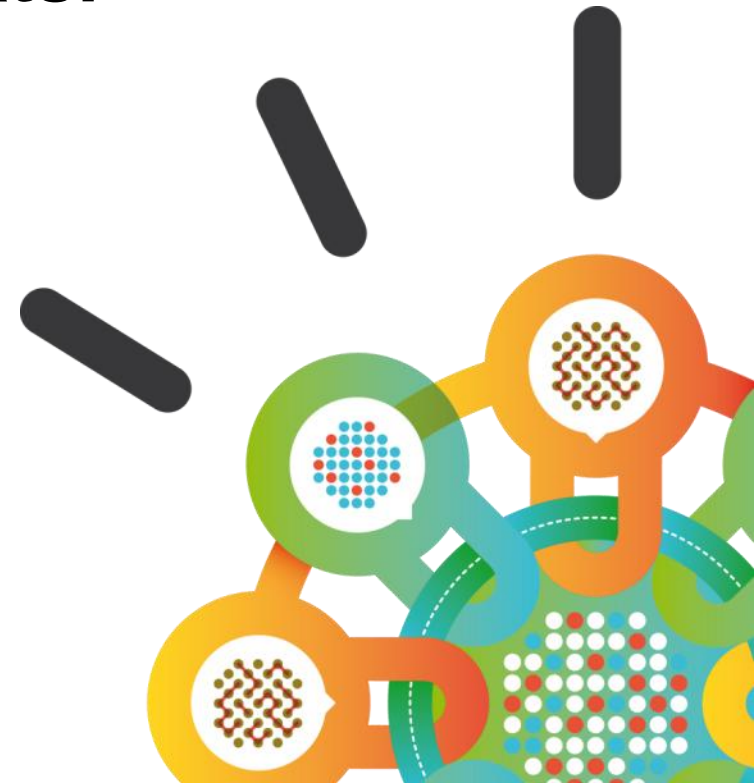


Security Intelligence.
Think Integrated.

Mobile, Cloud, Advanced Threats: A Unified Approach to Security

David Druker, Ph.D.
Senior Security Solution Architect
IBM



Business...

Security for Business

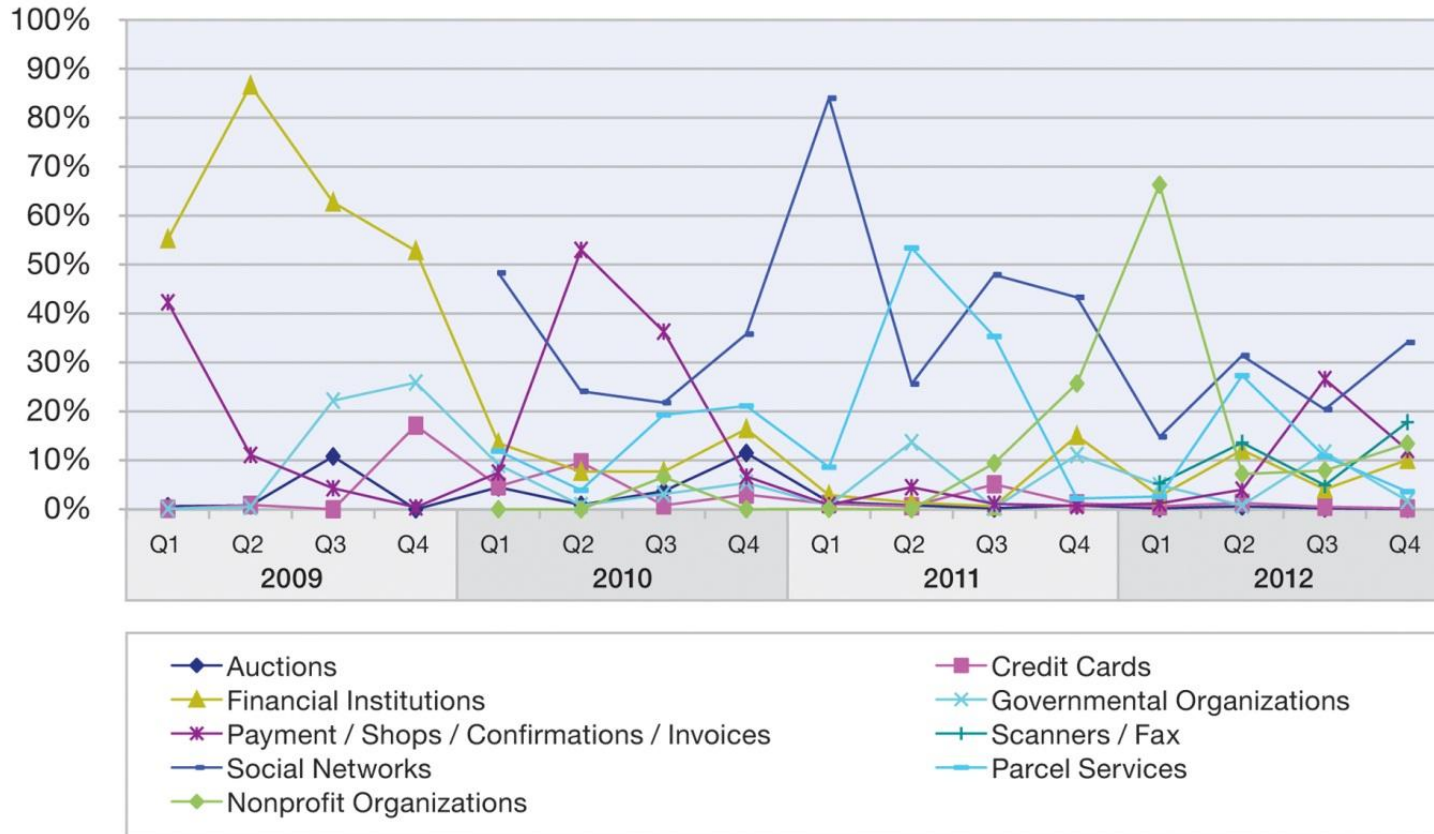
Common Business Functions

- Manufacturing or some other type of production
- Sales & distribution, both retail and through channels
- Marketing
- Management and administration
- Finance, accounting and legal
- Human Resources
- Information Technology (IT)

How Much Security?

Scam/Phishing Targets by Industry

2009 to 2012

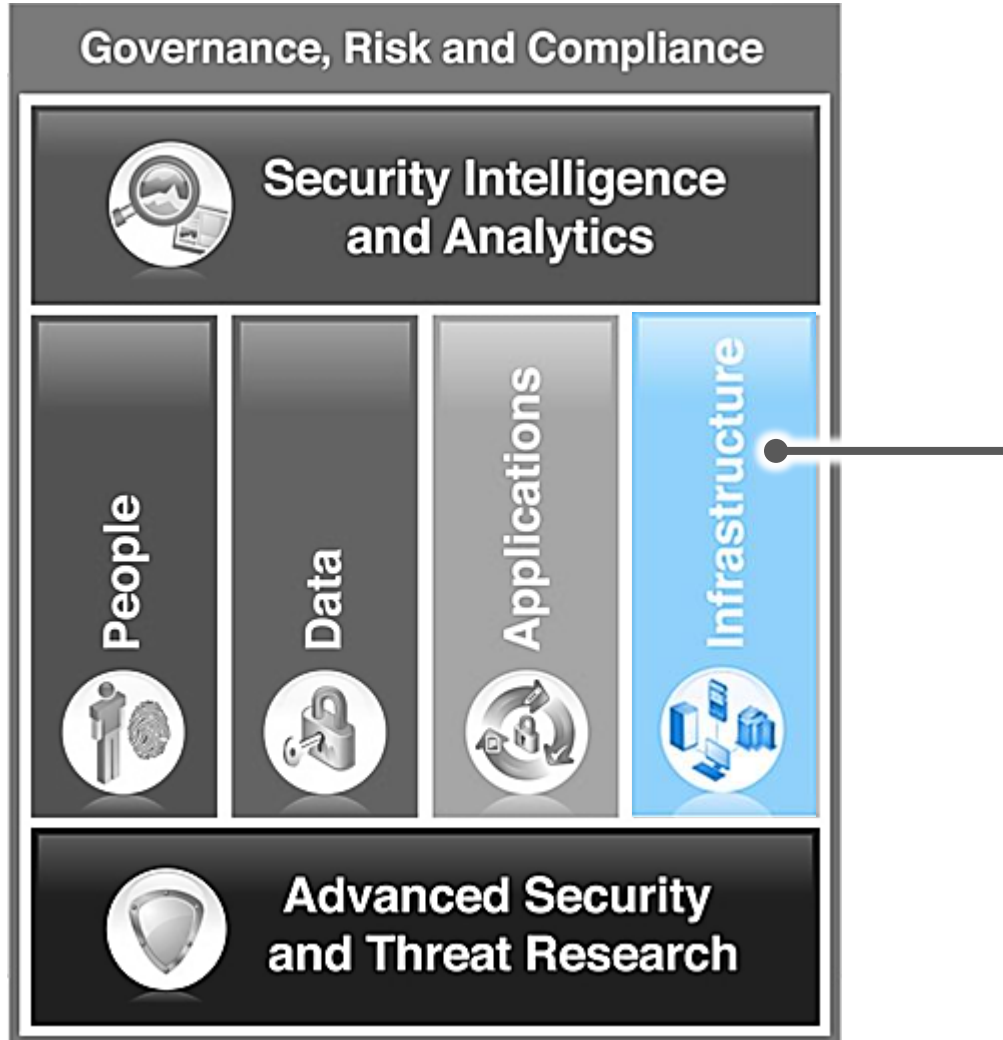


Source: IBM X-Force® Research and Development

IBM Security Framework



Infrastructure



Description

- Network
- Servers
- Endpoints (clients)

