

**Was ist Ihnen im Leben  
am Wichtigsten ?**



**Was ist Ihnen im Leben  
am Wichtigsten ?**

**Freiheit ?**



**Was ist Ihnen im Leben  
am Wichtigsten ?**

**Freiheit ?**

**Sicherheit ?**



**Was ist Ihnen im Leben  
am Wichtigsten ?**

**Freiheit ?**

**Sicherheit ?**

**Oder beides ?**



A photograph of a person in a yellow kayak on clear blue water. A shark is swimming in the foreground, its dorsal fin visible above the surface. The background shows a distant shoreline with a hill under a clear blue sky.

**Können Sie ohne  
Sicherheit**

**wirklich frei und  
entspannt (über)leben?**



# Wie Sie die Sicherheitslücken Ihrer Web-Applikationen schließen

Rüdiger Gmach

IBM Security Systems Division, IBM Österreich

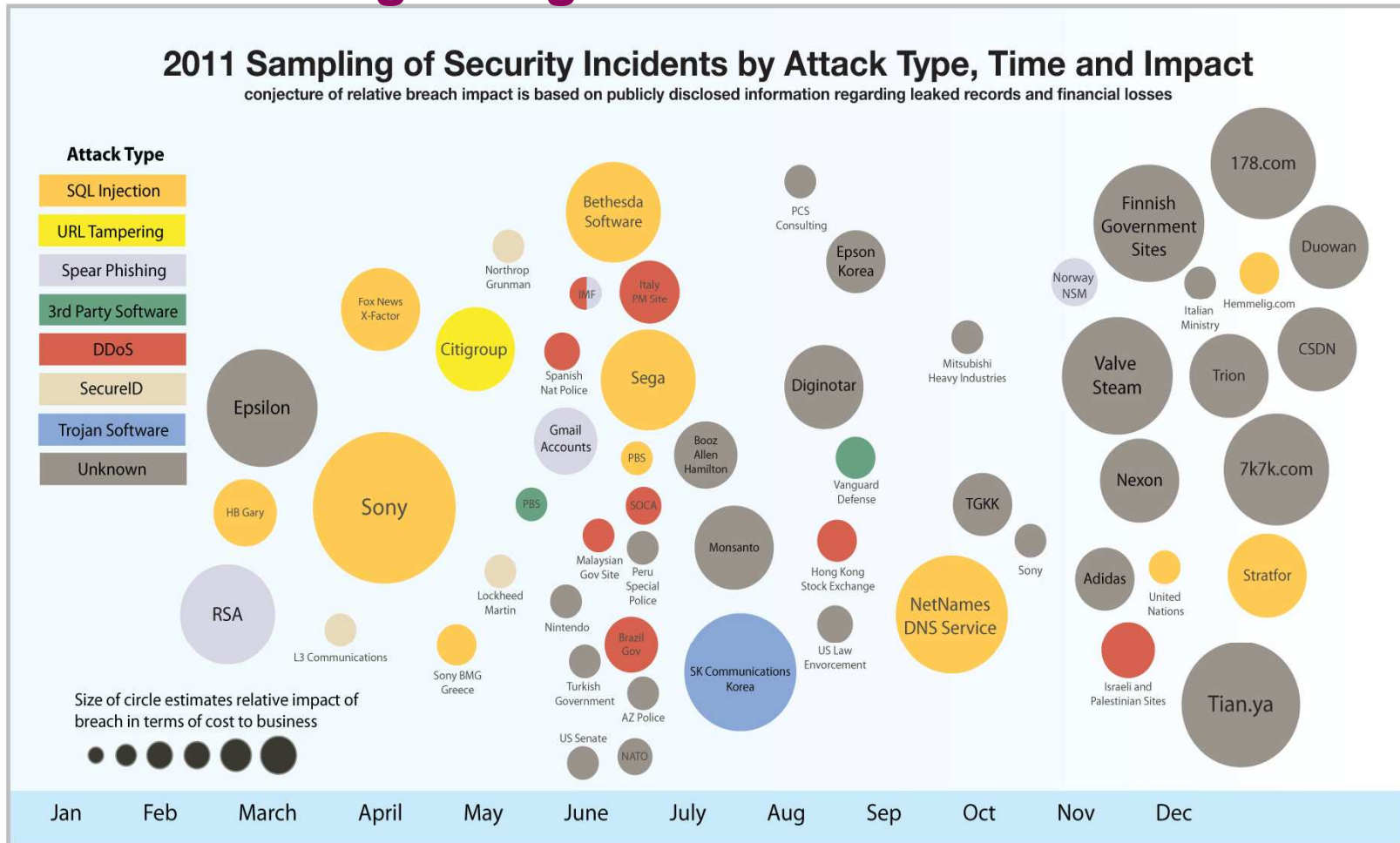


IBM **Software** &  
**InnovationDay** 2012

Smarte Software für Ihr Business



# Zielgerichtete Angriffe erschüttern Firmen und Regierungen



Source: IBM X-Force® Research and Development

©2012 IBM Corporation

# Österreich – Insel der Seeligen??? Leider nicht!

BRZ



Namen und Adressen von etwa 3000 Kunden

Polizei



Datensätze von 24.938 österreichischen Polizisten online veröffentlicht

GIS



214.000 Kundendaten mit ca. 97.000 Kontodaten

Politische Parteien

eMail Zugang, Web Seiten . . .

WKÖ



6 200 Kundendaten

Justizministerium

Webseite lahmgelegt

TGKK



600 475 Datensätze - Namen, Versicherungsnummern und Adressen von zahlreichen Prominenten.

