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 ?


Können Sie ohne
Sicherheit
wirklich frei und
entspannt (über)leben?

Wie Sie die Sicherheitslücken Ihrer Web-Applikationen schließen

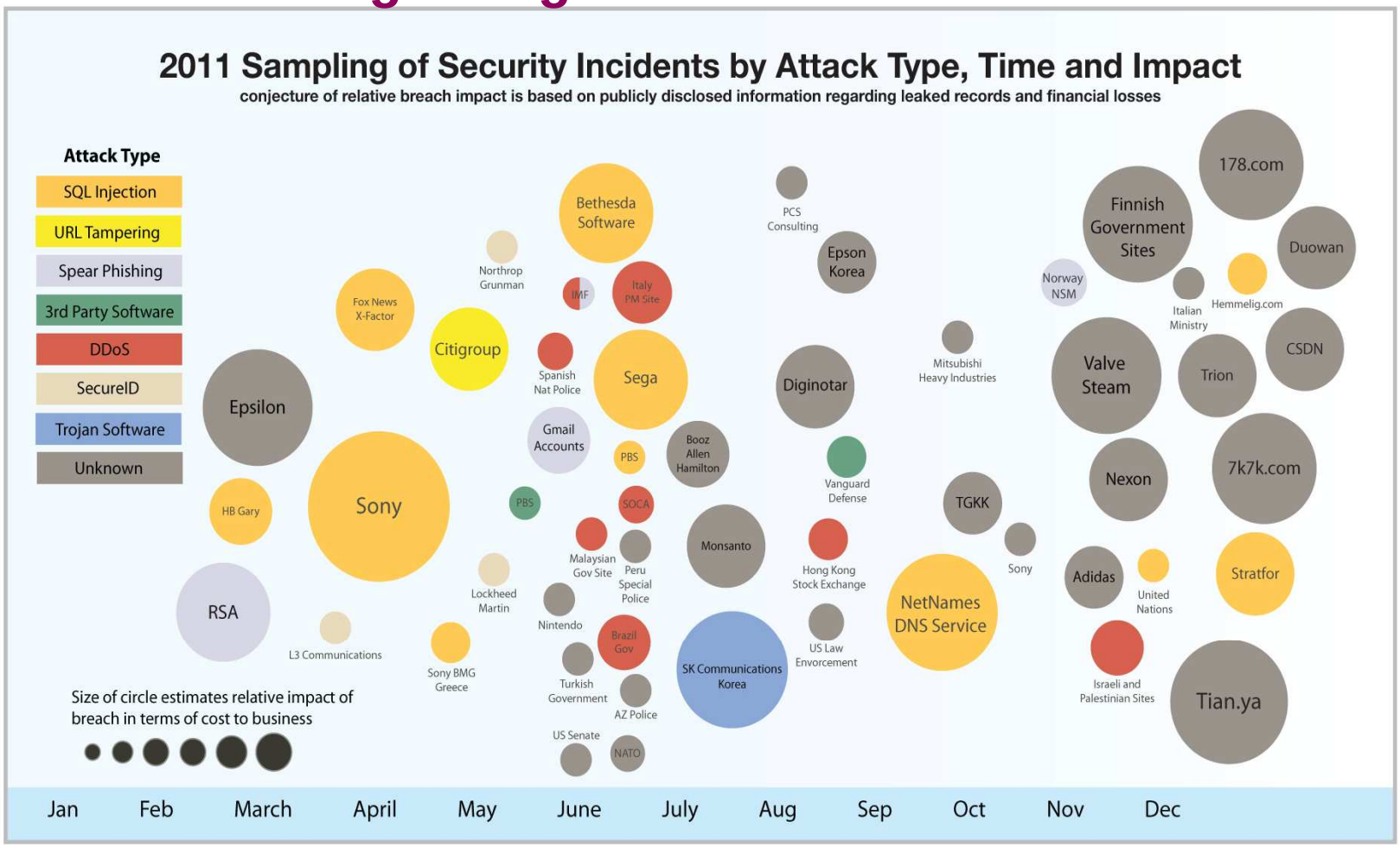
Rüdiger Gmach

IBM Security Systems Division, IBM Österreich

IBM Software & Innovation Day 2012

Smarte Software für Ihr Business

Zielgerichtete Angriffe erschüttern Firmen und Regierungen



Source: IBM X-Force® Research and Development

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

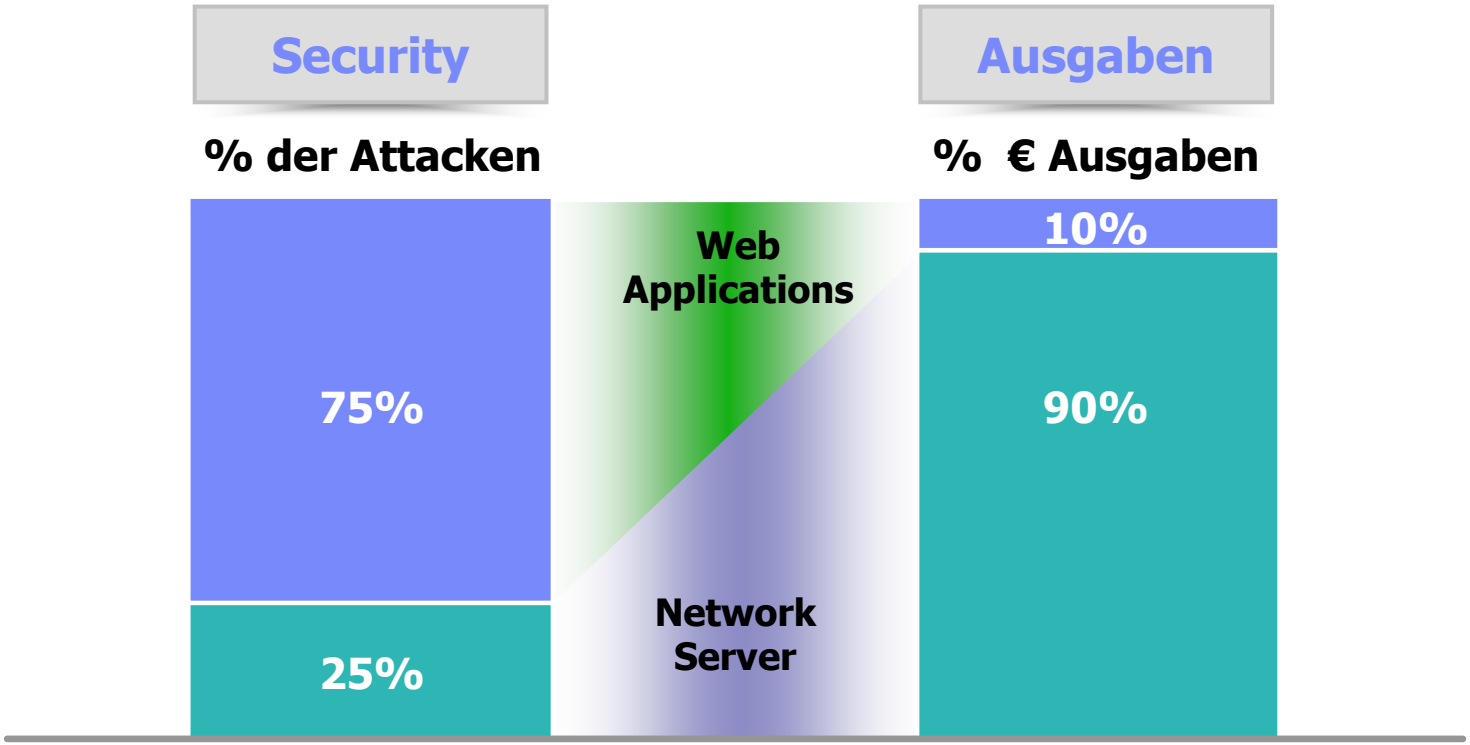
15-jähriger Hacker aus NÖ knackte 259 Firmen

