

BusinessConnect
A New Era of Smart
12th June 2014

Security Intelligence

A New Era of Security

for a New Era of Computing

Martin Borrett
Director of the IBM Institute for Advanced Security
Europe



Welcome
to the
**New
Normal!**

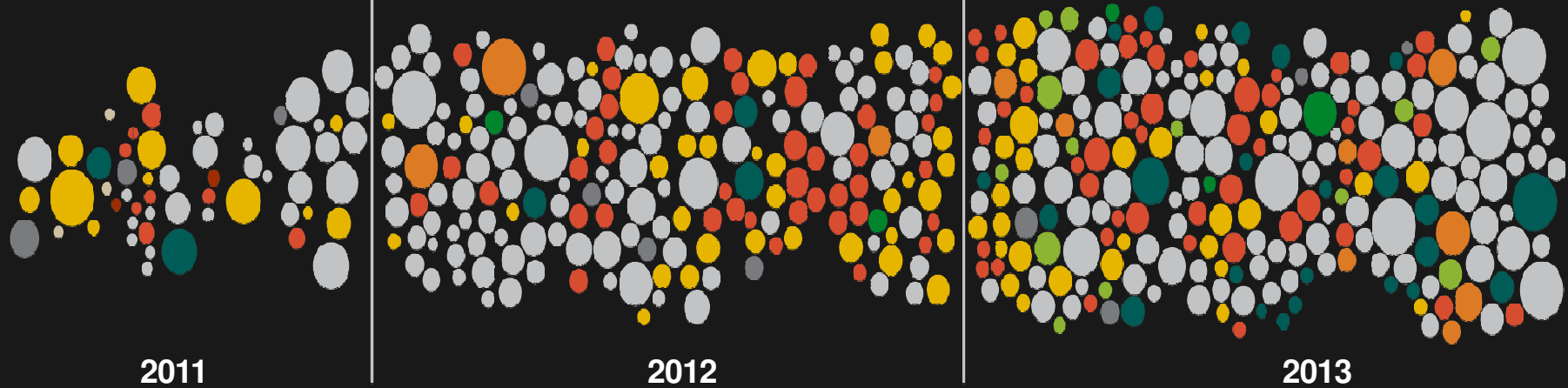


We are in an era of continuous breaches

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

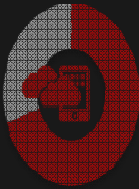


Attack types

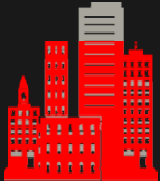
- SQL injection
- Spear phishing
- DDoS
- Third-party software
- Physical access
- Malware
- XSS
- Watering hole
- Undisclosed

61% of organizations say
Data theft and cybercrime
are the greatest threats
to their reputation

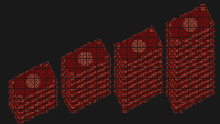
2012 IBM Global Reputational Risk & IT Study

 **70%**
of security exec's
are concerned about
cloud and mobile security

2013 IBM CISO Survey

 **83%**
of enterprises
have difficulty finding the
security skills they need

2012 ESG Research



Average U.S.
breach cost

\$11M+

*2013 Cost of Cyber Crime Study
Ponemon Institute*

Mobile malware grew

614%  in one year

from March 2012 to March 2013

2013 Juniper Mobile Threat Report

85  tools from

45  vendors

IBM client example

Security leaders are more accountable than ever before



Your Board and CEO demand a strategy

WE NEED A NEW APPROACH: A Three Point Plan

1 INTELLIGENCE

Use insights and analytics for smarter defense

2 INNOVATION

Use cloud and mobile to improve security

3 INTEGRATION

Use an integrated approach to stay ahead of the threat

INTELLIGENCE

Use analytics and insights for smarter defense



Use anomaly detection and algorithm-based controls across every domain

Build an intelligence vault around your crown jewels

Prepare your response for the inevitable

INNOVATION

Use cloud and mobile to improve security



Own the security agenda for innovation

Embed security on day one

Use cloud, mobile, social and big data to improve security

INTEGRATION

Use an integrated approach to stay ahead of the threat



Develop a risk-aware security strategy

Deploy a systematic approach

Harness the knowledge of professionals

How is
IBM helping
customers
achieve
these goals?