ORF



Cryptoworks-Verschlüsselung betroffen sind rund 1,3 Mio. Smartcards

T-Mobile



Online Shop mit ca. 100000 Kundendaten inkl. Kennwörter

**Hacker stehlen Österreich 488.000 Tonnen CO2 Rechte**

**15-jähriger Hacker aus NÖ knackte 259 Firmen**

©2012 IBM Corporation



# Web Applications Security hat höchste Priorität

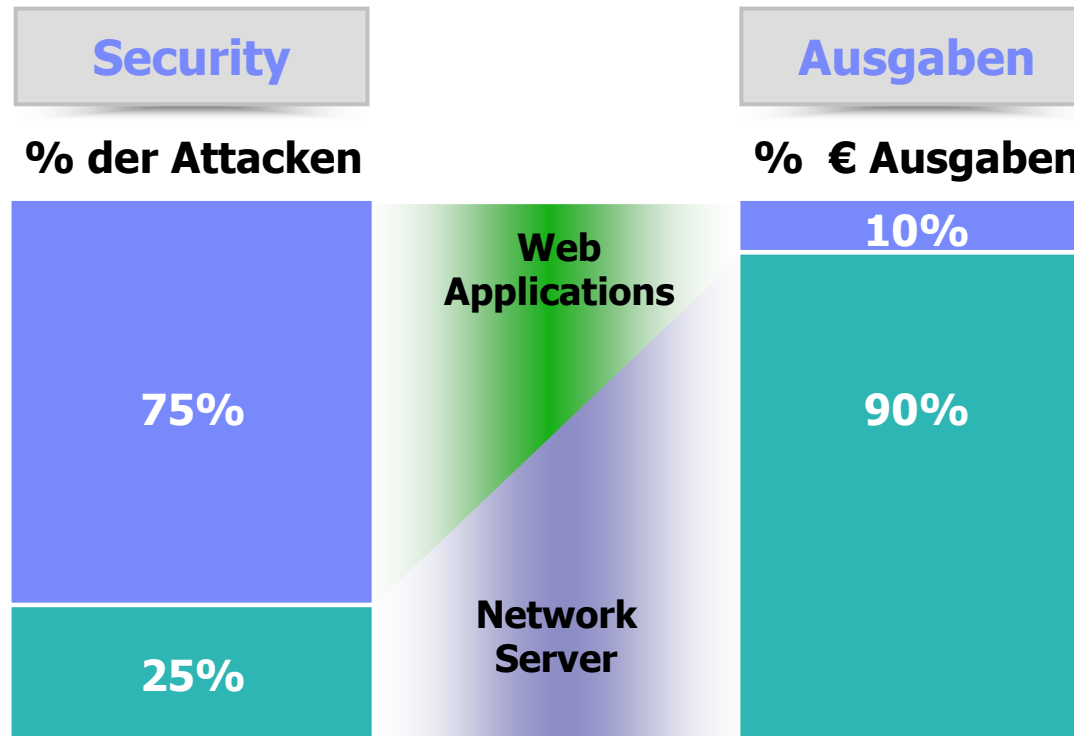
- **Web Applikationen sind #1 Focus der Hacker:**
  - 75% aller Attacken finden auf Applikationsebene statt (Gartner)
  - XSS und SQL Injection sind #1 und #2 aller bekanntgegebenen Schwachstellen (Mitre)
- **Die meisten Web-Sites sind verwundbar:**
  - 78% der leicht ausnutzbaren Schwachstellen betreffen Web-Applikationen (Symantec)
  - 90% aller Web-Sites sind von Attacken auf Applikationseben verletzbar (Watchfire)
  - 80% aller Organisationen sind / waren von Web-Applikationsattacken betroffen (Gartner)
- **Web Applikationen sind wertvolle Ziele für Hacker:**
  - Kunden-Daten, Kreditkarten, Identitätsdiebstahl, Betrug, Entstellung des Web-Auftrittes, etc...
- **Security Compliance Anforderungen:**
  - Payment Card Industry (PCI) Standards, GLBA, HIPPA, FISMA
- ***Security Compliance ist die stärkste Motivation für Unternehmen um Web Application Security zu adressieren.***

©2012 IBM Corporation



Security

# Die Herausforderung für Organisationen



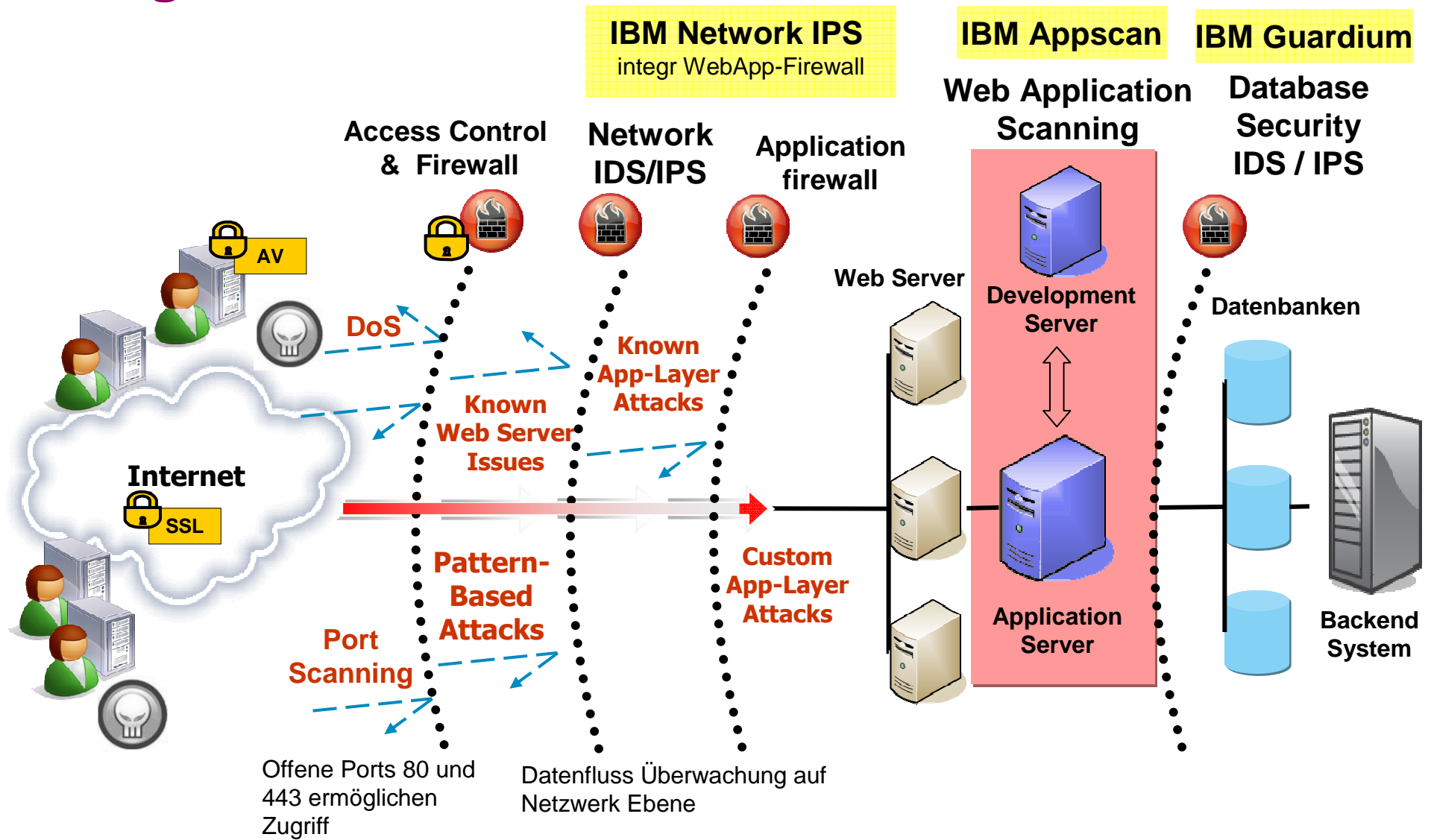
**75%** aller Attacken auf die Information Security richten sich gegen den Web Application Layer

Sources: Gartner, Watchfire

©2012 IBM Corporation



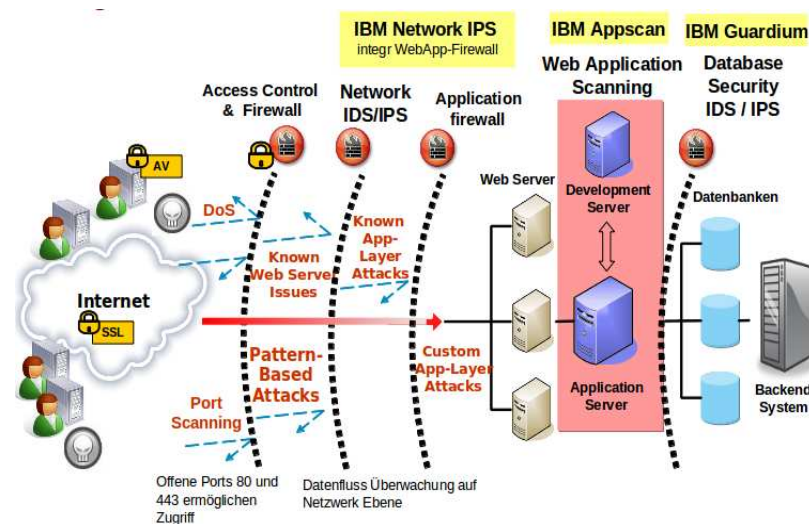
# Angriffsvektoren und Abwehr





# IBM Security NIPS

Die Network Intrusion Detection & Prevention mit eingebauter Web-Application Firewall