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 ausnützbaren 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.***

Security

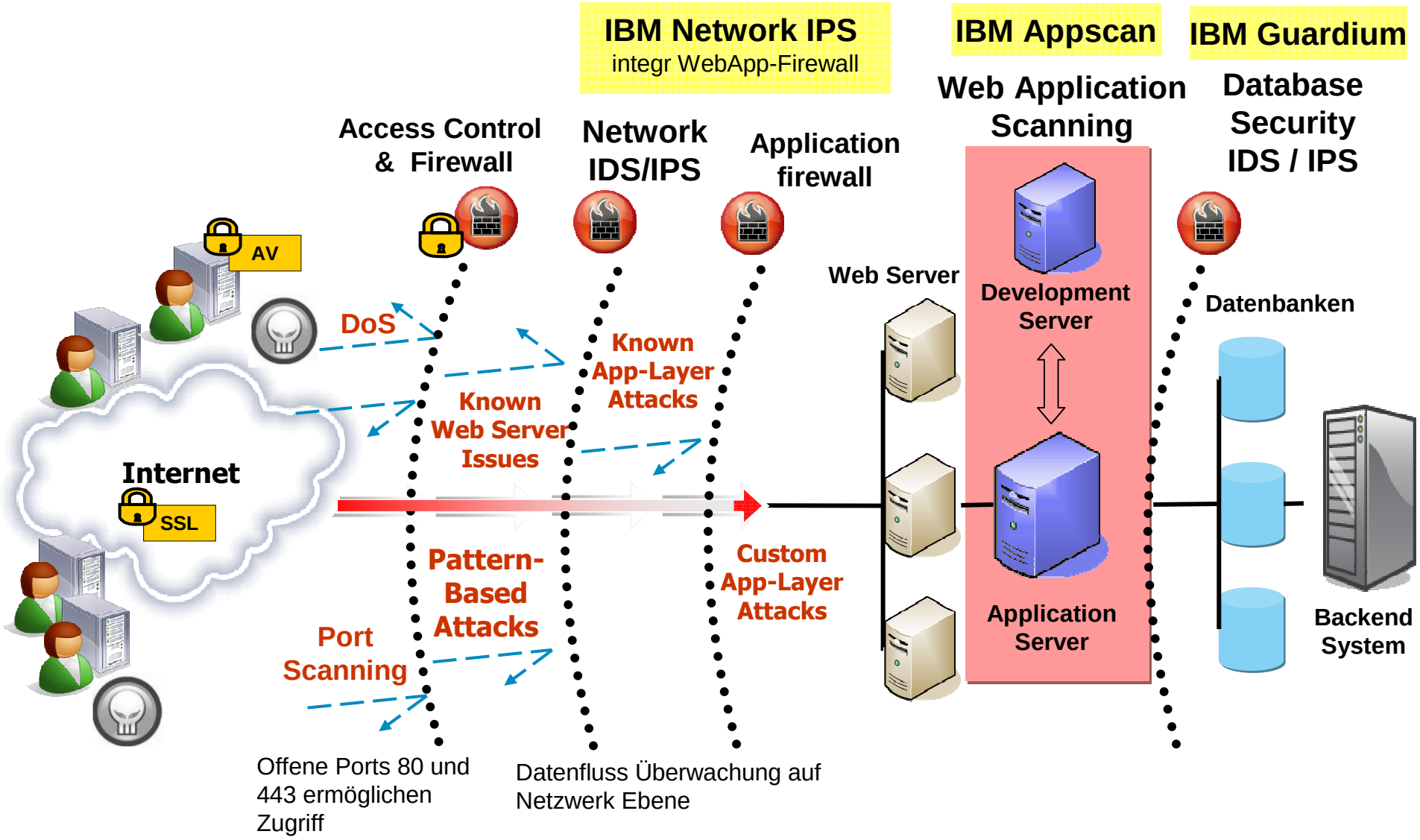
Die Herausforderung für Organisationen



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

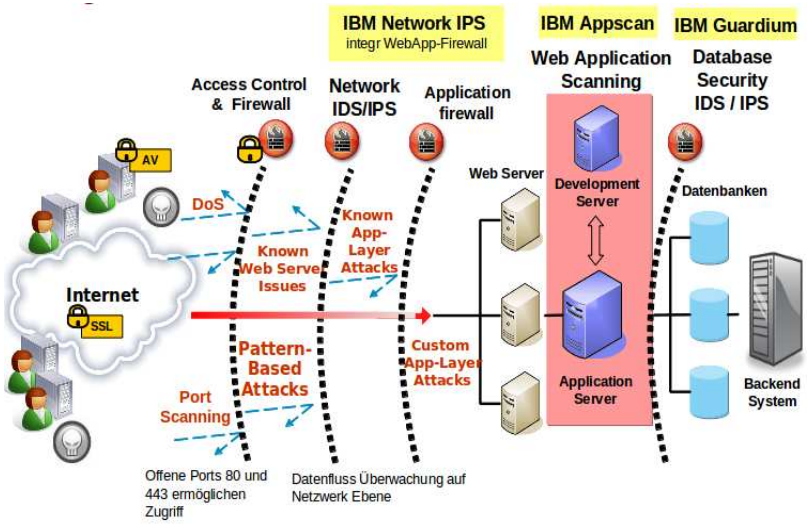
Sources: Gartner, Watchfire

Angriffsvektoren und Abwehr



IBM Security NIPS

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

