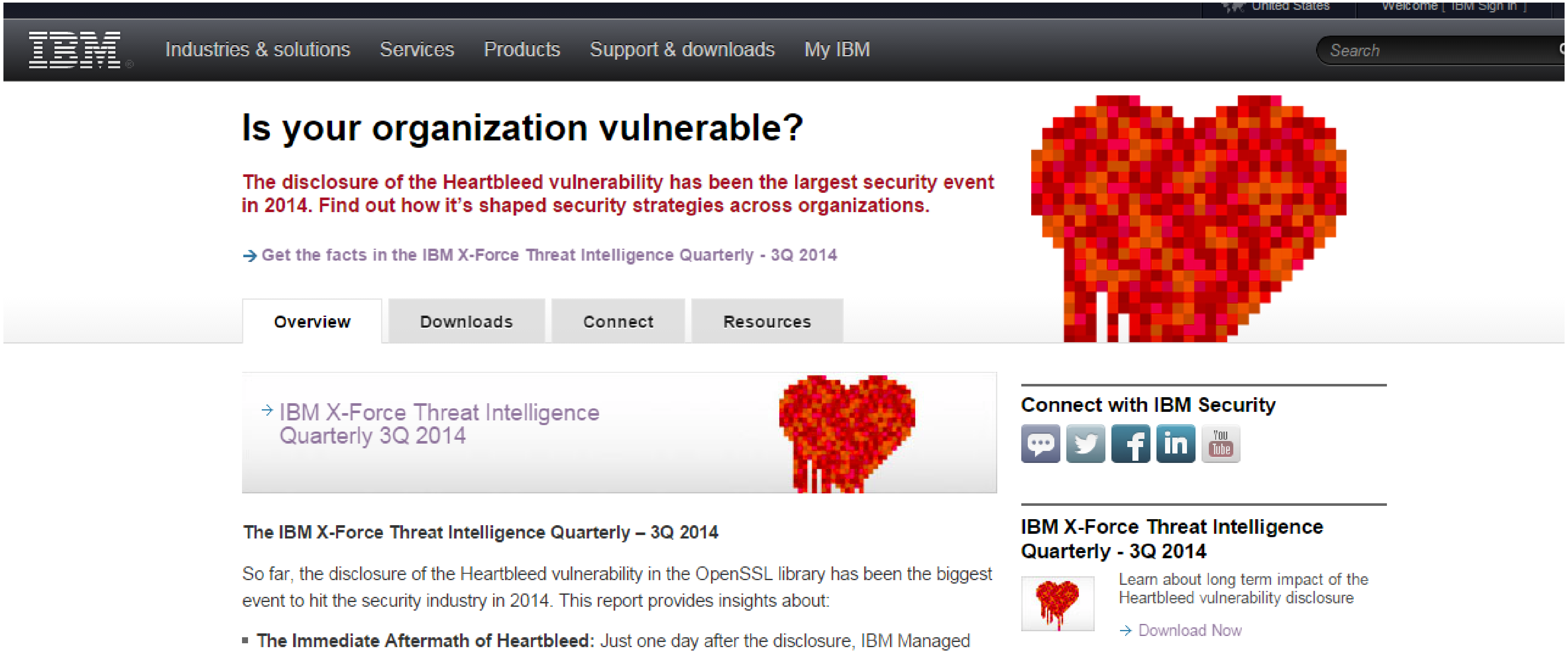
Security Intelligence.
Think Integrated.

X-Force Threat Intelligence Quarterly Review



© 2014 IBM Corporation

Threat Intelligence Quarterly



Is your organization vulnerable?

The disclosure of the Heartbleed vulnerability has been the largest security event in 2014. Find out how it's shaped security strategies across organizations.

→ Get the facts in the IBM X-Force Threat Intelligence Quarterly - 3Q 2014

→ IBM X-Force Threat Intelligence Quarterly 3Q 2014

The IBM X-Force Threat Intelligence Quarterly – 3Q 2014

So far, the disclosure of the Heartbleed vulnerability in the OpenSSL library has been the biggest event to hit the security industry in 2014. This report provides insights about:

- **The Immediate Aftermath of Heartbleed:** Just one day after the disclosure, IBM Managed

Connect with IBM Security

IBM X-Force Threat Intelligence Quarterly - 3Q 2014

Learn about long term impact of the Heartbleed vulnerability disclosure

→ Download Now

More than

half a billion records

of personally identifiable information (PII) were leaked in 2013.

