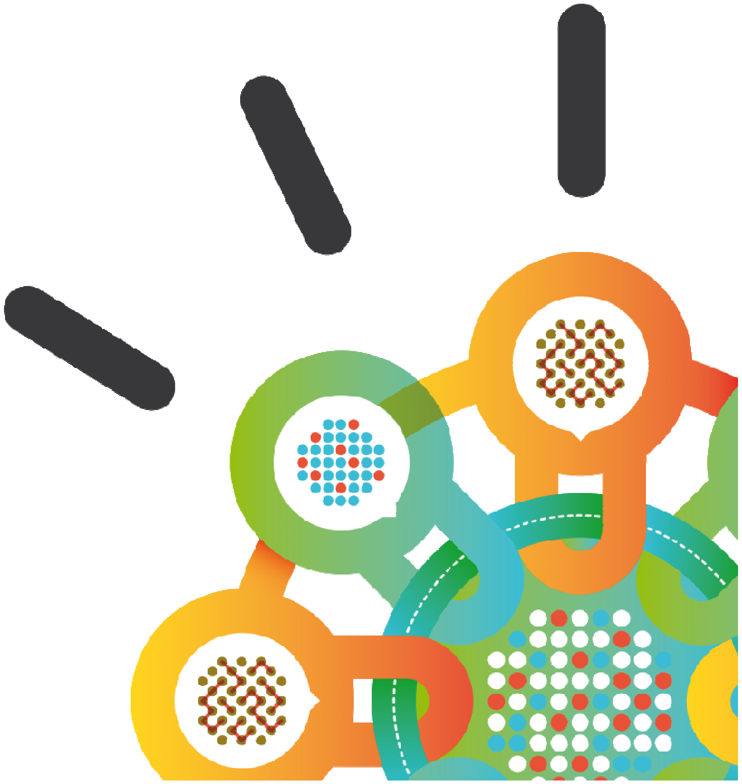
Security Intelligence.
Think Integrated.

# IBM Security Systems

*Business Partner Meeting*

*2. / 3. Juli, München*



© 2014 IBM Corporation

# Agenda – Tag 1

| | |
|---|---|
| 11:00 | Begrüßung |
| 11:15 | State of the Union |
| 11:45 | Prevent. Detect. Respond. |
| 12:30 | Mittagspause |
| 13:30 | APT Abwehr und Malware Blocking – Trusteer Apex |
| 14:30 | QRadar Incident Forensics |
| 15:45 | Pause |
| 16:15 | IT Compliance und ISO 27001 |
| 17:15 | Q&A |
| | |
| 19:00 | Abendveranstaltung |

© 2014 IBM Corporation

# Agenda – Tag 2

| | |
|---|---|
| 09:00 | IAM, Lösungen für Cloud und Mobile Access |
| 10:00 | Security für die Cloud |
| 11:00 | Pause |
| 11:30 | Appscan 9.0 |
| 12:30 | Software Group Services |
| 13:15 | Q & A anschließend Gemeinsames Mittagessen |

© 2014 IBM Corporation

# IBM Security Offers a Comprehensive Product Portfolio

| Security Intelligence and Analytics | | | | |
|---|---|---|---|---|
| QRadar Log Manager | QRadar SIEM | QRadar Risk Manager | QRadar Vulnerability Manager | 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 Manager | Guardium Database Activity Monitoring | AppScan Source | Network Intrusion Prevention (GX) | Trusteer Apex |
| Access Manager Family | Guardium Encryption Expert | AppScan Enterprise / Standard | Next Generation Network Protection (XGS) | FiberLink MaaS360 |
| Privileged Identity Manager | Guardium / Optim Data Masking | DataPower Web Security Gateway | SiteProtector Threat Management | Endpoint Manager |
| Federated Identity Management | Key Lifecycle Manager | Security Policy Manager | QRadar Network Anomaly Detection | Host Protection |
| Directory Integrator / Directory Server | | | | zSecure |

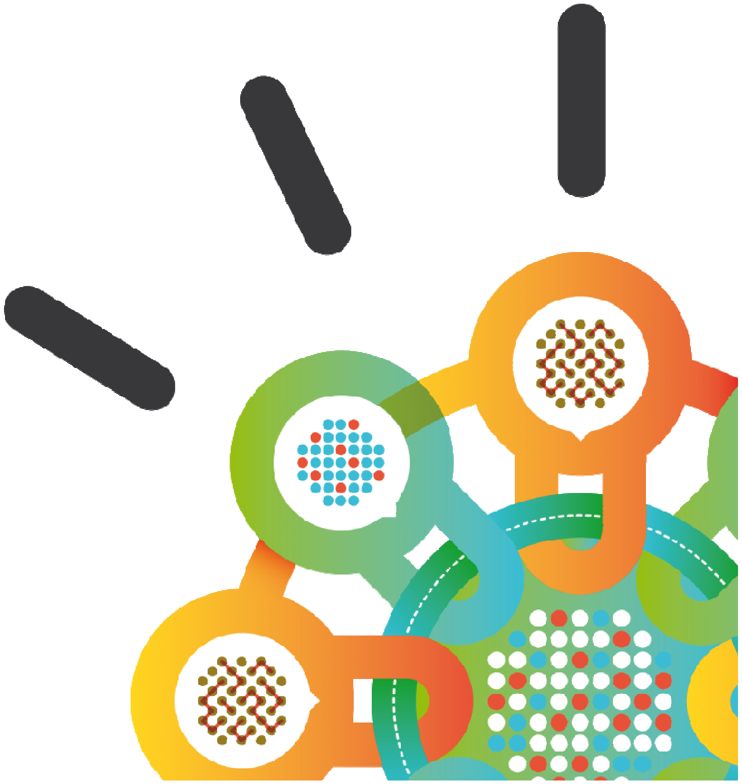
**IBM X-Force Research**

© 2014 IBM Corporation

Security Intelligence.
Think Integrated.

# IBM Threat Protection System

*A dynamic, integrated system to disrupt the lifecycle of advanced attacks and prevent loss*



© 2014 IBM Corporation

# We are in an era of continuous breaches

*Attackers are relentless, victims are targeted, and the damage toll is rising*

### Operational Sophistication

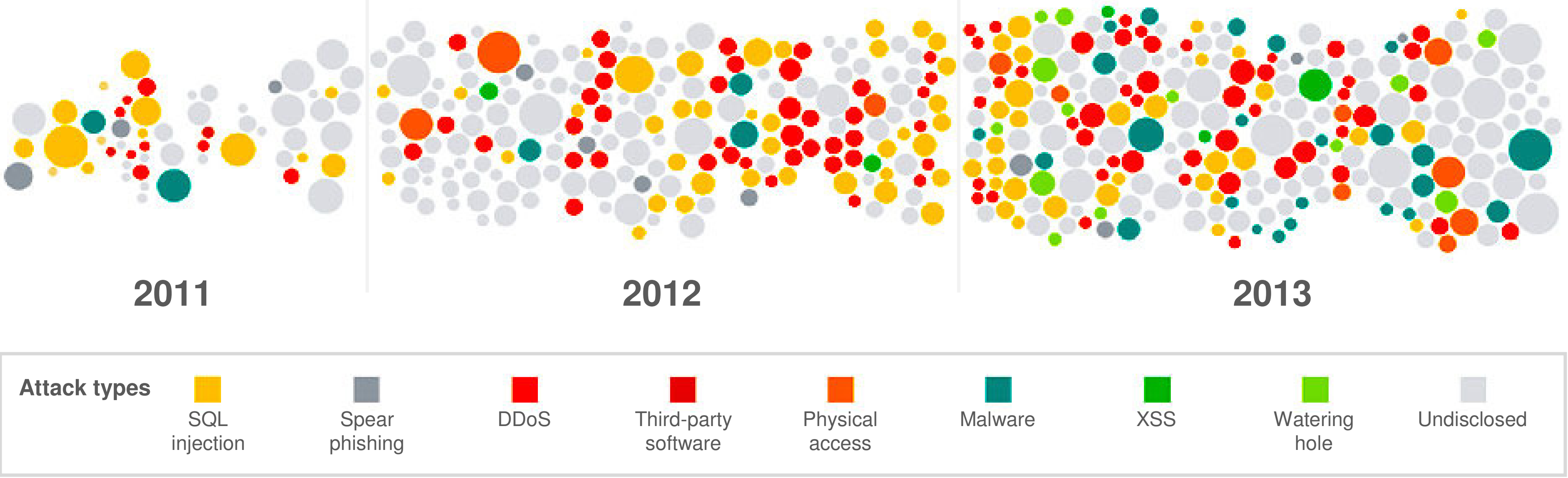
IBM X-Force® declared **Year of the Security Breach**

### Near Daily Leaks of Sensitive Data

**40% increase** in reported data breaches and incidents

### Relentless Use of Multiple Methods

**500,000,000+ records** were leaked, while the future shows no sign of change



Source: IBM X-Force Threat Intelligence Quarterly – 1Q 2014

*Note: Size of circle estimates relative impact of incident in terms of cost to business.*