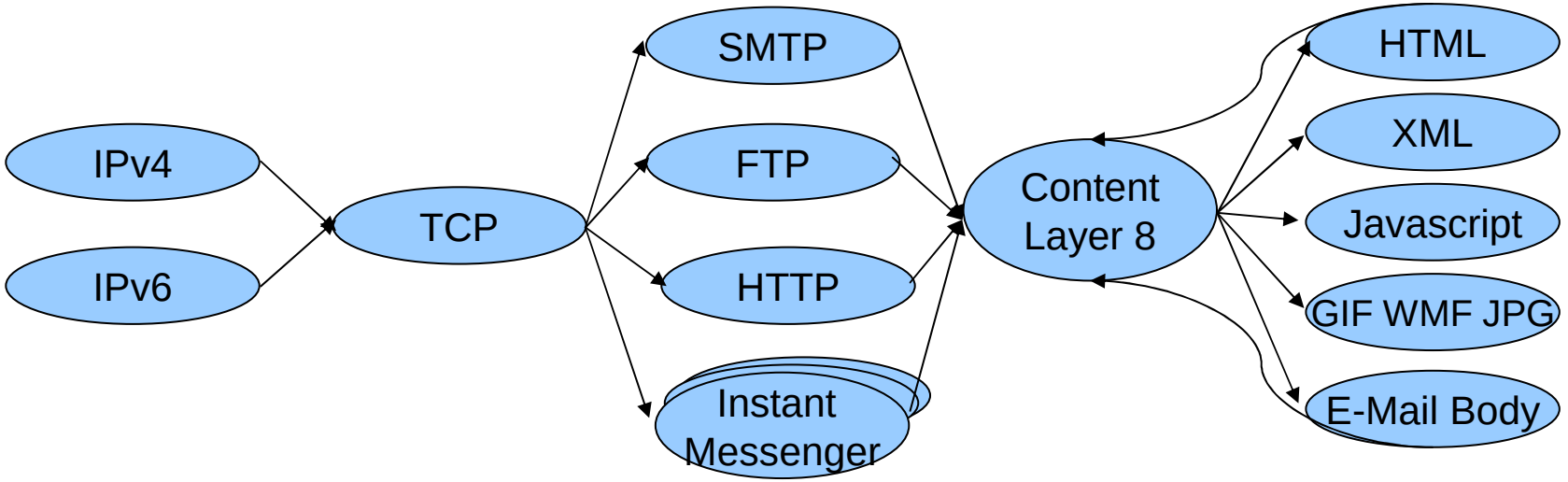


IBM Software & Innovation Day 2012

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

Security Effectiveness: Ahead of the Threat

Top 61 Vulnerabilities - 2009

341 Average days *Ahead of the Threat*

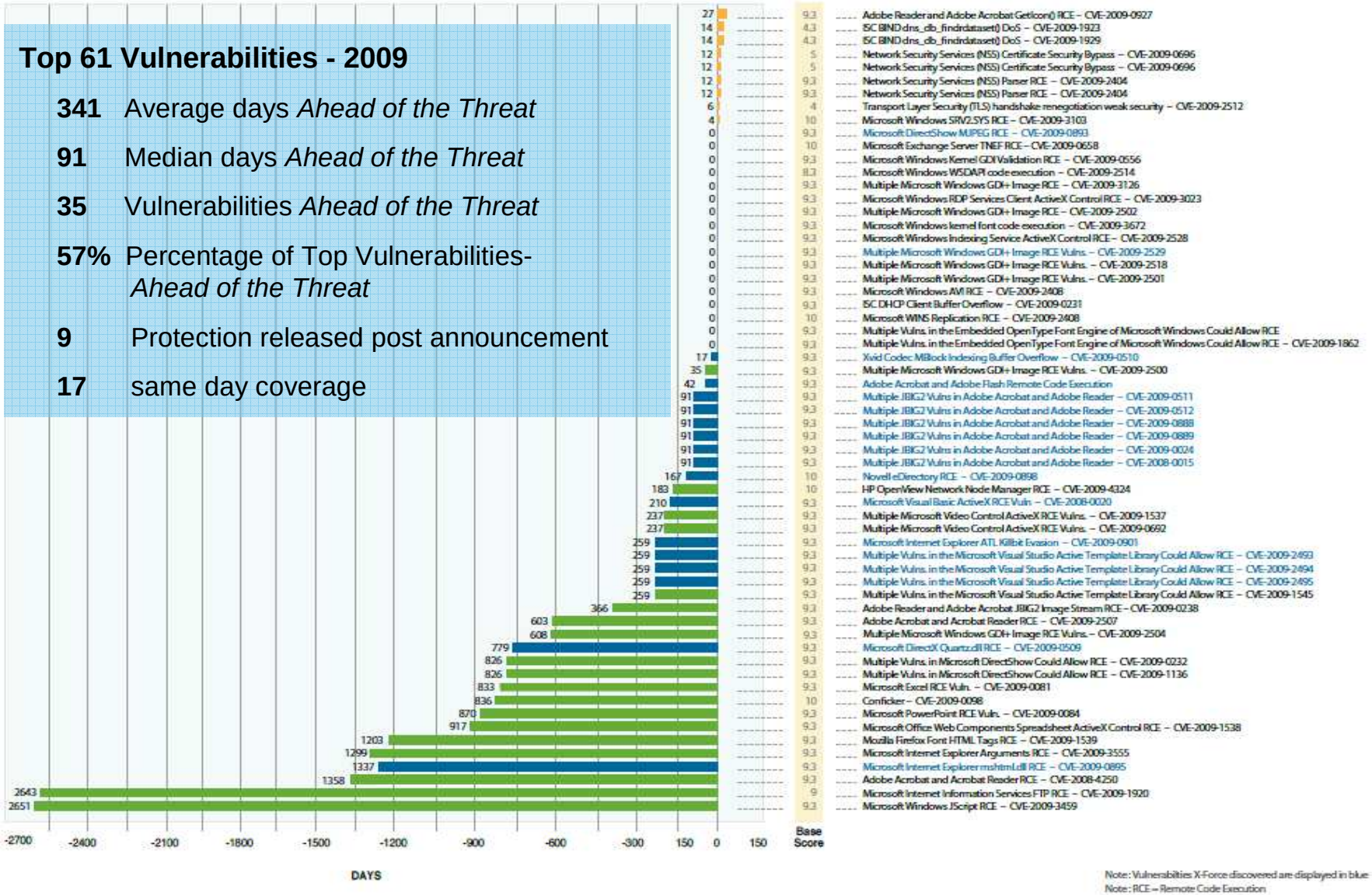
91 Median days *Ahead of the Threat*

35 Vulnerabilities *Ahead of the Threat*

57% Percentage of Top Vulnerabilities-*Ahead of the Threat*

9 Protection released post announcement