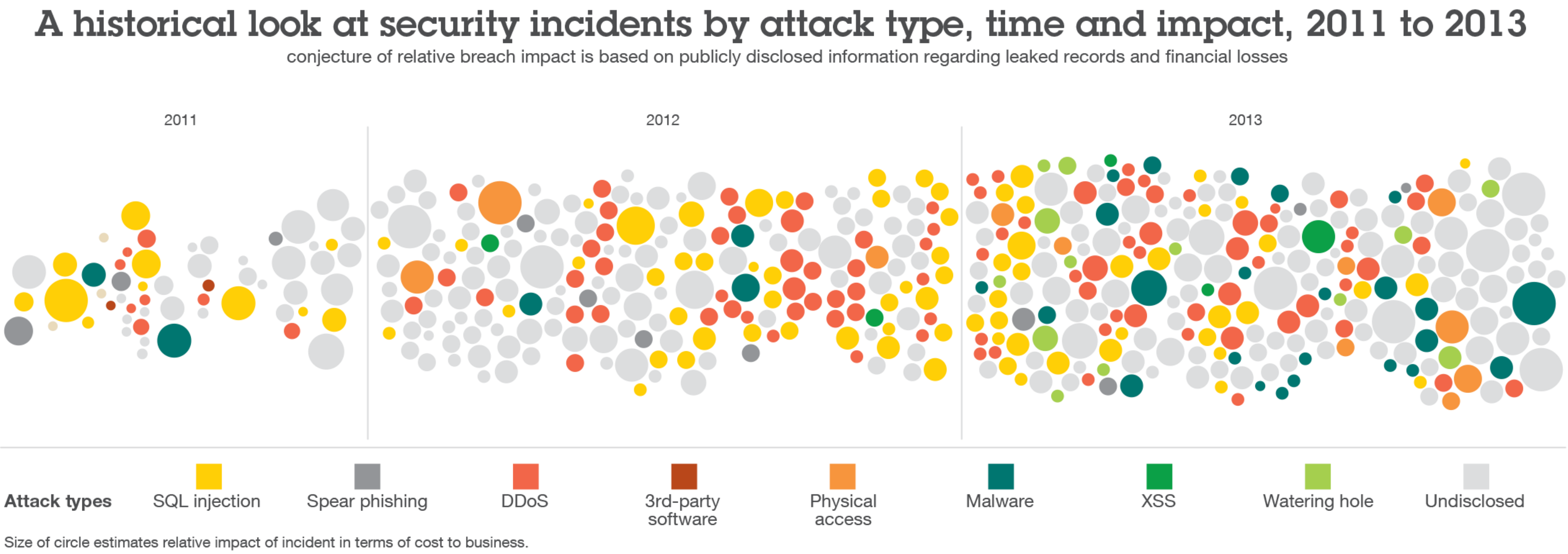
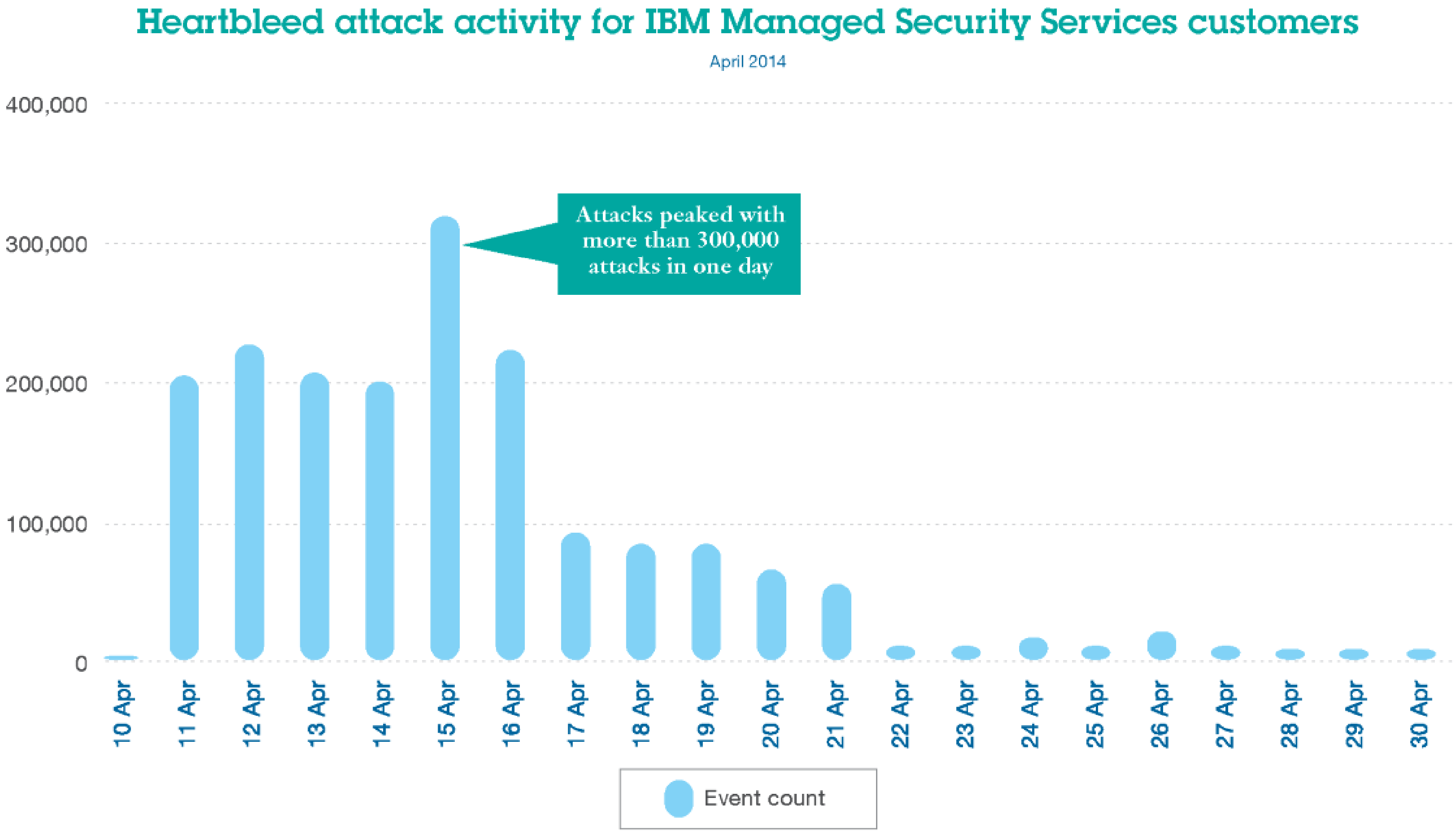


Figure 1. A historical look at security incidents by attack type, time and impact, 2011 to 2013

Source: IBM X-Force® Research and Development

© 2014 IBM Corporation

After Heartbleed was disclosed, MSS witnessed over 300,000 attacks in 24 hrs, and average of 3.47 attacks per second for more than hundreds of customers!