# Was ist besonders bei Advanced Persistent Threats?

## Advanced

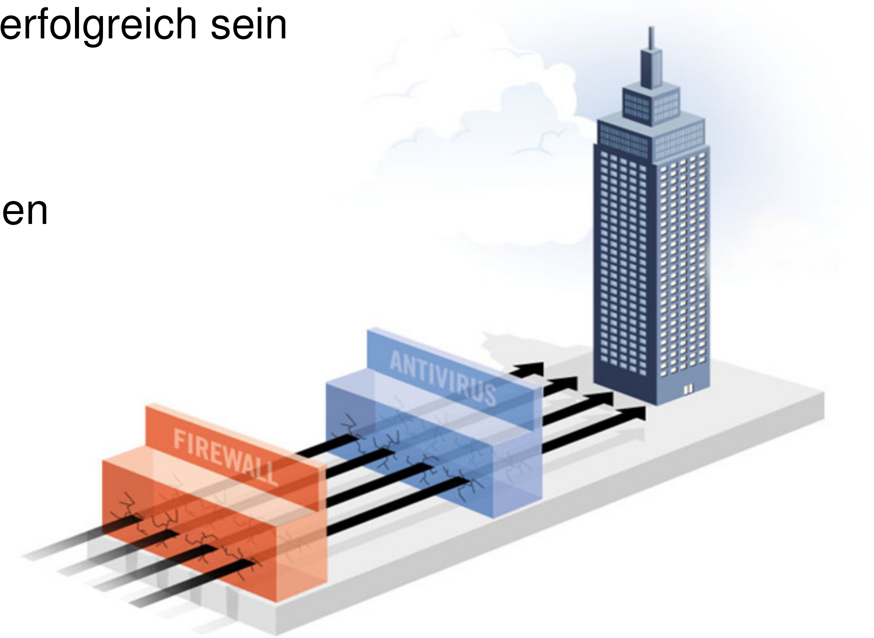
- Ausnutzen unbekannter (zero-day) Schwachstellen
- Erweiterte, angepasste “Malware” die nicht von AV Lösungen erkannt wird
- Koordinierte, hoch entwickelte Angriffe, die mehrere Module verwenden

## Persistent

- Lange Angriffslaufzeiten (Durschschnitt: 1 Jahr; Längster bisher 4.8 Jahre)[1]
- Angreifer sind auf ein Ziel gerichtet – Sie werden erfolgreich sein

## Threat

- Zielgerichtet auf bestimmte Personen oder Gruppen um interessante Daten zu erhalten
- So wenig auffallen, wie möglich