Security

- Load balancing
- Firewall
- Intrusion Prevention
 - Network
 - Endpoints
- Endpoint management

People



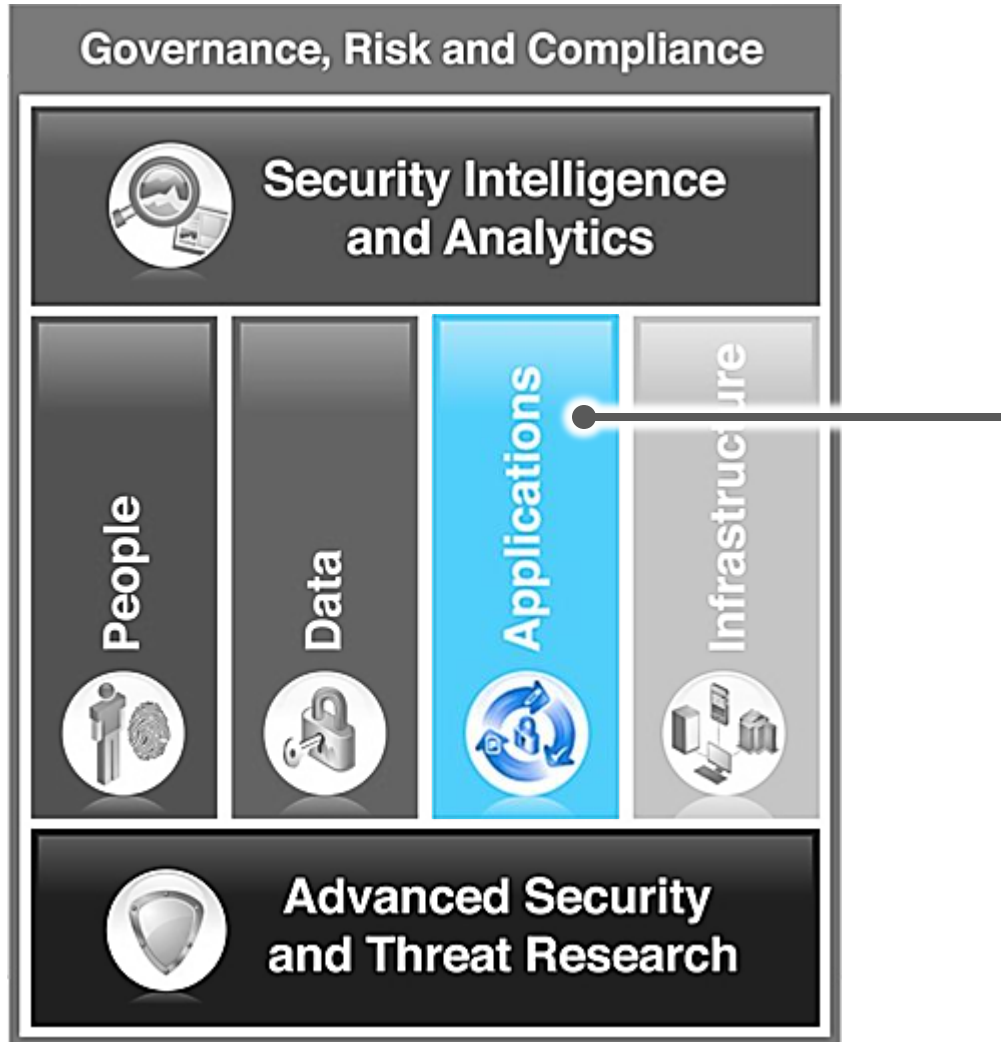
Description

- Employees
- Contractors & partners
- Customers
- Customers of partners

Security

- Identity management
 - Role management
 - User provisioning
 - Privileged identity management
 - Governance
 - Entitlements
- AAA
 - Authentication
 - Authorization
 - Auditing
- Identity federation
- Single sign-on

Applications



Description

- System apps
- Traditional Web apps
- Web 2.0 apps

Security

- Discovery
- Scanning & pentesting
 - Static
 - Dynamic
- Vulnerability analysis
- Runtime enforcement of entitlements

Data



Description

- SQL databases
- Non-relational databases
- Big data stores
- Unstructured data

Security

- Discovery
- Data classification
- Vulnerability analysis
- Activity monitoring
- Data masking
- Encryption management

Security Intelligence and Analytics



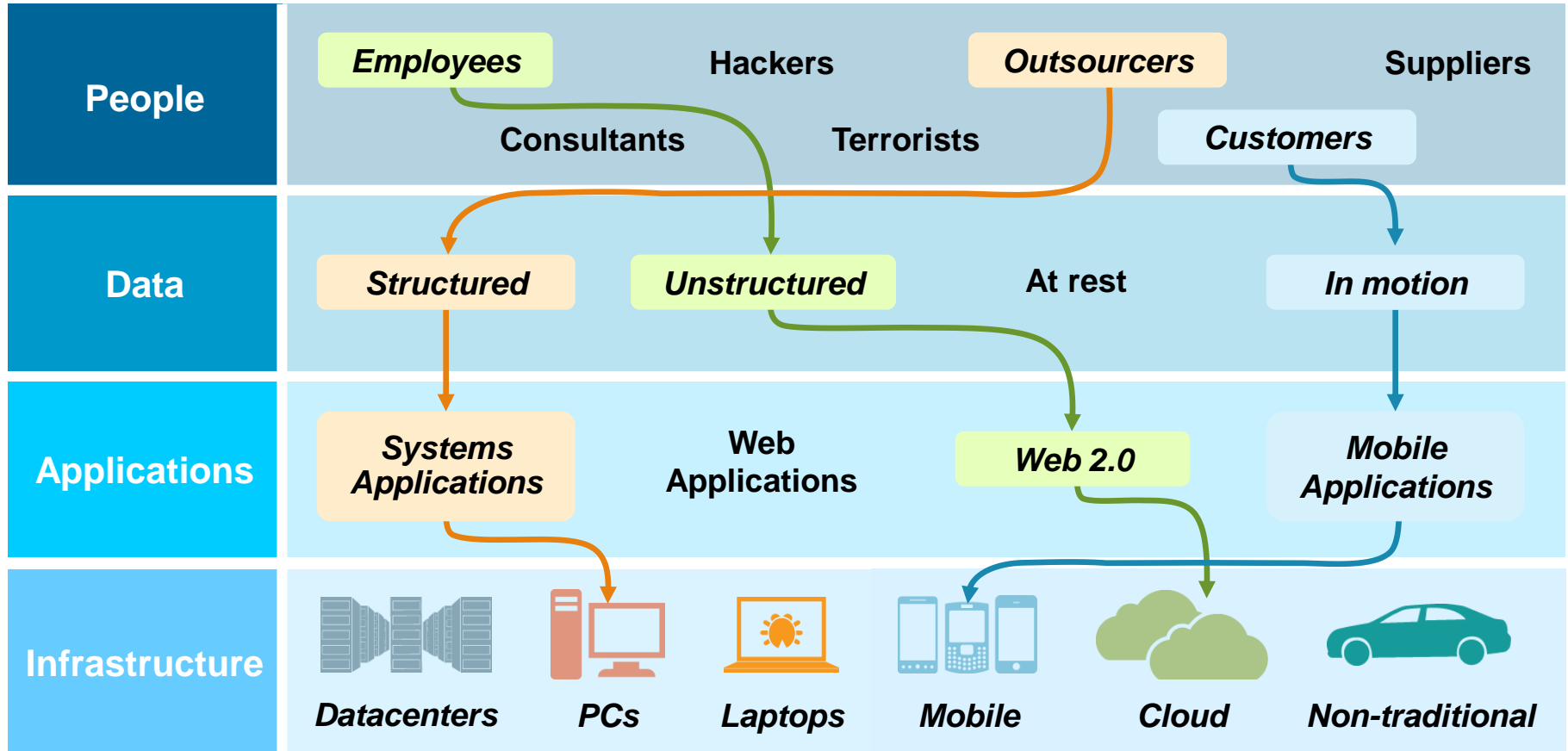
Description

- Information & insight from all security data
- Mathematical analyses of all relevant data