Heartbleed attack activity for IBM Managed Security Services customers

April 2014

Attacks peaked with more than 300,000 attacks in one day

Figure 1. Attack activity related to the Heartbleed vulnerability, as noted for IBM Managed Security Services customers, in April 2014

Source: IBM X-Force® Research and Development

© 2014 IBM Corporation

MSS continues to average 7k attacks per day – mostly from malicious hosts.

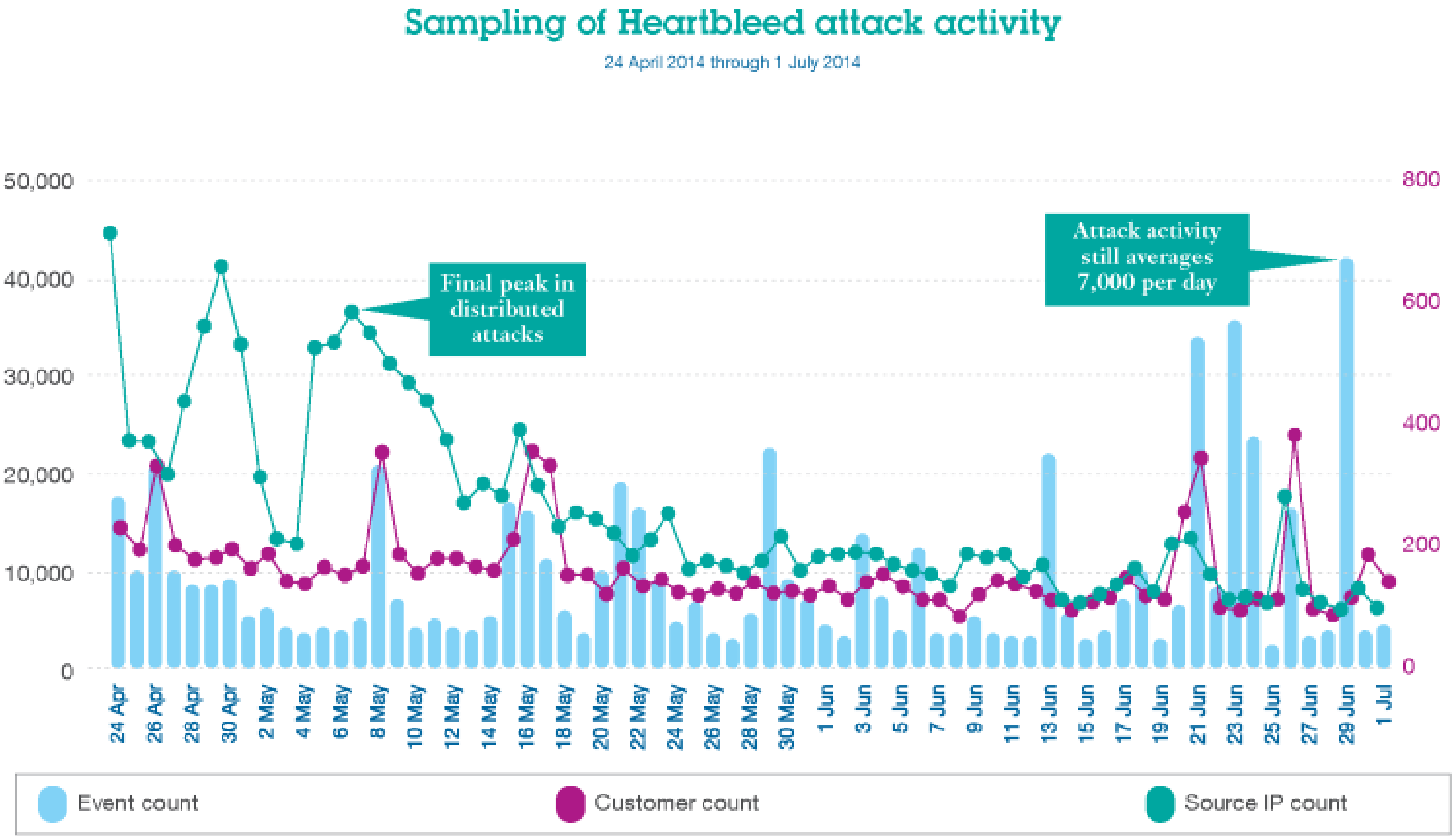


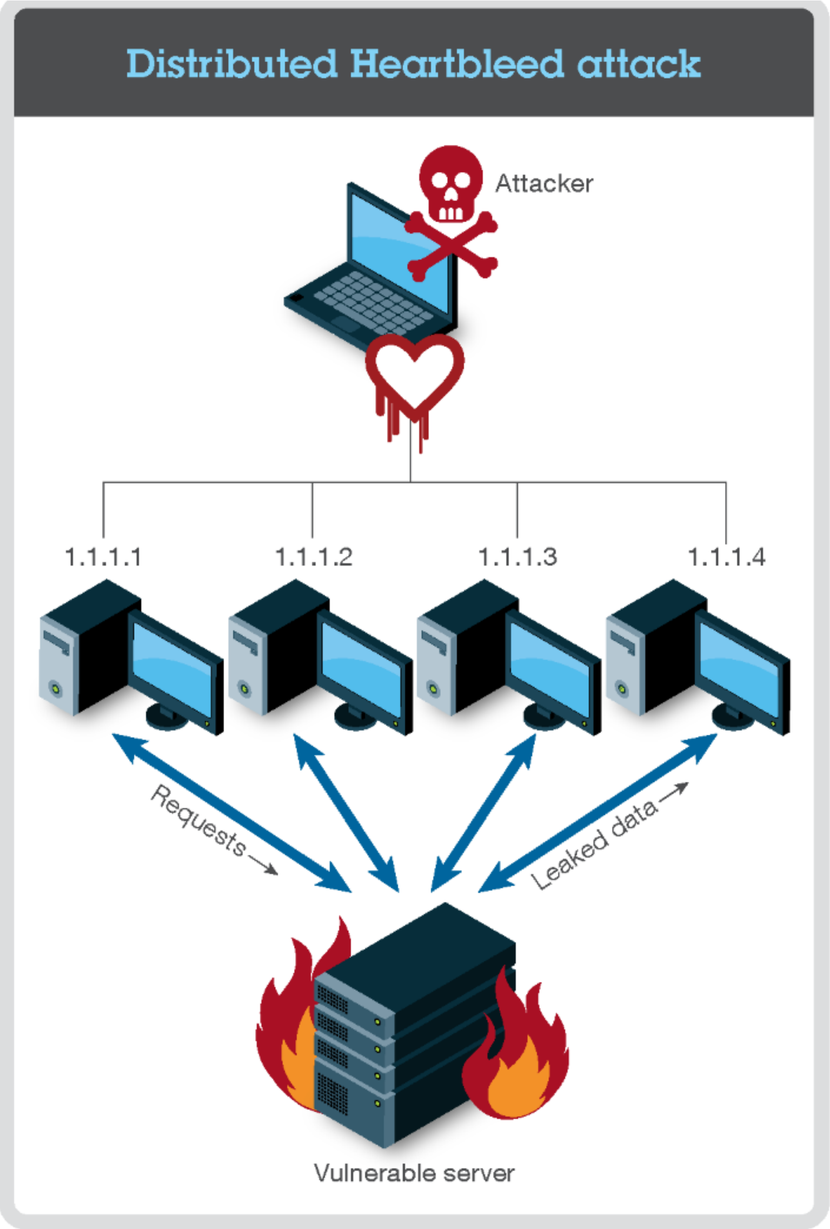
Figure 3. Sampling of Heartbleed attack activity for IBM Managed Security Services customers, 24 April 2014 through 1 July 2014

Source: IBM X-Force® Research and Development

© 2014 IBM Corporation

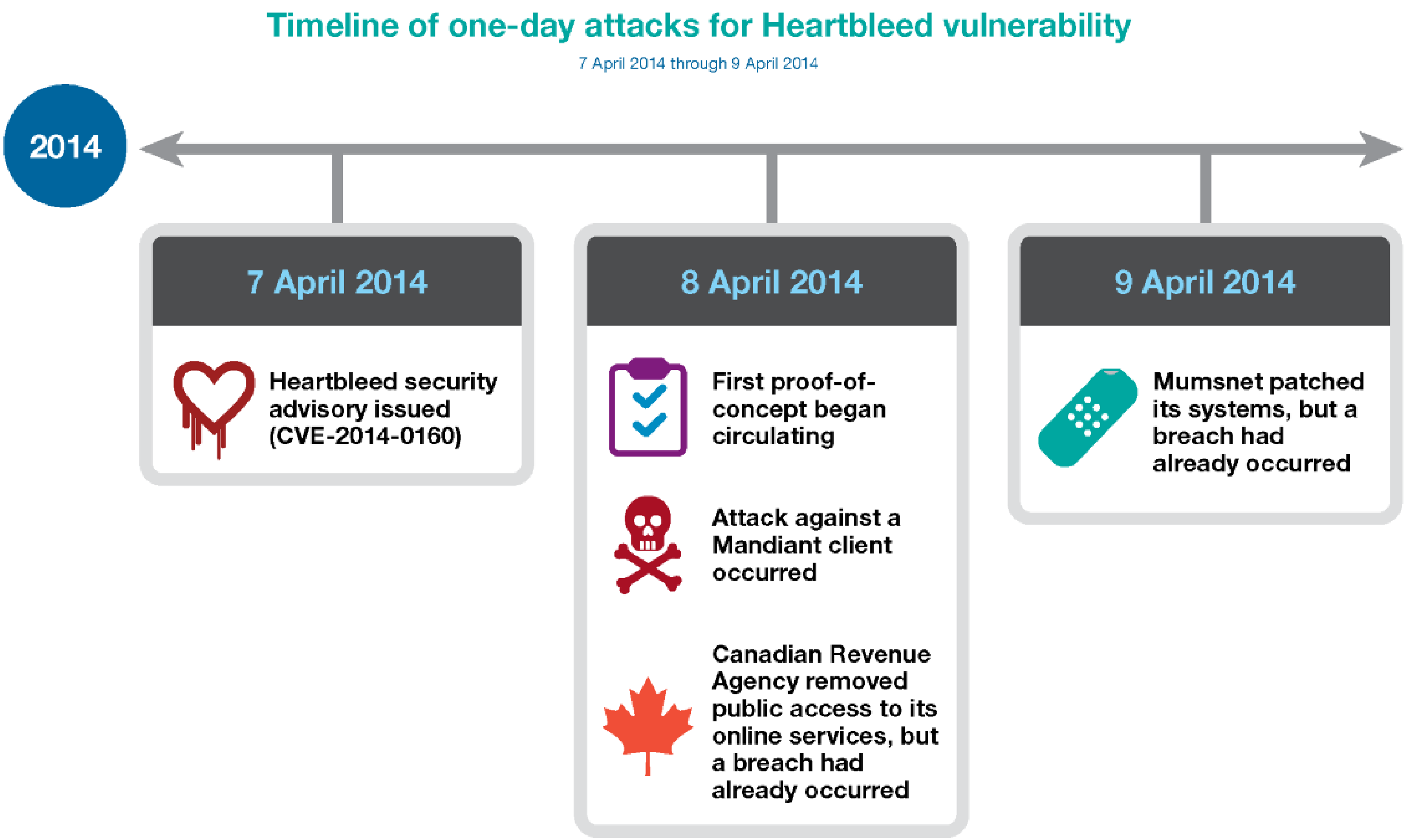
Rather than a single IP address executing the attack repeatedly, many of the attacks used a distributed method.