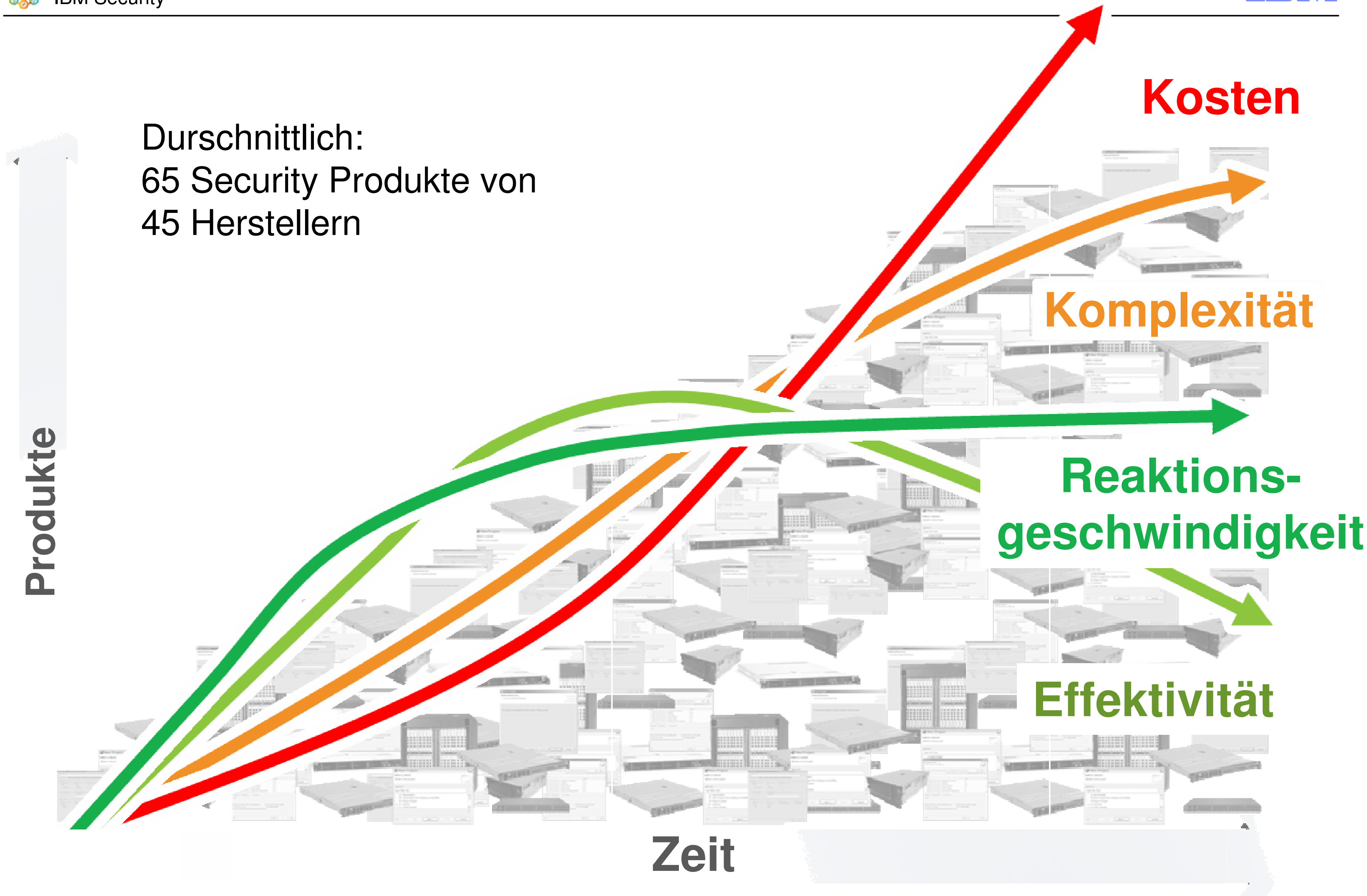


[1] Source: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

© 2014 IBM Corporation

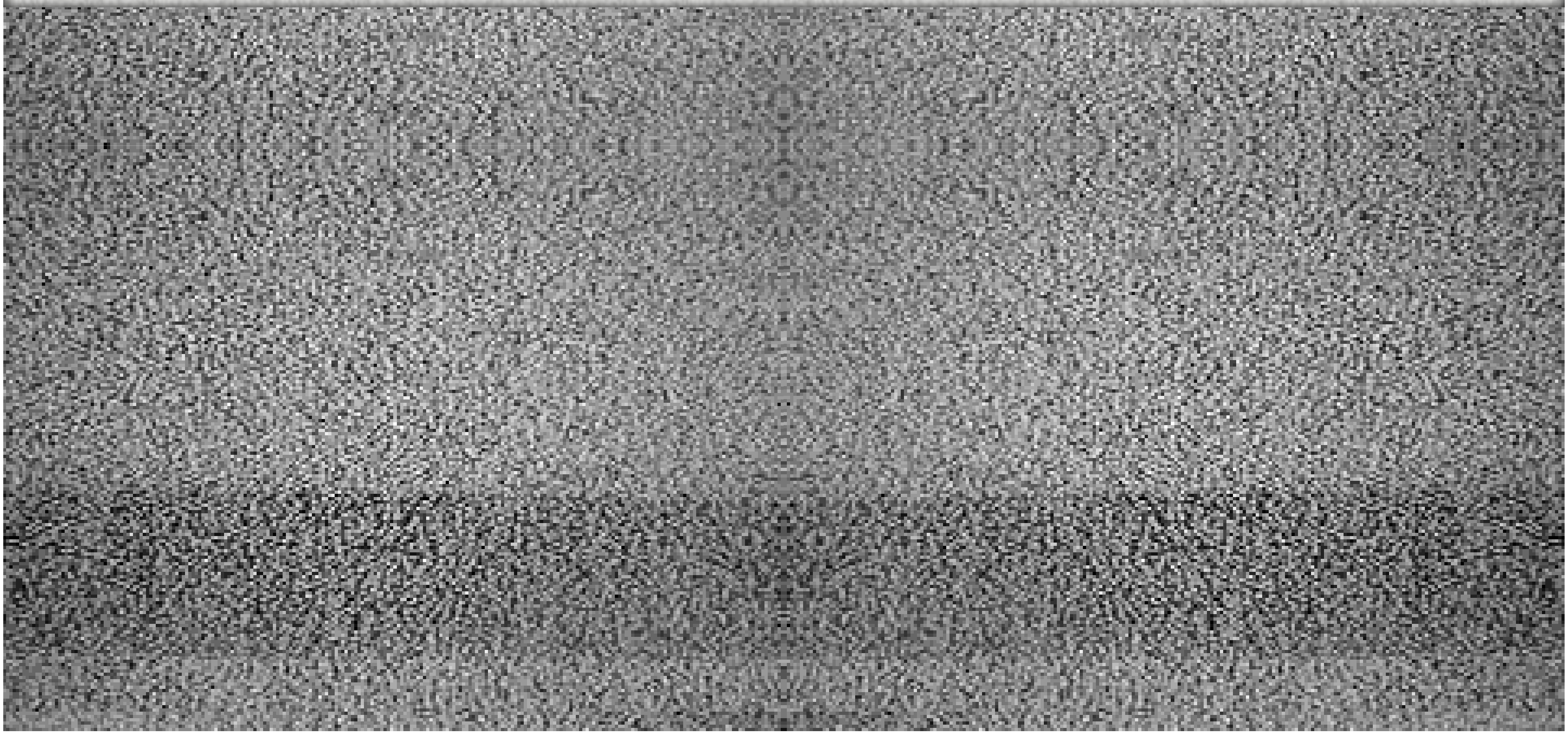
Products
Time

Durschnittlich:
65 Security Produkte von
45 Herstellern

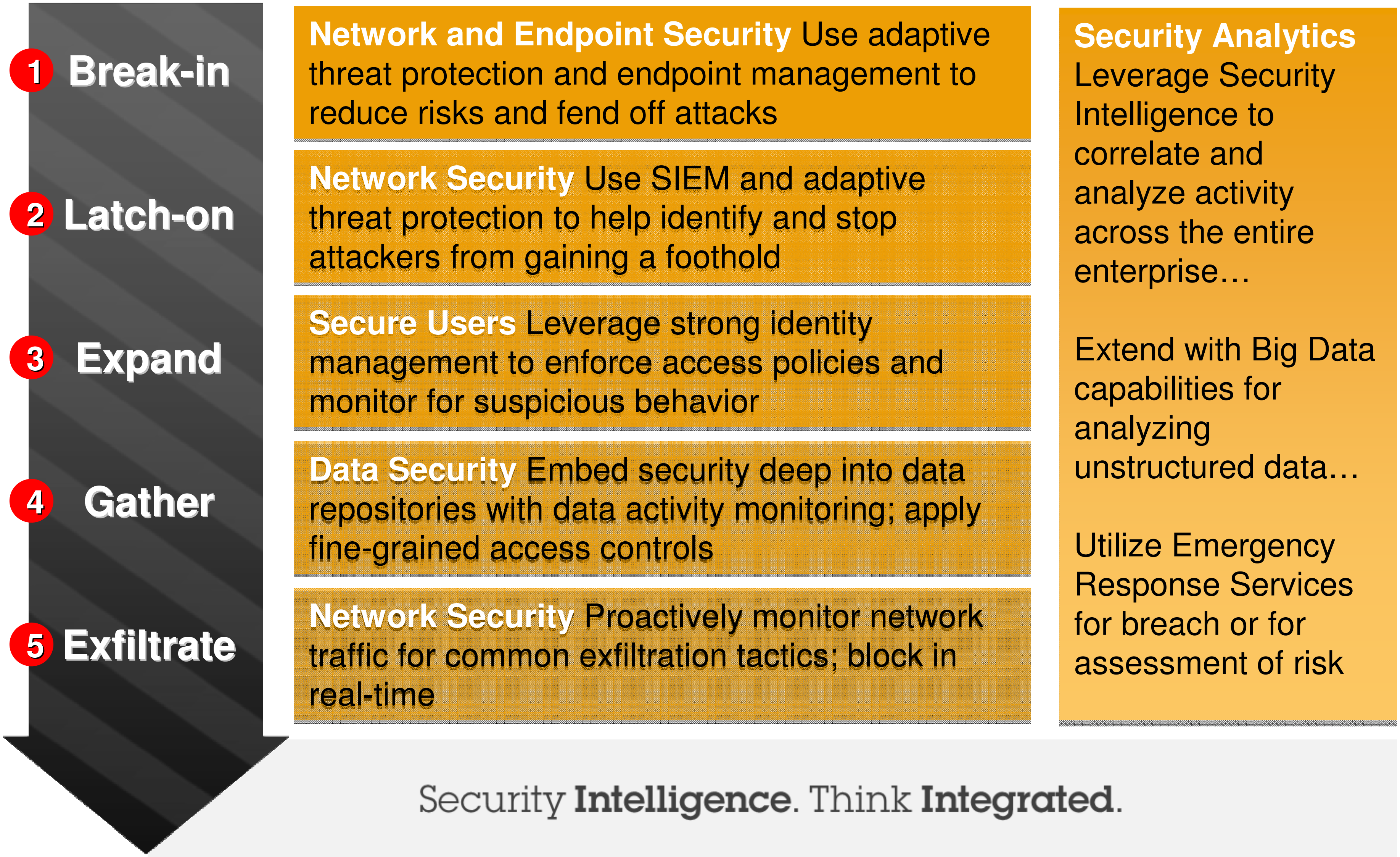


© 2014 IBM Corporation

# Ihr Security Team sieht nur Rauschen



# IBM's approach to defending against state-sponsored attacks



1 Break-in

**Network and Endpoint Security** Use adaptive threat protection and endpoint management to reduce risks and fend off attacks

2 Latch-on

**Network Security** Use SIEM and adaptive threat protection to help identify and stop attackers from gaining a foothold

3 Expand

**Secure Users** Leverage strong identity management to enforce access policies and monitor for suspicious behavior

4 Gather

**Data Security** Embed security deep into data repositories with data activity monitoring; apply fine-grained access controls

5 Exfiltrate

**Network Security** Proactively monitor network traffic for common exfiltration tactics; block in real-time

**Security Analytics** Leverage Security Intelligence to correlate and analyze activity across the entire enterprise…

Extend with Big Data capabilities for analyzing unstructured data…

Utilize Emergency Response Services for breach or for assessment of risk

Security **Intelligence**. Think **Integrated**.

© 2014 IBM Corporation

# Four truths about advanced threat protection

*Despite increasing challenges, organizations can protect themselves by adopting the right strategy*

## 1 Prevention is mandatory

Traditional methods of prevention have often failed, leaving many to believe detection is the only way forward. This is a dangerous proposition.

## 2 Security Intelligence is the underpinning

Specialized knowledge in one domain is not enough. It takes enterprise-wide visibility and maximum use of data to stop today's threats.

## 3 Integration enables protection

The best defense is relentless improvement. Technologies must seamlessly integrate with processes and people across the entire lifecycle of attacks.

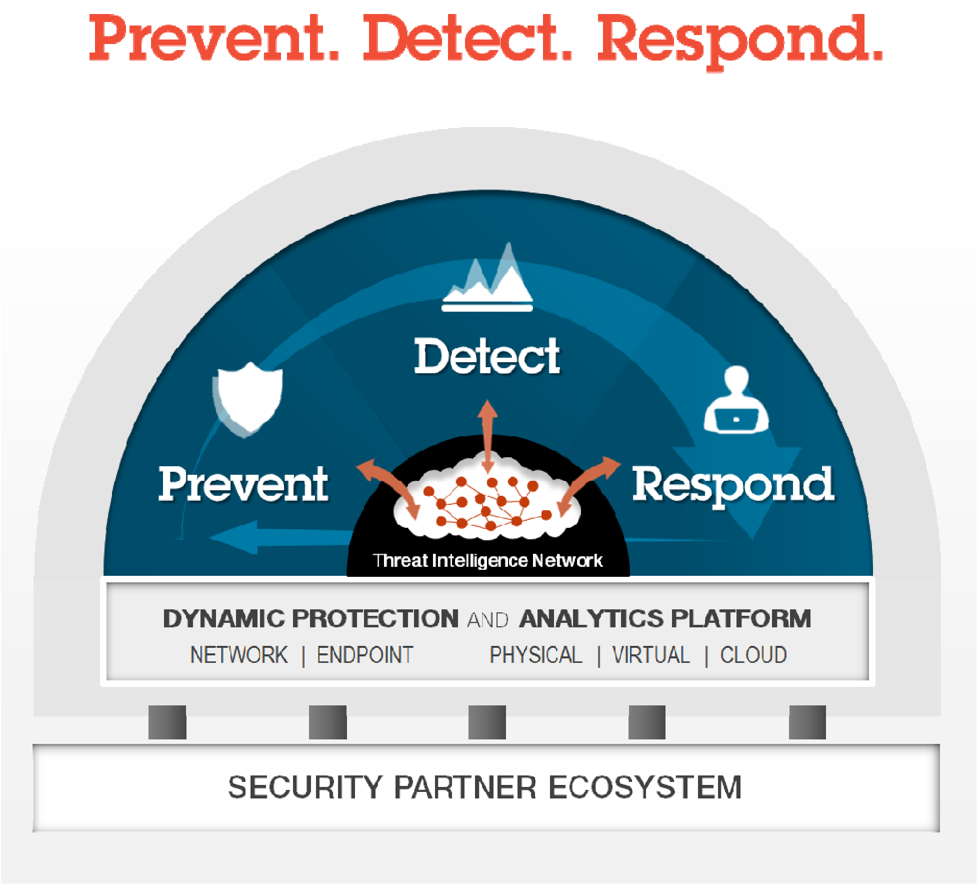
## 4 Openness must be embraced

Security teams need the ability to share context and invoke actions between communities of interest and numerous new and existing security investments.