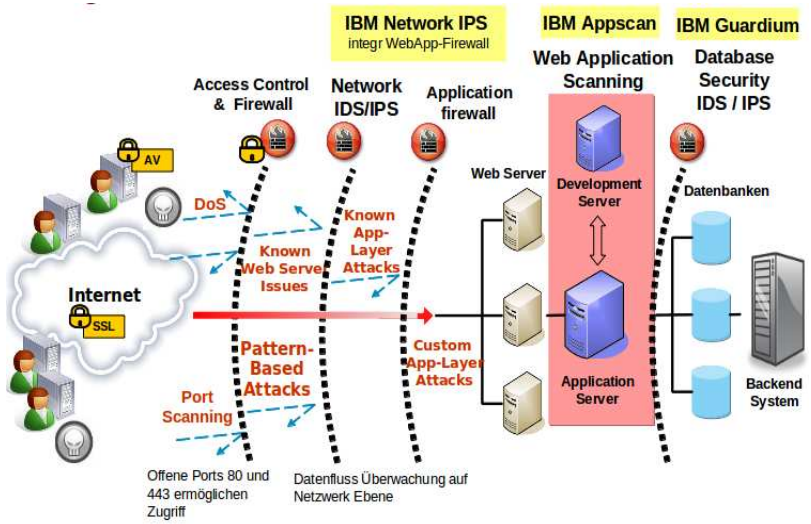
17 same day coverage



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



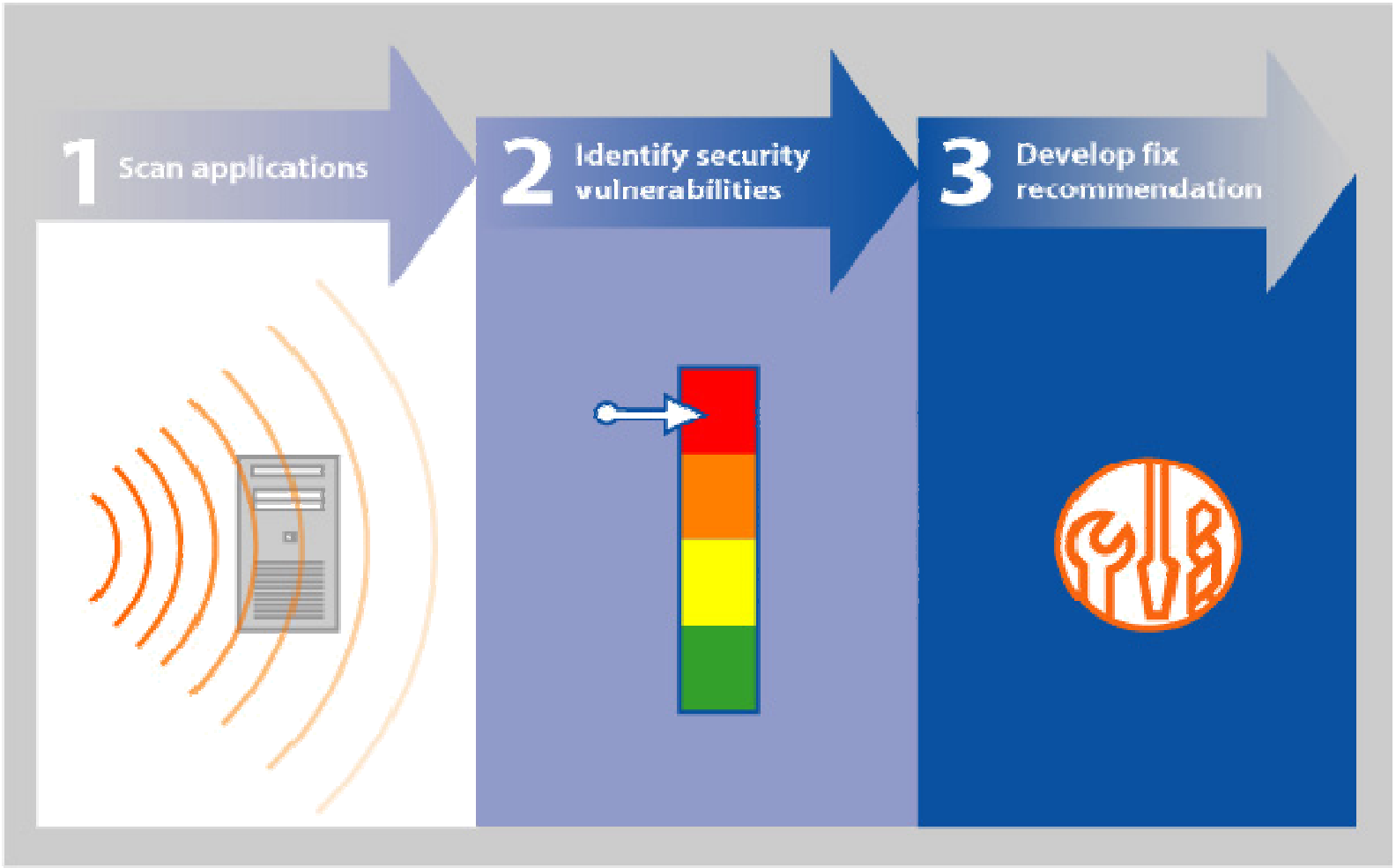
IBM Software & Innovation Day 2012

Smarte Software für Ihr Business

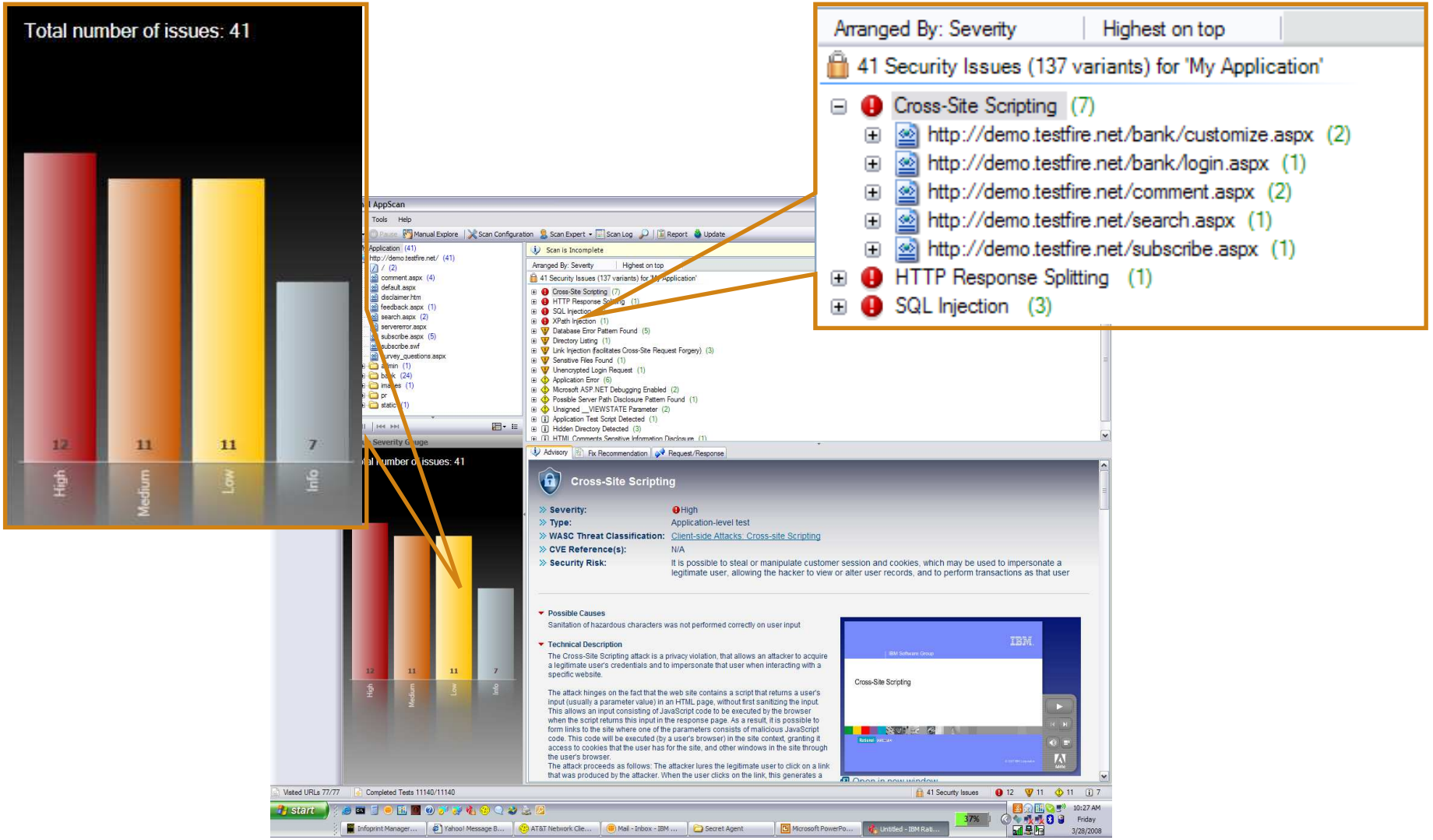
Pain Point: Web 2.0 Technologies

- 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

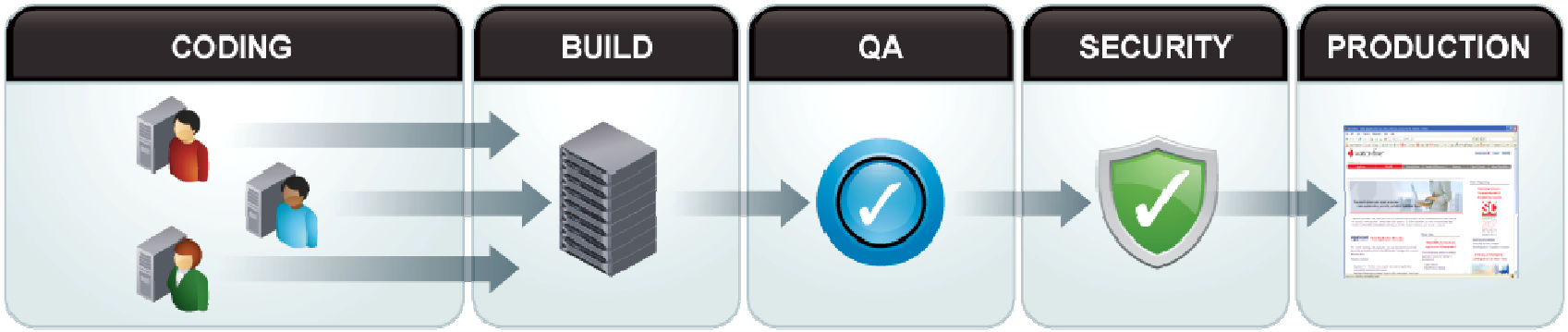
How Does IBM Rational AppScan Work?