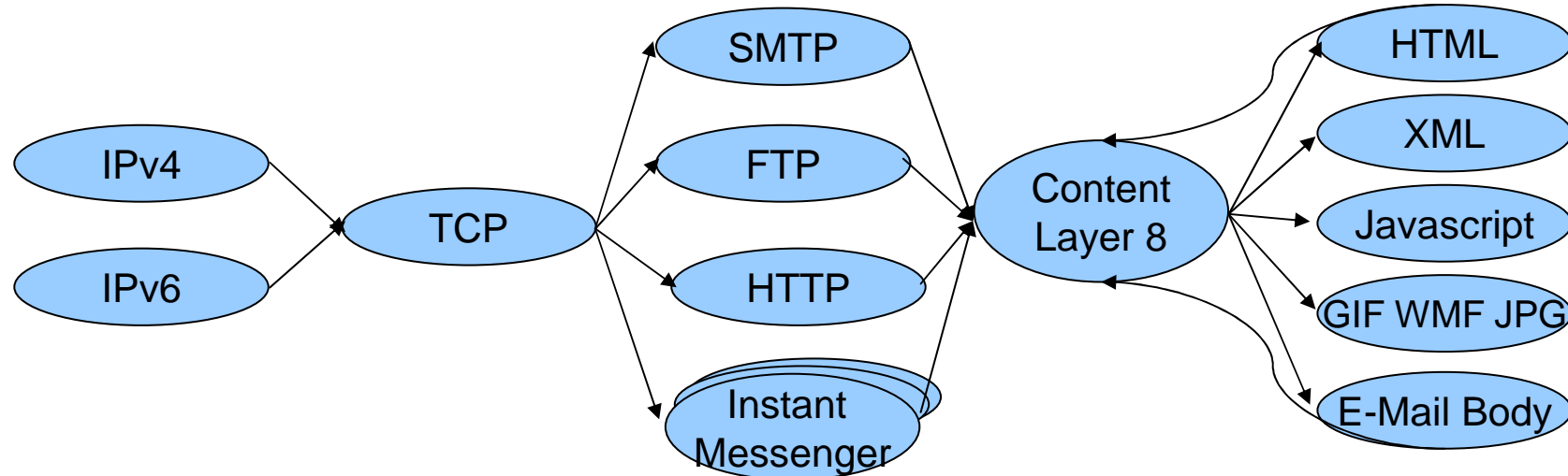


IBM Software &  
Innovation Day 2012  
Smarte Software für Ihr Business



# Protokoll & Inhalts Analyse auf allen Ebenen

- Simulation des Protokoll- und Content-Stacks eines verletzlichen Systems
- Normalisierung auf jeder Protokoll- und Content-Ebene



- Schutz gegen neue Angriffstechnologien
- Automatische Anpassung an neue Anforderungen und Markt-Bedürfnisse (Updates von X-Force)

# Web Application Security

Schutz für Web Anwendungen gegen höher entwickelte Angriffe auf Applikations-Ebene, wie z.B. :

- SQL (Structured Query Language) Injection
- XSS (Cross-site scripting)
- PHP (Hypertext Preprocessor) file-includes
- CSRF (Cross-site request forgery)
- IBM NIPS bietet intelligente Injection Logic Engine
- Abwehr technisch hochentwickelter Angriffe
- Erfüllung gesetzlicher IT Security-Vorschriften

**Web Angriffe werden immer komplexer**

**Web Schutz kann dennoch einfach bleiben**

# IBM Virtual Patch Technology

- Typically, more than **50%** of all vulnerabilities disclosed during a year have no vendor-supplied patches available to remedy the vulnerability by year end.
- Shielding a vulnerability from exploitation independent of a software patch
- Enables a responsible patch management process that can be adhered to without fear of a breach
- IBM is a MAPP (Microsoft Active Protections Program) partner



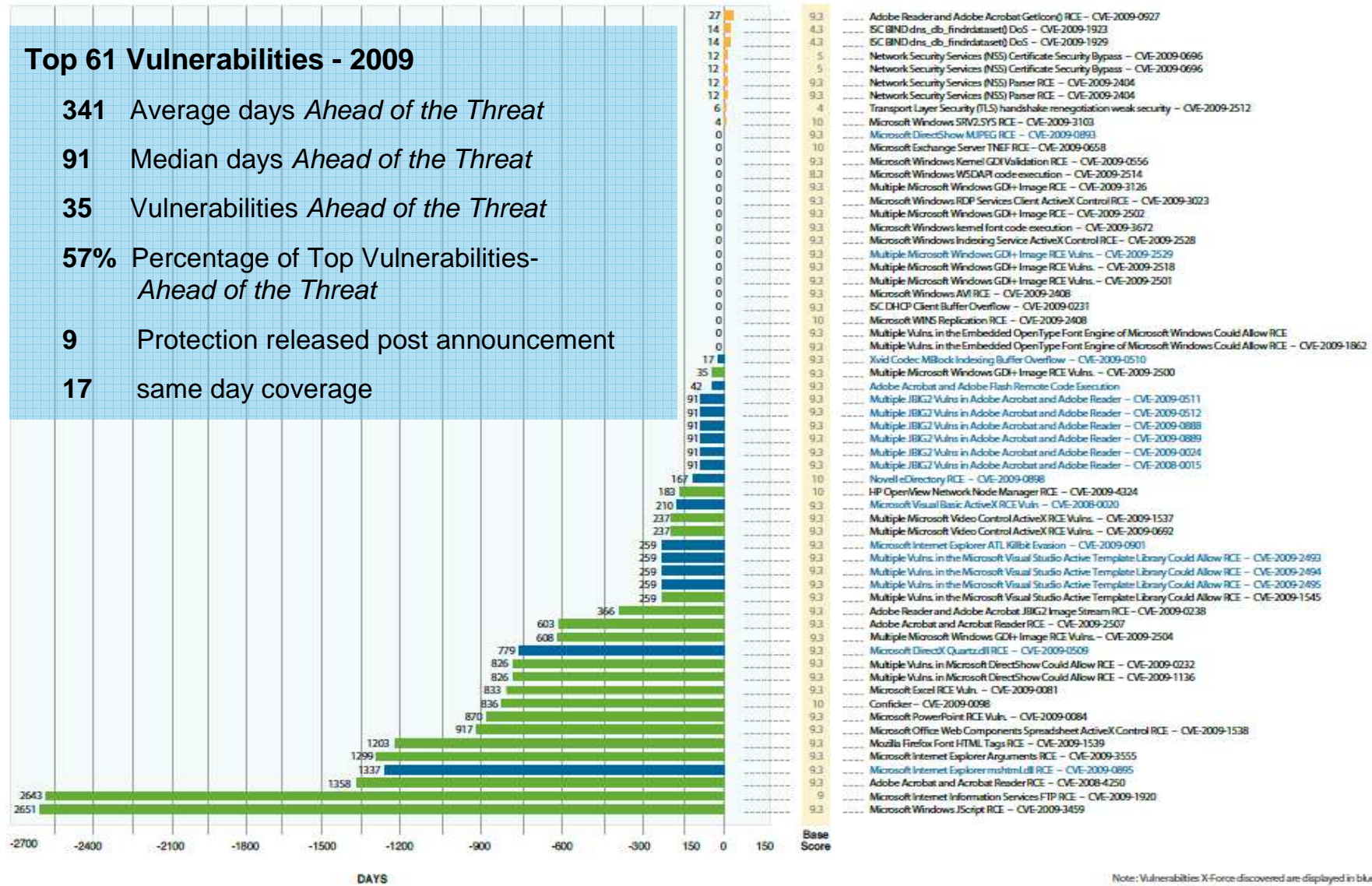
©2012 IBM Corporation



# Security Effectiveness: Ahead of the Threat

## Top 61 Vulnerabilities - 2009

- 341** Average days *Ahead of the Threat*
- 91** Median days *Ahead of the Threat*
- 35** Vulnerabilities *Ahead of the Threat*
- 57%** Percentage of Top Vulnerabilities-  
*Ahead of the Threat*
- 9** Protection released post announcement
- 17** same day coverage