© 2014 IBM Corporation

# Introducing the IBM Threat Protection System

*A dynamic, integrated system to disrupt the lifecycle of advanced attacks and prevent loss*


Prevent. Detect. Respond.
Detect
Prevent
Respond
Threat Intelligence Network
DYNAMIC PROTECTION AND ANALYTICS PLATFORM
NETWORK | ENDPOINT
PHYSICAL | VIRTUAL | CLOUD
SECURITY PARTNER ECOSYSTEM

***Made possible by the following:***

## Accelerated Roadmap

*Significant investment across 10 development labs to fast-track advanced threat protection offerings*

## Unique Integrations

*Strategic focus on connecting IBM products to streamline intelligence sharing and take action*

## New Partnerships

*Coordinated outreach across the industry to bring together interoperable products for our customers*

© 2014 IBM Corporation

# Focus on critical points in the attack chain with preemptive defenses on both the endpoint and network

| | Exploit Disruption | Malware Quarantine | User Protection |
|---|---|---|---|
| Trusteer Apex Malware Protection<br>On the Endpoint | **Prevent malware installs**<br>•Verify the state of applications<br>•Block exploit attempts used to deliver malware | **Prevent control channels**<br>•Stop direct outbound malware communications<br>•Protect against process hijacking | **Prevent credential loss**<br>•Block keyloggers<br>•Stop credential use on phishing sites<br>•Limit reuse of passwords |
| On the Network<br>IBM Security Network Protection XGS | **Prevent mutated exploits**<br>•Verify the state of network protocols<br>•Block unknown exploits with behavioral heuristics | **Prevent active beaconing**<br>•Stop malware and botnet control traffic with real-time reputation and SSL inspection | **Prevent malicious apps**<br>•Block access to malicious websites<br>•Prevent web application misuse |

# IBM Security Network Protection (XGS)

*Unprecedented levels of network security, visibility and control*

- **Protection from sophisticated and constantly evolving threats**
  - Behavioral detection fights 0-day attacks
  - Protects against entire classes of vulnerabilities
- **Discover and disrupt previously unknown threats on the network**
  - Shows application and web use by user
  - Detects and blocks malicious traffic
  - Policy-based monitoring and blocking
  - 20B URL database now includes Trusteer ENHANCED
- **Seamless deployment and integration**
  - Flexible performance, interfaces and options
  - Ability to send flow data feeds to QRadar NEW
  - Receive quarantine triggers from QRadar

NSS LABS

*Ranked 2nd out of 10 IPS vendors for blocking exploits in 2013 group test*

*Received ICSA certification for Network IPS and PAM engine in 2013*

TEST REPORT Tolly.

*Provided superior protection from mutated threats vs. SNORT engine*

INFO~TECH RESEARCH GROUP

*Ranked "Champion" in latest IDPS vendor landscape report*

> *"…IBM performed extremely well in this testing, achieving an overall score of 95.7%. This speaks to the ability of the IBM IPS to perform against the types of constantly evolving threats that are often seen in today's networks."*
> Vikram Phatak, Chairman and CEO of NSS Labs

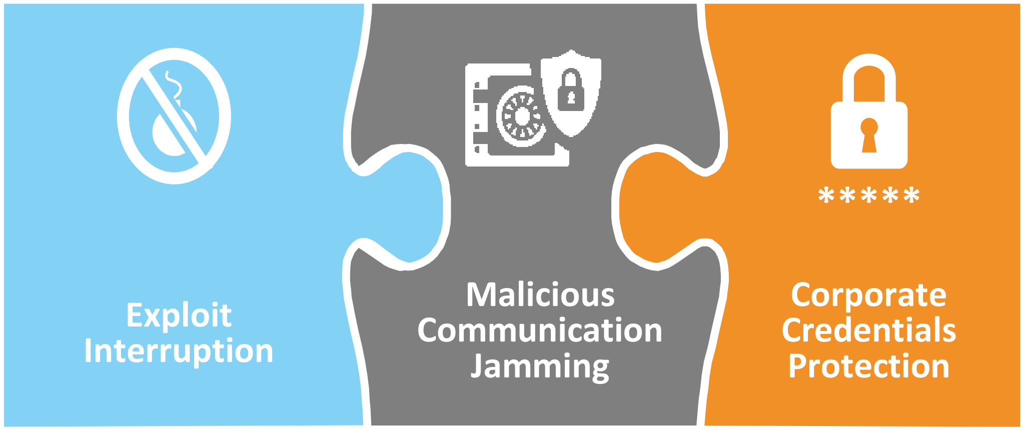
© 2014 IBM Corporation

# Trusteer Apex

*Malware Prevention Utilizing Three Layers of Protection*

- **Exploit Interruption**
  - Stop exploitation of user application vulnerabilities
  - Prevent drive-by downloads
- **Malicious Communication Jamming**
  - Block malware communication
  - Prevent information theft
- **Corporate Credentials Protection**
  - Block key-loggers
  - Prevent submission on phishing sites
  - Prevent reuse on public consumer sites
- **New Capabilities**
  - Java lockdown protection
  - Cloud-based file inspection
  - QRadar integration

NEW


*****
Exploit Interruption
Malicious Communication Jamming
Corporate Credentials Protection

© 2014 IBM Corporation

# Continuously monitor security-relevant activity from across the entire organization

### Predict and prioritize security weaknesses before adversaries do

•Use automated vulnerability scans and rich security context

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

Pre-Attack Analytics

**IBM Security QRadar Vulnerability Manager**

**IBM Security QRadar Security Intelligence Platform**

### Detect activity and anomalies outside normal behavior

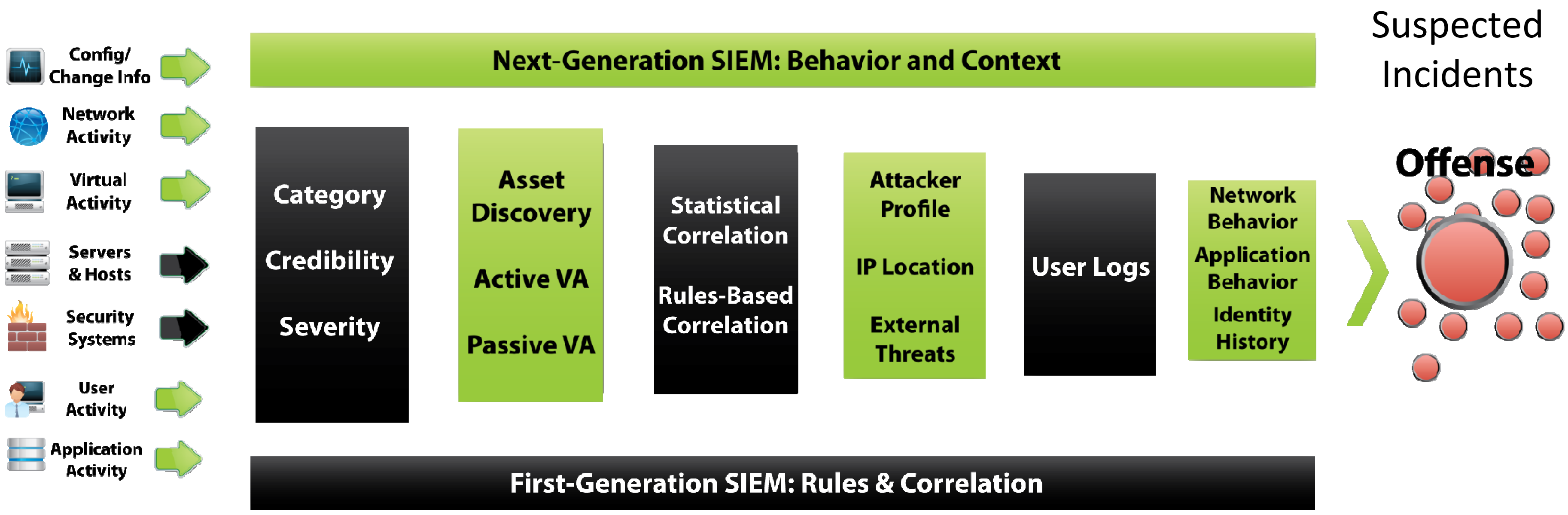
•Correlate and baseline massive sets of data

