Security Intelligence.
Think Integrated.
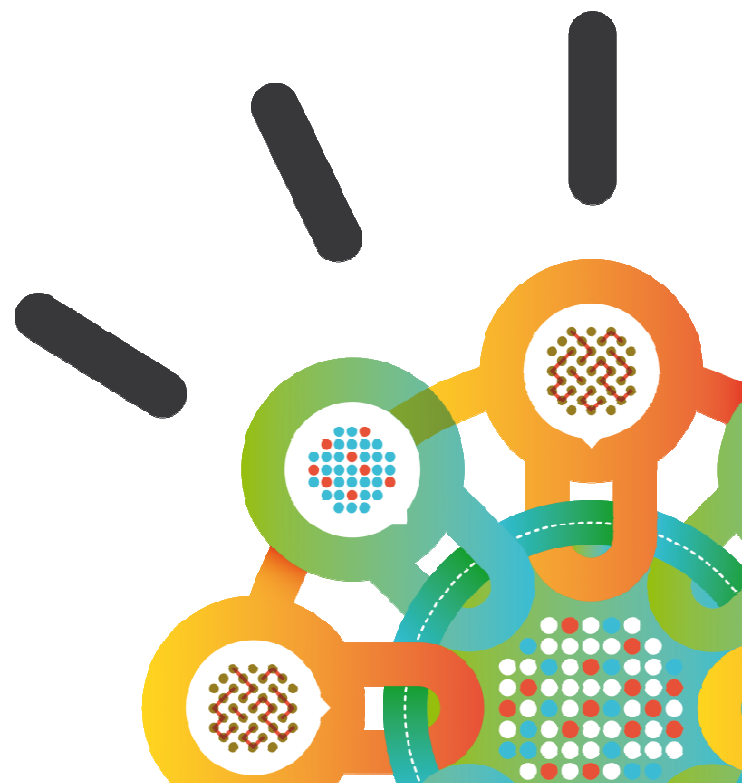
IBM Security

A New Era of Security
for a New Era of Computing
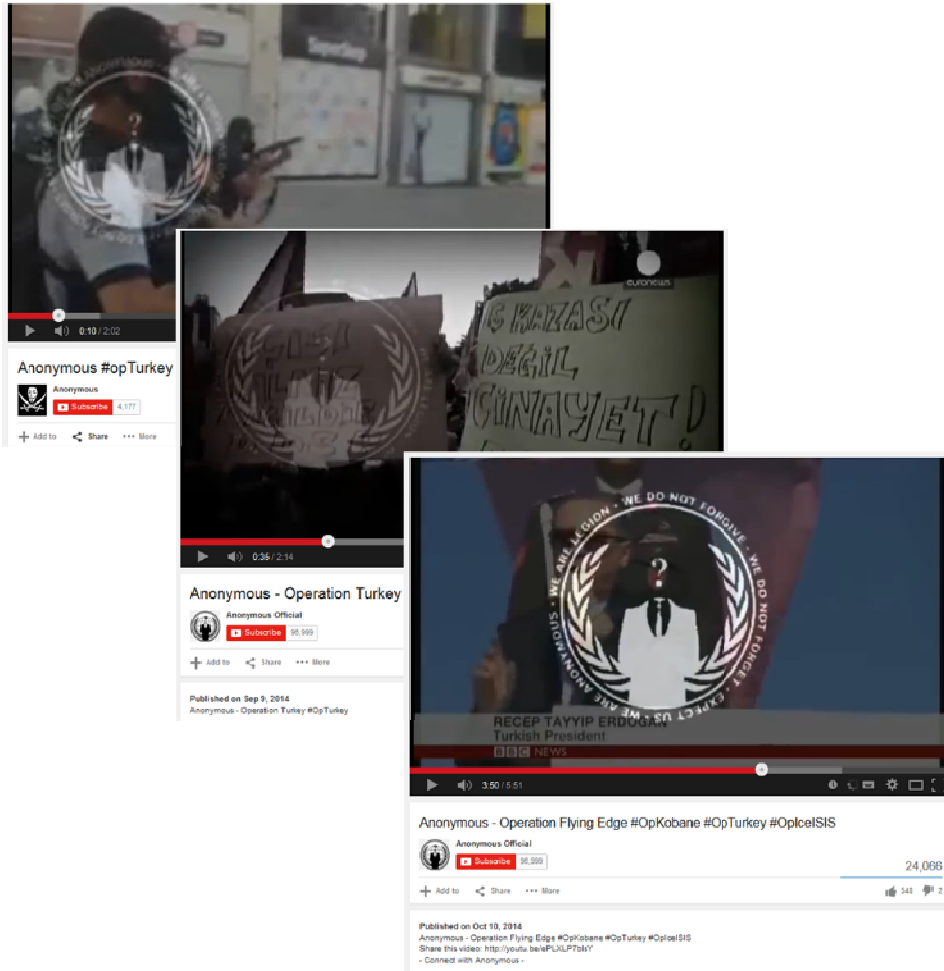
Engin Özbay
IBM Security Country Leader

enginoz@tr.ibm.com
0 530 3171654

Hacktivism against Turkey

Syrian Electronic Army

The Hacked Website's :

1 - The Saudi Ministry of Defense
Website: http://moda.gov.sa

2 - Saudi Arabia Defense Industries
Website: mic.gov.sa

3 - Admission gate of the Armed Forces
Website: afca.gov.sa

4 - Saudi government site
Website: csc.edu.sa

5 - General Directorate of Military Works
Website: gdmw.gov.sa

6 - General Directorate of Military Survey
Website: gdms.gov.sa

7 - a Saudi government site
Website: psmpq.org.sa

7 - a Saudi government site
Website: safous.gov.sa

8- Royal Saudi Land Forces
Website link : rslf.gov.sa

9- Royal Saudi Navy Foces
Website link : rsnf.gov.sa

10- http://mic.org.sa

Turkey Files

Publish Date 2015-02-07

Turkey - Ministry Of Defense

Latest Messages in this Category:

#	Subject	Date	From	To
1365	[konu yok]	Nov 7, 2012 8:56 AM	IBRAHIM LÜTFI NUHOĞLU [ibrahim.nuhoglu@msb.gov.tr]	Murad BAYAR [mbayar@ssm.gov.tr]
1313	İlet: Acil	Nov 6, 2012 2:44 PM	IBRAHIM LÜTFI NUHOĞLU [ibrahim.nuhoglu@msb.gov.tr]	maitburo@gmail.com
1362	Corum Ziyareti Taslağı	Oct 31, 2012 12:36 PM	IBRAHIM LÜTFI NUHOĞLU [ibrahim.nuhoglu@msb.gov.tr]	Derya AYDIN [derya.aydin@icisleri.gov.tr]
1366	[konu yok]	Oct 9, 2012 11:33 AM	MSB PROTOKOL [msb.protocol@msb.gov.tr]	Mehmet ERKAN [merkan@ssm.gov.tr], Yasemin SERGEN [ysergen@ssm.gov.tr]
1364	görüşme hakkında	Oct 3, 2012 2:51 PM	ISMET YILMAZ [ismet.yilmaz@msb.gov.tr]	Murad BAYAR [mbayar@ssm.gov.tr]
663	Ektis Sahibliği	Jul 30, 2012 6:59 AM	Vedat Gül [vgul@TCCB.GOV.TR]	ibrahim.nuhoglu@msb.gov.tr
1363	Milli Savunma Komisyonu Brifing	Nov 22, 2011 2:03 PM	IBRAHIM LÜTFI NUHOĞLU [ibrahim.nuhoglu@msb.gov.tr]	Murad BAYAR [mbayar@ssm.gov.tr]
428	[no subject]	Mar 7, 2011 12:12 PM	IBRAHIM LÜTFI NUHOĞLU [ibrahim.nuhoglu@msb.gov.tr]	Ahmet Muhtar Gün [ahmet.gun@mfa.gov.tr]

Home | Files | Categories | Messages | Advanced Search | Media | About | Contact

Home » Files » Turkey Files » Categories » Turkish Presidency

Turkish Presidency

					o	Attachments
398	Mektuplar	Oct 15, 2012 12:08 AM	Melahat Tek [mtek@TCCB.GOV.TR]	Hüseyin Avni Karslıoğlu; O. Koray Ertaş; Fahri Türker Oba	0	⬇
571	AGÜ oturma düzenleri	Oct 15, 2012 12:08 AM	Erbil ÖZDEMIR [eozdemir@tccb.gov.tr]	Vedat Gül [vgul@TCCB.GOV.TR]	0	⬇
81	"Gizri Mektuplar"	Oct 15, 2012 12:08 AM	Hüseyin Avni Karslıoğlu	Yaşar BEYDOĞAN [ybeydogan@TCCB.GOV.TR]	0	⬇
134	Başbakanımızın ziyareti	Oct 15, 2012 12:08 AM	Kasım Yeksler [yeksler@TCCB.GOV.TR]	İşmira Tospunoğlu [tospcioglu@mfa.gov.tr]	0	⬇
425	FW: Davetli/askeri protokol	Oct 15, 2012 12:08 AM	Nilüfer Kanat GÜLBAHÇE [nkgulbahce@TCCB.GOV.TR]	Lütfiye Sezin Sezik Demri [sdemri@TCCB.GOV.TR], Merve ATAK [matak@TCCB.GOV.TR], Mektap DÖNMEZ [mdonmez@TCCB.GOV.TR]	0	⬇
833	RE: War-CB	Oct 15, 2012 12:08 AM	Mehmet Ferden Çarıkçı	Tahir Bora ATATANIR, O. Koray Ertaş	0	⬇
874	TBMM Açılış Tutanak	Oct 1, 2012 4:42 AM	Ferhat Alkan [ferkata@TCCB.GOV.TR]	CbOzelkalem, Hacı Ahmet Sever, Sadik ARSLAN, Mehmet Ferden Çarıkçı, Osman Çanget, Bleki Ferhan ÖZDABAN, Süleyman kLAŞT	0	⬇
658	25 Eleni sayılı Basın Listesi	Sep 28, 2012 6:22 AM	Ferhat Alkan [ferkata@TCCB.GOV.TR]	PROTOKOL MUDURLUGU	0	⬇
670	29 Eleni Tebekat davetgesi gönderilecekler listesi	Sep 27, 2012 11:13 AM	Ferhat Alkan [ferkata@TCCB.GOV.TR]	ssagman@mfa.gov.tr, brahinkaya@mfa.gov.tr, m1246@yahoo.com, Hidayet Baysakter [hbaysaktar@mfa.gov.tr], kaykan@mfa.gov.tr	0	⬇
693	Saadi Velahi Programı	Sep 24, 2012 12:33 PM	Erşat Hürmüzlü [hurmuzlu@TCCB.GOV.TR]	Tahir Bora ATATANIR [tratatanir@TCCB.GOV.TR]	0	⬇

Go to page: « Previous 1 2 3 4 5 6 7 8 9 10 Next »