Easy to Understand Results – Issues and Priorities



AppScan: advanced security testing collaboration & governance through application lifecycle



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

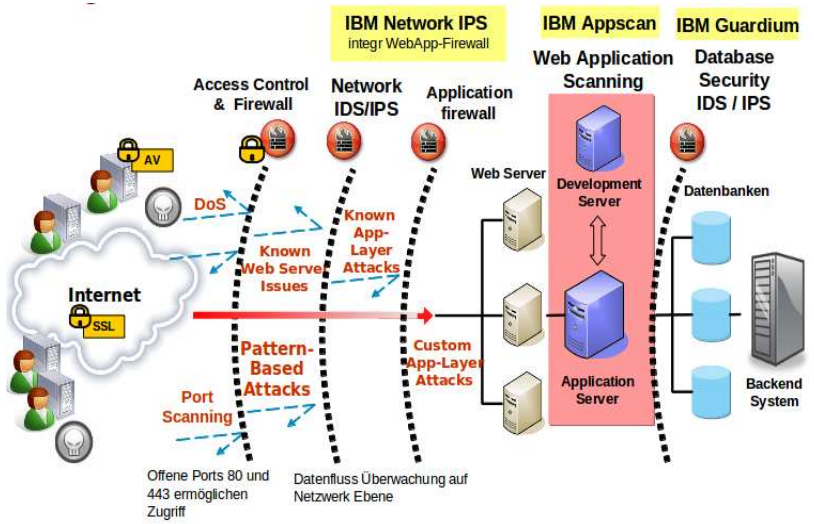
AppScan Standard

AppScan Enterprise

AppScan Source

IBM Guardium Database Security

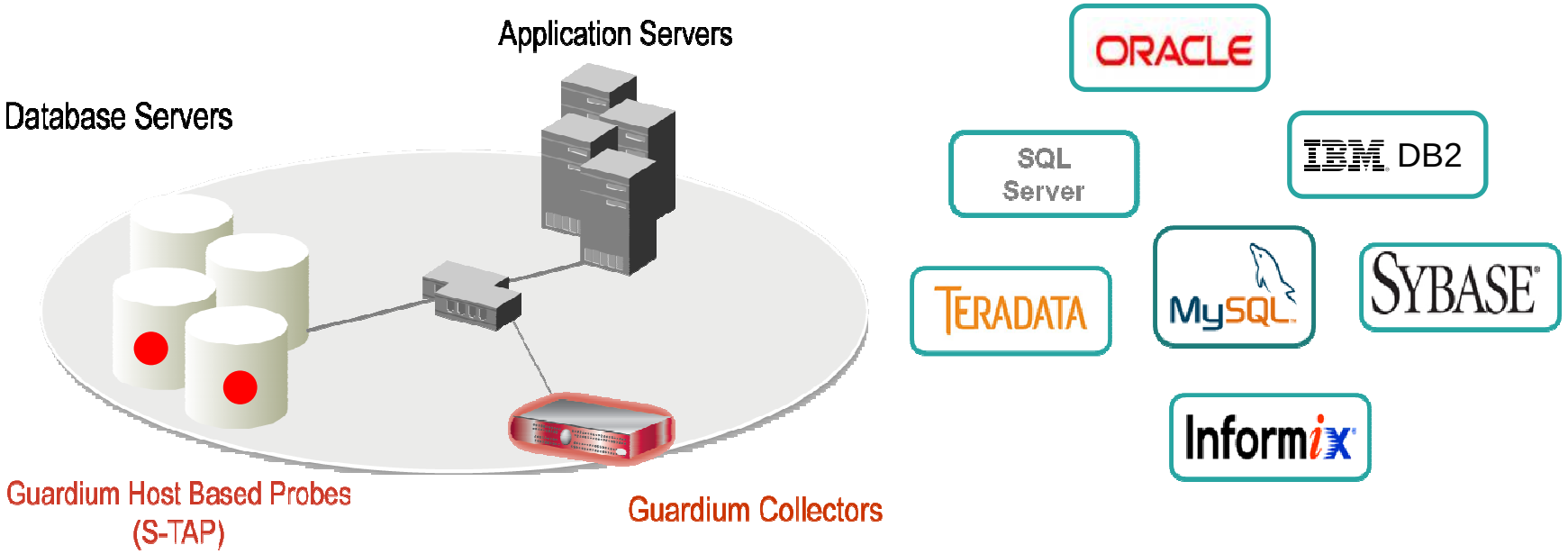
Die Appliance, die Ihre Datenbank effizient und sicher schützt