Security

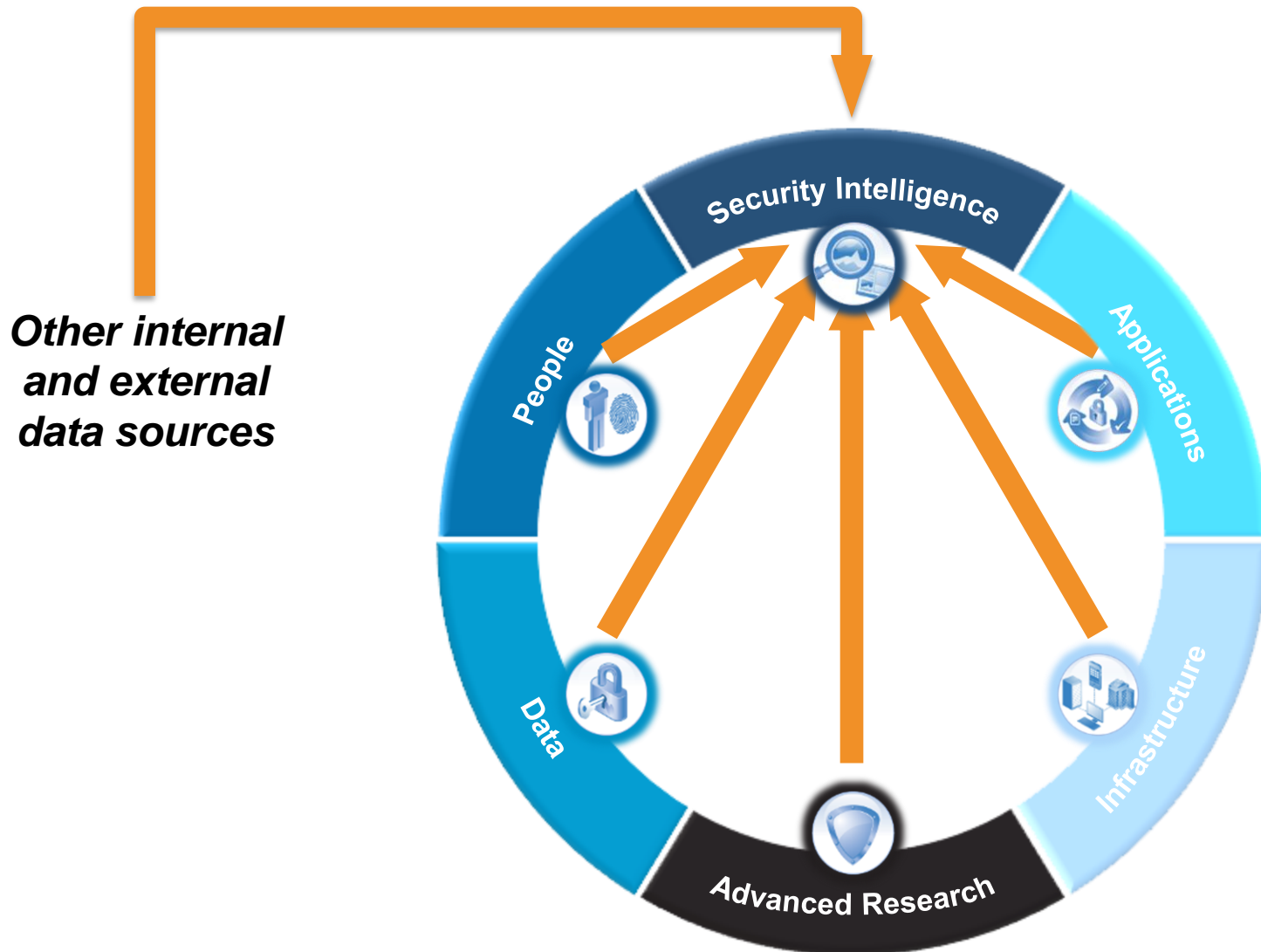
- Security Information and Event Management
- Network flow analysis
- Vulnerability scanning
- Event correlation
- Attack identification
- Anomaly Detection

Interrelated Technology Domains & Unpredictable Attack Paths

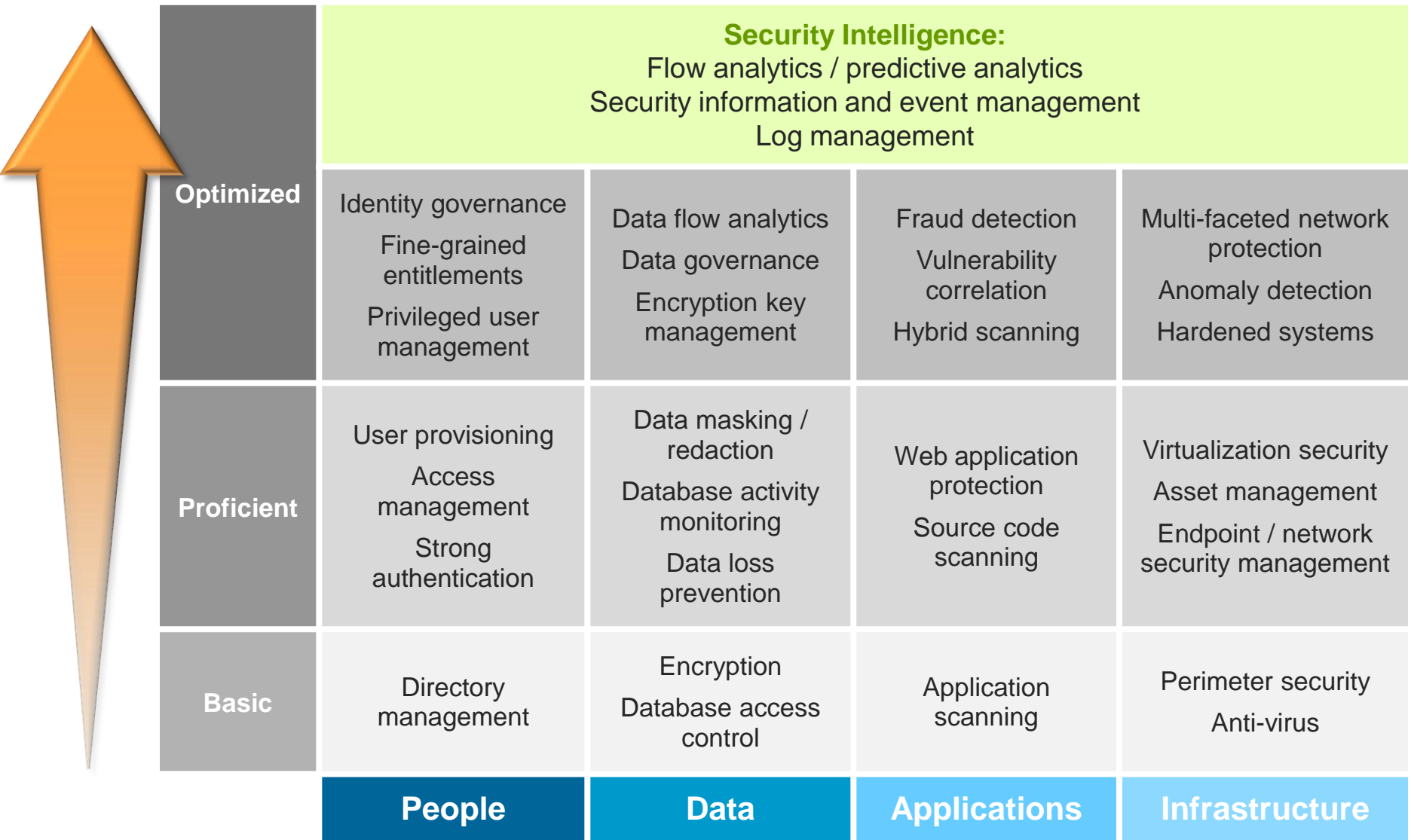


...require *unified security* approaches.