Turkish Defense Industries
Publish Date 2015-02-07

Murad Bayar
Publish Date 2015-02-07

Turkish Presidency
Publish Date 2015-02-07

Ersat Hurmuzlu
Publish Date 2015-02-07

Turkey - Ministry Of Defense
Publish Date 2015-02-07

Turkish Grand National Assembly
Publish Date 2015-02-07

Ministry of Foreign
Publish Date 2015-02-07

Turkish Air Force
Publish Date 2015-02-07

Emre Yunt
Publish Date 2015-02-07

Turkish Prime Minister
Publish Date 2015-02-07

Hayati Yazıcı
Publish Date 2015-02-07

Sakir Ozkan Torunlar
Publish Date 2015-02-07

Ertugrul Gunay
Publish Date 2015-02-07

Ahmad Mukhtar Gun
Publish Date 2015-02-07

Malware Encounter Rate – # 2

Figure 33. Encounter rate trends for the locations with the most computers reporting malware encounters in 1H14, by number of computers reporting.
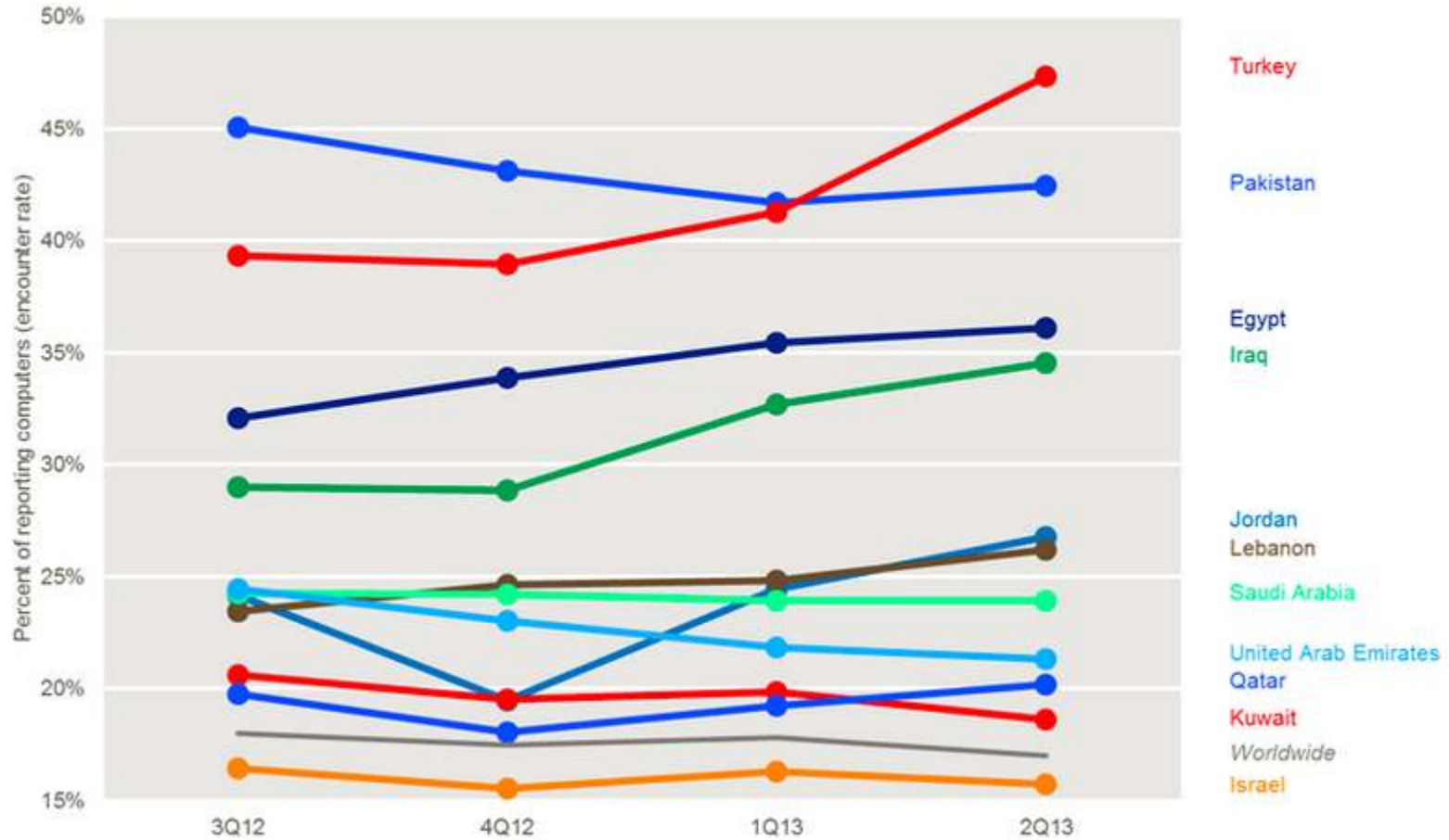
	Country/Region	3Q13	4Q13	1Q14	2Q14
1	United States	16.7 %	13.0 %	13.0 %	12.3 %
2	Brazil	43.1 %	36.8 %	34.0 %	30.5 %
3	Russia	31.7 %	28.9 %	28.7 %	26.4 %
4	Turkey	41.3 %	45.5 %	45.7 %	40.5 %
5	France	24.2 %	23.0 %	20.2 %	16.8 %
6	India	51.0 %	47.1 %	50.5 %	41.7 %
7	Mexico	39.8 %	36.7 %	38.6 %	32.1 %
8	Germany	18.1 %	14.8 %	13.6 %	13.5 %
9	Italy	28.3 %	26.1 %	25.5 %	20.4 %
10	United Kingdom	18.2 %	14.5 %	13.5 %	13.3 %

The telemetry data generated by Microsoft security products from computers whose administrators or users choose to opt in to provide data to Microsoft includes information about the location of the computer, as determined by IP geolocation.

Locations are ordered by the number of computers reporting detections in 1H14.

Source: www.microsoft.com/sir

Microsoft Regional Security Intelligence Report

Malware Encounter Rates – Middle East – 3Q12 to 2Q13

Source: www.microsoft.com/sir

Microsoft Regional Security Intelligence Report

Crypto-ransomware attacks in the EMEA

Country	Percentage
Italy	31.19%
Turkey	22.19%
France	8.04%
UK	6.43%
Spain	4.50%
Russia	2.89%
South Africa	2.25%
Netherlands	2.25%
Monaco	1.61%
Germany	1.61%
Austria	1.61%
Others	15.43%

Figure 3. Top infected countries in the EMEA region, November 2014
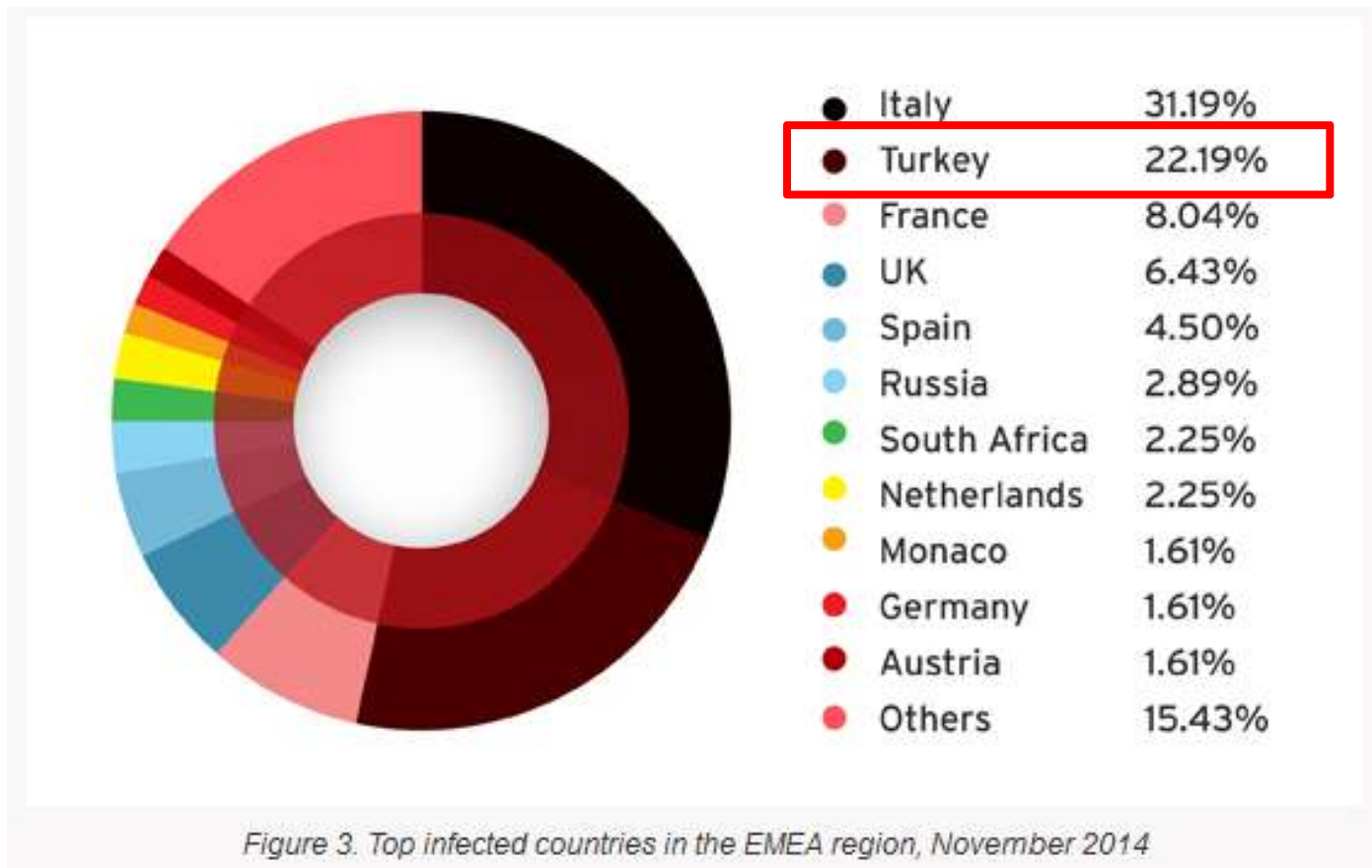
Based on feedback collected via the Trend Micro Smart Protection Network

Source: trendmicro.com

Crypto-Ransomware Goes Local in EMEA Region

© 2015 IBM Corporation

Command & Control Server Contamination Ratio

C&C server contamination ratio

August 2014

Figure 4. C&C server contamination as a percentage of the total number of systems in a country, August 2014
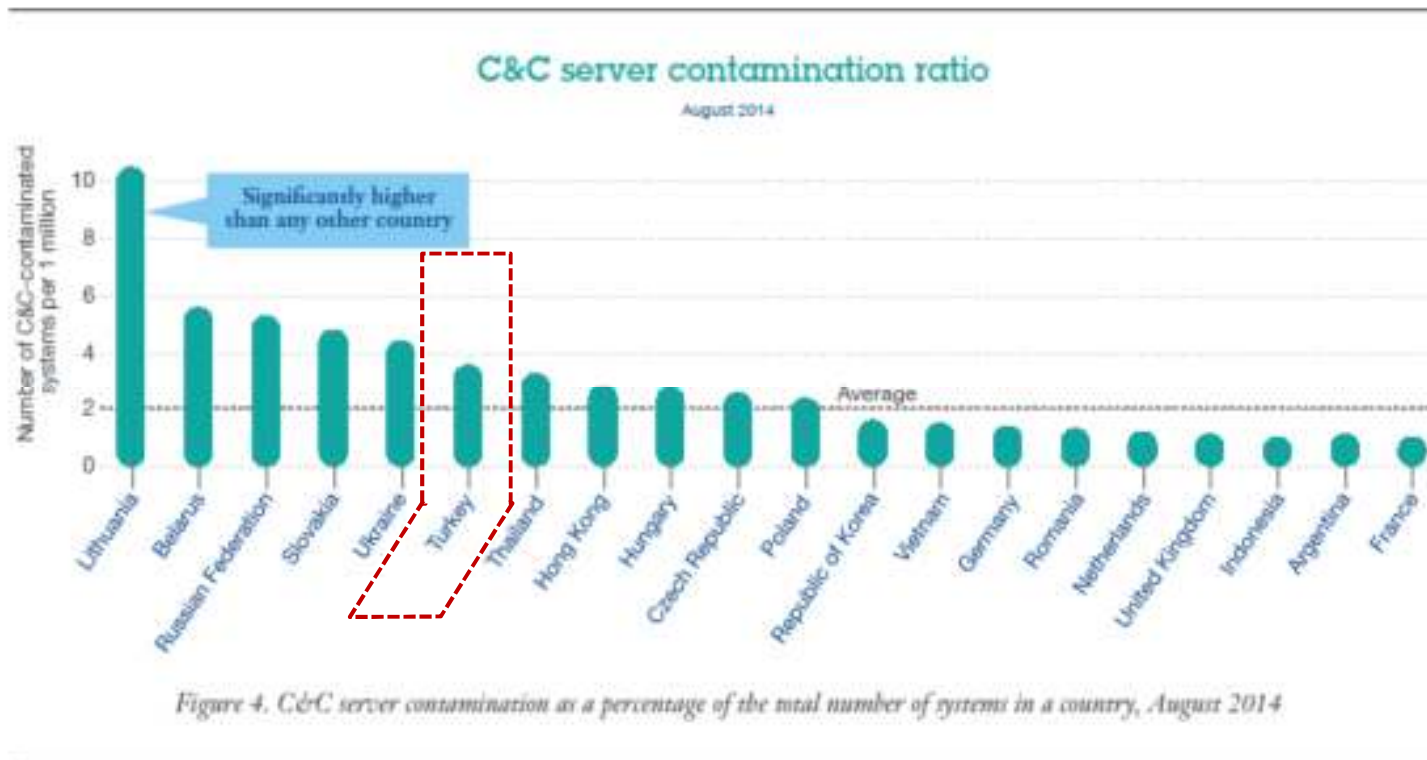
Distributed Denial of Service Attachs