IBM Software & Innovation Day 2012

Smarte Software für Ihr Business

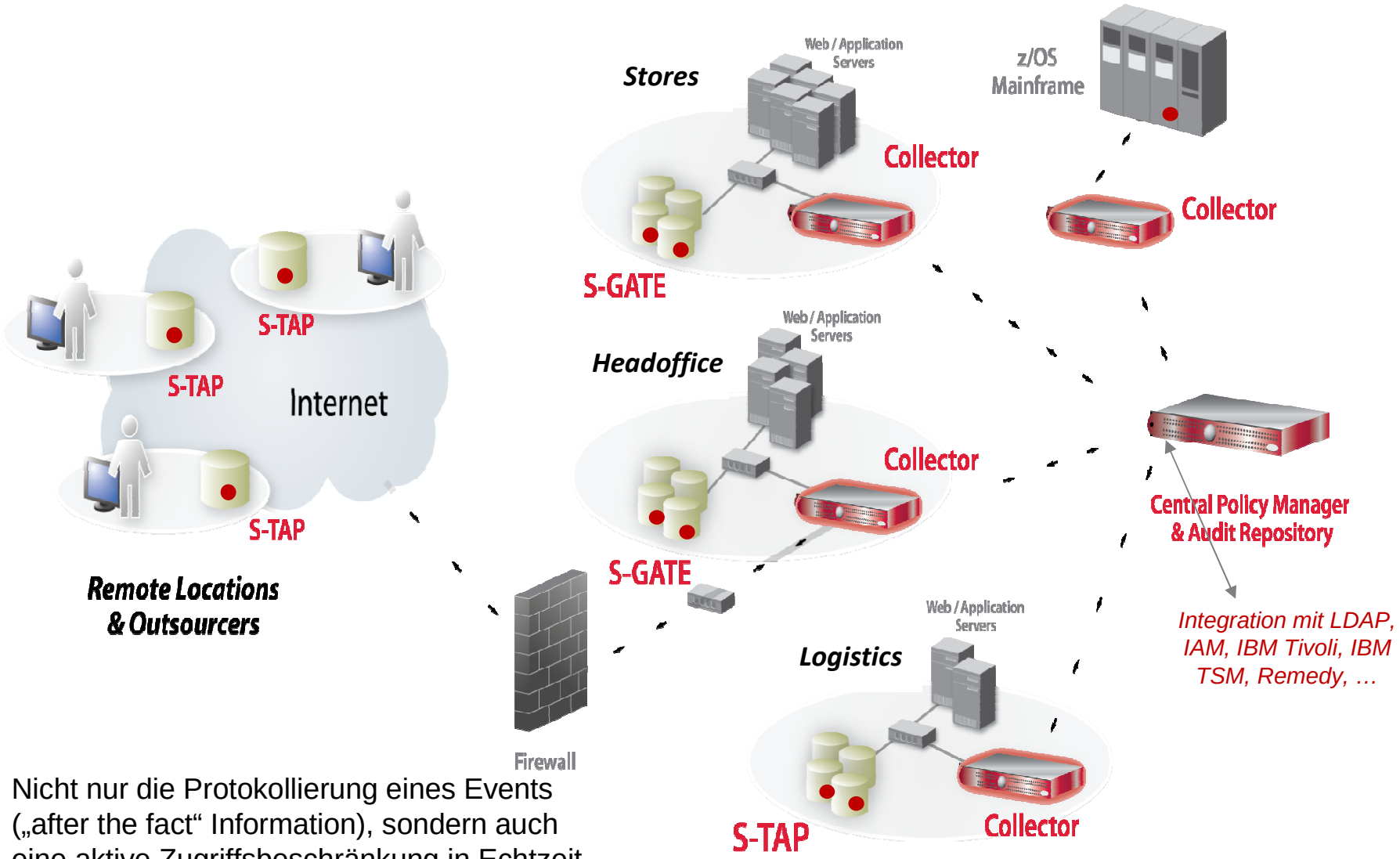
Datenbanküberwachung in Echtzeit



- 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.)