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

Real-time Attack Analytics

**IBM Security QRadar SIEM**

# QRadar Next-Generation SIEM: Security Intelligence

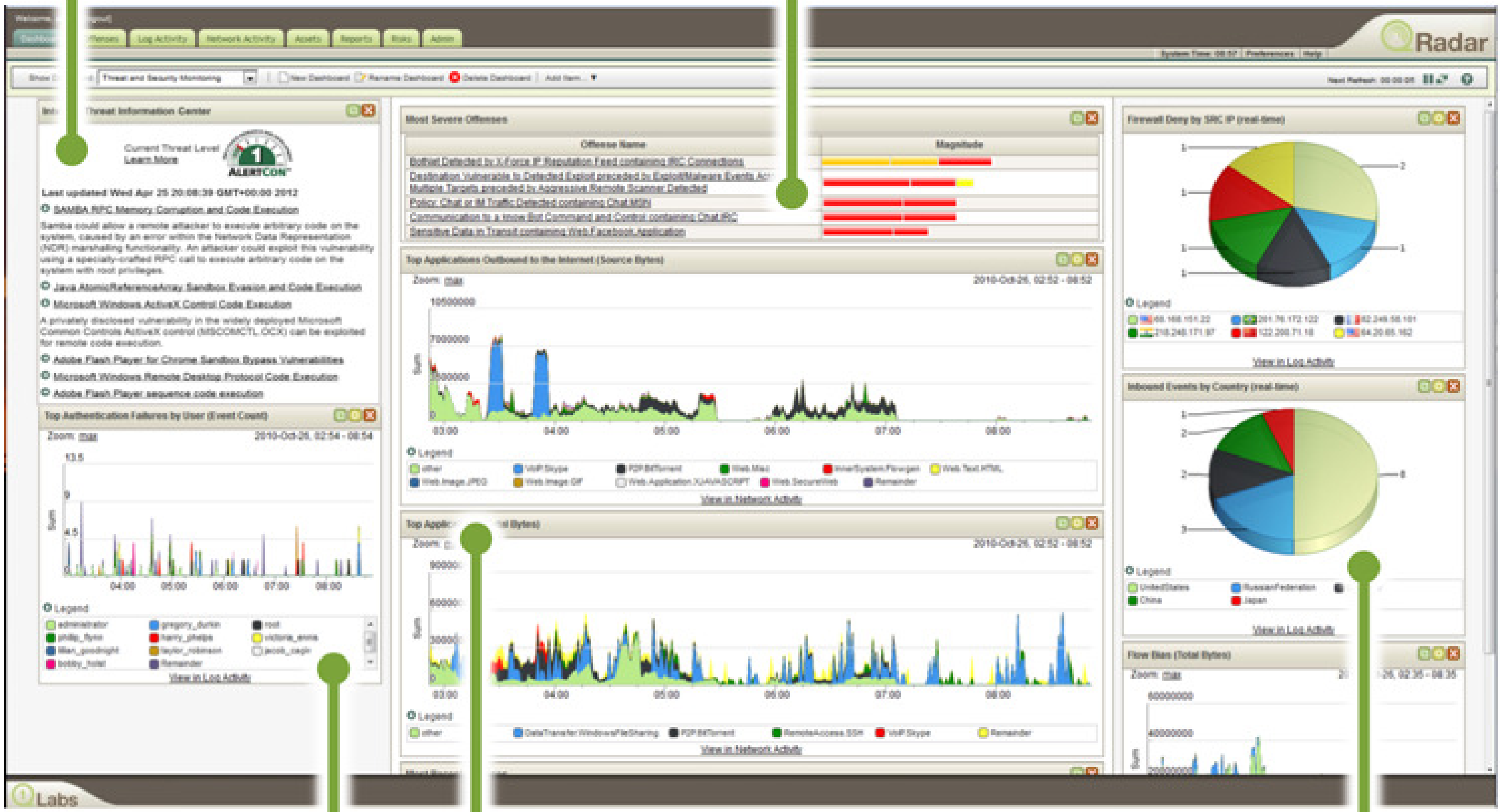


© 2014 IBM Corporation

# Dashboard

IBM X-Force® Threat Information Center

Real-time Security Overview w/ IP Reputation Correlation



Threat Information Center

Current Threat Level
Learn More

1 ALERTCON

Last updated Wed Apr 25 20:08:39 GMT+00:00 2012

- SAMBA RPC Memory Corruption and Code Execution

Samba could allow a remote attacker to execute arbitrary code on the system, caused by an error within the Network Data Representation (NDR) marshalling functionality. An attacker could exploit this vulnerability using a specially-crafted RPC call to execute arbitrary code on the system with root privileges.

- Java AtomicReferenceArray Sandbox Evasion and Code Execution
- Microsoft Windows ActiveX Control Code Execution

A privately disclosed vulnerability in the widely deployed Microsoft Common Controls ActiveX control (MSCOMCTL.OCX) can be exploited for remote code execution.

- Adobe Flash Player for Chrome Sandbox Bypass Vulnerabilities
- Microsoft Windows Remote Desktop Protocol Code Execution
- Adobe Flash Player sequence code execution

Most Severe Offenses

| Offense Name | Magnitude |
|---|---|
| Botnet Detected by X-Force IP Reputation Feed containing IRC Connections | |
| Destination Vulnerable to Detected Exploit preceded by Exploit/Malware Events Ac<br>Multiple Targets preceded by Aggressive Remote Scanner Detected | |
| Policy: Chat or IM Traffic Detected containing Chat MSN | |
| Communication to a know Bot Command and Control containing Chat IRC | |
| Sensitive Data in Transit containing Web.Facebook.Application | |

Identity and User Context

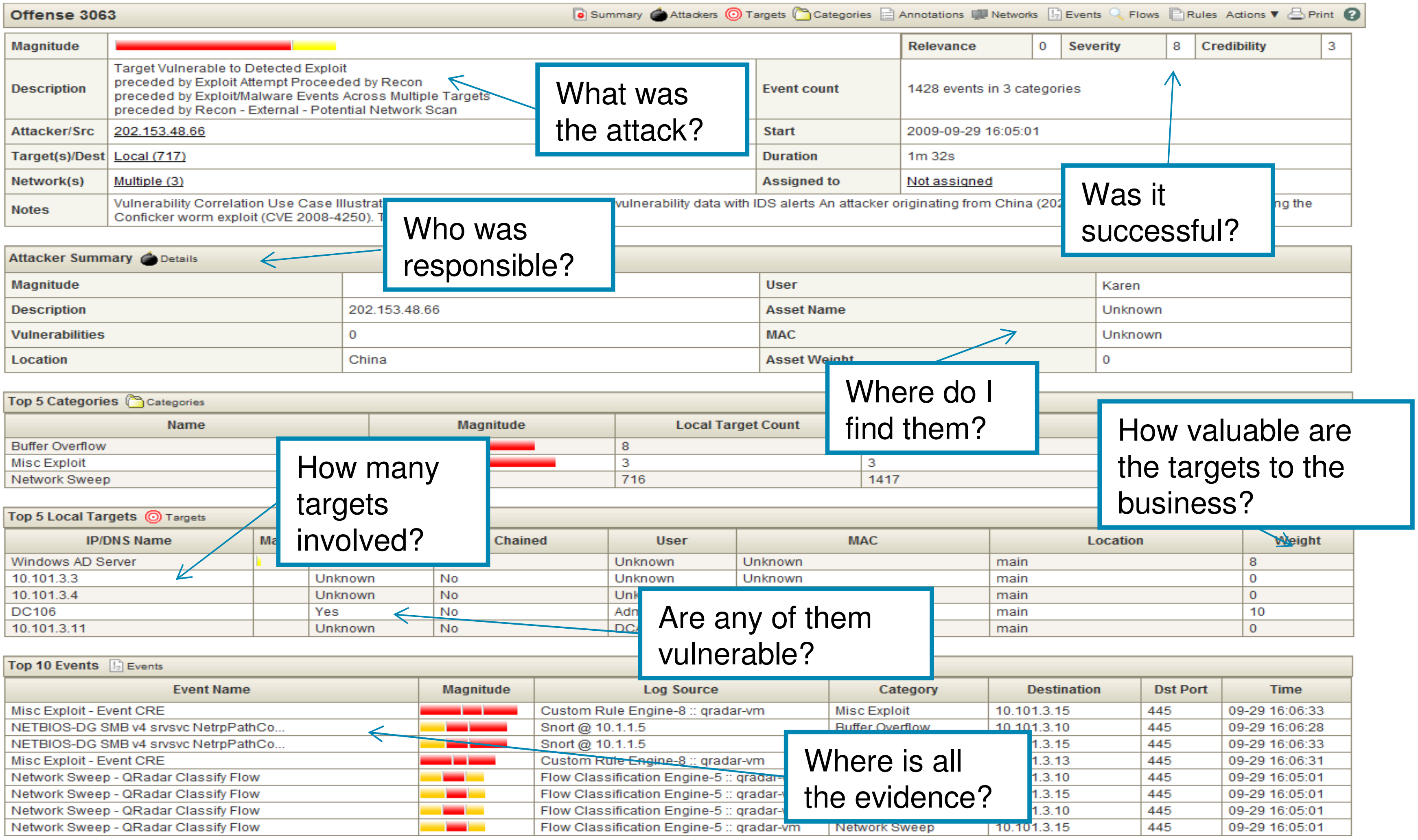
Real-time Network Visualization and Application Statistics

Inbound Security Events

© 2014 IBM Corporation

# *QRadar SIEM* Offense Management

## Klare, detaillierte und vollständige Informationen :



**Offense 3063**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Magnitude | 🟥🟨 | | Relevance | 0 | Severity | 8 | Credibility 3 |
| Description | Target Vulnerable to Detected Exploit<br>preceded by Exploit Attempt Proceeded by Recon<br>preceded by Exploit/Malware Events Across Multiple Targets<br>preceded by Recon - External - Potential Network Scan | Event count | 1428 events in 3 categories | | | | |
| Attacker/Src | 202.153.48.66 | Start | 2009-09-29 16:05:01 | | | | |
| Target(s)/Dest | Local (717) | Duration | 1m 32s | | | | |
| Network(s) | Multiple (3) | Assigned to | Not assigned | | | | |
| Notes | Vulnerability Correlation Use Case Illustrat vulnerability data with IDS alerts An attacker originating from China (202 ng the<br>Conficker worm exploit (CVE 2008-4250). T | | | | | | |

What was the attack?

Was it successful?

**Attacker Summary** Details

| | | | |
|---|---|---|---|
| Magnitude | | User | Karen |
| Description | 202.153.48.66 | Asset Name | Unknown |
| Vulnerabilities | 0 | MAC | Unknown |
| Location | China | Asset Weight | 0 |

Who was responsible?

Where do I find them?

**Top 5 Categories** Categories

| Name | Magnitude | Local Target Count | |
|---|---|---|---|
| Buffer Overflow | 🟥 | 8 | |
| Misc Exploit | 🟥 | 3 | 3 |
| Network Sweep | | 716 | 1417 |

How many targets involved?

How valuable are the targets to the business?