- Top 10 sources of malicious, non-spoofed DDoS traffic in Q1 2014

Saudi Arabia
4.46%

South Korea
4.65%

Indonesia
5.29%

Italy
5.34%

Brazil
6.12%

Germany
7.63%

Turkey
12.65%

United States
21.30%

China
17.79%

Thailand
14.77%

Prolexic Quarterly Global DDoS Attack Report Q1 2014
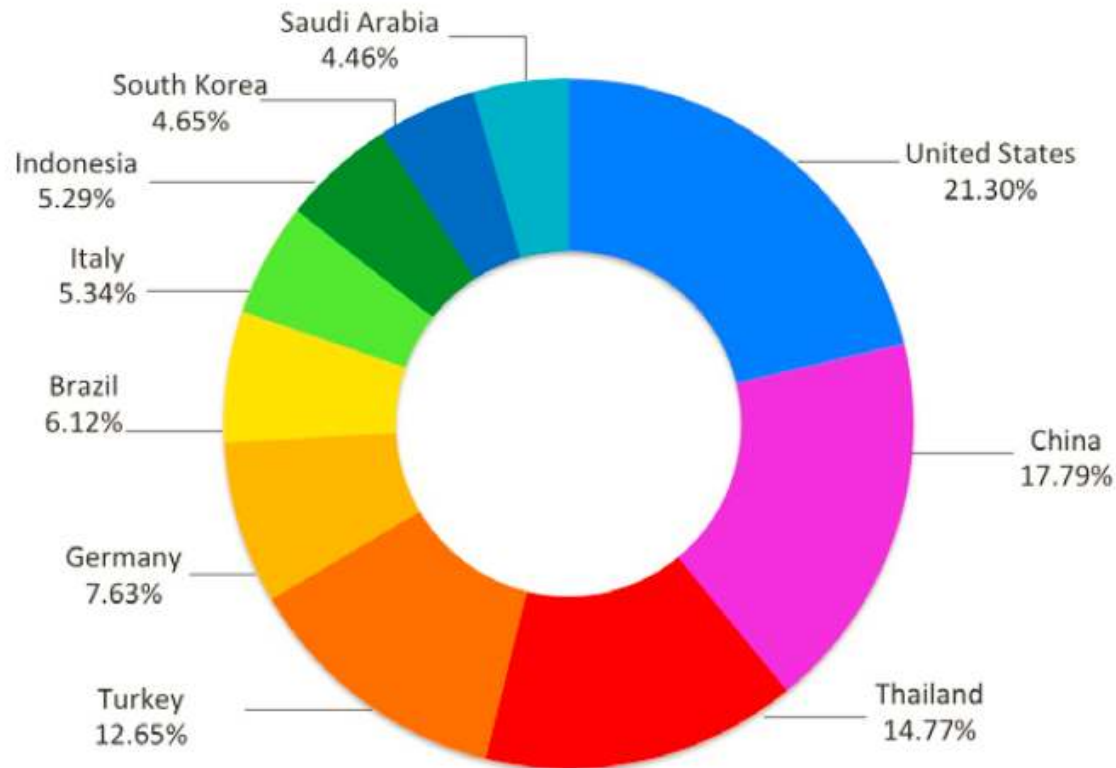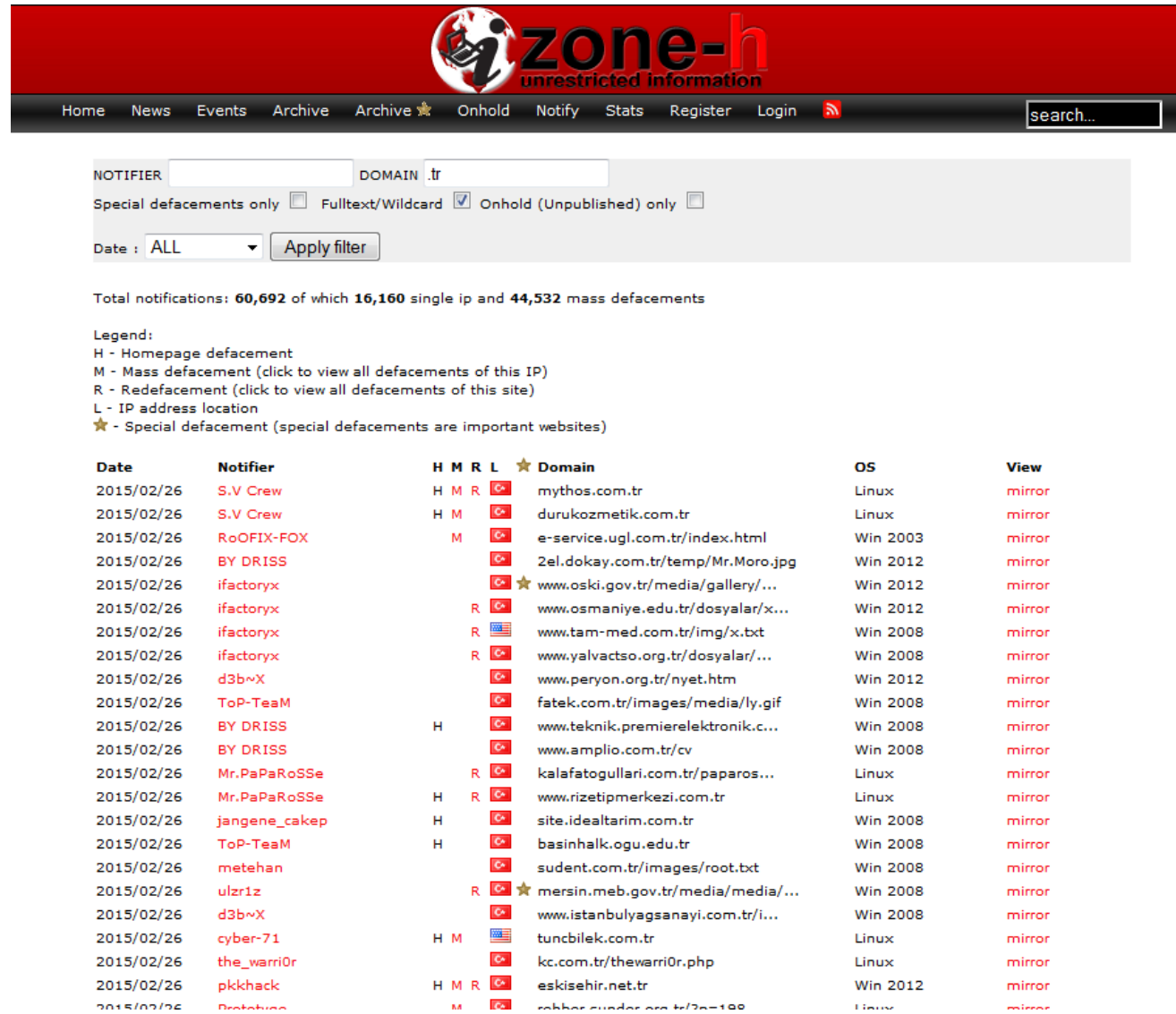
Turkey - Website defacements cause reputation impact

Zone-H reported more then 60,692 defacements for the .tr domain

8,145 gov.tr defacements

100+ defacements in 2015 alone

NOTIFIER [   ] DOMAIN [.tr   ]

Special defacements only ☐ Fulltext/Wildcard ☑ Onhold (Unpublished) only ☐

Date : [ALL ▼] [Apply filter]

Total notifications: **60,692** of which **16,160** single ip and **44,532** mass defacements

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important websites)

| Date	Notifier	H	M	R	L	★	Domain	OS	View
2015/02/26	S.V Crew	H	M	R	🇹🇷		mythos.com.tr	Linux	mirror
2015/02/26	S.V Crew	H	M		🇹🇷		durukozmetik.com.tr	Linux	mirror
2015/02/26	RoOFIX-FOX		M		🇹🇷		e-service.ugl.com.tr/index.html	Win 2003	mirror
2015/02/26	BY DRISS				🇹🇷		2el.dokay.com.tr/temp/Mr.Moro.jpg	Win 2012	mirror
2015/02/26	ifactoryx				🇹🇷	★	www.oski.gov.tr/media/gallery/...	Win 2012	mirror
2015/02/26	ifactoryx			R	🇹🇷		www.osmaniye.edu.tr/dosyalar/x...	Win 2012	mirror
2015/02/26	ifactoryx			R	🇺🇸		www.tam-med.com.tr/img/x.txt	Win 2008	mirror
2015/02/26	ifactoryx			R	🇹🇷		www.yalvactso.org.tr/dosyalar/...	Win 2008	mirror
2015/02/26	d3b~X				🇹🇷		www.peryon.org.tr/nyet.htm	Win 2012	mirror
2015/02/26	ToP-TeaM				🇹🇷		fatek.com.tr/images/media/ly.gif	Win 2008	mirror
2015/02/26	BY DRISS	H			🇹🇷		www.teknik.premierelektronik.c...	Win 2008	mirror
2015/02/26	BY DRISS				🇹🇷		www.amplio.com.tr/cv	Win 2008	mirror
2015/02/26	Mr.PaPaRoSSe			R	🇹🇷		kalafatogullari.com.tr/paparos...	Linux	mirror
2015/02/26	Mr.PaPaRoSSe	H		R	🇹🇷		www.rizetipmerkezi.com.tr	Linux	mirror
2015/02/26	jangene_cakep	H			🇹🇷		site.idealtarim.com.tr	Win 2008	mirror
2015/02/26	ToP-TeaM	H			🇹🇷		basinhalk.ogu.edu.tr	Win 2008	mirror
2015/02/26	metehan				🇹🇷		sudent.com.tr/images/root.txt	Win 2008	mirror
2015/02/26	ulzr1z			R	🇹🇷	★	mersin.meb.gov.tr/media/media/...	Win 2008	mirror
2015/02/26	d3b~X				🇹🇷		www.istanbulyagsanayi.com.tr/i...	Win 2008	mirror
2015/02/26	cyber-71	H	M		🇺🇸		tuncbilek.com.tr	Linux	mirror
2015/02/26	the_warri0r				🇹🇷		kc.com.tr/thewarri0r.php	Linux	mirror
2015/02/26	pkkhack	H	M	R	🇹🇷		eskisehir.net.tr	Win 2012	mirror
2015/02/26	Prototype		M		🇹🇷		rahher.cundar.org.tr/?p=198	Linux	mirror