This enabled attackers to have a large, diversified attack surface and the flexibility to overcome rudimentary blocking strategies.



© 2014 IBM Corporation

One-day attack methods demonstrate how quickly attackers rush to exploit a vulnerability like Heartbleed.



Timeline of one-day attacks for Heartbleed vulnerability

7 April 2014 through 9 April 2014

2014

7 April 2014

Heartbleed security advisory issued (CVE-2014-0160)

8 April 2014

First proof-of-concept began circulating

Attack against a Mandiant client occurred

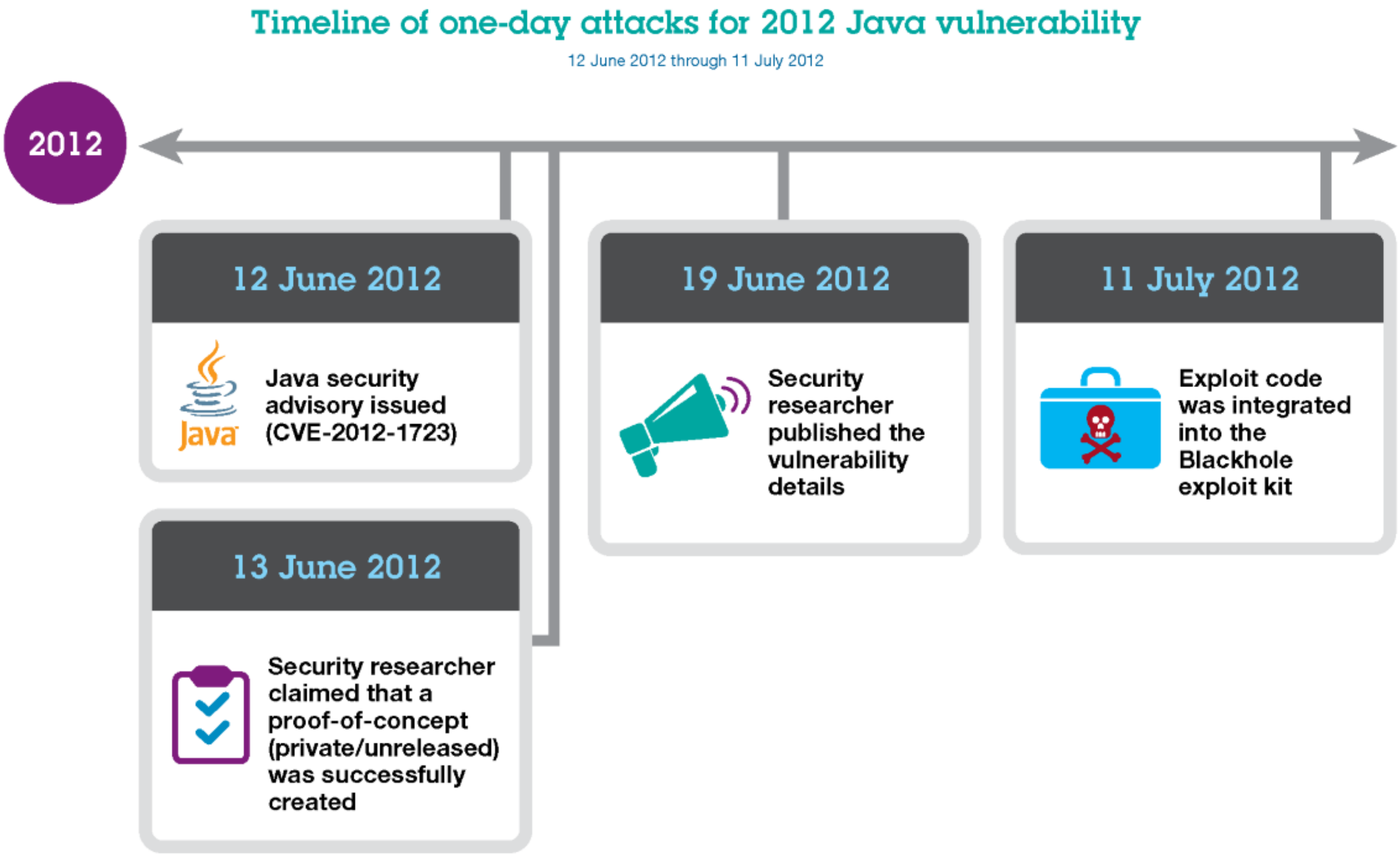
Canadian Revenue Agency removed public access to its online services, but a breach had already occurred

9 April 2014

Mumsnet patched its systems, but a breach had already occurred

Figure 4. Timeline of one-day attacks for Heartbleed vulnerability (CVE-2014-0160), 7 April 2014 through 9 April 2014

X-Force noted this trend was similar to a 2012 disclosure of a Java vulnerability.