Unified (Integrated) Security



How Much Security: Security Maturity Model



Trends Driving Security Innovation

Advanced Threats

Sophisticated, targeted attacks designed to gain continuous access to critical information are increasing in severity and occurrence



*Advanced Persistent Threats
Stealth Bots Targeted Attacks
Designer Malware Zero-days*

Mobile Computing

Securing employee-owned devices and connectivity to corporate applications are top of mind as CIOs broaden support for mobility



Enterprise Customers

Cloud Computing

Cloud security is a key concern as customers rethink how IT resources are designed, deployed and consumed



Regulation and Compliance

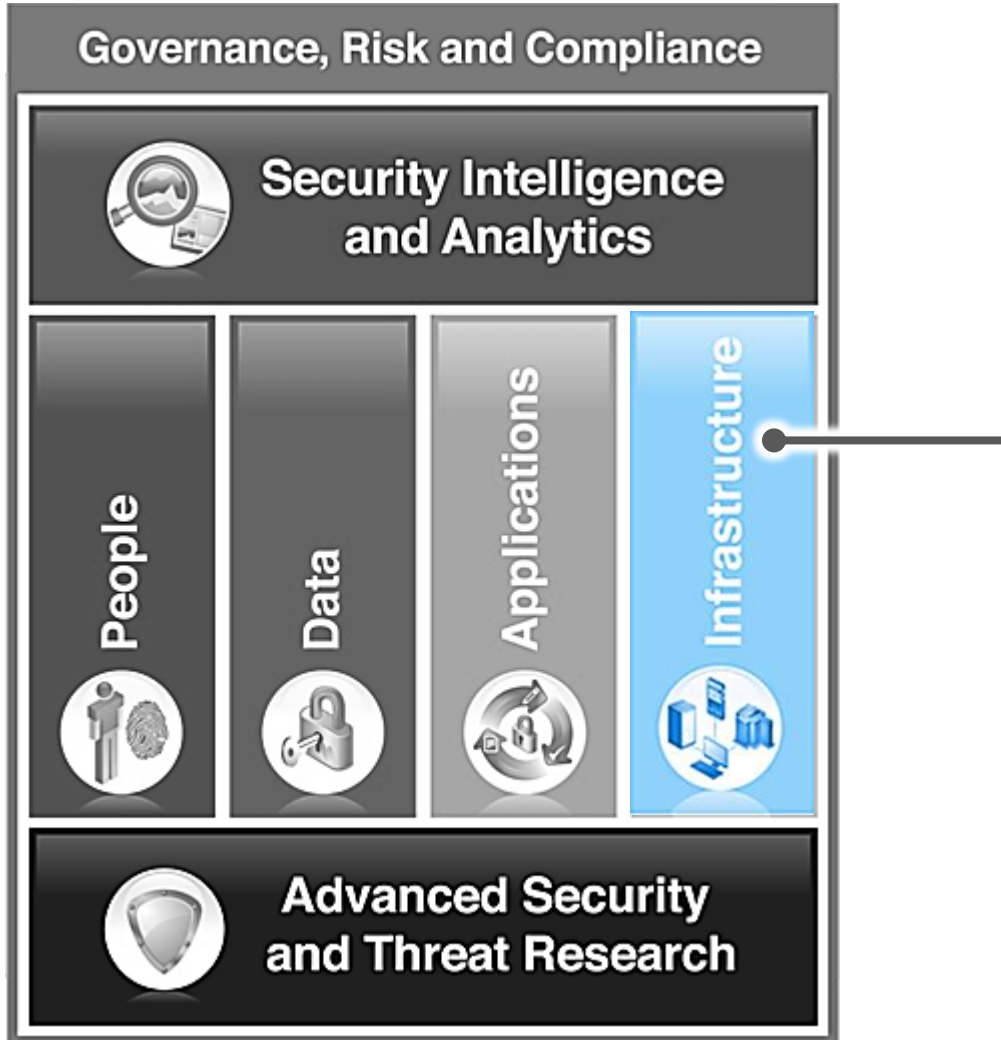
Regulatory and compliance pressures are mounting as companies store more data and can become susceptible to audit failures



Cloud Computing & Mobile Devices

New Requirements?

Infrastructure with Cloud and Mobile



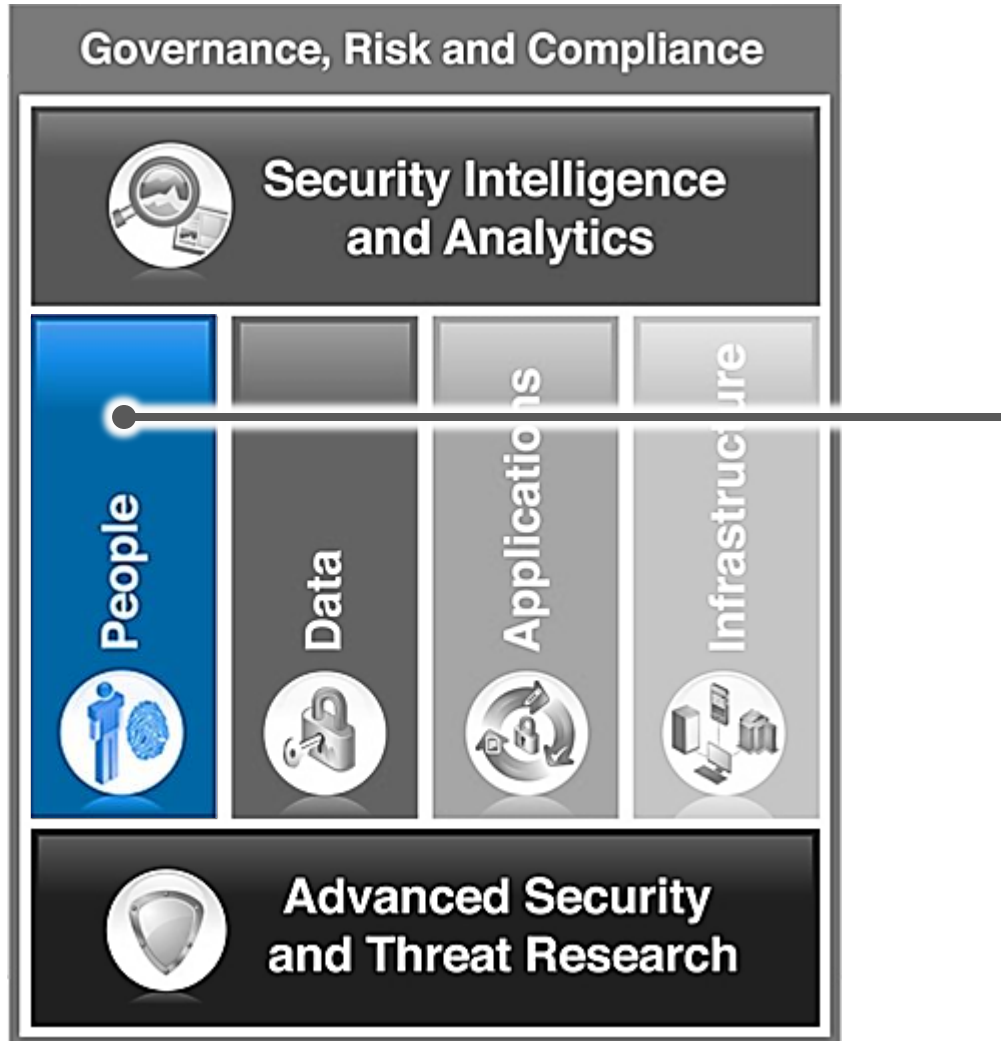
Description

- Network
- Servers
- Endpoints (clients)
- **Cloud**
- **Mobile devices**

Security

- Load balancing
- Firewall
- Intrusion Prevention
 - Network
 - Endpoints
- Endpoint management
- **Hypervisor protection**
- **Mobile connection security**
- **Mobile device management**