Turkey based companies have also been targeted

IBM Security

Malicious or criminal attacks are the leading root cause of a data breach…and result in the highest cost per record
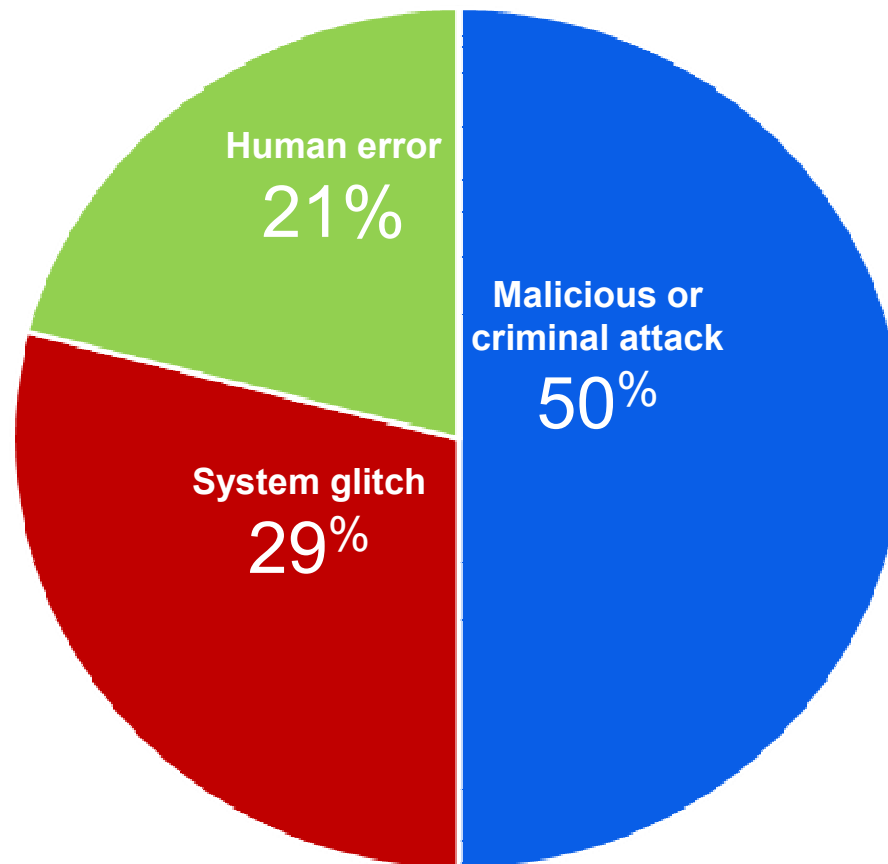
What business does today's ambitious criminal go into?

Global Black Market on Drugs $288B

Marijuana

Cocaine

Heroin

Cybercrime >35%

Cost of Global CyberCrime $388B

Online Scams

Credit Card Fraud

Phishing

Malware

Virus
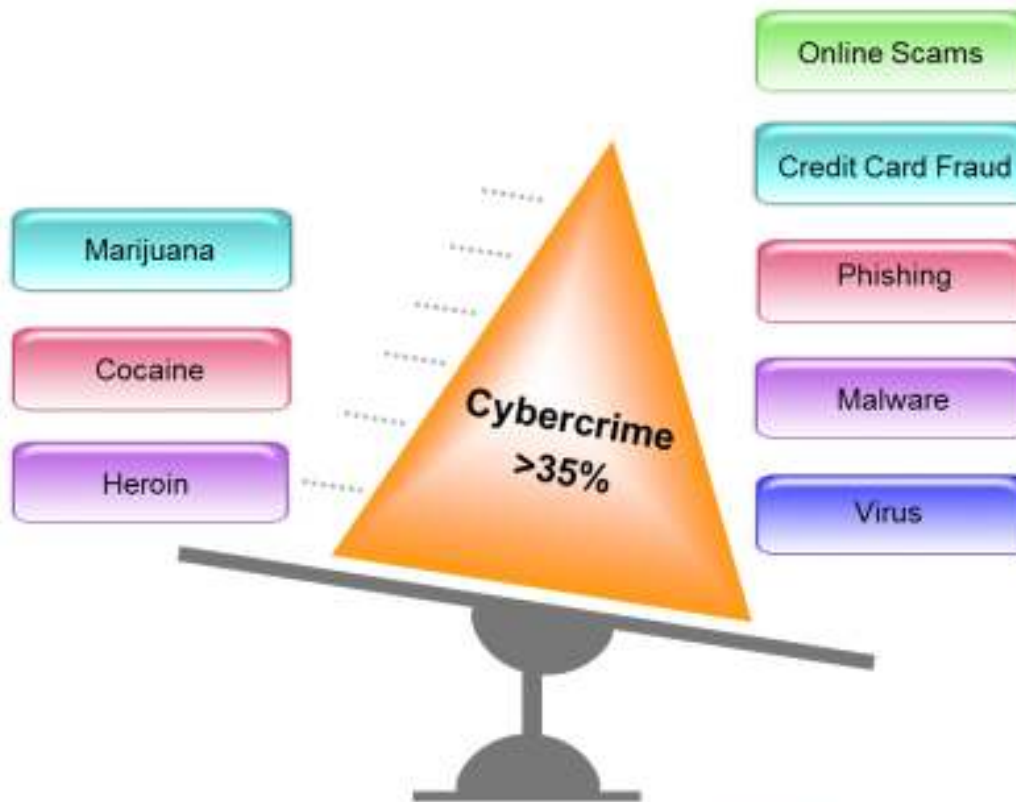
http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02

Operational Sophistication
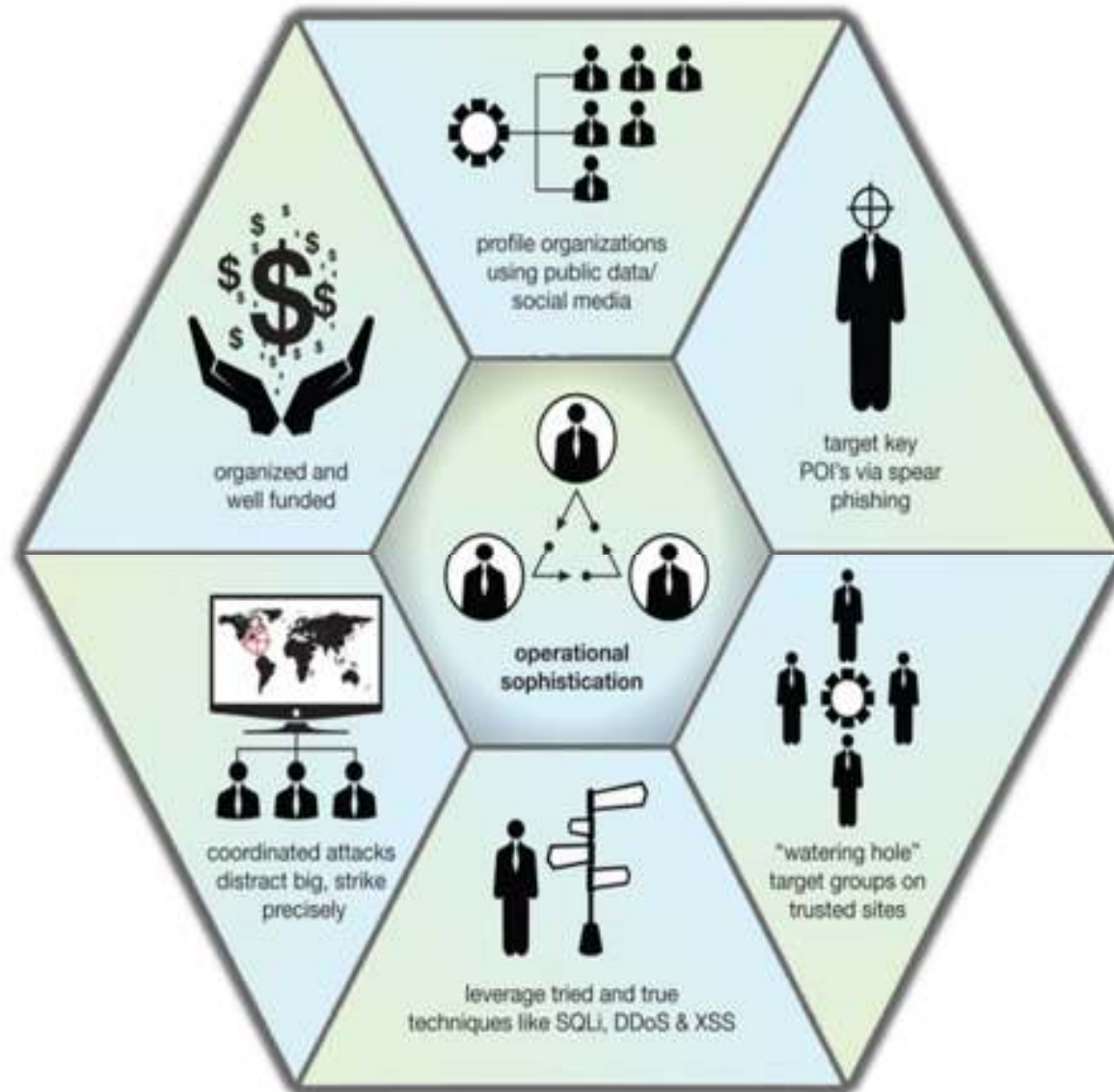
Security leaders are more accountable than ever before

CEO	CFO / COO	CIO	CHRO	CMO
Loss of market share and reputation Legal exposure Business continuity	Audit failure Fines and enforcement impact Financial loss	Impact to data and systems, (confidentiality, integrity and/or availability)	Violation of employee privacy	Loss of customer trust Loss of brand reputation
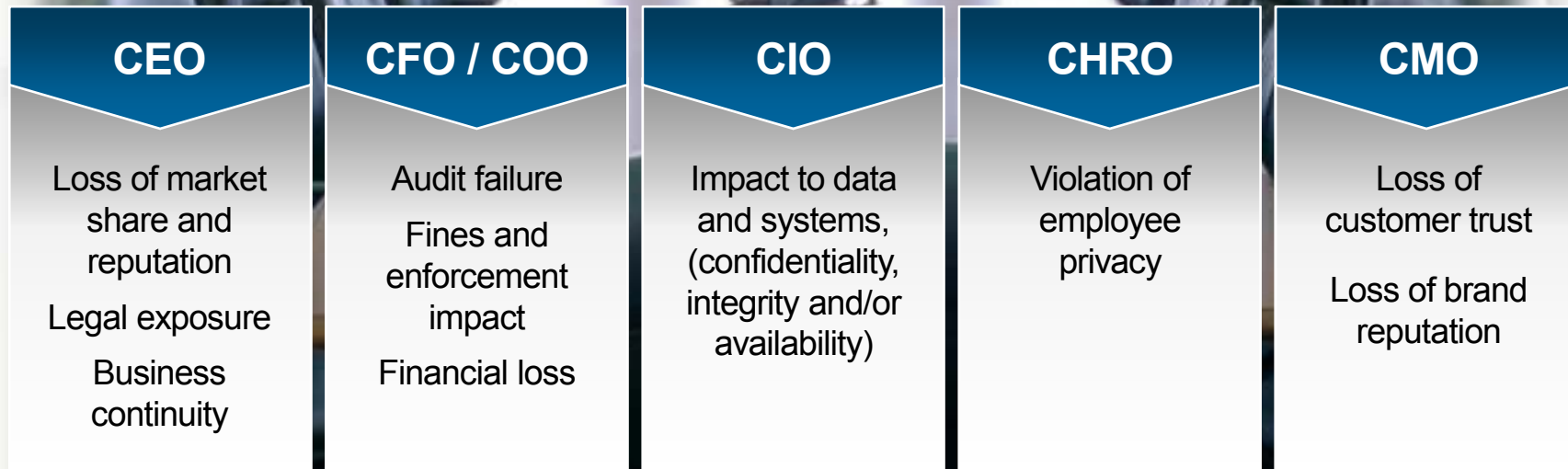
Your board and CEO demand a strategy