Timeline of one-day attacks for 2012 Java vulnerability

12 June 2012 through 11 July 2012

2012

12 June 2012

Java security advisory issued (CVE-2012-1723)

13 June 2012

Security researcher claimed that a proof-of-concept (private/unreleased) was successfully created

19 June 2012

Security researcher published the vulnerability details

11 July 2012

Exploit code was integrated into the Blackhole exploit kit

Figure 5. Timeline of one-day attacks for 2012 Java vulnerability (CVE-2012-1723), 12 June 2012 through 11 July 2012

Source: IBM X-Force® Research and Development

© 2014 IBM Corporation

There was a decline in vulnerability disclosures in the first half of 2014; this could be the first reduction since 2011.

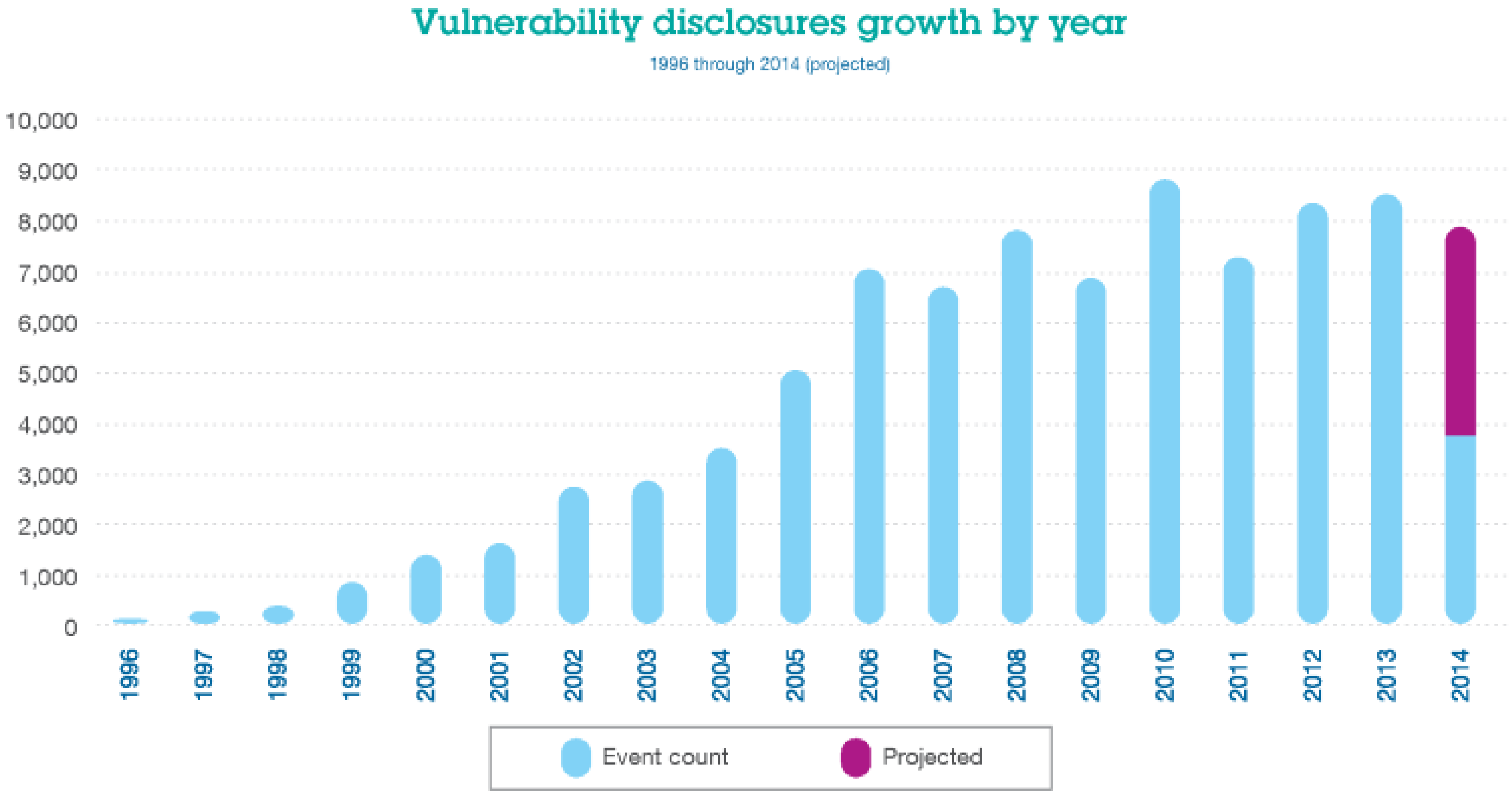
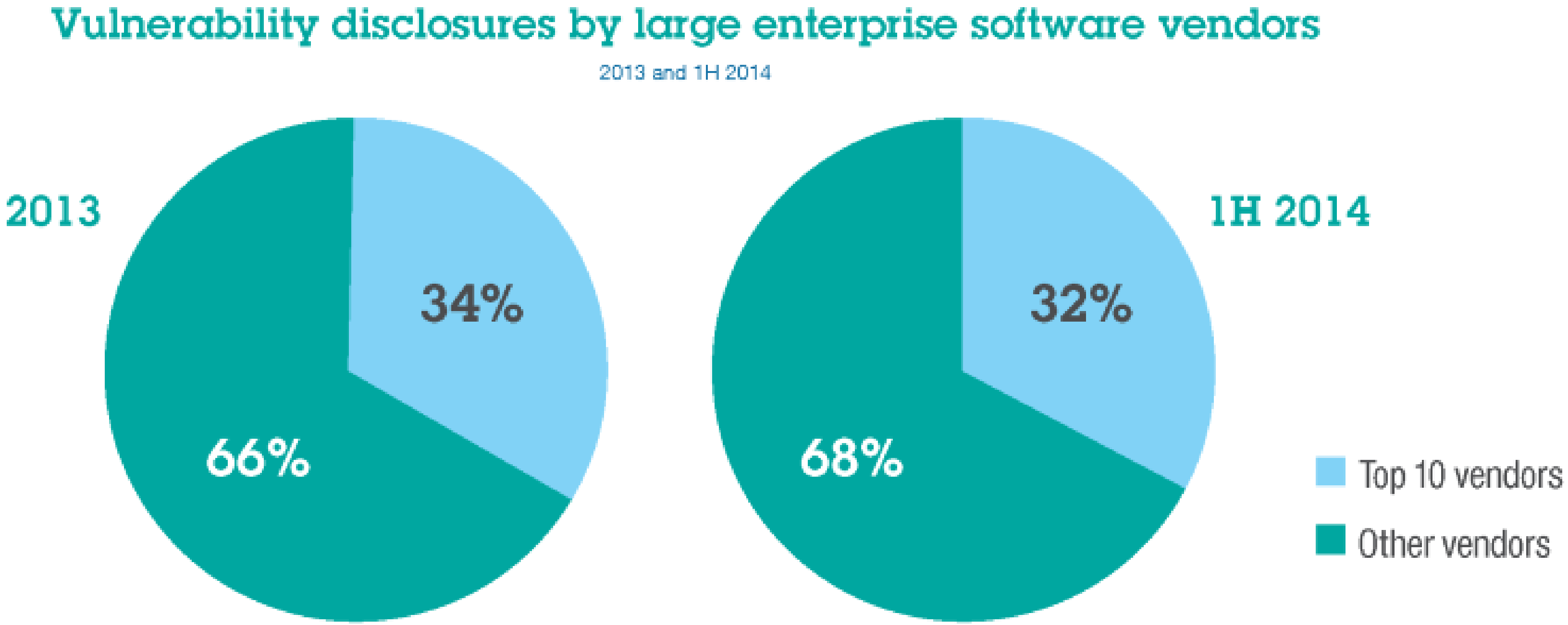