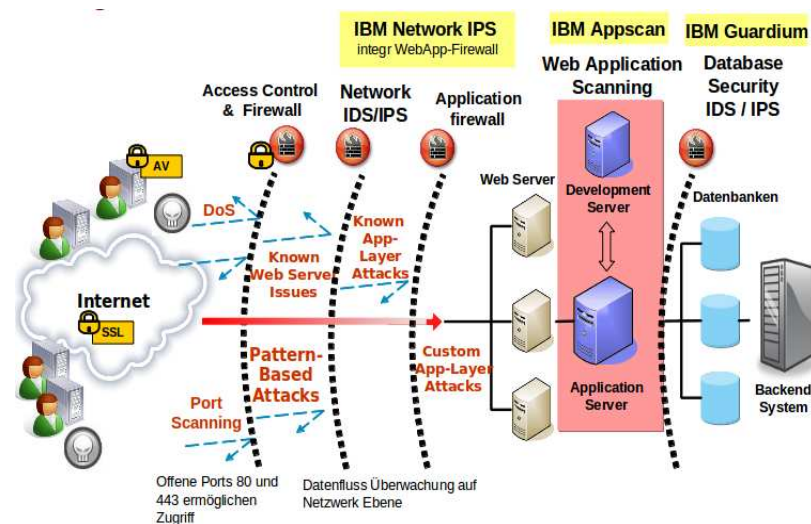
Note: Vulnerabilities X-Force discovered are displayed in blue.  
Note: RCE = Remote Code Execution





# IBM AppScan

Das Tool das ihre WebApps von innen und von außen auf Sicherheitslücken testet



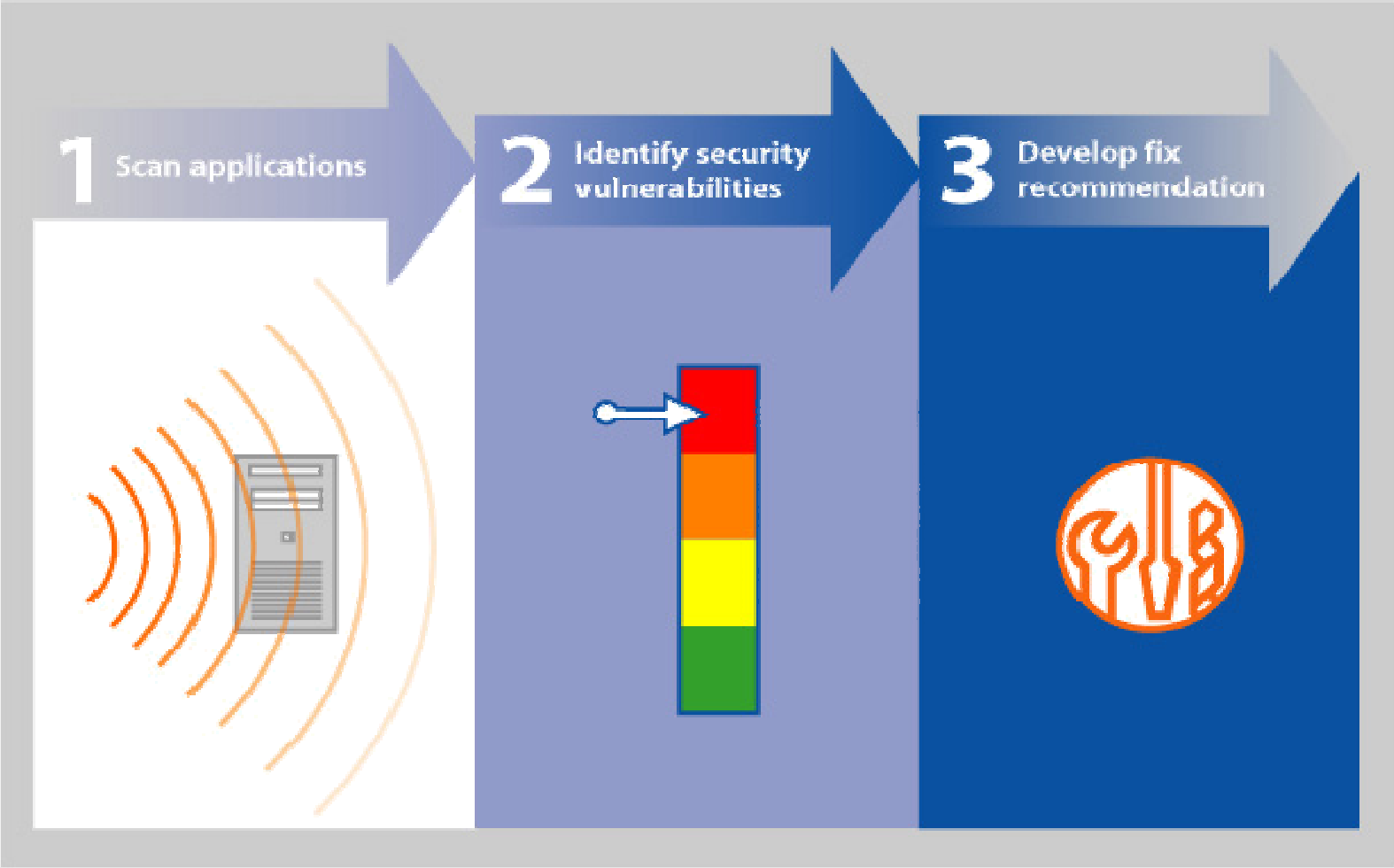
IBM Software & Innovation Day 2012  
Smarte Software für Ihr Business



# Pain Point: Web 2.0 Technologies

- Customers are using the latest Web 2.0 technologies to build interactive Web Applications for their end users
  - Web Services
  - Flash
  - AJAX
  - .....
- These technologies require advanced exploring and testing capabilities which many scanners can not handle