IBM Security invests in best-of-breed technologies
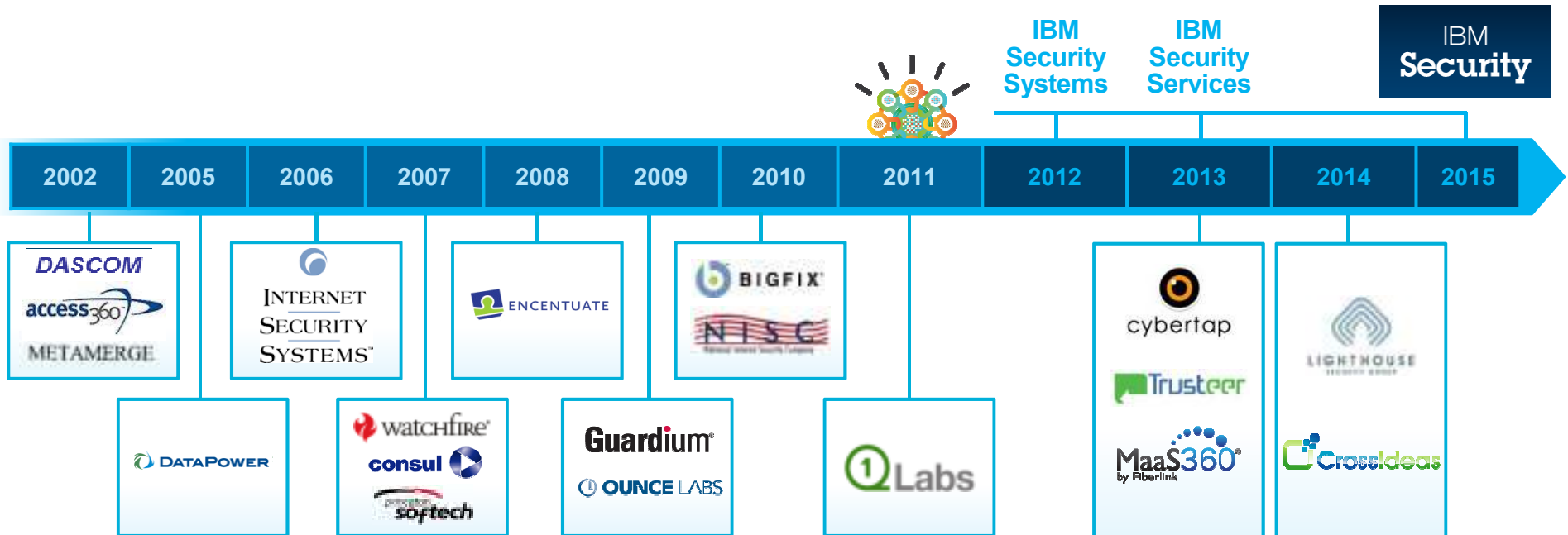
…and we are relentless innovators

- **70⁺** new or updated offerings in the last 12 months
- Major innovations in every IBM security domain

IBM Security Strategy

1 **Support the CISO agenda**

CISO, CIO, and Line-of-Business
Deliver a broad portfolio of solutions differentiated
through their integration and innovation to address the latest trends

HELP!

2 **Innovate around megatrends**

Key Security Trends

Advanced Threats | **Cloud** | **Mobile and Internet of Things** | **Compliance Mandates** | **Skills Shortage**

3 **Lead in selected segments**

IBM Security Portfolio

| Strategy, Risk and Compliance | Cybersecurity Assessment and Response |

Security Intelligence and Operations

| Advanced Fraud Protection | Identity and Access Management | Data Security | Application Security | Network, Mobile and Endpoint Protection |

Advanced Threat and Security Research

IBM helps protect against new, complex security challenges

1 **Optimize security program**
Integrate security silos, reduce complexity, and lower costs

2 **Stop advanced threats**
Use analytics and insights for smarter integrated defense

3 **Protect critical assets**
Use context-aware, role-based controls to help prevent unauthorized access

4 **Safeguard cloud and mobile**
Employ cloud and mobile initiatives to build a new, stronger security posture

1 Optimize your security program
Integrate security silos, reduce complexity, and lower costs

Risk-Aware Culture & Strategy

End-to-End Security Intelligence

Intelligent Threat Protection & Response

Assess and transform your security maturity

Benchmark your security maturity versus peers and define a roadmap for the future

Build a next generation security operations capability

Use integrated solutions to stop unknown attacks and detect malicious activity

Get help from the experts

Engage professionals to hunt the attackers, deploy solutions or help run operations

IBM Security Services Portfolio

Security Strategy, Risk and Compliance
- Security Risk Assessment
- Security HealthCheck
- Information Sec Assessment
- Policy Development
- Cloud Security Consulting
- PCI, SCADA Compliance

Cybersecurity Assessment and Response
- Emergency Response Services
- Penetration Testing
- Application Security Assessment
- Application Source Code Assessment

Security Operations Optimization
- Strategy and assessment
- Design and deployment

Data and Application Security
- Data Security Strategy and Assessment
- Encryption
- Data Loss Prevention

Identity & Access Management
- Identity Assessment and Strategy
- User Provisioning / Access Mgmt
- Total Authentication Solution
- Managed / Cloud Identity

Infrastructure and Endpoint
- Deployment and migration
- Staff augmentation

Managed Security Services
- Managed SIEM
- Intrusion Detection & Prevention
- Firewall Mgmt
- Managed DDOS
- Unified Threat Mgmt
- Managed Protection
- X-Force Threat Analysis
- Hosted E-mail and Web Security
- Hosted Vulnerability Mgmt
- Hosted Security Event and Log Mgmt
- Hosted Application Sec Mgmt

IBM's global experience in IT Security

- 🟧 Security Operations Centers
- 🟢 Security Research Centers
- ⬜ Security Solution Development Centers
- 🏛 Institute for Advanced Security Branches

IBM Research

IBM Institute for Advanced Security
Enabling cybersecurity innovation and collaboration

Research
17B analyzed web pages & images
40M spam & phishing attacks
76K documented vulnerabilities
Billions of intrusion attempts daily
Millions of unique malware samples

Managed Security Services
10 Global SOC locations
20,000+ devices under contract
3,700+ MSS clients worldwide
20B+ events managed per day
133 monitored countries

A financial services firm teams with IBM to build its first SOC

Optimize Your Security Investments

Identified and blocked

650+

suspicious incidents
in the first 6 months
of SOC operations

Business Challenge

- The bank did not have the security skills and resources to build its first SOC within the aggressive milestones set by their Board

- Wanted global protection for 16,000,000 accounts across 44 countries

IBM Security Solution benefits

- Automated real-time advanced analytics

- 24x7 SOC management and incident response support

- 13M+ events evaluated per day
  from 400K+ assets and 28K+ active log sources

- ~$2M lower cost than in-house management

2 Stop advanced threats
Use analytics and insights for smarter integrated defense

Protect against fraud and targeted attacks

Stop sophisticated threats in real-time with next-generation defenses

Detect advanced threats with security intelligence

Gain visibility and respond to breaches faster with big data analytics

Deploy integrated security

Reduce operating costs and complexity with integrated controls and managed services

Introducing the IBM Threat Protection System

IBM delivers a dynamic, integrated system to disrupt the lifecycle of advanced threats

Attack Chain

1 **Break-in**

2 **Latch-on**

3 **Expand**

4 **Gather**

5 **Exfiltrate**

Prevent. Detect. Respond.

Detect

Prevent

Respond

Threat Intelligence Network

DYNAMIC PROTECTION AND **ANALYTICS PLATFORM**

NETWORK | ENDPOINT   PHYSICAL | VIRTUAL | CLOUD

SECURITY PARTNER ECOSYSTEM
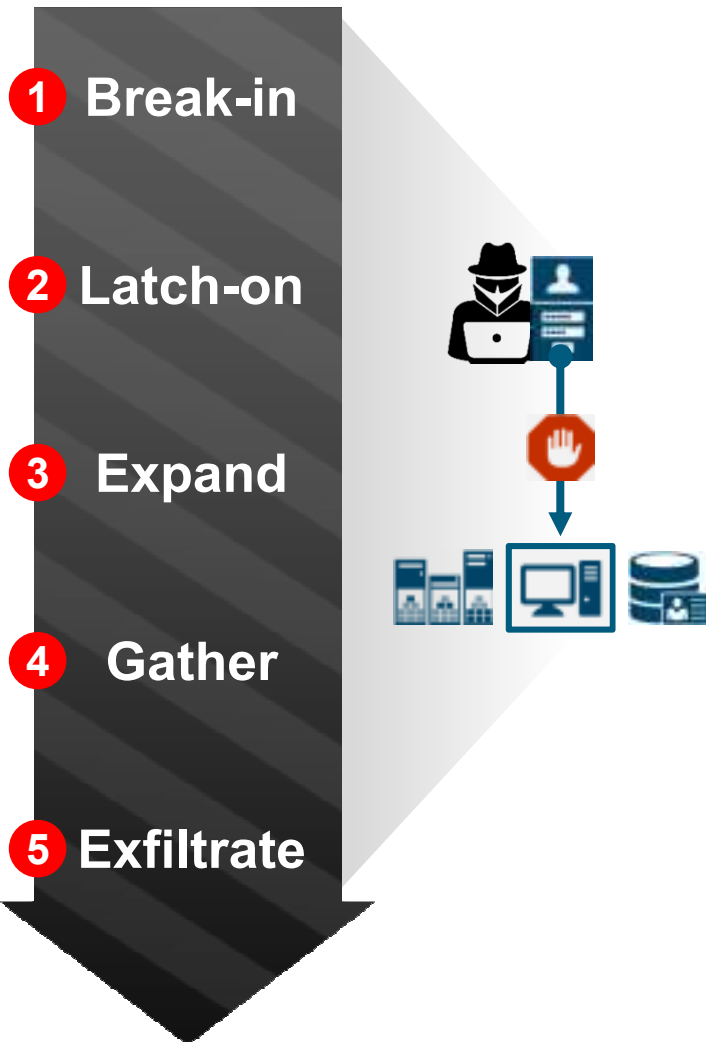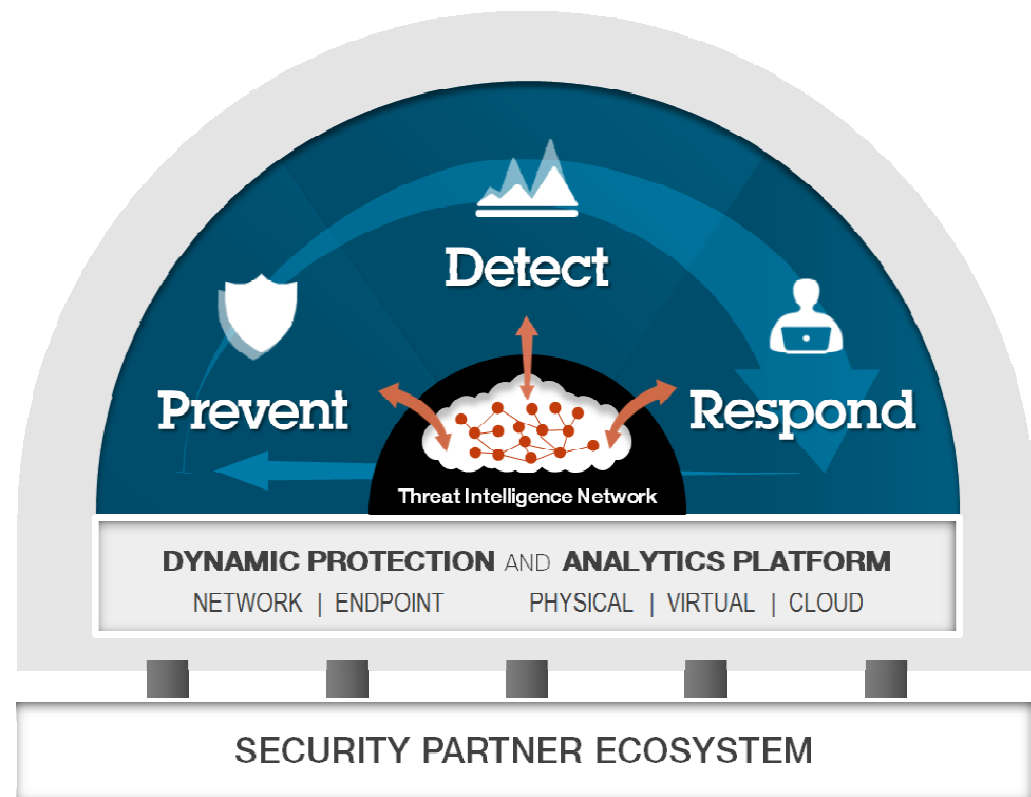
Focus on critical points in the attack chain with preemptive defenses on both the endpoint and network