**Top 5 Local Targets** Targets

| IP/DNS Name | Ma | | Chained | User | MAC | Location | Weight |
|---|---|---|---|---|---|---|---|
| Windows AD Server | 🟨 | | | Unknown | Unknown | main | 8 |
| 10.101.3.3 | | Unknown | No | Unknown | Unknown | main | 0 |
| 10.101.3.4 | | Unknown | No | Unk | | main | 0 |
| DC106 | | Yes | No | Adm | | main | 10 |
| 10.101.3.11 | | Unknown | No | DC/ | | main | 0 |

Are any of them vulnerable?

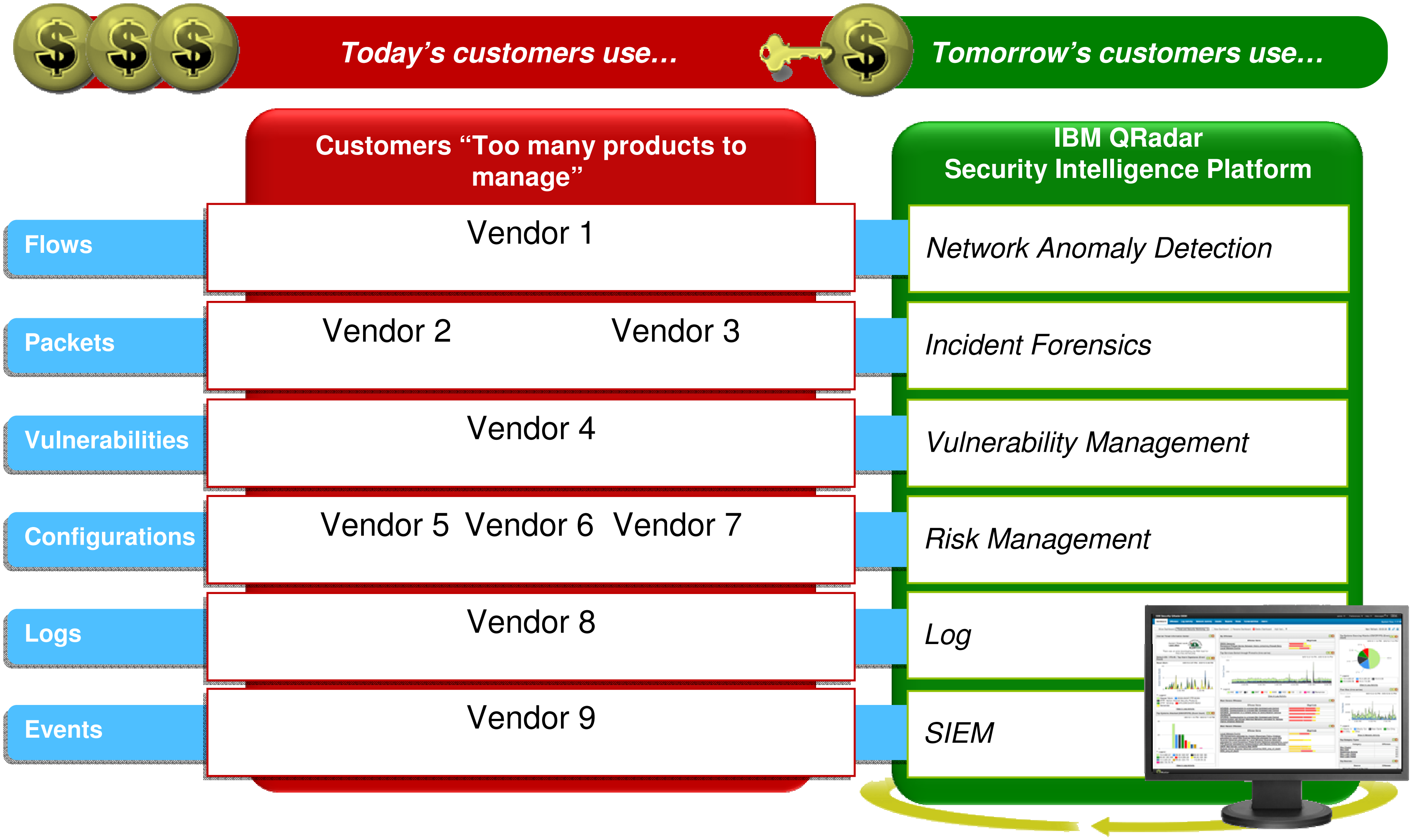
**Top 10 Events** Events

| Event Name | Magnitude | Log Source | Category | Destination | Dst Port | Time |
|---|---|---|---|---|---|---|
| Misc Exploit - Event CRE | 🟥🟥🟥 | Custom Rule Engine-8 :: qradar-vm | Misc Exploit | 10.101.3.15 | 445 | 09-29 16:06:33 |
| NETBIOS-DG SMB v4 srvsvc NetrPathCo... | 🟨🟥🟥 | Snort @ 10.1.1.5 | Buffer Overflow | 10.101.3.10 | 445 | 09-29 16:06:28 |
| NETBIOS-DG SMB v4 srvsvc NetrPathCo... | 🟨🟥🟥 | Snort @ 10.1.1.5 | | 1.3.15 | 445 | 09-29 16:06:33 |
| Misc Exploit - Event CRE | 🟥🟥🟥 | Custom Rule Engine-8 :: qradar-vm | | 1.3.13 | 445 | 09-29 16:06:31 |
| Network Sweep - QRadar Classify Flow | 🟨🟥🟨 | Flow Classification Engine-5 :: qradar- | | 1.3.10 | 445 | 09-29 16:05:01 |
| Network Sweep - QRadar Classify Flow | 🟨🟥🟨 | Flow Classification Engine-5 :: qradar- | | 1.3.15 | 445 | 09-29 16:05:01 |
| Network Sweep - QRadar Classify Flow | 🟨🟥🟨 | Flow Classification Engine-5 :: qradar- | | 1.3.10 | 445 | 09-29 16:05:01 |
| Network Sweep - QRadar Classify Flow | 🟨🟥🟨 | Flow Classification Engine-5 :: qradar-vm | Network Sweep | 10.101.3.15 | 445 | 09-29 16:05:01 |

Where is all the evidence?

© 2014 IBM Corporation

# Consolidate and integrate to reduce complexity and cost



*Today's customers use…*

*Tomorrow's customers use…*

**Customers "Too many products to manage"**

- **Flows**: Vendor 1
- **Packets**: Vendor 2, Vendor 3
- **Vulnerabilities**: Vendor 4
- **Configurations**: Vendor 5, Vendor 6, Vendor 7
- **Logs**: Vendor 8
- **Events**: Vendor 9

**IBM QRadar Security Intelligence Platform**

- *Network Anomaly Detection*
- *Incident Forensics*
- *Vulnerability Management*
- *Risk Management*
- *Log*
- *SIEM*

© 2014 IBM Corporation

# IBM Security QRadar SIEM

*Web-based command console for Security Intelligence*

QRadar® SIEM

- **Delivers actionable insight focusing security teams on high probability incidents**
  - – Employs rules-based correlation of events, flows, assets, topologies, and vulnerabilities
- **Detects and tracks malicious activity over extended time periods, helping uncover advanced threats often missed by other solutions**
  - – Consolidates ‘big data’ security incidents within purpose-built, federated database repository
- **Provides anomaly detection to complement existing perimeter defenses**
  - – Calculates identity and application baseline profiles to as

**Optimized threat analysis**

**Daily volume of events, flows, incidents**

**2,000,000,000**

**automatically analyzed to find**

**20 – 25**

**potential offenses to investigate**

> *“The average time to implement QRadar was 5.5 months versus 15.2 months (nearly 3X) for other market-leading competitor solutions.”*
>
> Source: Ponemon Institute LLC primary research, “IBM QRadar Evidence of Value”

© 2014 IBM Corporation

# Yes, we can!

© 2014 IBM Corporation

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

## 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 Framework 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

24x7

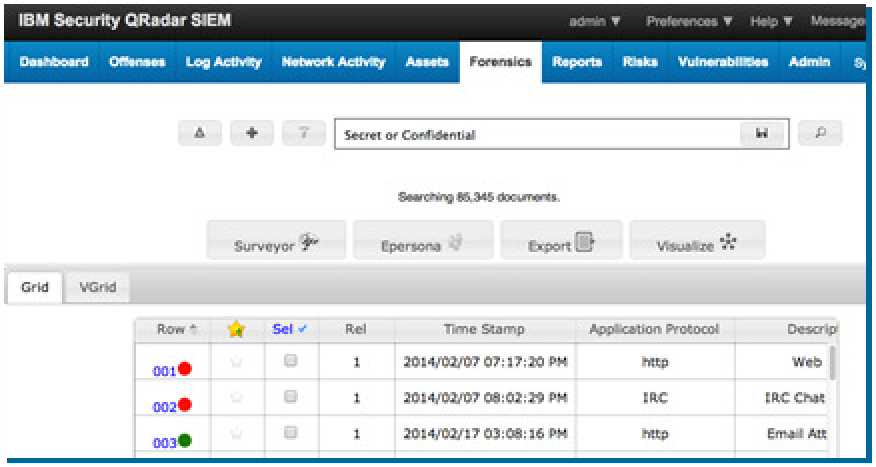
**IBM Emergency Response Services**

QRadar ®
Incident Forensics

# Intuitive investigation of security incidents

## Features:

- Employs Internet search engine technology closing security team skill gaps
- Creates rich ‘digital impression’ visualizations of related content
- Adds full packet captures to complement SIEM security data collection and analytics