# How Does IBM Rational AppScan Work?



# Easy to Understand Results – Issues and Priorities

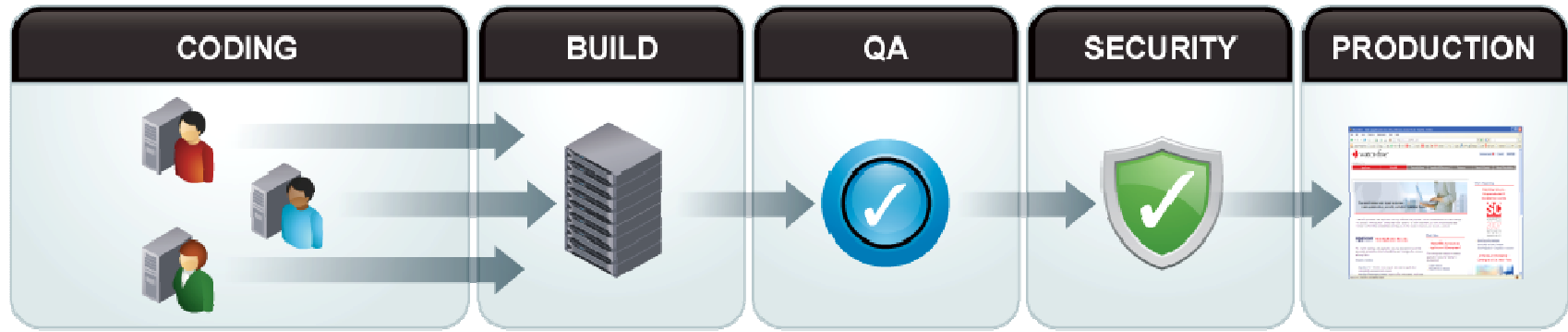
The screenshot displays the IBM AppScan interface. On the left, a bar chart titled 'Total number of issues: 41' shows the distribution of issues by severity: High (12), Medium (11), Low (11), and Info (7). The main window shows a list of 41 security issues, sorted by severity. A callout box highlights the top issues:

- Aranged By: Severity | Highest on top
- 41 Security Issues (137 variants) for 'My Application'
- Cross-Site Scripting (7)
  - http://demo.testfire.net/bank/customize.aspx (2)
  - http://demo.testfire.net/bank/login.aspx (1)
  - http://demo.testfire.net/comment.aspx (2)
  - http://demo.testfire.net/search.aspx (1)
  - http://demo.testfire.net/subscribe.aspx (1)
- HTTP Response Splitting (1)
- SQL Injection (3)

The detailed view of a Cross-Site Scripting issue is shown below:

- Severity:** High
- Type:** Application-level test
- WASC Threat Classification:** Client-side Attacks: Cross-site Scripting
- CVE Reference(s):** N/A
- Security Risk:** It is possible to steal or manipulate customer session and cookies, which may be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user.
- Possible Causes:** Sanitation of hazardous characters was not performed correctly on user input.
- Technical Description:** The Cross-Site Scripting attack is a privacy violation, that allows an attacker to acquire a legitimate user's credentials and to impersonate that user when interacting with a specific website. The attack hinges on the fact that the web site contains a script that returns a user's input (usually a parameter value) in an HTML page, without first sanitizing the input. This allows an input consisting of JavaScript code to be executed by the browser when the script returns this input in the response page. As a result, it is possible to form links to the site where one of the parameters consists of malicious JavaScript code. This code will be executed (by a user's browser) in the site context, granting it access to cookies that the user has for the site, and other windows in the site through the user's browser. The attack proceeds as follows: The attacker lures the legitimate user to click on a link that was produced by the attacker. When the user clicks on the link, this generates a

# AppScan: advanced security testing collaboration & governance through application lifecycle



**Challenge to Share Test Results and Enable Self-Testing in the SDLC**



**AppScan Standard**

**AppScan Enterprise**

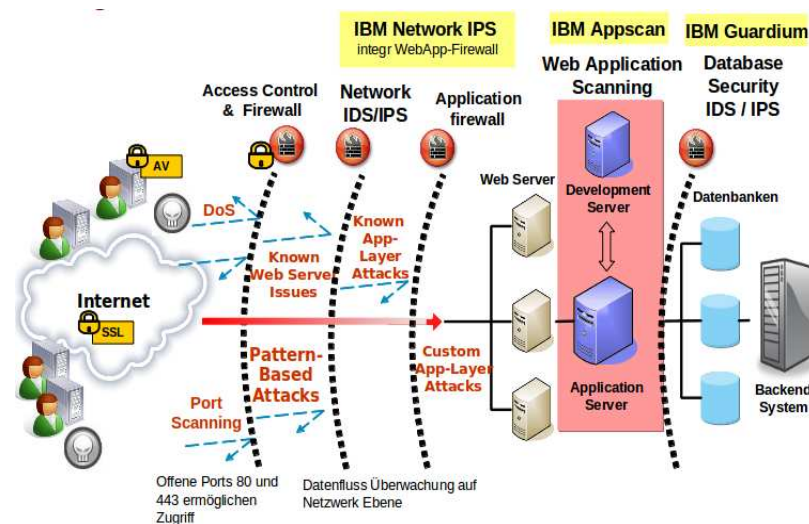
**AppScan Source**





# IBM Guardium Database Security

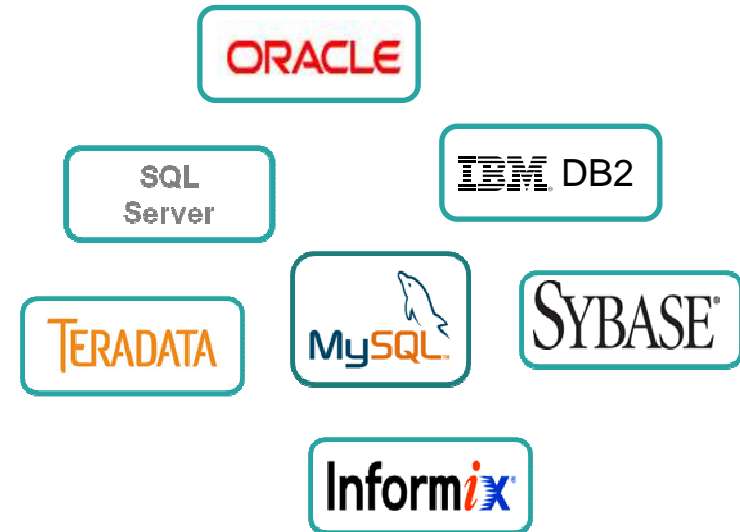
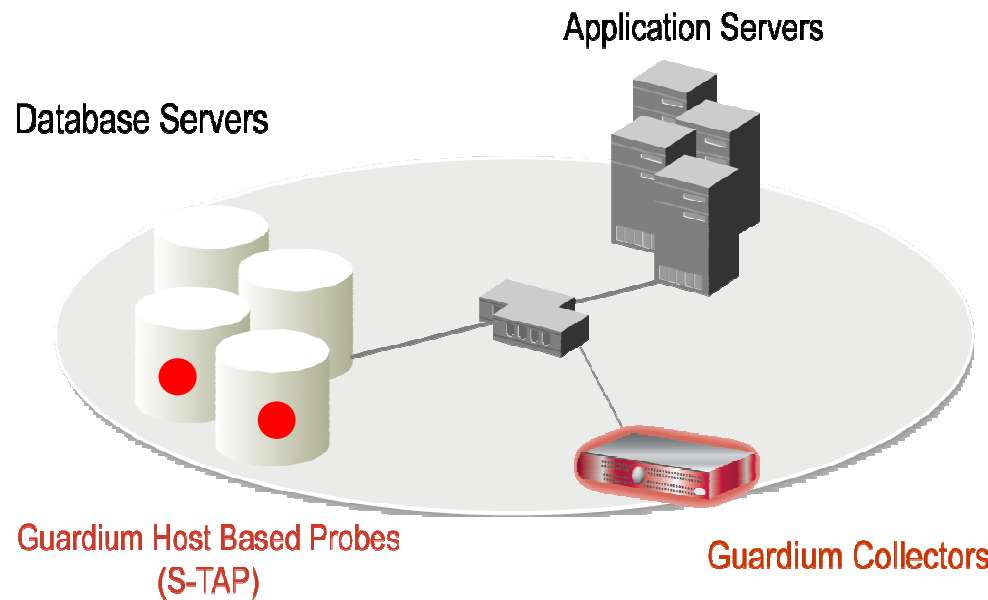
Die Appliance, die Ihre Datenbank effizient und sicher schützt