ENDPOINT

Prevent malware installs	**Prevent control channels**	**Prevent credential loss**
• Verify the state of applications • Block exploit attempts used to deliver malware	• Stop direct outbound malware communications • Protect against process hijacking	• Block keyloggers • Stop credential use on phishing sites • Limit reuse of passwords

Exploit Disruption	*Malware Quarantine*	*User Protection*

NETWORK

Prevent mutated exploits	**Prevent active beaconing**	**Prevent malicious apps**
• Verify the state of network protocols • Block unknown exploits with behavioral heuristics	• Stop malware and botnet control traffic with real-time reputation and SSL inspection	• Block access to malicious websites • Protect against web application misuse

On the Endpoint
Trusteer Apex Malware Protection

On the Network
IBM Security Network Protection XGS

Prevent

X-

Continuously monitor security-relevant activity from across the entire organization

Pre-Attack Analytics

Predict and prioritize security weaknesses before adversaries

- Use automated vulnerability scans and rich security context

- Emphasize high-priority, unpatched, or defenseless assets requiring attention

IBM Security QRadar Vulnerability Manager

IBM Security QRadar
Security Intelligence Platform

Real-time Attack Analytics

Detect activity and anomalies outside normal behavior

- Correlate and baseline massive sets of data

- From logs, events, flows, user activity, assets, locations, vulnerabilities, external threats, and more

IBM Security QRadar SIEM

Detect

Intelligent, integrated and automated vulnerability management
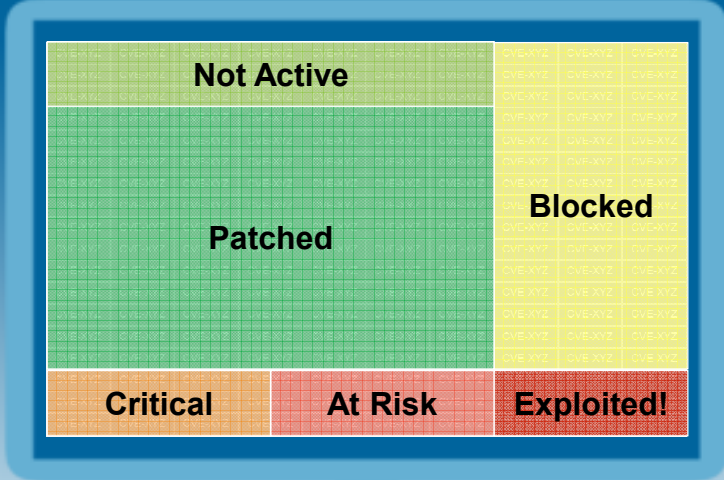

Traditional Security
Common Vulnerabilities and Exposures (CVEs)

IBM Security
Vulnerability Management

Not Active

Patched

Blocked

Critical   At Risk   Exploited!

IBM QRadar Vulnerability Manager

Integrated Security Intelligence to reduce costs and increase visibility

Traditional SIEM 6 products from 6 vendors are needed		IBM Security Intelligence and Analytics
Flows	ARBOR NETWORKS — Lancope — riverbed Think fast.	
Packets	EMC² RSA — SOLERA NETWORKS	
Vulnerabilities	QUALYS — RAPID7 — tenable network security	
Configurations	algosec FIREMON — skybox security — tufin — REDSEAL NETWORKS	
Logs	loglogic — splunk>	
Events	HP ArcSight — McAfee — EMC² RSA	

IBM QRadar
Security Intelligence Platform

An integrated, unified architecture in a single web-based console

Rapidly investigate breaches, retrace activity, and learn from findings to remediate weaknesses

Respond

Post-Attack Incident Forensics

Reduce the time to fully discover what happened and when it occurred

- Index and reconstruct attack activity and content from full-packet network data
- Apply search engine technology and advanced visualizations
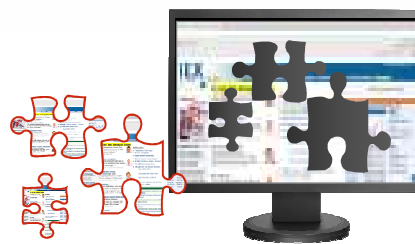
**IBM Security
QRadar Incident Forensics**

Rapid Response Integrations

Quickly expand security coverage to prevent further harm

- Share indicators across control points
- Dynamically apply customized rules

**IBM Security
Capability Integrations**

Emergency Response Services

Help prepare for and withstand security breaches more effectively

- Gain access to key resources that can enable faster recovery and help reduce incident business impact

**IBM Emergency
Response Services**

Share, analyze, and act upon information gathered from an ecosystem of third-party products

Security Partner Ecosystem Integrations

IBM Security Partner Ecosystem

- 90+ vendors
- 450+ products
- Complimentary integrated solutions
- Strengthens the threat protection lifecycle
  - Leverage a vibrant ecosystem of security products
  - Increase visibility, collapse information silos, and provide insights on advanced attacks
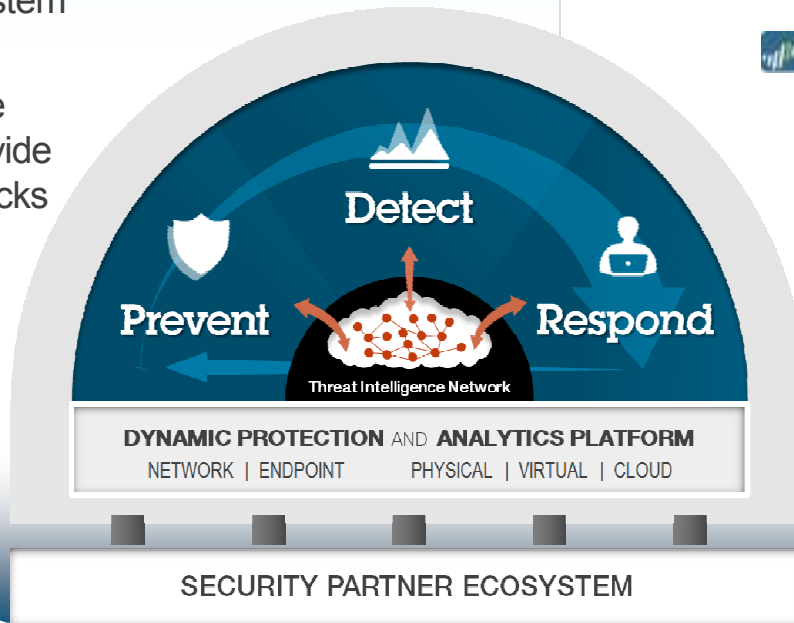
Advanced Threat Protection Integrations

TREND MICRO — Trend Micro Deep Security
IBM XGS Quarantine and Blocking

FireEye — FireEye Web Malware Protection System
IBM XGS Quarantine and Blocking

DAMBALLA — Damballa Failsafe
IBM XGS Quarantine and Blocking

paloalto — Palo Alto Firewalls
Trusteer Apex integration

Additional IBM QRadar Partners Include

CISCO   QUALYS

websense

BLUE COAT   proofpoint   JUNIPER

Detect

Prevent   Respond

Threat Intelligence Network

DYNAMIC PROTECTION AND **ANALYTICS PLATFORM**
NETWORK | ENDPOINT   PHYSICAL | VIRTUAL | CLOUD

SECURITY PARTNER ECOSYSTEM
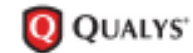
An international energy company identifies critical events to investigate

Stop Advanced Threats with Security Intelligence

An international energy firm analyzes

2 billion

events per day to find

20 – 25

potential offenses to investigate
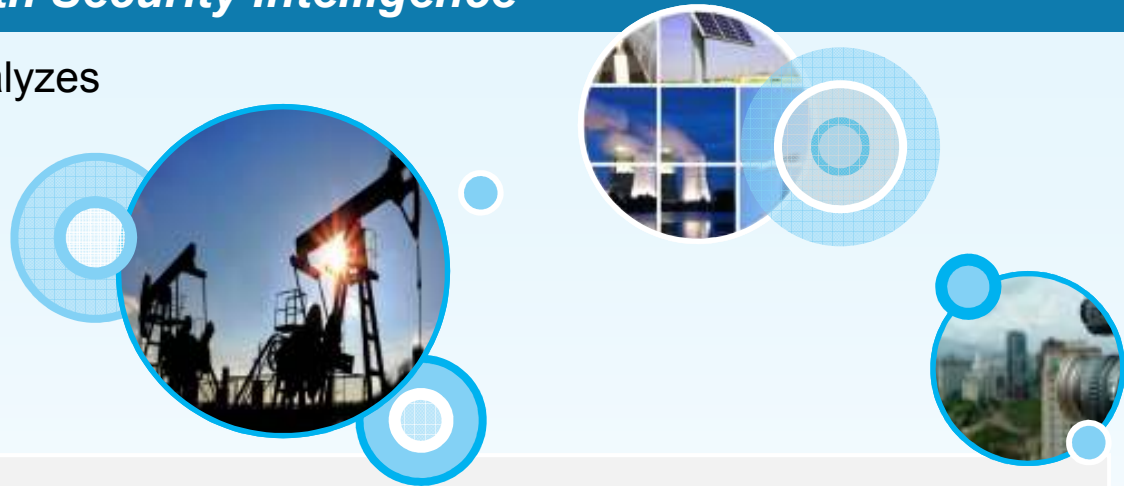
Business Challenge

- Reducing huge number of events to find the ones that need to be investigated
- Automating the process of analyzing security data

IBM Security Solution Benefits

- Combined analysis of historical data with real-time alerts to gain a 'big picture' view and uncover patterns of unusual activity humans miss
- Immediately block suspected traffic

3 **Protect critical assets**
Use context-aware, role-based controls to help prevent unauthorized access