Secret or Confidential

Searching 85,345 documents.

| Row | ★ | Sel ✓ | Rel | Time Stamp | Application Protocol | Descrip |
|---|---|---|---|---|---|---|
| 001 🔴 | ☆ | □ | 1 | 2014/02/07 07:17:20 PM | http | Web |
| 002 🔴 | ☆ | □ | 1 | 2014/02/07 08:02:29 PM | IRC | IRC Chat |
| 003 🟢 | ☆ | □ | 1 | 2014/02/17 03:08:16 PM | http | Email Att |

## Benefits:

- Reduces incident investigation periods from days or hours to minutes
- Helps determine root cause of successful breaches helping prevent recurrences
- Compiles evidence against malicious entities breaching secure systems and deleting or stealing sensitive data

**Wins the race against time**

*Research findings indicate enterprise organizations want increased awareness of advanced threats without the need for additional resources and forensics expertise.*

ESG

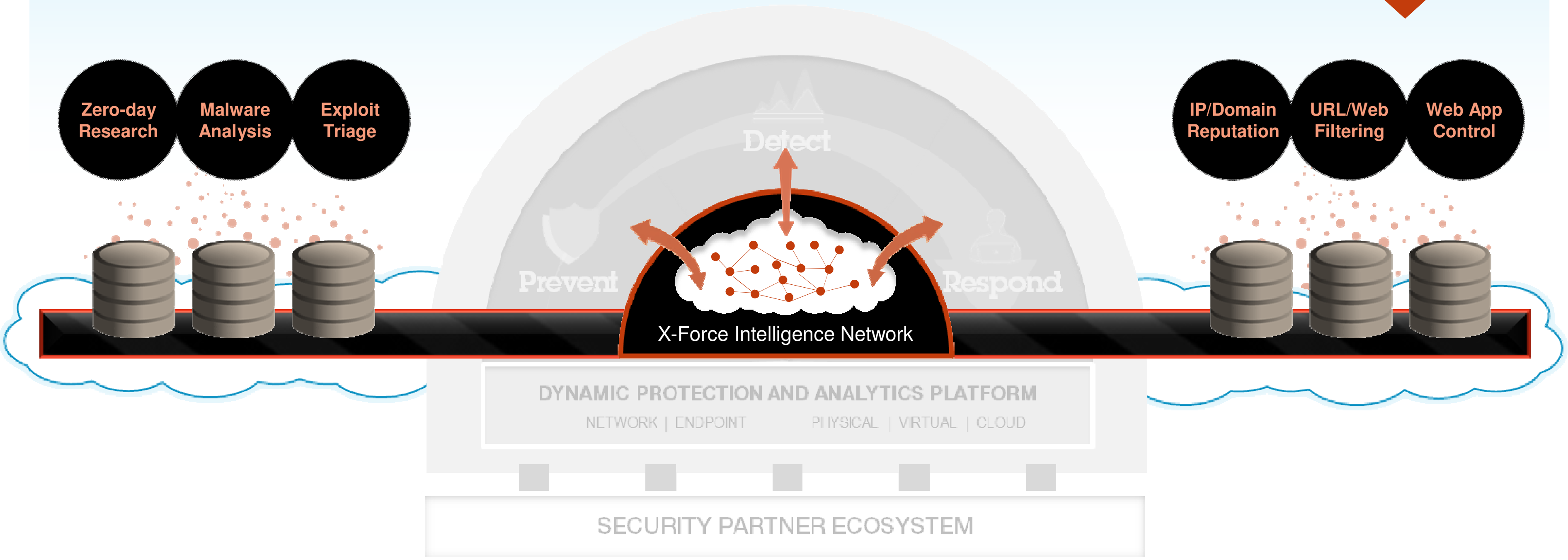
# Leverage threat intelligence with product integrations that draw upon human and machine-generated information

## Global Threat Intelligence

- Combines the renowned expertise of X-Force with Trusteer malware research
- Catalog of 70K+ vulnerabilities, 22B+ web pages, and data from 100M+ endpoints
- Intelligence databases dynamically updated on a minute-by-minute basis

NEW Trusteer an IBM Company

*Real-time sharing of Trusteer intelligence*



© 2014 IBM Corporation

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

## Security Partner Ecosystem Integrations

*IBM works with a broad set of technology vendors who provide complementary solutions and are integrated with our security products*

### Strengthen the threat protection lifecycle

- Leverage a vibrant ecosystem of security products
- Increase visibility, collapse information silos, and provide insights on advanced attacks

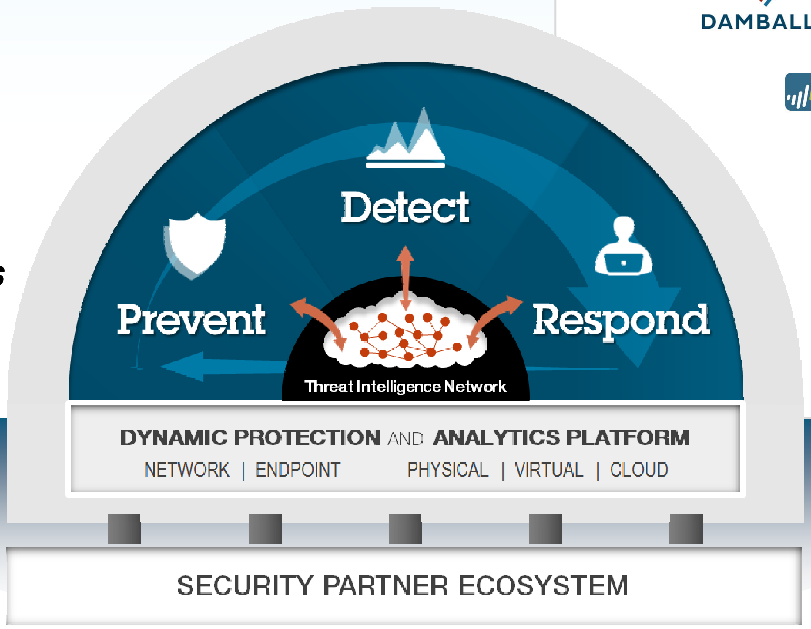
***IBM Security Partner Ecosystem 90+ vendors and 400+ products***

**Planned Advanced Threat Protection Integrations:**

| | |
|---|---|
| TREND MICRO | *Trend Micro Deep Security*<br>*IBM XGS Quarantine and Blocking* |
| FireEye | *FireEye Web Malware Protection System*<br>*IBM XGS Quarantine and Blocking* |
| DAMBALLA | *Damballa Failsafe*<br>*IBM XGS Quarantine and Blocking* |
| paloalto NETWORKS | *Palo Alto Firewalls*<br>*Trusteer Apex integration* |