IBM Software &  
Innovation Day 2012

Smarte Software für Ihr Business

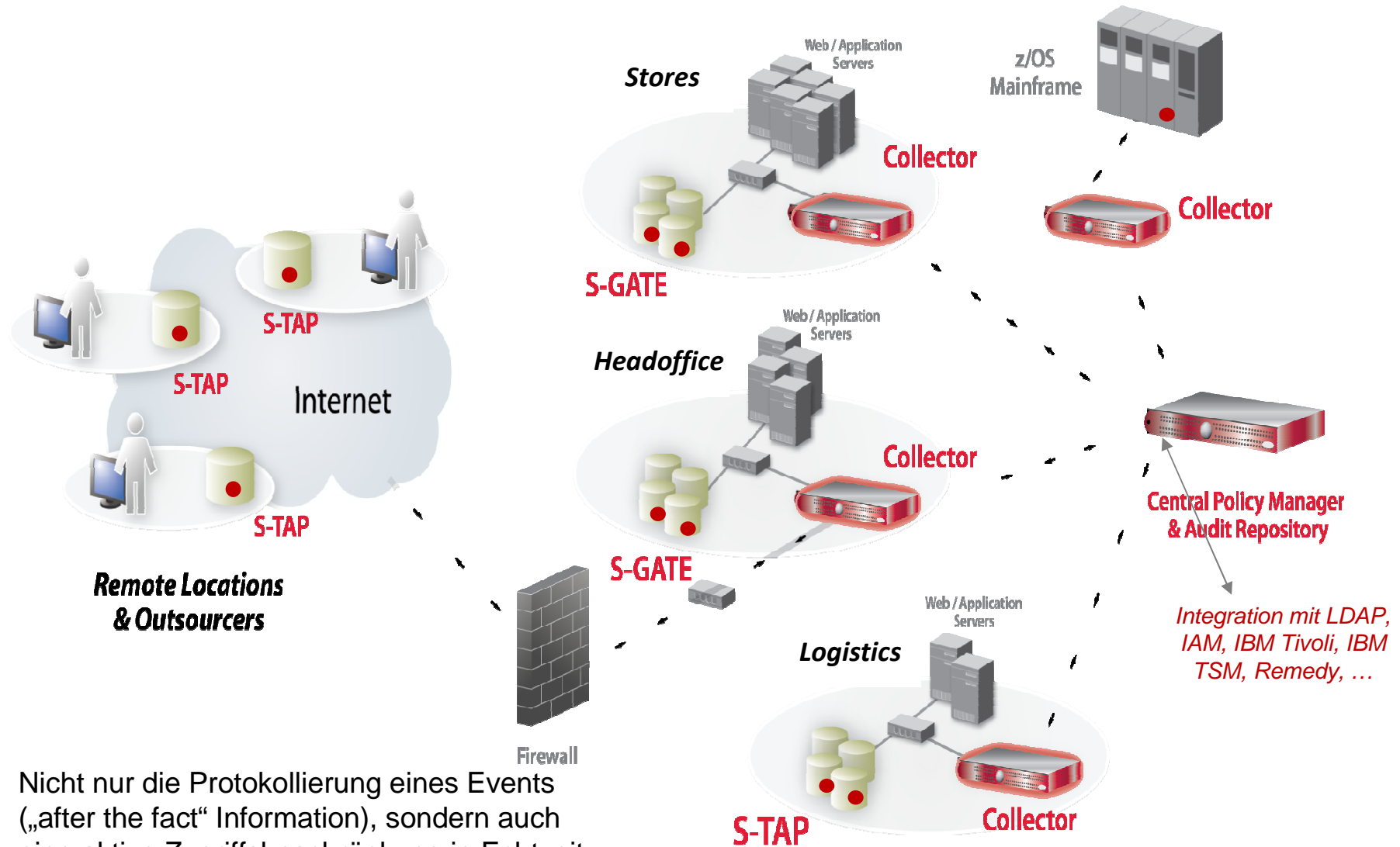
# Datenbanküberwachung in Echtzeit



- Nicht-invasive Architektur
  - Außerhalb der Datenbanken
  - Minimaler Einfluss auf Performance (2-3%)
  - Keine Änderungen der DBMS oder Anwendungen
- Unterstützung heterogener Systemlandschaften
- Zentralisiertes Auditing im Guardium Collector
- 100% Transparenz inkl. Zugriffe lokaler DBAs
- Realisiert Vier-Augen-Prinzip (Separation of duties)
- Verlässt sich nicht nur auf lokale DBMS logs, die von Angreifern gelöscht werden können
- Granulare Regeln & Echtzeit Auditing
  - *Wer, Was, Wann, Wie*
- Automatisiertes Compliance Reporting, sign-offs & Eskalationen (SOX, PCI, NIST, etc.)

©2012 IBM Corporation

# Skalierbare Multi-Tier Architektur



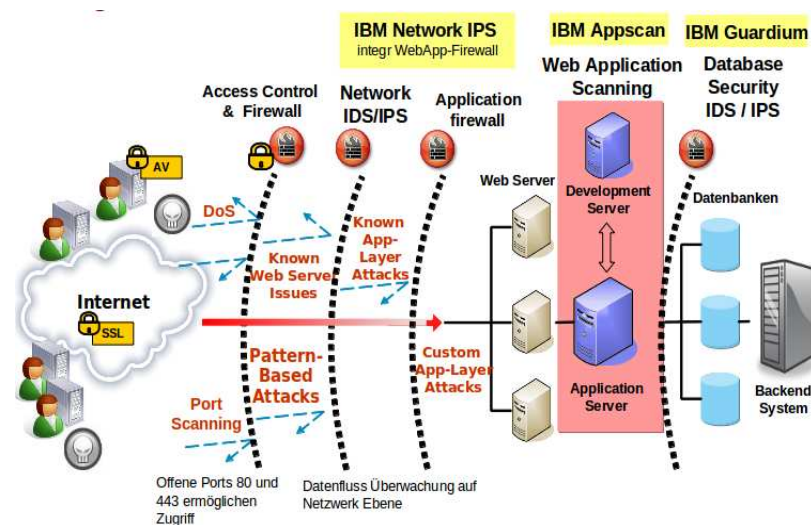
- Nicht nur die Protokollierung eines Events („after the fact“ Information), sondern auch eine aktive Zugriffsbeschränkung in Echtzeit