Use context-aware controls to prevent unauthorized access

Validate "who is who" across the enterprise and the cloud, help defend against unauthorized access

Identify and protect your "crown jewels"

Discover and classify critical data assets; monitor who is accessing that data and from where

Manage application security risk

Discover and classify applications, help identify and remediate vulnerabilities, address security from day one

End-to-end products and services to protect your critical assets

Identity and Access Management

IAM Assessment and Strategy	Architect and Design	Implement and Deploy	Manage
Process & Method	*Product*	*Assets and Tools*	*People*

IBM Value

Data Security and Privacy

"Crown Jewels" Protection	Discovery and Classification	Database Security	Encryption and DLP

Jane Doe
111-11-XXXX
XXXX

Data Protection Throughout the Data Lifecycle

Application Security

Application Security Management

Test *Applications in Development*	Monitor and Protect *Deployed Applications*

IBM InfoSphere Guardium, IBM Security Identity and Access Manager, IBM Security AppScan, and IBM Services

4 Safeguard cloud and mobile
Employ cloud and mobile initiatives to build a new, stronger security posture

IaaS   PaaS   SaaS
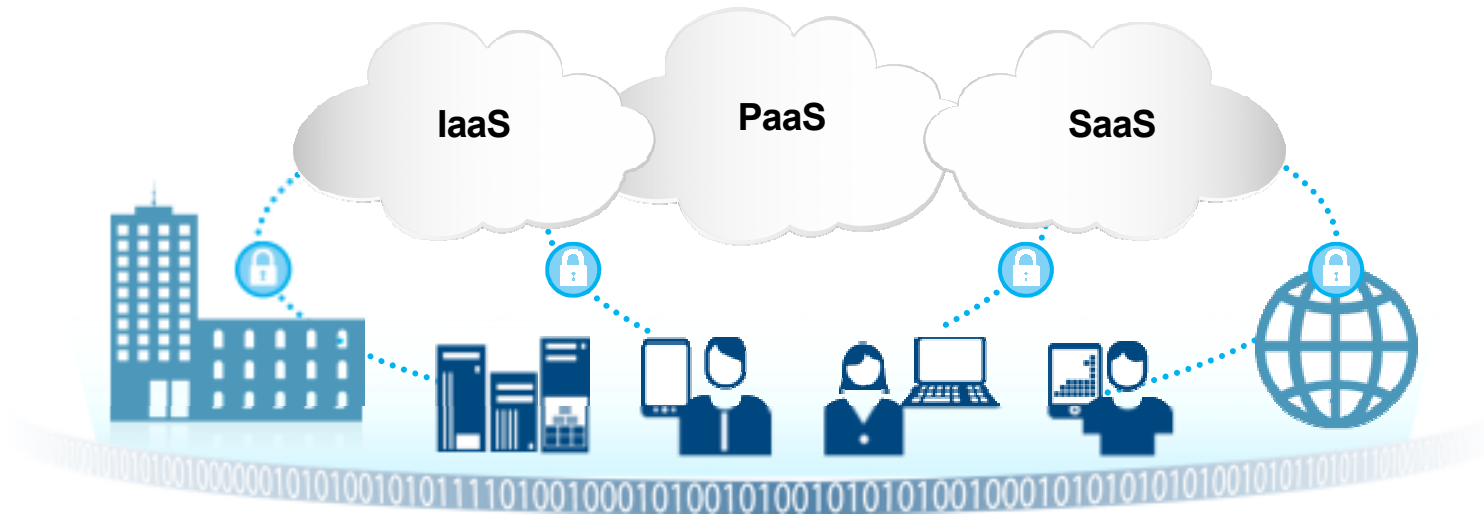
Maintain cloud visibility and control

Manage users, protect data, harden workloads and gain visibility while supporting compliance in the cloud

Help protect the mobile enterprise

Protect devices, content, applications and transactions; address security from day one

Cloud is rapidly transforming the enterprise

Data archive

App development

HR, CRM, SCM

SOFTLAYER
an IBM Company

IBM Bluemix

100+ IBM Offerings

Online website

IaaS
Infrastructure services

PaaS
Development services

SaaS
Business applications

Govern the usage of cloud

Protect workloads and data in the cloud

Detect threats with visibility across clouds
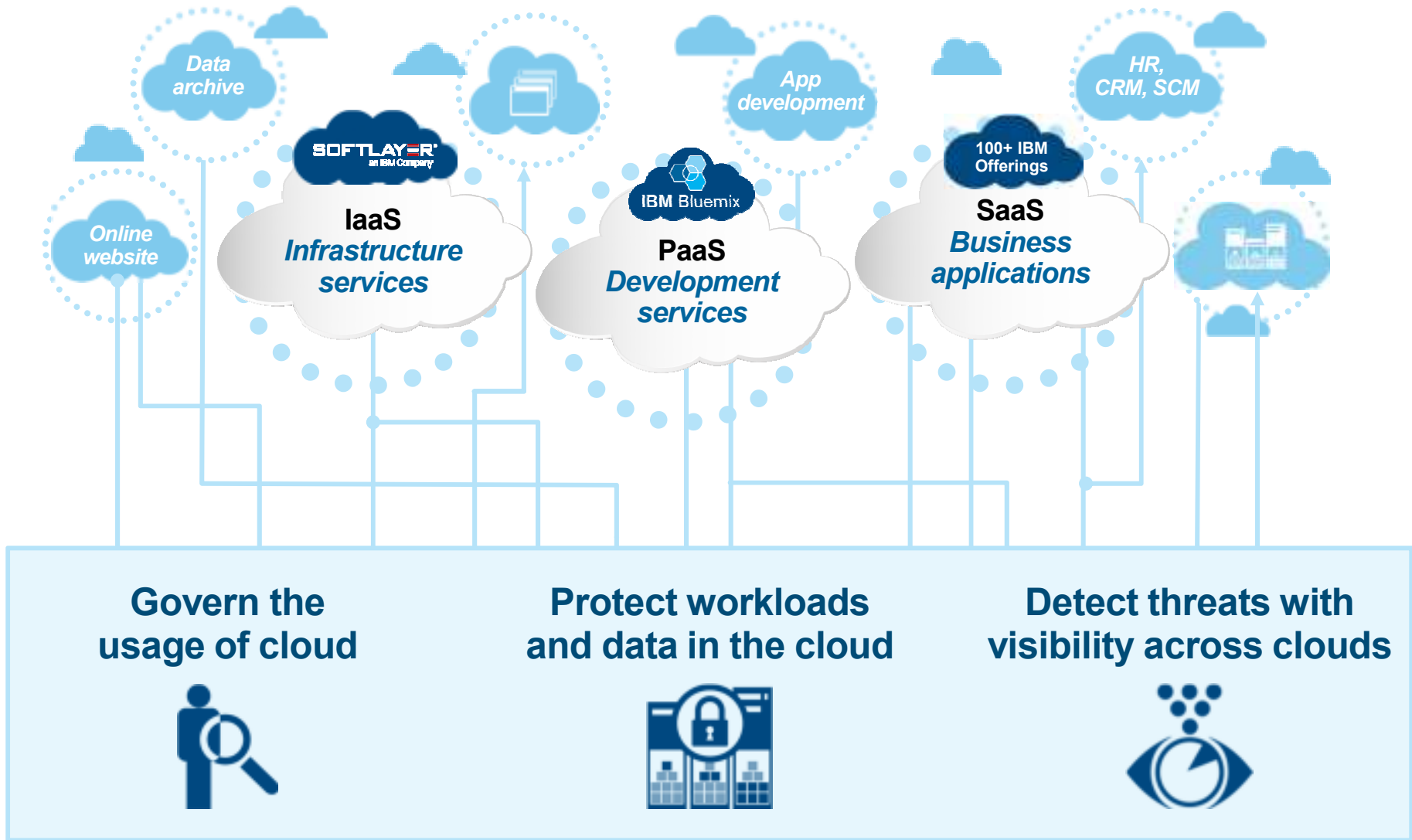
IBM Cloud Security Portfolio

IaaS   PaaS   SaaS
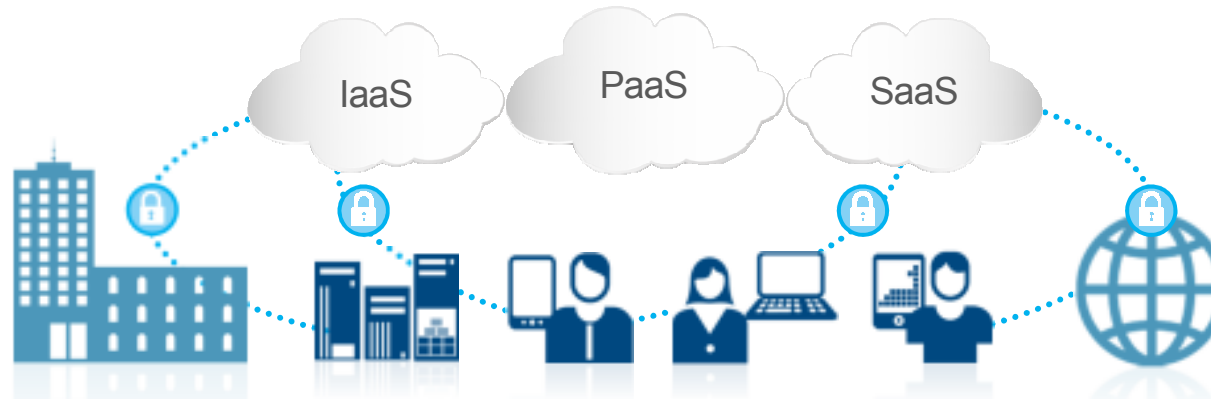
Manage Access	Protect Data	Gain Visibility
Safeguard people, applications, and devices connecting to the cloud	*Identify vulnerabilities and help prevent attacks targeting sensitive data*	*Monitor the cloud for security breaches and compliance violations*
▪ Cloud Identity Services **NEW!** ▪ Cloud Sign On Service **NEW!** ▪ Cloud Access Manager **NEW!** ▪ Cloud Privileged Identity Manager **NEW!**	▪ Cloud Data Activity Monitoring **NEW!** ▪ Cloud Mobile Application Analyzer **NEW!** ▪ Cloud Web Application Analyzer **NEW!**	▪ Cloud Security Intelligence **NEW!**

Optimize Security Operations
Deliver a consolidated view of your security operations – at unprecedented speed and agility

▪ Security Intelligence and Operations Consulting Services **NEW!**

▪ Cloud Security Managed Services **NEW!**

▪ Intelligent Threat Protection Cloud **NEW!**

IBM Security solutions for the mobile enterprise

Device Security	Content Security	Application Security	Transaction Security
• Manage the mobile enterprise with BYOD, BYOA, secure e-mail and document sharing	• Secure file and document sharing across devices and employees including integration with SharePoint	• Instrument applications with security protection by design • Identify vulnerabilities in new, existing or purchased apps	• Secure mobile transactions from customers, partners and suppliers
IBM MaaS360	**IBM MobileFirst Platform**	**IBM Security AppScan**	**IBM Security Access Manager**	**IBM Security Trusteer**

IBM Mobile Security Services

Security Intelligence

Correlate mobile security events with broader infrastructure including log management, anomaly detection and vulnerability management for proactive threat avoidance

IBM QRadar Security Intelligence Platform

IBM has the world's broadest and deepest security portfolio

SECURITY TRENDS	Advanced Threats	Cloud	Mobile and Internet of Things	Compliance Mandates	Skills Shortage

IBM Security Portfolio

Strategy, Risk and Compliance	Cybersecurity Assessment and Response

Security Intelligence and Operations

Advanced Fraud Protection	Identity and Access Management	Data Security	Application Security	Network, Mobile and Endpoint Protection