People with Cloud and Mobile



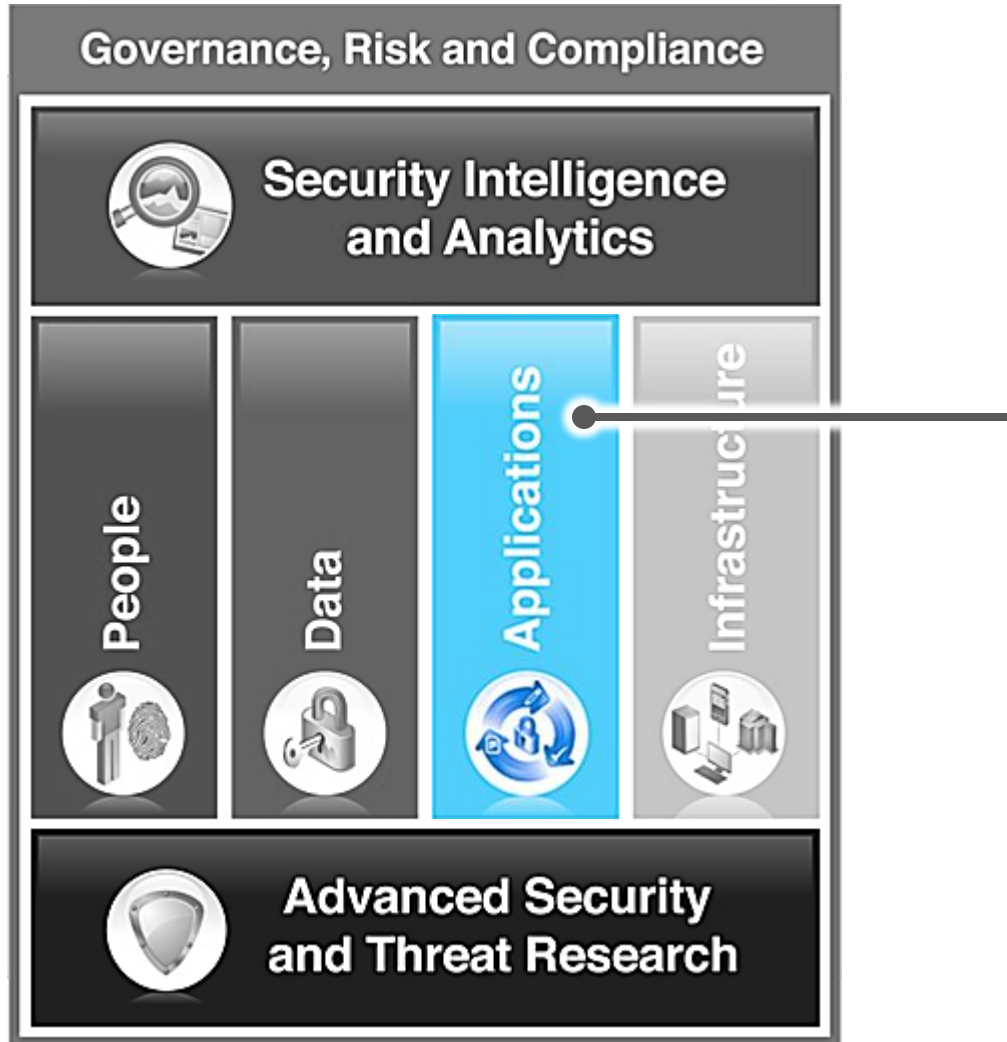
Description

- Employees
- Contractors & partners
- Customers
- Customers of partners
- **Cloud & Mobile users**

Security

- Identity management
 - Role management
 - User provisioning
 - Privileged ID management
 - Governance
 - Entitlements
- AAA at runtime
 - Authentication
 - Authorization
 - Auditing
- Identity federation
- Single sign-on
- **Context-based authentication & authorization**

Applications with Cloud and Mobile



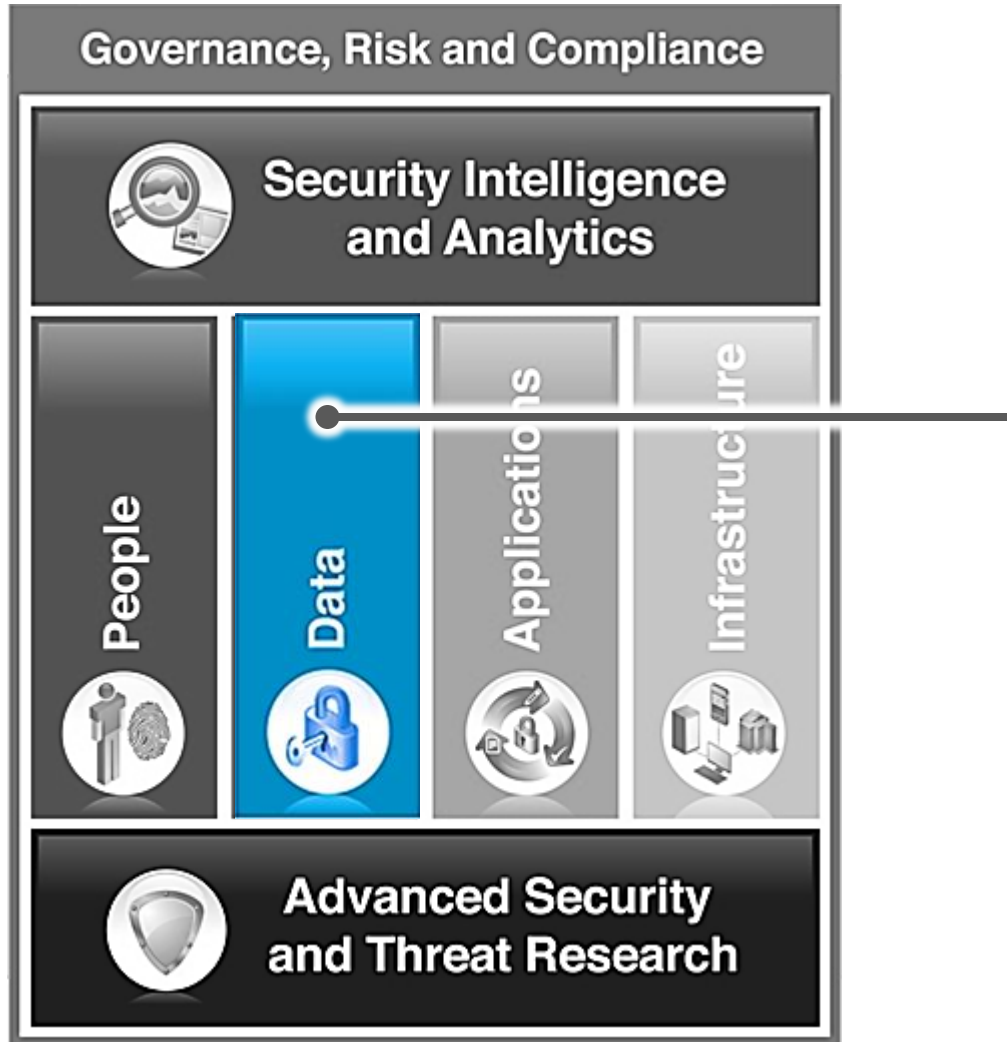
Description

- System apps
- Traditional Web apps
- Web 2.0 apps
- **Public & private cloud apps**
- **Mobile apps**

Security

- Discovery
- Scanning & pentesting
 - Static
 - Dynamic
- Vulnerability analysis
- Runtime enforcement of entitlements
- **Cloud app discovery**
- **Mobile app scanning**
- **Mobile app secure containers**
- **Mobile app registration**

Data with Cloud and Mobile



Description

- SQL databases
- Non-relational databases
- Big data stores
- Unstructured data
- **Data in clouds and across clouds**
- **Data in compromised mobile devices**

Security

- Discovery
- Data classification
- Vulnerability analysis
- Activity monitoring
- Data masking
- Encryption management
- **Cloud DB activity monitoring**
- **Secure mobile data design**

Security Intelligence and Analytics with Cloud and Mobile



Description

- Information & insight from all security data
- Mathematical analyses of all relevant data
- **Separate and combine cloud instance data**
- **Identify attacks against mobile infrastructure**