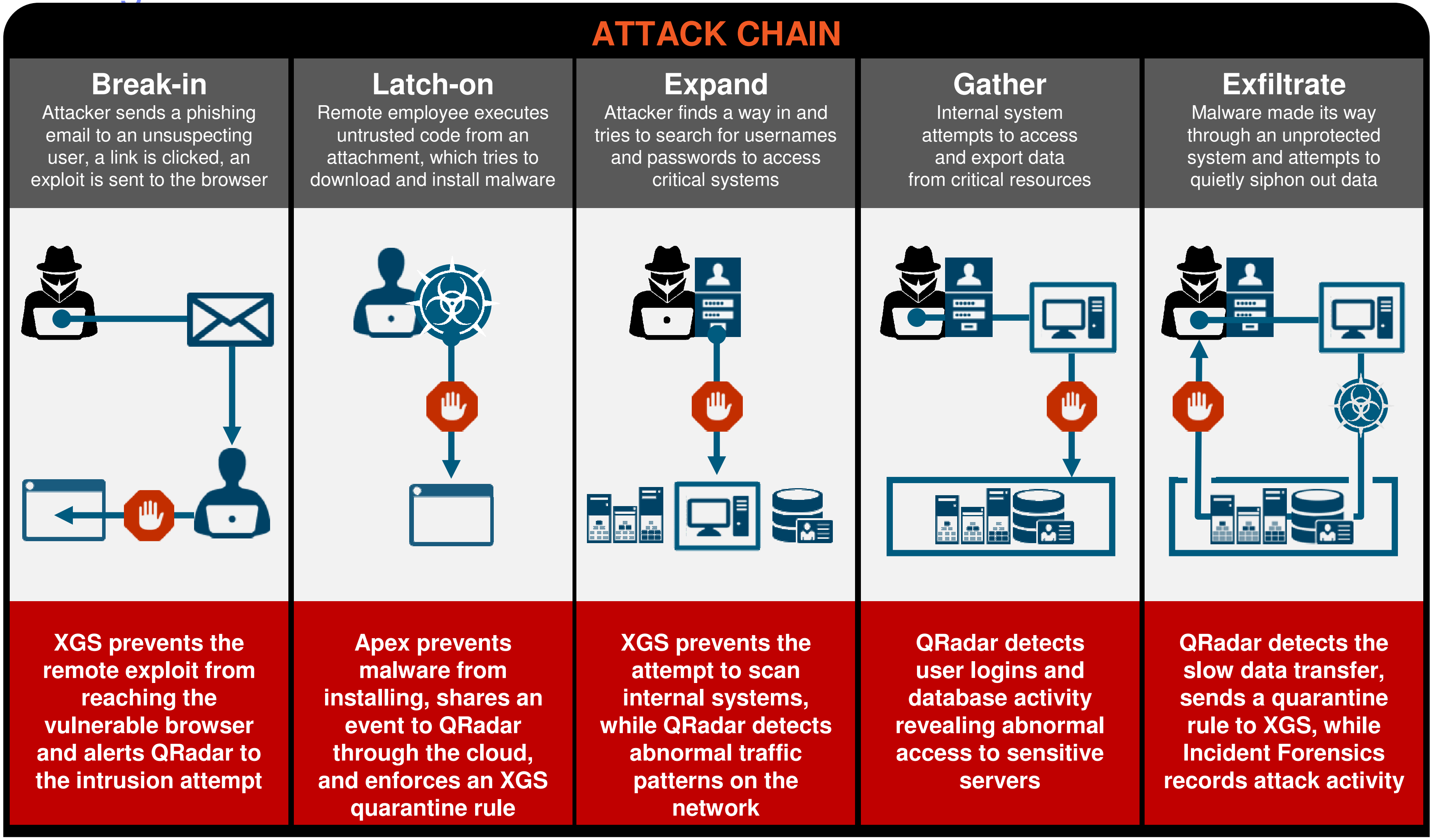
**Additional Example QRadar Partners:**

CISCO, websense, QUALYS, BLUE COAT, proofpoint, JUNIPER NETWORKS


Detect
Prevent
Respond
Threat Intelligence Network
DYNAMIC PROTECTION AND ANALYTICS PLATFORM
NETWORK | ENDPOINT
PHYSICAL | VIRTUAL | CLOUD
SECURITY PARTNER ECOSYSTEM

© 2014 IBM Corporation

# Examples of breaking the attack chain through integrated intelligence



## ATTACK CHAIN

### Break-in

Attacker sends a phishing email to an unsuspecting user, a link is clicked, an exploit is sent to the browser

**XGS prevents the remote exploit from reaching the vulnerable browser and alerts QRadar to the intrusion attempt**

### Latch-on

Remote employee executes untrusted code from an attachment, which tries to download and install malware

**Apex prevents malware from installing, shares an event to QRadar through the cloud, and enforces an XGS quarantine rule**

### Expand

Attacker finds a way in and tries to search for usernames and passwords to access critical systems

**XGS prevents the attempt to scan internal systems, while QRadar detects abnormal traffic patterns on the network**

### Gather

Internal system attempts to access and export data from critical resources

**QRadar detects user logins and database activity revealing abnormal access to sensitive servers**

### Exfiltrate

Malware made its way through an unprotected system and attempts to quietly siphon out data

**QRadar detects the slow data transfer, sends a quarantine rule to XGS, while Incident Forensics records attack activity**

© 2014 IBM Corporation

# IBM is uniquely positioned to offer integrated protection

## 1 Smarter Prevention

### Trusteer Apex Endpoint Malware Protection

NEW *Java Lockdown Protection - granular control of untrusted code, cloud-based file inspection, and QRadar integration*

### IBM Security Network Protection XGS

NEW *Advanced Threat Quarantine integration from QRadar and third-party products, inclusion of Trusteer intelligence into XGS*

## 2 Security Intelligence

### IBM Security QRadar Security Intelligence

NEW *Data Node appliance, new flow and event APIs, and QRadar Vulnerability Manager scanning improvements*

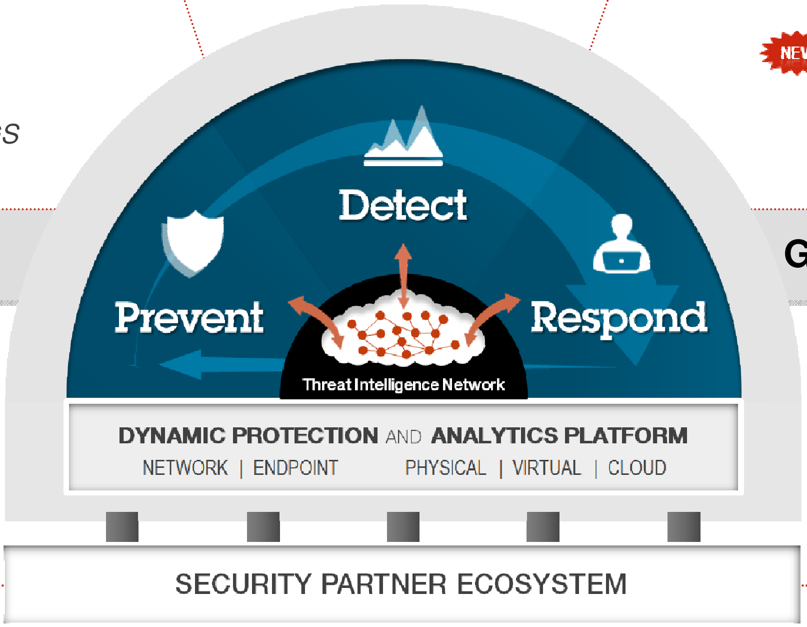
## 3 Continuous Response

### IBM Security QRadar Incident Forensics

NEW *Integrated forensics module with full packet search and visual reconstruction of relationships*

### IBM Emergency Response Services

NEW *Increased global coverage and expertise related to malware analysis and forensics*



Detect

Prevent

Respond

Threat Intelligence Network

DYNAMIC PROTECTION AND ANALYTICS PLATFORM

NETWORK | ENDPOINT PHYSICAL | VIRTUAL | CLOUD

SECURITY PARTNER ECOSYSTEM

## 4 Global Threat Intelligence

### IBM X-Force Threat Intelligence

NEW *New real-time sharing of Trusteer threat intelligence from 100M+ endpoints with X-Force*

## 5 Open Integrations

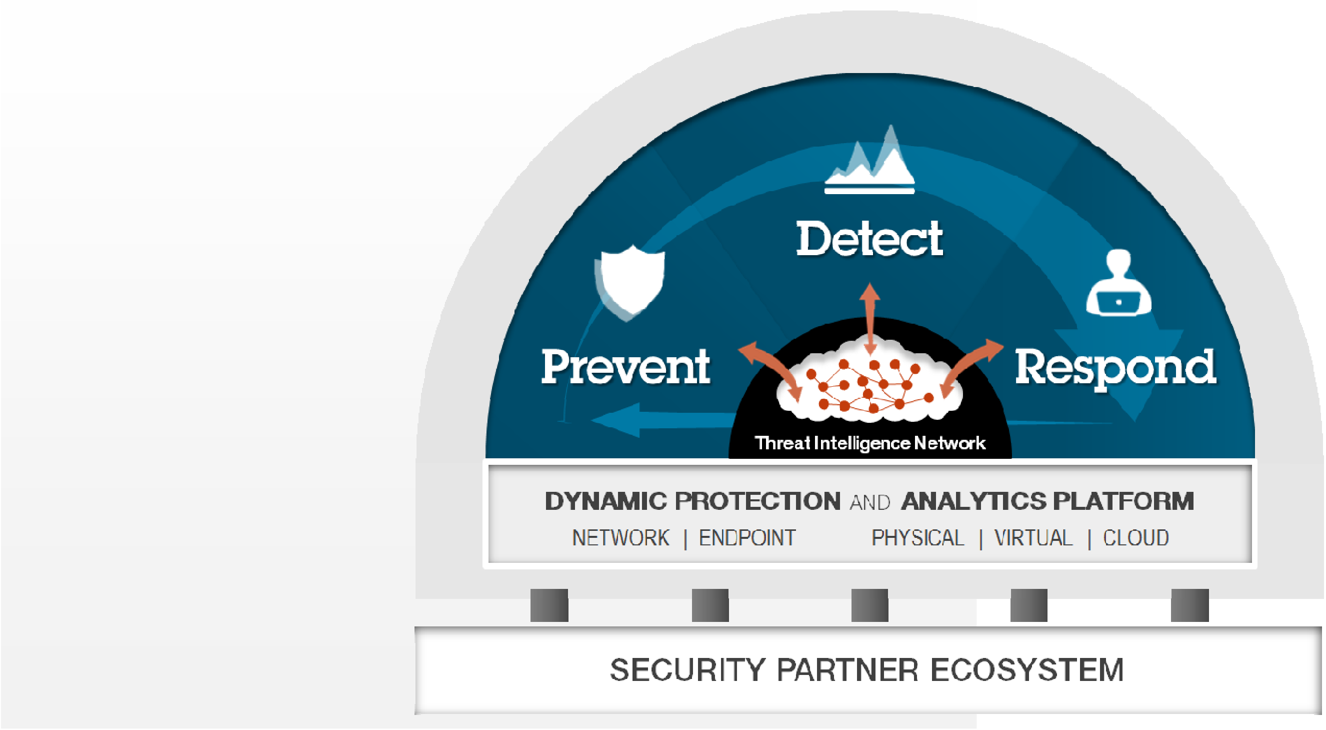
### Ready for IBM Security Intelligence Ecosystem

NEW *New functionality from partners including FireEye, TrendMicro, Damballa and other protection vendors*

© 2014 IBM Corporation

# Fragen?

Prevent. Detect. Respond.


Detect
Prevent
Respond
Threat Intelligence Network
DYNAMIC PROTECTION AND ANALYTICS PLATFORM
NETWORK | ENDPOINT
PHYSICAL | VIRTUAL | CLOUD
SECURITY PARTNER ECOSYSTEM

© 2014 IBM Corporation