# IBM Security Systems

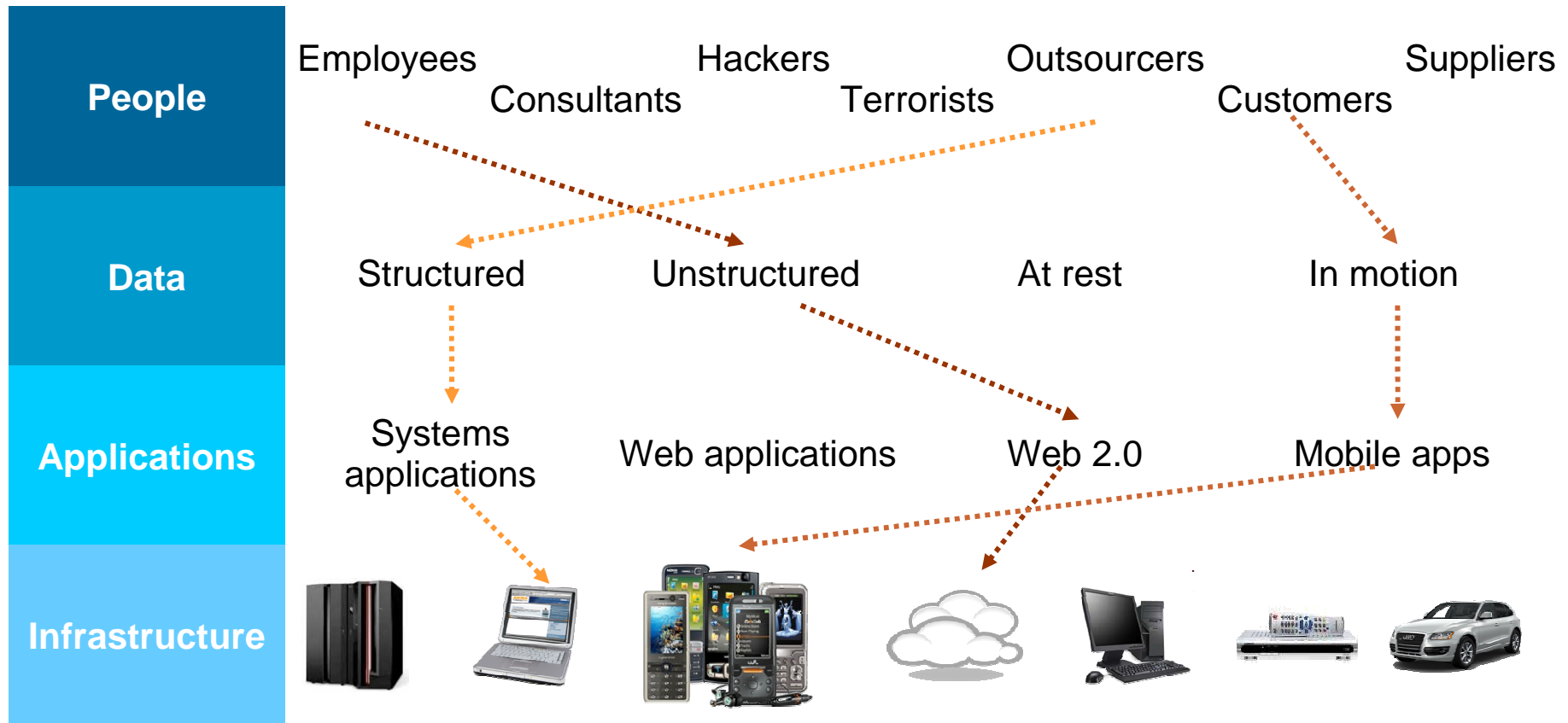
bietet Ihnen „end-to-end“ Information Security