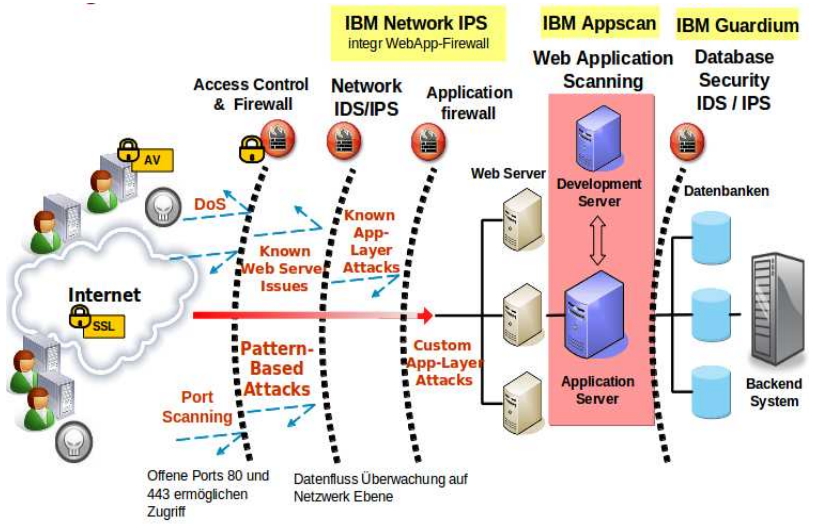
Skalierbare Multi-Tier Architektur



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

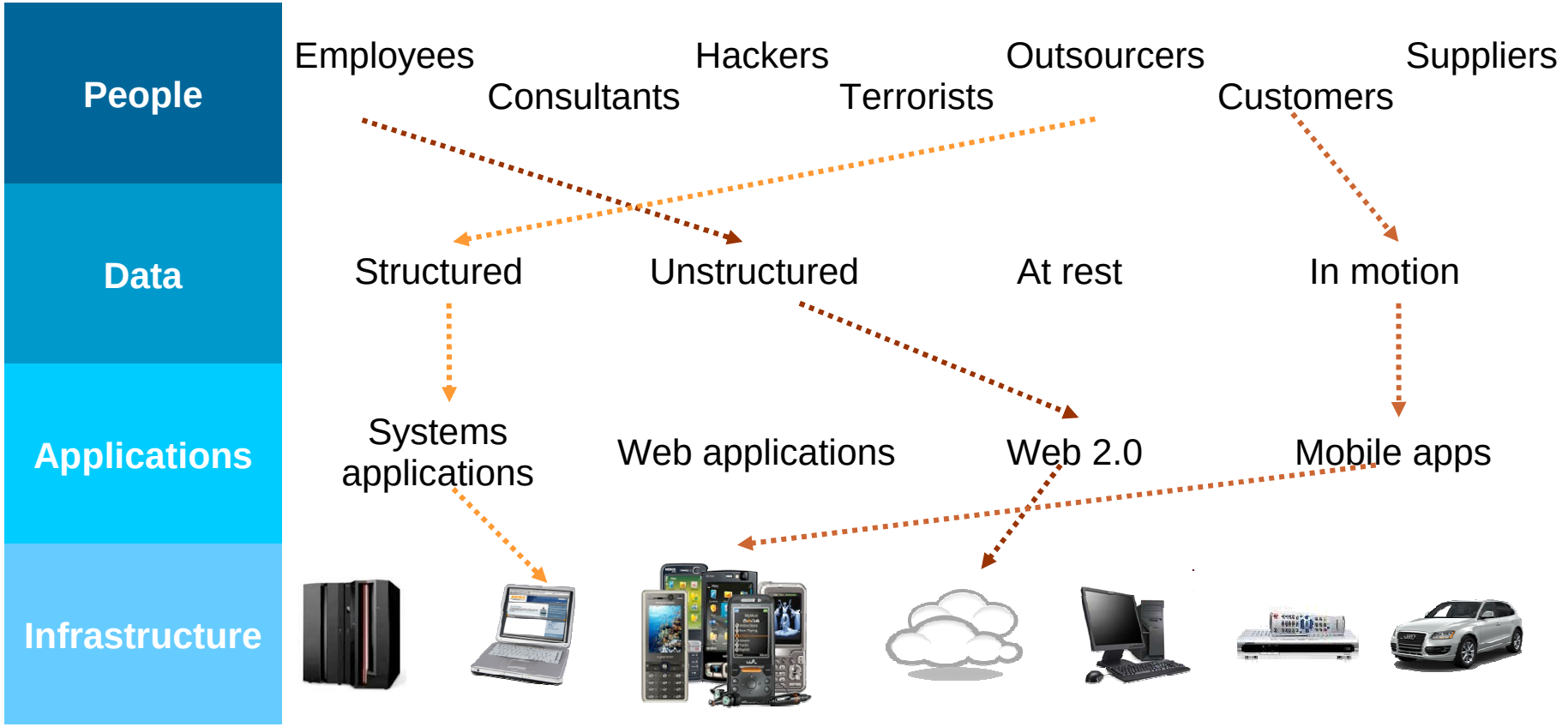
IBM Security Systems

bietet Ihnen „end-to-end“ Information Security



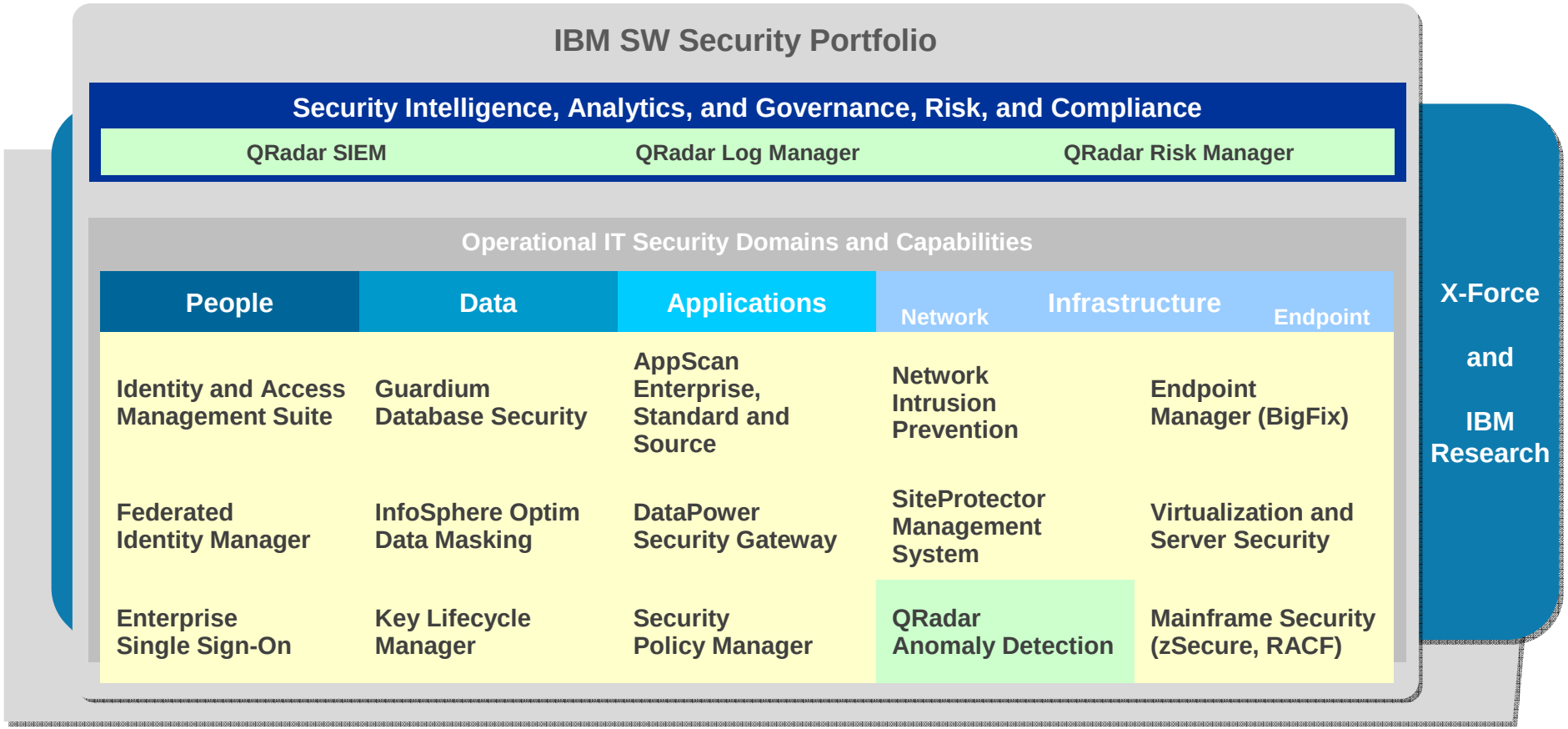
IBM**Software**&
InnovationDay**2012**