Advanced Threat and Security Research
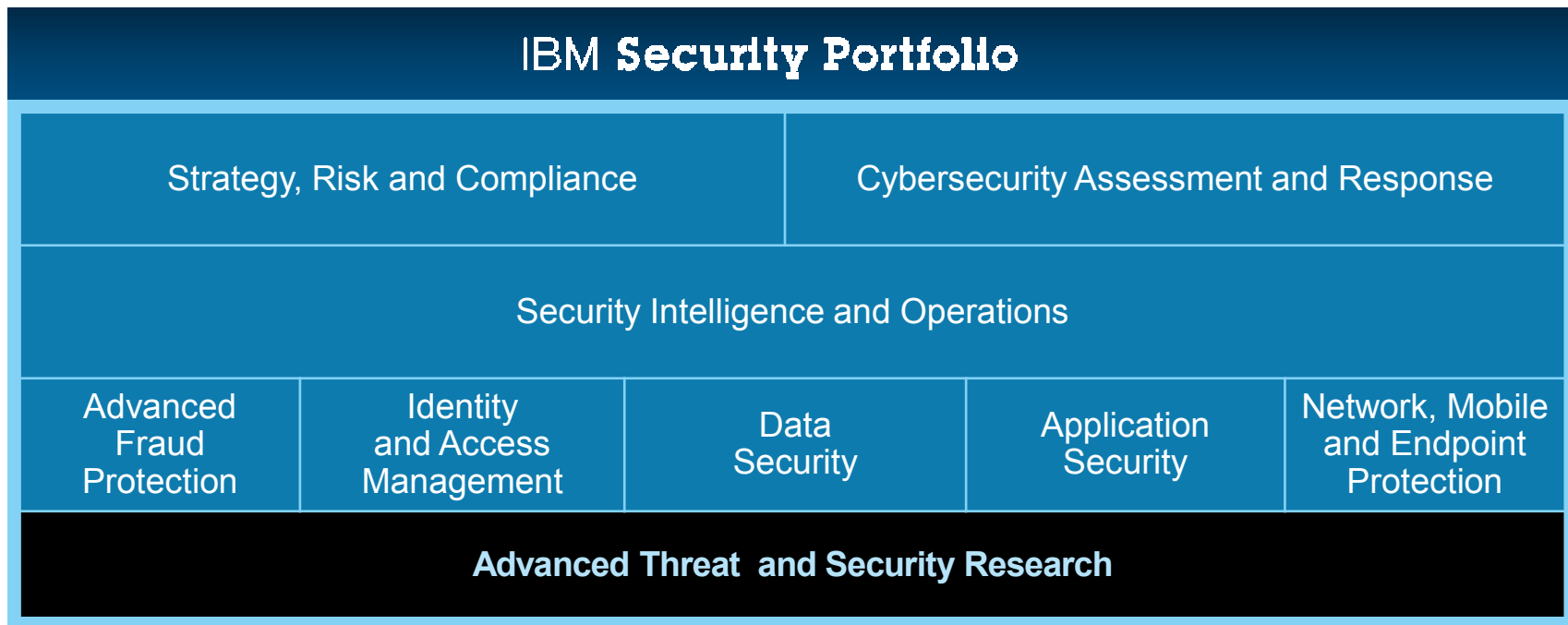
DELIVERY MODELS	Management Consulting	Systems Integration	Integrated Products	Security as a Service	Managed Security	Partner Ecosystem

Analysts have noticed

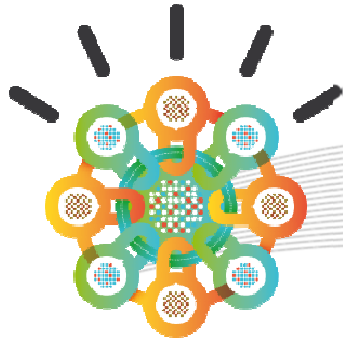| Domain	Market Segment / Report	Gartner Magic Quadrant	Forrester Wave	IDC Market Share / Scape
Security Intelligence	Security Information and Event Management (SIEM)	**Leader** *2014*		**Leader** *2013*
Fraud Protection	Web Fraud Detection *(Trusteer)*	**Leader** *2013*		
Identity and Access Management	Federated Identity Management and Single Sign-On			**Leader** *2013*
	Identity and Access Governance	**Leader** *2015*	**Strong Contender** *2013*	
	Role Management and Access Recertification		**Contender** *2011*	
	Web Access Management (WAM)	**Leader** *2013 MarketScope*		
	Mobile Access Management	**Leader**, *2014 Customer Value, Frost & Sullivan*		
	Identity Provisioning Management	**Leader**, *2014 Leadership Compass, KuppingerCole*		
Data Security	Database Auditing and Real-Time Protection		**Leader** *2011*	
	Data Masking	**Leader** *2014*		
Application Security	Application Security Testing *(dynamic and static)*	**Leader** *2014*	**Leader** *2014*	**Leader** *2013*
Network, Endpoint and Mobile Security	Network Intrusion Prevention Systems (NIPS)	**Challenger** *2014*		
	Endpoint: Client Management Tools	**Leader** *2014*		
	Endpoint Protection Platforms (EPP)	**Visionary** *2014*	**Strong Performer** *2013*	
	Mobile Security *(Fiberlink)*	**Leader** *2014*	**Leader** *2014*	
Consulting and Managed Services	Managed Security Services (MSS)	**Leader** *2014 (AP, NA, WW)*	**Leader** *2014 (NA)*	**Leader** *2014*
	Information Security Consulting Services		**Leader** *2013*	
	Public Cloud Service Providers' Security (IBM Bluemix)		**Strong Contender** *2014*	

Note: Rankings compiled as of January, 2015   ☐ *Rankings not yet available*

IBM Security Systems: Leading solutions in every domain
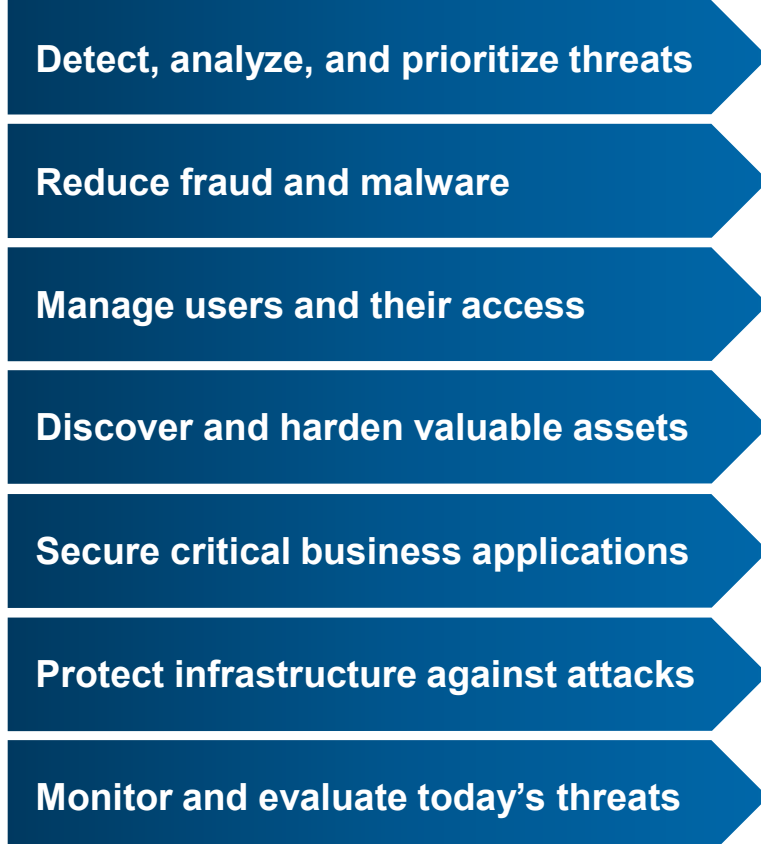
SYSTEMS
Industry-leading security solutions

Security Intelligence and Analytics

Advanced Fraud Protection

People

Data

Applications

Infrastructure

Advanced Security and Threat Research

Detect, analyze, and prioritize threats	**QRadar**
Reduce fraud and malware	**Trusteer**
Manage users and their access	**Identity and Access Management**
Discover and harden valuable assets	**InfoSphere Guardium**
Secure critical business applications	**AppScan**
Protect infrastructure against attacks	**Network and Endpoint Protection**
Monitor and evaluate today's threats	**IBM X-Force**

A new way to think about security

IBM Security

INTELLIGENCE is the new defense
It helps prevent threats faster and make more informed decisions

INTEGRATION is the new foundation
It puts security in context and automates protection

EXPERTISE is the new focus
It is essential to leverage global knowledge and experience to stay ahead

The IBM Security Portfolio

Services
Products

Cybersecurity Assessment and Response

Threat Intelligence Advisory	X-Force Threat Analysis	Penetration Testing	Incident Preparation	Emergency Response

Strategy, Risk and Compliance

Security Maturity Benchmarking	Security Strategy and Roadmap Development	Security Risk Assessment and Program Design	Industrial Controls (NIST, SCADA)	Payment Card Advisory (PCI)

Security Intelligence and Analytics

Emergency Response	Managed SIEM	Incident Planning	Cyber Threat Intel	Security Operations Center Design Services
QRadar SIEM	QRadar Log Manager	QRadar Risk Mgr	QRadar Vulnerability Mgr	QRadar Incident Forensics

Advanced Fraud Protection

Trusteer Rapport	Trusteer Pinpoint Malware Detection	Trusteer Pinpoint ATO Detection	Trusteer Mobile Risk Engine

People	Data	Applications	Network	Infrastructure	Endpoint
Identity Strategy and Assessment	Data Security and Assessment	Embedded Device Testing	Firewall / IDPS / UTM Management		
			Web Protection and Managed DDoS		
User Provisioning and Access Mgmt	Encryption	Penetration Testing	Hosted Web, E-mail and Vulnerability Management		
			Deployment and Migration		
Total Authentication Solution	Data Loss Prevention	Application Security Assessment	Staff Augmentation		
Managed and Cloud Identity		Mobile Application Testing			
Identity and Access Governance	Guardium Data Security	AppScan Source	Network Intrusion Prevention		Trusteer Apex
Identity and Access Management	Guardium Database Vulnerability Mgmt	AppScan Dynamic	Next Generation Network Protection		Mobile & Endpoint Management
Privileged Identity Management	Guardium / Optim Data Masking	DataPower SOA Security	SiteProtector Threat Management		Virtualization and Server Security
Federated Access and SSO	Key Lifecycle Manager	Security Policy Manager	Network Anomaly Detection		Mainframe Security

IBM X-Force and Trusteer Threat Intelligence

Learn more about IBM Security
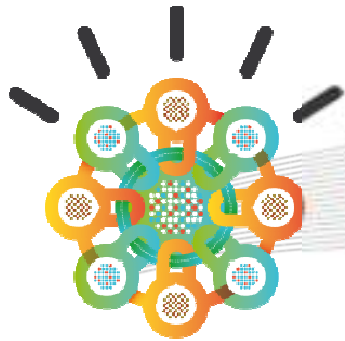
IBM Security
Intelligence. Integration. Expertise.

TOP 3 enterprise security software vendor in total revenue

20 industry analyst reports rank IBM Security as a **LEADER**

133 countries where IBM delivers managed security services

10K clients protected *including*…

24 of the top 33 banks in Japan, North America, and Australia

Visit our website
IBM Security Website

Watch our videos
IBM Security YouTube Channel

Read new blog posts
SecurityIntelligence.com

Follow us on Twitter
@ibmsecurity

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, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, 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 ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Thank You

www.ibm.com/security

IBM