Security

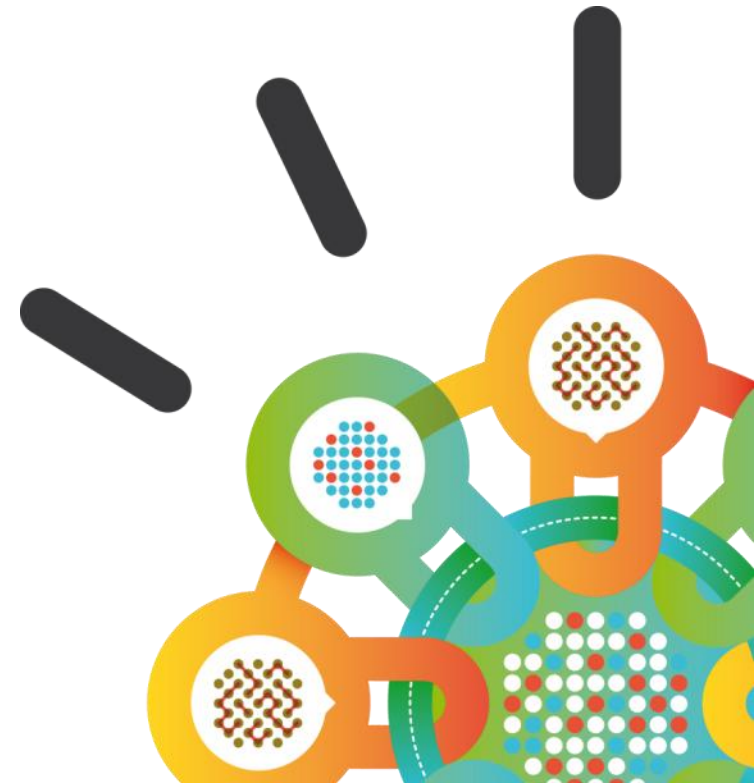
- Security Information and Event Management
- Network flow analysis
- Vulnerability scanning
- Event correlation
- Attack identification
- Anomaly Detection
- **Collect data from elastic cloud infrastructure**
- **Identify mobile attacks**

Resources

- ibm.com/security
- Security Architecture
 - [*Using the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security*](#), IBM Redbook
 - [Open Enterprise Security Architecture](#), The Open Group
- [IBM Institute for Advanced Security](#)
- [IBM Security YouTube Channel](#)
- [IBM X-Force](#)
- [IBM Cloud Security](#)
- [IBM Mobile Security](#)
- [IBM Managed Security Services](#)
- [IBM Security Intelligence with Big Data](#)
- [IBM MobileFirst Security](#)
- [IBM developerWorks Security](#)

Security Intelligence.
Think Integrated.

Resources & Backup Slides




[IBM Software](#) > [Products](#) >

IBM Security

Security intelligence. Think integrated.


[Solutions](#)
[Services](#)
[Resources](#)
[Connect](#)

It's a new IT world. How secure are you?

IBM helps thousands of [clients](#) address the challenges of securing their people, data, applications and infrastructure. The IBM Security Framework provides a more integrated, intelligent approach to security. The application of security intelligence and analytics along with external threat intelligence, helps organizations to detect, analyze and remediate threats that point products will always miss.

[→ Learn more](#)



IBM Security Framework

Connect with IBM Security



What's New?

- [↔ 2013 Gartner Magic Quadrant for SIEM Report](#)
- [→ IBM X-Force 2012 Annual Trend and Risk Report](#)
- [↔ Extending Security Intelligence with Big Data Solutions](#)
- [▶ For healthcare, change is in the air – and in the cloud \(869KB\)](#)
- [▶ IBM Point of View: Security and Cloud Computing \(382KB\)](#)

IBM Security Products by Capability


Bridge the gap between your goals and the capabilities needed to meet them. The IBM

Search by IBM Security Product

Looking for a specific product? Search here:



Using the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security



Building a business security reference model based on standards and common practices

Connecting business drivers with IT security and risk management

Explaining the value in a real world business scenario

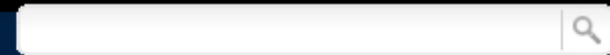
Open Enterprise Security Architecture (O-ESA)

A Framework and Template for
Policy-Driven Security



IBM Institute for Advanced Security

Where global security leaders go to share intelligence and collaborate



[Home](#) | [Blogs](#) | [CIO and CISO Essentials](#) | [Industries](#) | [Global Branches](#) | [Resource Library](#) | [Events](#) | [About](#)

Welcome to the Institute

The IBM Institute for Advanced Security is a collaborative organization providing CIOs, CISOs and security leaders a place to engage in industry, regulatory, and technical advancements. Please join our community to gain access to whitepapers, live events with our Institute experts, contribute and respond on security topics, [join a user group](#) or regional chapter to collaborate, and connect and share experiences and information with other security leaders around the world.

[JOIN THE COMMUNITY](#)

[FIND A USER GROUP](#)

Mobile Security Forum

CISO and CIO Essentials

2013 Gartner Critical Capabilities for SIEM



The new report assesses 13 SIEM technologies by evaluating the capabilities that are critical for the support of threat management, compliance, and general SIEM deployment use cases. Read the full report to learn how IT security organizations can define their SIEM requirements and select technology.

[Download the Report](#)

Industry Insights

Webcast Replay: How New NFC

Featured User Group Meeting

Italian Security User Group 2013 Meeting

Friday July 5th in Padova, IT

To view the User Group meeting agenda and to register for the event, [click here](#). You must be a member of the **Italy - Security Group** to join the meeting.

[More Information and Registration](#)

Security Leaders

Attention User Group Leaders and Liaisons – Introduction and Site Training



Official IBM Security Channel

IBM ibm.com/security



IBM Security Systems

✓ Subscribed



904



Videos

Discussion

About



What to watch next



3:54

The role big data plays in solving complex security challenges

by IBMSecuritySolutions

4,070 views

Recent activity



6:50

Demo: IBM Security AppScan and IBM SiteProtector Integration

uploaded 3 weeks ago



5:59

Demo: Integration between IBM Security AppScan and QRadar

uploaded 3 weeks ago



11:51

Demo: Analyzing Results in IBM AppScan Standard

uploaded 3 weeks ago

IBM Security

[Overview](#)[Big Data](#)[Cloud](#)[Mobile](#)

Real security in a virtual world

Transforming cloud security from inhibitor to enabler



Nine out of 10 global CEOs view the cloud as critical to their business plans. And while the cloud can increase productivity with anywhere, anytime information access, it also introduces additional security risks that can become an inhibitor to cloud adoption. To mitigate risk to your

cloud environment and data, a proactive approach to identity, application and threat protection should be embraced to enable confidence in your cloud deployments.

IBM Security solutions strengthen security in the cloud by helping to:

- i. Administer, extend and authenticate identities and access to and from the cloud
- ii. Build, test and maintain secure cloud applications; monitor and audit enterprise databases and data-repositories
- iii. Prevent and defend against advanced threats with layered protection and analytics

You can realize cloud benefits within existing IT management constraints by having capabilities

Contact IBM

Considering a purchase?

[Request a quote](#)

[Email IBM](#)

[Or call us at: 1-877-426-3774](#)
Priority code: 109HJ03W

IBM SmartCloud Security



[IT services >](#)

IBM Security Services

IT security services that can protect enterprises against threats while helping to reduce costs and complexity



Building security into your business and IT processes and integrating it with your existing technology infrastructure and investments has never been more critical. Driving this need is the exponential growth of data center transformation, virtualization, social business, mobility and attack sophistication. To address these issues, you need to be able to make faster and more intelligent business decisions surrounding your overall security and risk management posture.

IBM Security Services can deliver the skills, expertise and technology to help you reduce the cost and complexity of securing your infrastructure. Powered by IBM X-FORCE® research and development, IBM provides solutions to help take you from planning and design through

Contact IBM

[Chat now](#)[E-mail us](#)[Request a conversation](#)

[or call us at 1-877-426-3287
\(US and Canada\) Mention 609CG98W](#)

Emergency Contact

If you are currently experiencing a security

IBM Security Intelligence with Big Data



IBM Security Intelligence with Big Data

With major security breaches and fraud incidents making international headlines, organizations are taking steps to address the growing problems of advanced persistent threats, fraud, and insider attacks.



Traditional security technologies lack the sophisticated capabilities and visibility required to detect and protect against such attacks. At best, they solve a single facet of the problem. Smart cyber criminals can skirt those defenses and blend into the background noise of an organization's operations. They're skilled and patient enough to perform stealthy

Contact IBM

Considering a purchase?

[Request a quote](#)

[Email IBM](#)

[Or call us at: 1-877-471-5227](#)
Priority code: 102PW03W



Extending Security Intelligence with Big Data Solutions

Learn about the latest security intelligence solution combining IBM QRadar and IBM InfoSphere BigInsights technologies

[Register Now](#)

↑ A Smarter Planet

IBM MobileFirst

 [Request a quote](#)
 [Email IBM](#)

Mobile enterprise

Why IBM

See it in action

Offerings

Developer resources

Conversations

[Overview](#)

[Strategy & Design](#)

[Platform](#)

[Management](#)

[Security](#)

[Analytics](#)

[Development & Integration](#)

[Events](#)

IBM MobileFirst Security



 **Mobile Security** — Enabling productivity, business agility and rich user experience

Secure transactions and access to your mobile enterprise

Transform your business with confidence while you maintain the trust of your customers, partners, and staff by providing secure transactions from an array of devices around the world. While increased agility helps encourage mobile engagements, it also increases the complexity of data protection — driving a greater need for visibility and control of mobile devices to help ensure compliance and prevent risk to proprietary data.