Figure 6. Vulnerability disclosures growth by year, 1996 through 2014 (projected)

© 2014 IBM Corporation

It is difficult to point to any one factor that has contributed to the decline in the number of vulnerability disclosures in 2014.

A decreasing number of vendors consistently reporting vulnerabilities might be contributing to the recent decline in total overall vulnerabilities disclosed.



Vulnerability disclosures by large enterprise software vendors

2013 and 1H 2014

Figure 7. Vulnerability disclosures by large enterprise software vendors, 2013 and 1H 2014

Source: IBM X-Force® Research and Development

© 2014 IBM Corporation

Plug-ins are responsible for 90% of total CMS vulnerabilities disclosed. This heightened risk leads to mass infection.

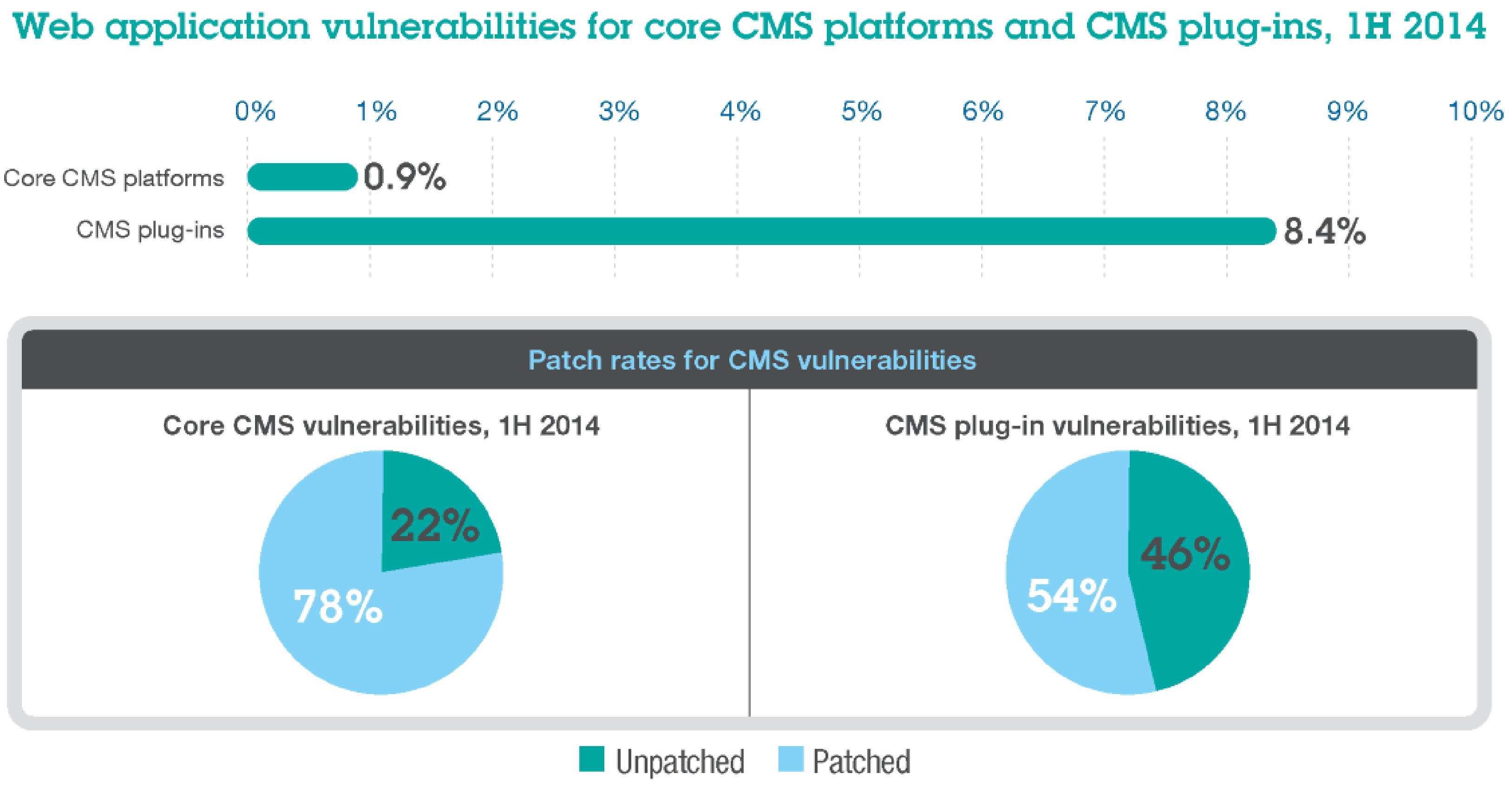


Figure 8. Web application vulnerabilities for core CMS platforms and CMS plug-ins, as a percentage of all disclosures and corresponding patch rates, 1H 2014

Source: IBM X-Force® Research and Development

© 2014 IBM Corporation

Does current CVSS scoring represent actual risk to networks and systems?

Heartbleed existed for two years and received a CVSS medium base score of 5.0.

CVSS base scores, 2012 through 1H 2014

CVSS score	Severity level