IBM Software & Innovation Day 2012

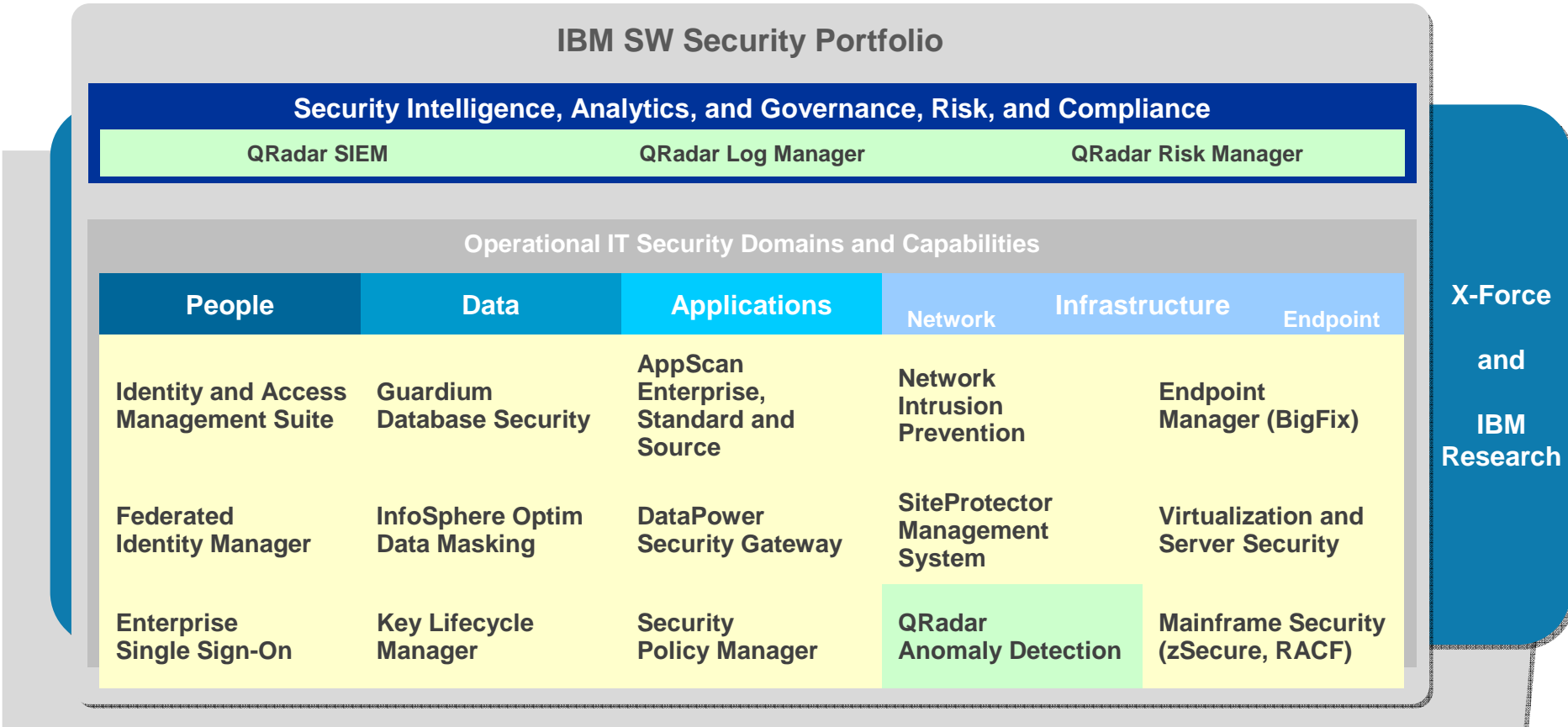
Smarte Software für Ihr Business

# IT Security umfasst 4 Dimensionen

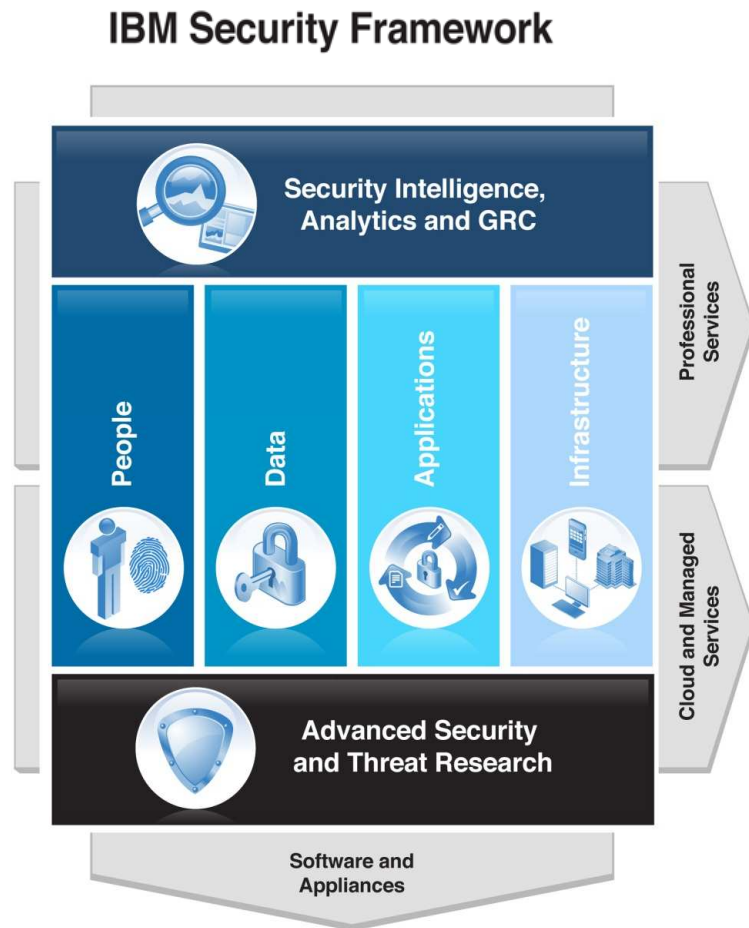


Es ist nicht mehr genug, die Grenze zu schützen –  
abgegrenzte punktuelle Produkte werden das Unternehmen nicht  
mehr ausreichend schützen

# Die 4 Säulen des IBM Security Software Portfolios



# IBM Security Systems

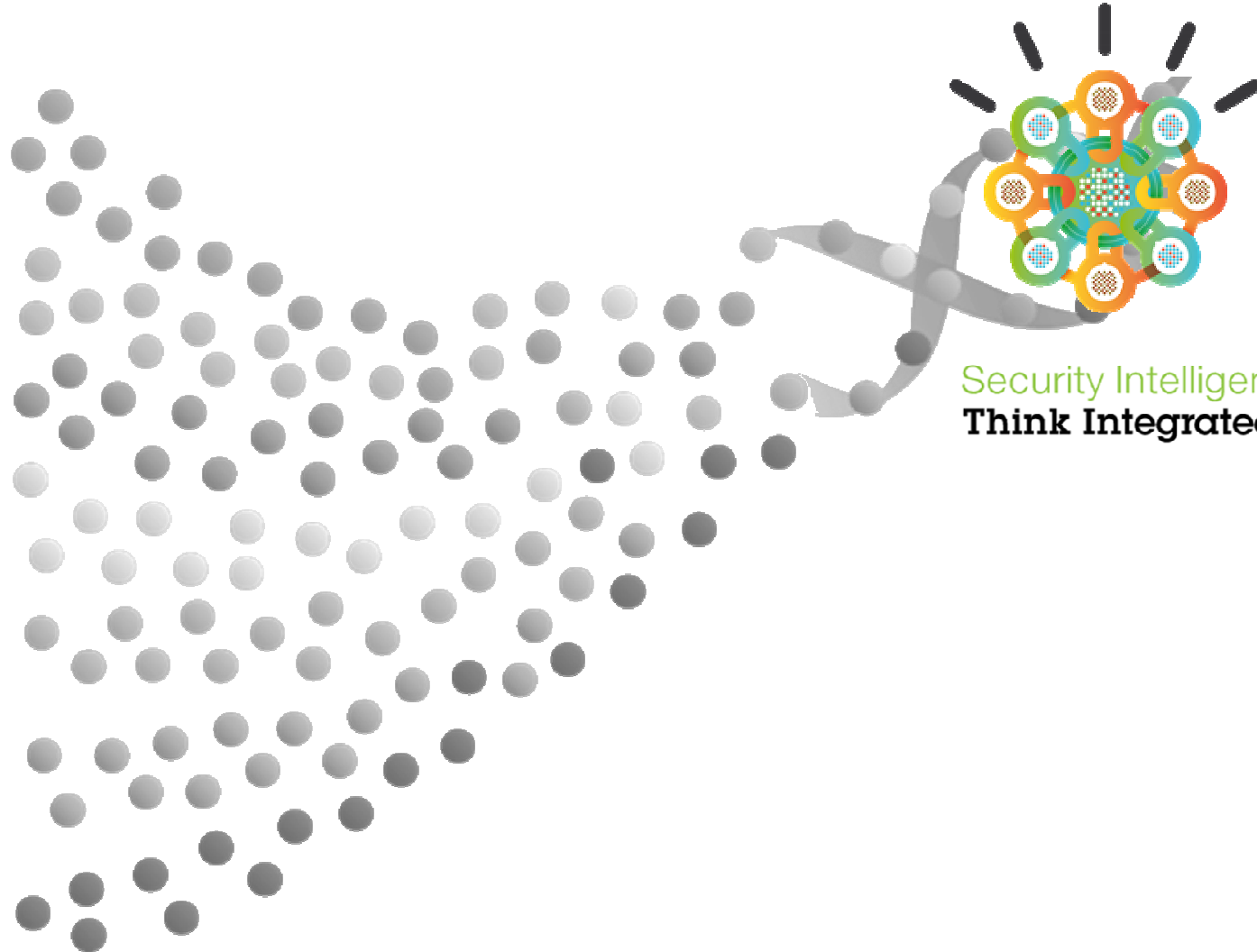
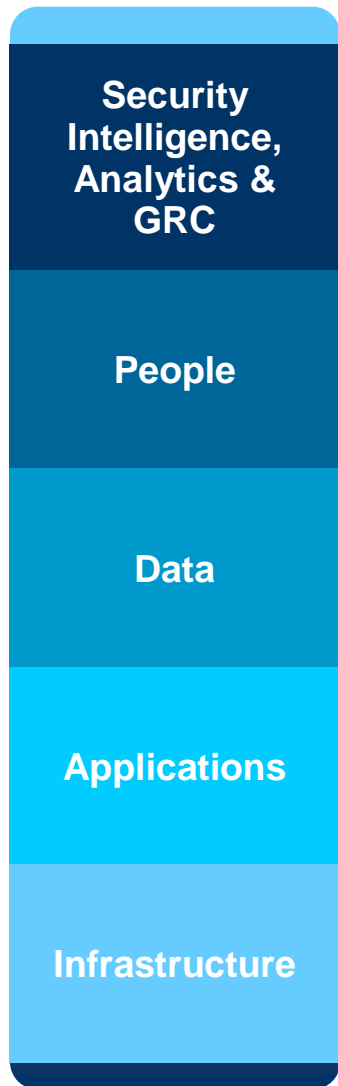


- IBM ist einziger Anbieter mit durchgängiger “end-to-end” Abdeckung aller IT-Security Themen
- > 6000 Security Ingenieure und Berater
- Mehrfach ausgezeichnete X-Force® Forschung
- Grösste Vulnerability Datenbank

Intelligence • Integration • Expertise

©2012 IBM Corporation

# Intelligente Lösungen bilden die DNA für die Sicherheit eines schlaueren, smarten Planeten



Security Intelligence.  
Think Integrated.

©2012 IBM Corporation