Smarte Software für Ihr Business

IT Security umfasst 4 Dimensionen

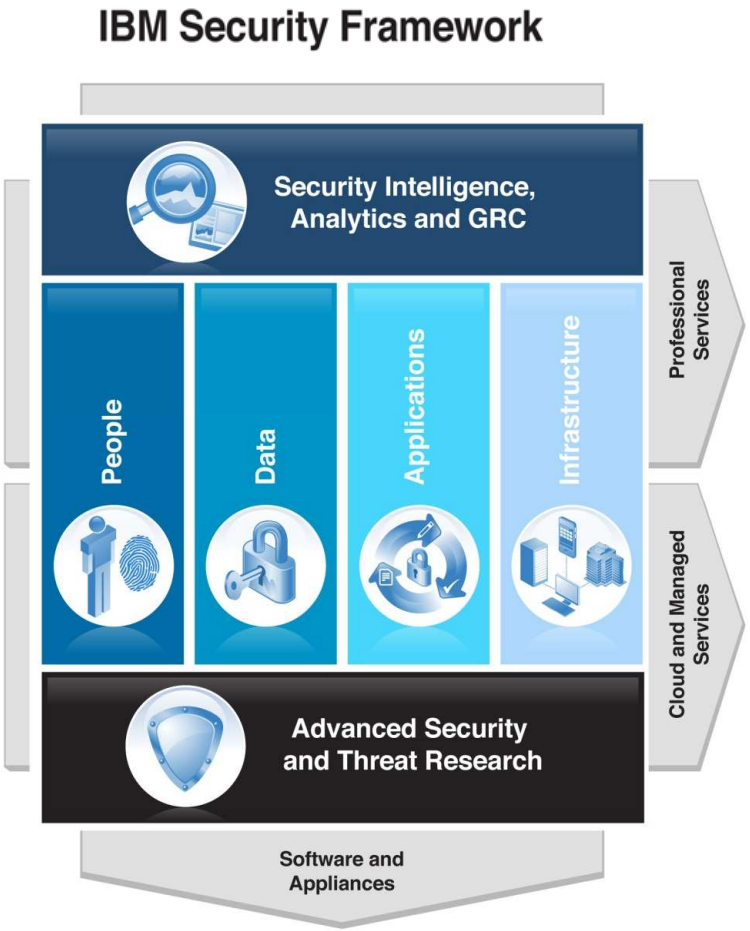


Es ist nicht mehr genug, die Grenze zu schützen – abgegrenzte punktuelle Produkte werden das Unternehmen nicht mehr ausreichend schützen

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

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