10	**Critical** A successful exploit is likely to have catastrophic adverse effects
7.0 – 9.9	**High** A successful exploit is likely to have significant adverse effects
4.0 – 6.9	**Medium** A successful exploit is likely to have moderate adverse effects
0.0 – 3.9	**Low** A successful exploit is likely to have limited adverse effects

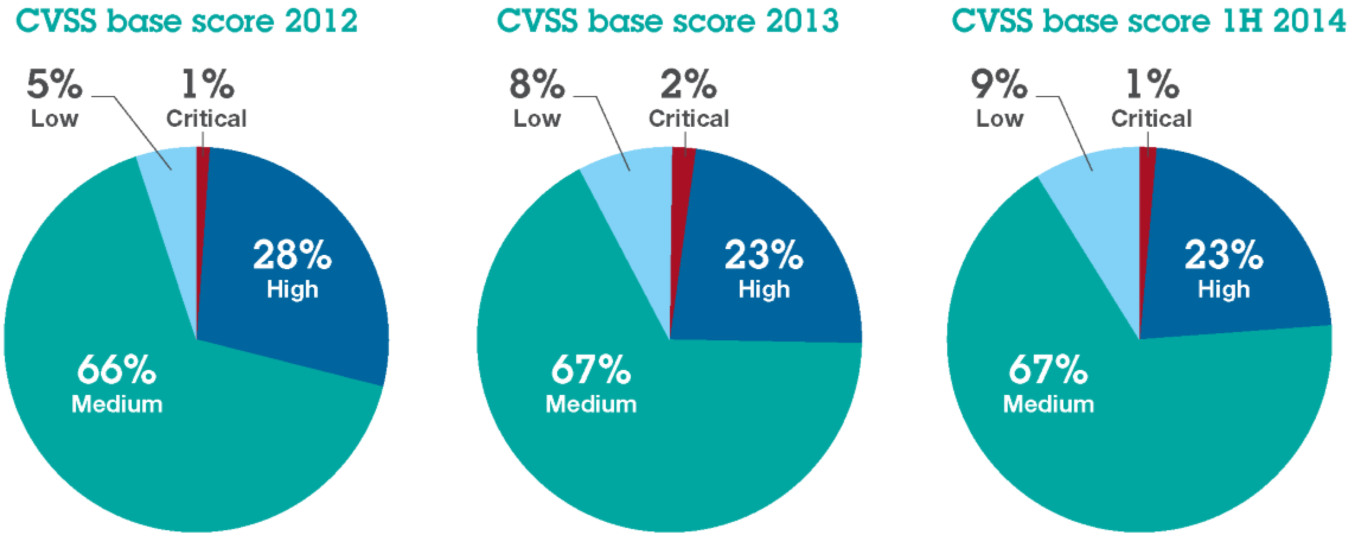


Figure 9. CVSS base scores, 2012 through 1H 2014

Source: IBM X-Force® Research and Development

What can you do to mitigate these threats?

- Keep up with threat intelligence.
- Maintain a current and accurate asset inventory.
- Have a patching solution that covers your entire infrastructure.
- Implement mitigating controls.
- Instrument your environment with effective detection.
- Create and practice a broad incident response plan.

© 2014 IBM Corporation

Connect with IBM X-Force Research & Development

Follow us at @ibmsecurity
and @ibmxforce

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

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

© 2014 IBM Corporation

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

© Copyright IBM Corporation 2014. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM’s sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.