We'll help you defend against malware, provide security-enabled connectivity and context-aware risk-based access control, and deliver security-conscious applications and application platforms.

developerWorks > Technical topics >

Security

Pragmatic, intelligent, risk-based practices.

Overview **Practices** Products Community

19 June 2013

Top story



IBM Security AppScan Standard: Scan and analyze results

Get started scanning for web application vulnerabilities with IBM Security AppScan Standard Edition, and then analyze the results. Configure AppScan for a dynamic scan of a new application, follow a case study that demonstrates using AppScan Standard to scan and test two web applications, and watch a five-step process to help you analyze the results of your scan.

Featured topics



Security for Linux on System z: Securing Your Network. Explore the unique technologies on System z that you can use to help harden a server farm and its network.



Introduction to Manual Explorer in IBM Security AppScan Enterprise 8.7.

Learn about the new Manual Explorer tool in IBM Security AppScan Enterprise V8.7 by using the step-by-step instructions in this article to install and configure the tool.

Popular topics

- Data protection
- Access control
- Identity management
- Cloud security
- Mobile security
- Java security

Getting started

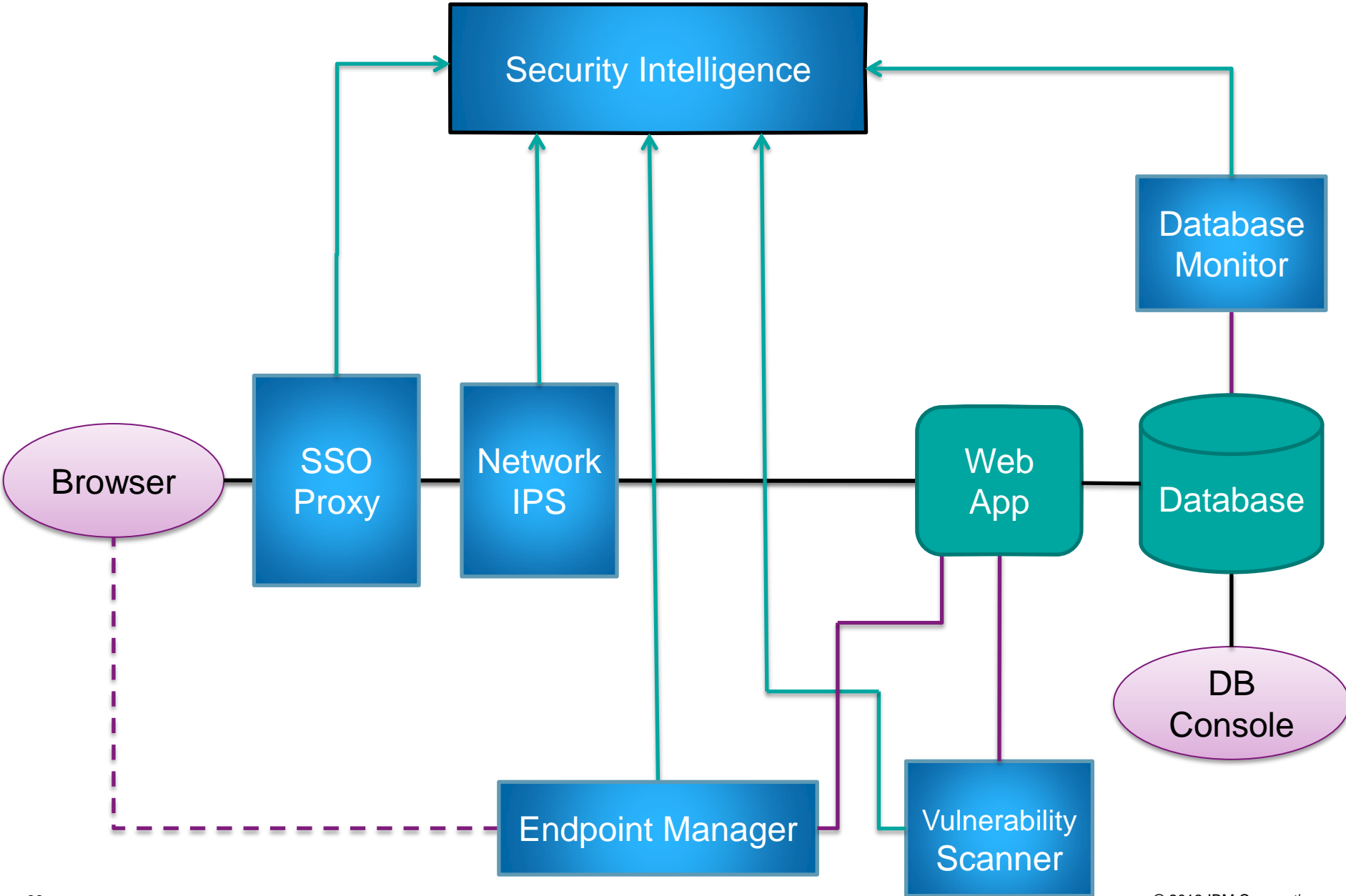
Upcoming events

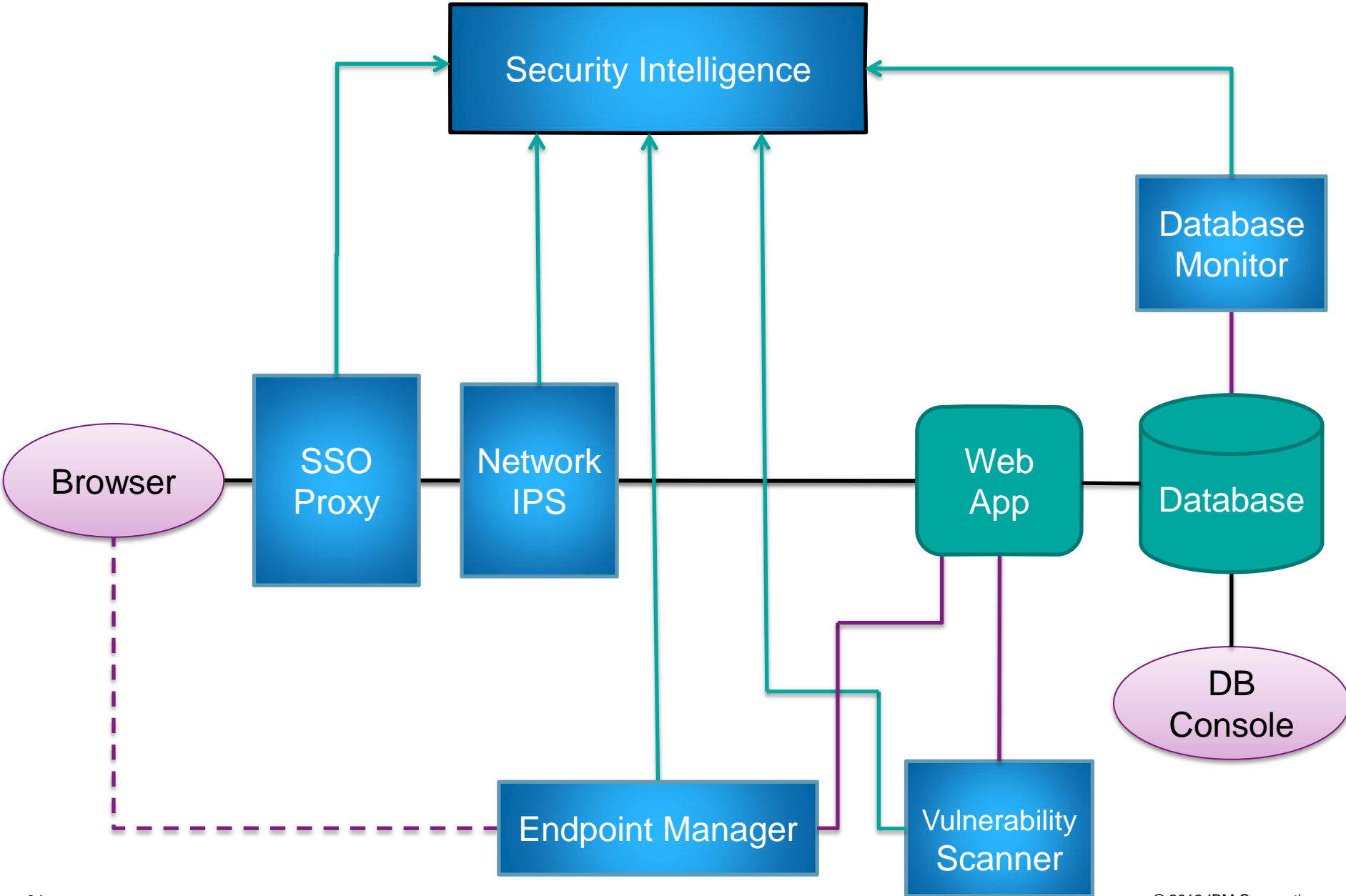
Related links

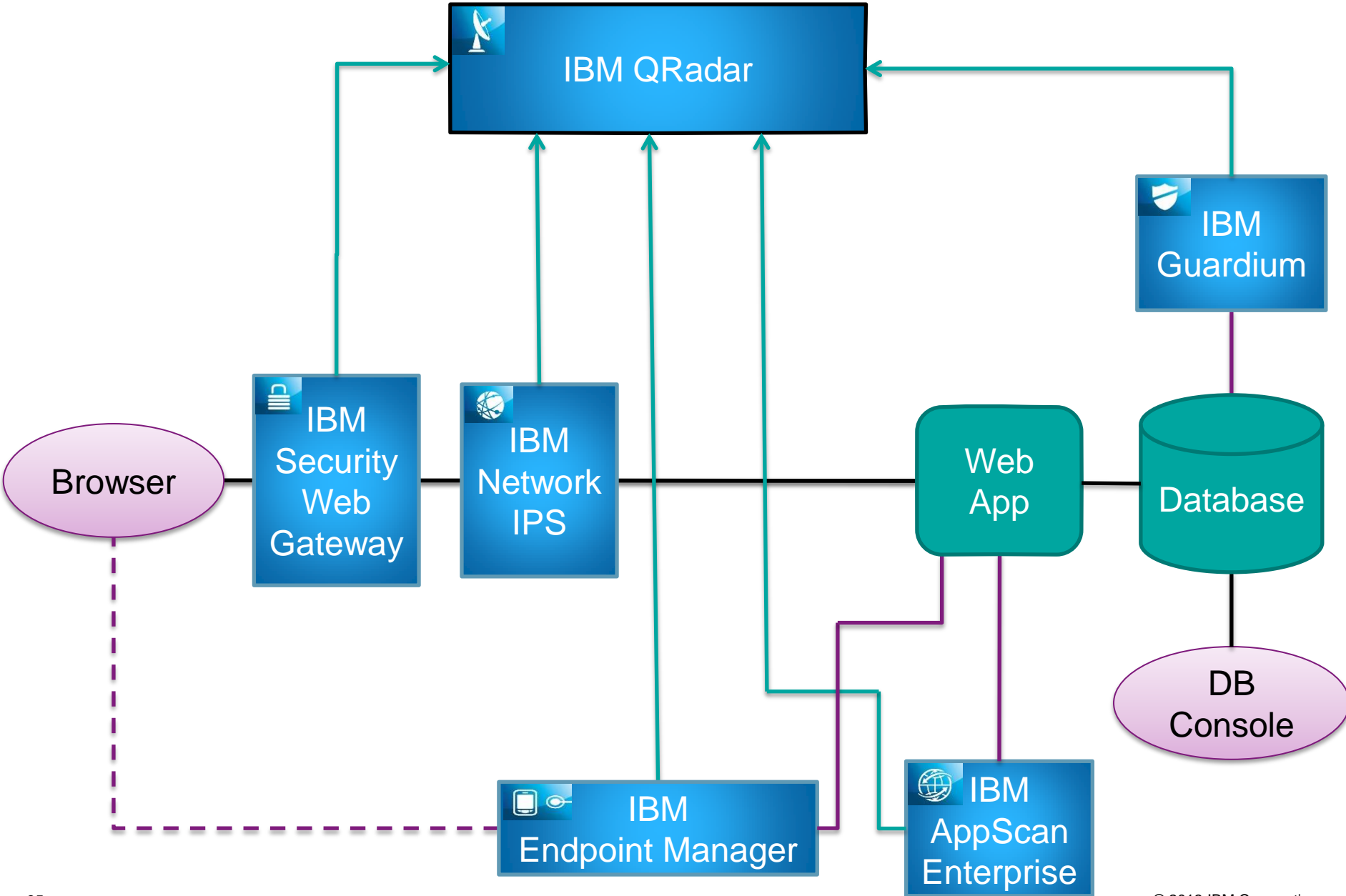
dW Community update

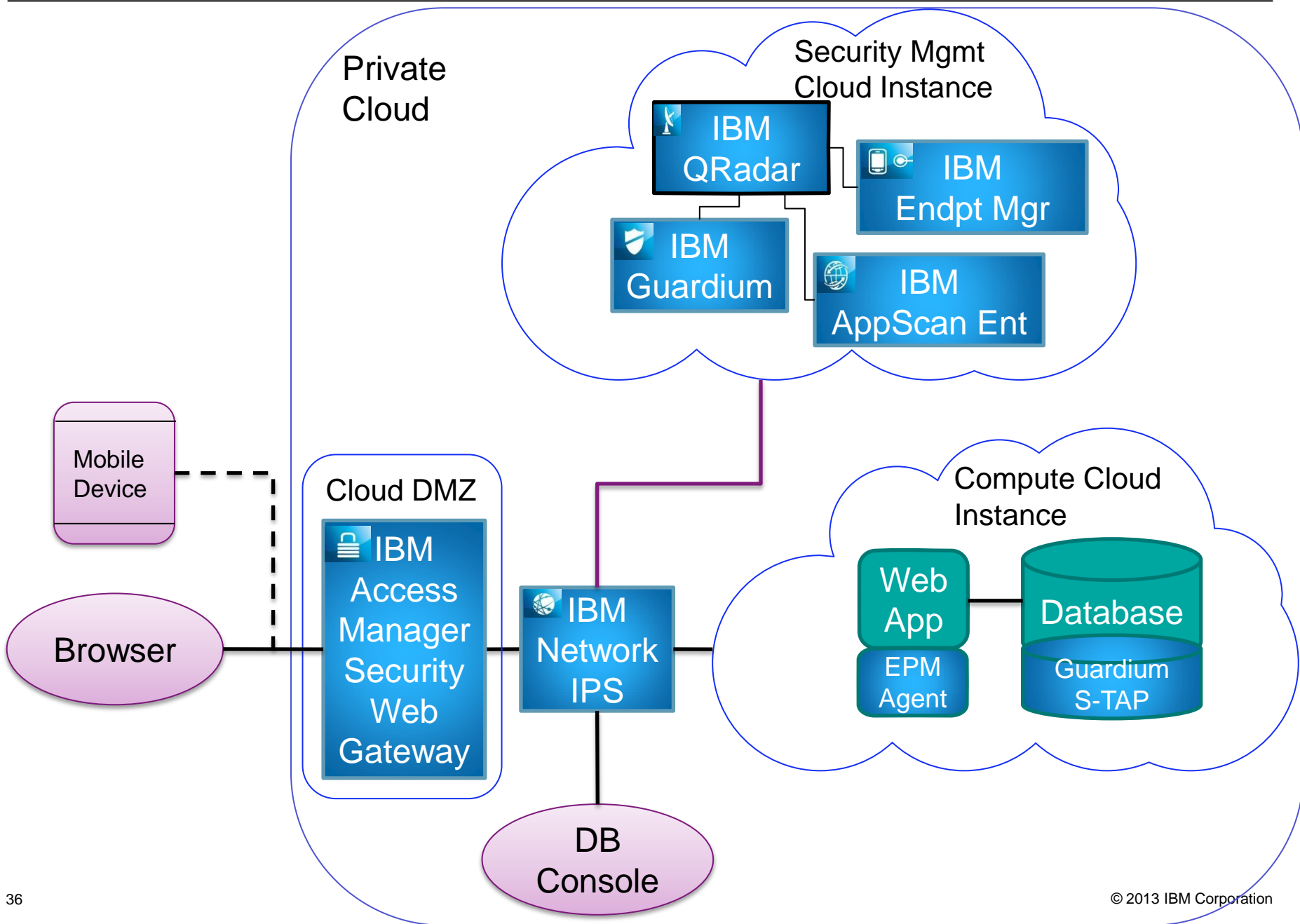


om.com/developerworks/security/# [Trend and Risk Report](#). Listen in discussion the risk assessment









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.



ibm.com/security

© **Copyright IBM Corporation 2013. 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.