An integrated portfolio shapes a new approach to security



CISO's changing role



Security mega trends

-  *Advanced threats*
-  *Cloud*
-  *Mobile*
-  *Compliance*
-  *Skills shortage*

The CISO's changing role



Influencers

- Confident / prepared
- Strategic focus

Protectors

- Less confident
- Somewhat strategic
- Lack necessary structural elements

Responders

- Least confident
- Focus on protection and compliance

How they differ

have a dedicated CISO



have a security/risk committee



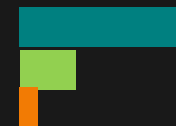
have information security as a board topic



use a standard set of security metrics to track their progress



focused on improving enterprise communication/collaboration



focused on providing education and awareness



The Importance of Metrics

Responders Protector Influencer

Compliance



Risk and ability to deal w/ future threats



Vulnerability



Education and awareness



Speed of recovery from incidents



Day-to-day security operations



Attacks identified and thwarted



Cost



New technology and innovation efforts



Dealing with Advanced Threats: The IBM Threat Protection System

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



Accelerated Roadmap

Significant investment across 10 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

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



On the Endpoint

Prevent malware installs

Prevent control channels

Prevent credential loss

Exploit Disruption

Malware Quarantine

User Protection

On the Network

XGS

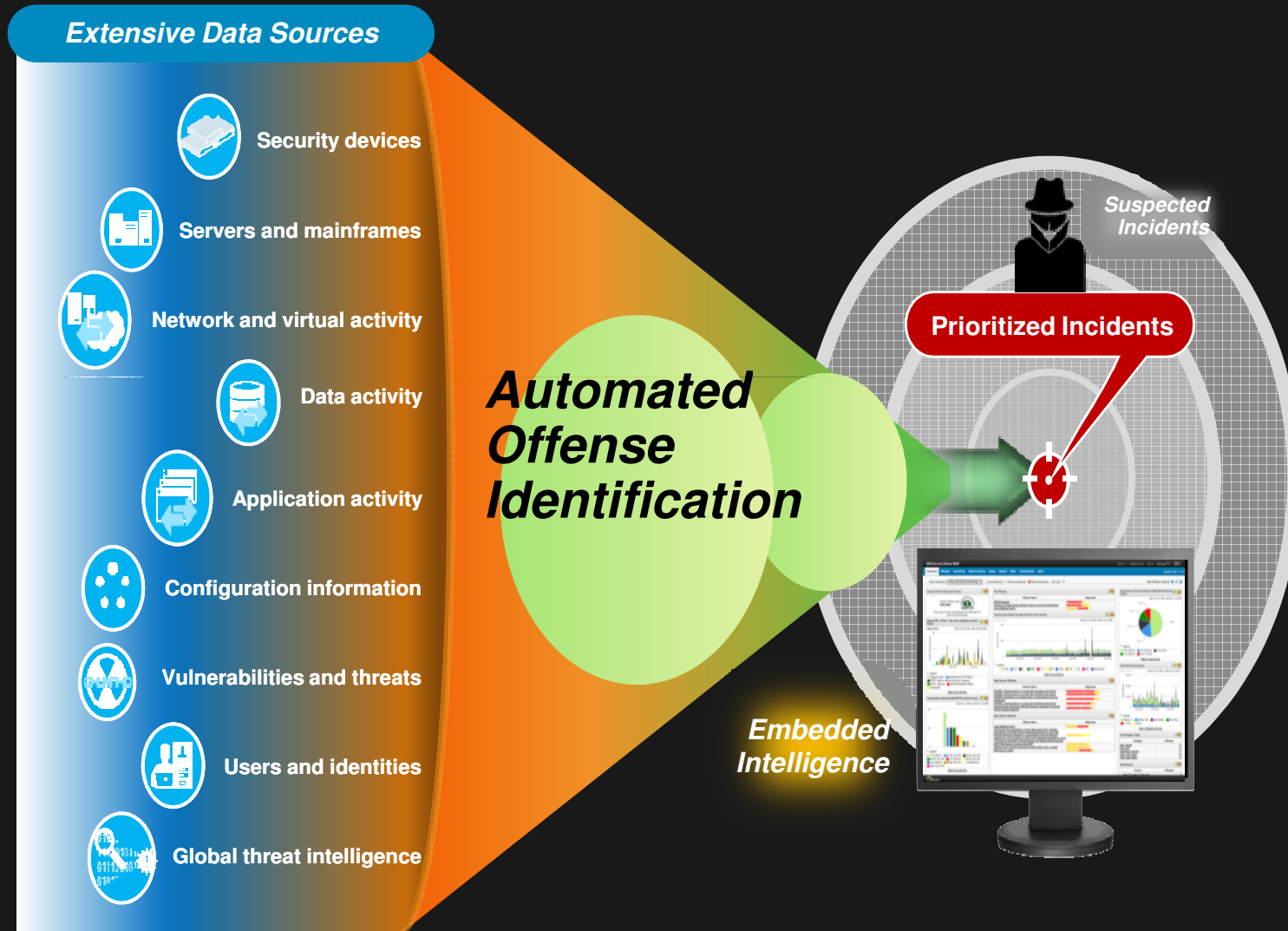


Prevent mutated exploits

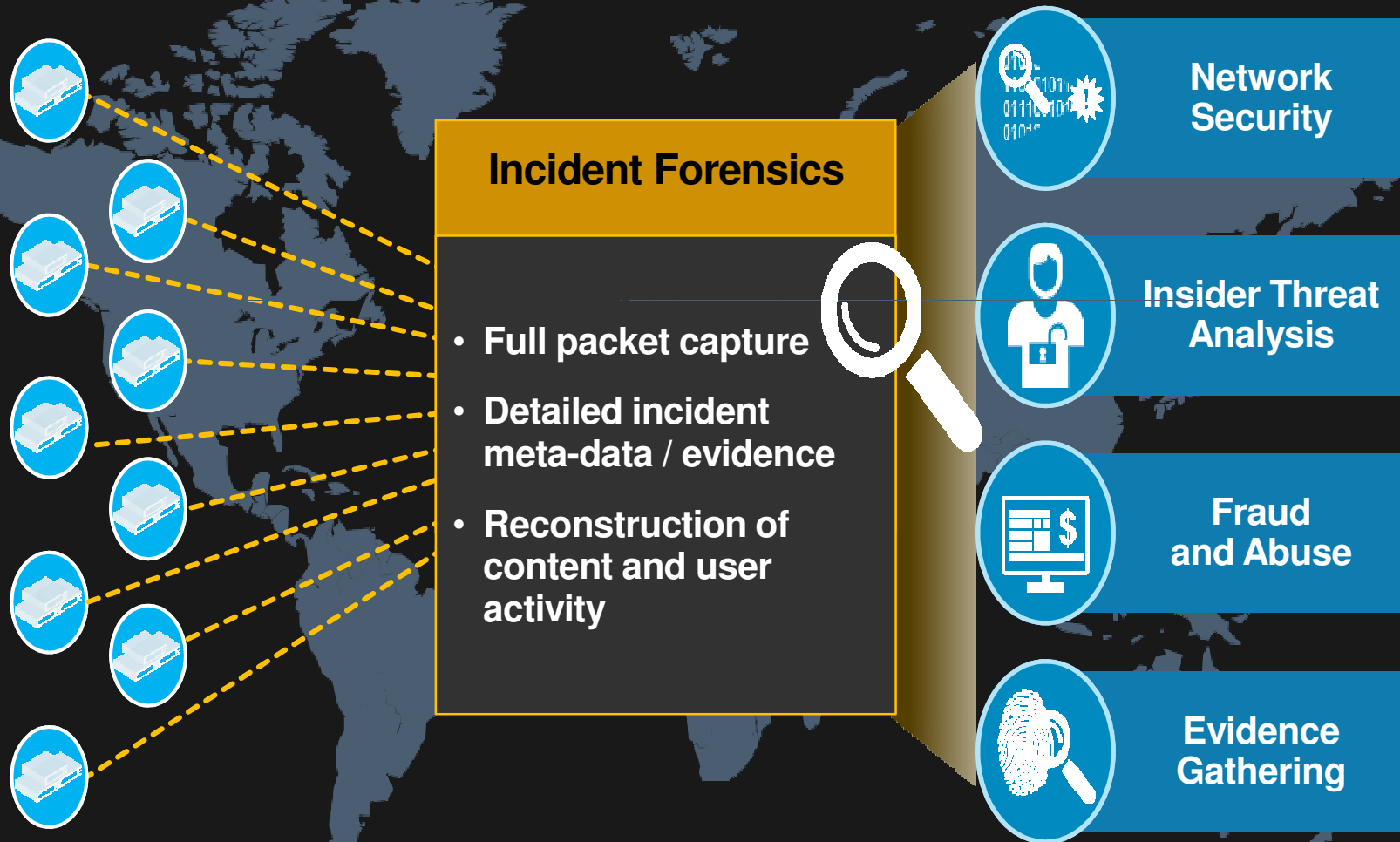
Prevent active beaconing

Prevent malicious behavior

Continuously monitor security-relevant activity from everywhere

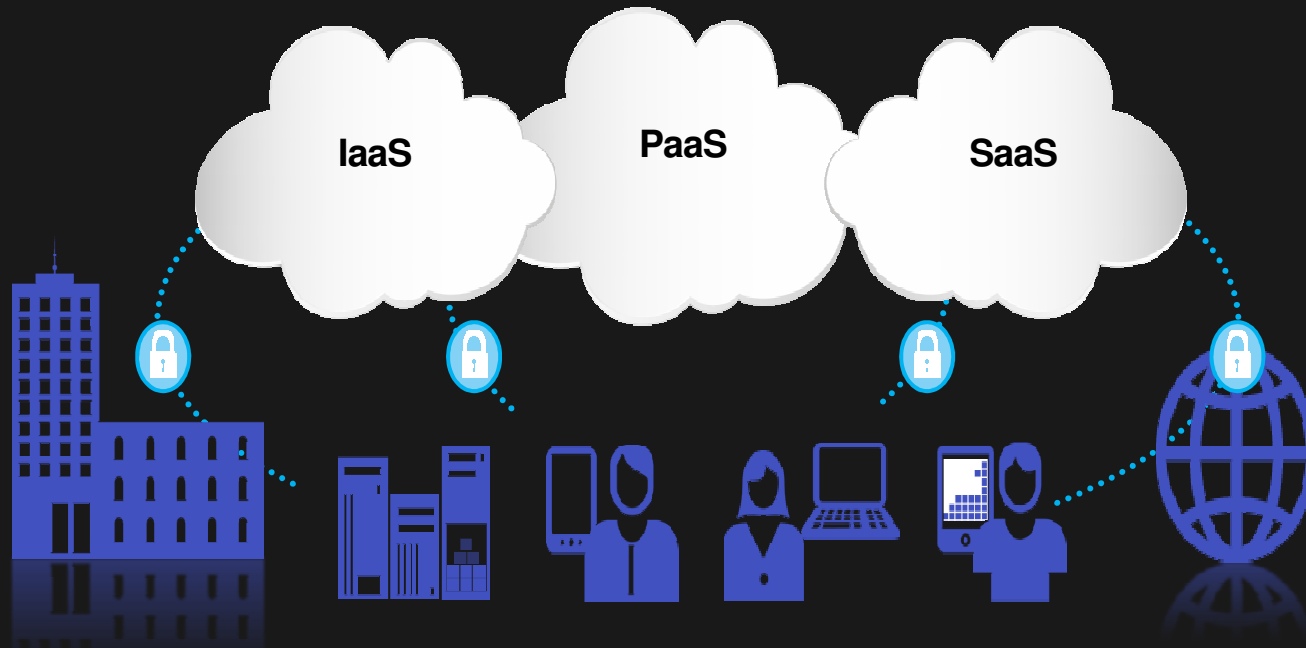


Quickly investigate breaches, retrace activity, and learn from findings to remediate weaknesses



Employ Cloud to Improve Security

Protecting the cloud data center, and next-gen business and application platforms



***Manage
Identities
and Protect
User Access***

***Monitor and
Audit
Applications
and Data***

***Scan and
Protect
the Network
from Threats***

***Establish
Intelligence
Across the
Cloud***

Extending enterprise-grade security to and from the Cloud

Delivering security from the cloud

Fraud Prevention

Millions

of endpoints protected for the world's top financial institutions

IBM Trusteer

Mobile Security

Millions

of cloud-managed devices for thousands of global customers

IBM Fiberlink

Web Protection

Thousands

of servers providing DDoS protection in the cloud

IBM + Akamai

Solutions to protect cloud workloads

Security Intelligence

Analytics

and real-time correlation to stop cloud threats

IBM QRadar

End-to-end Protection

Controls

for cloud users, data, apps and infrastructure

IBM Security Systems

Skills and Expertise

Services

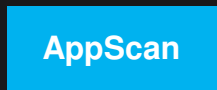
to design, deploy and manage cloud security

IBM Security Services

Protect the mobile enterprise with smarter security



Build security into mobile from day one



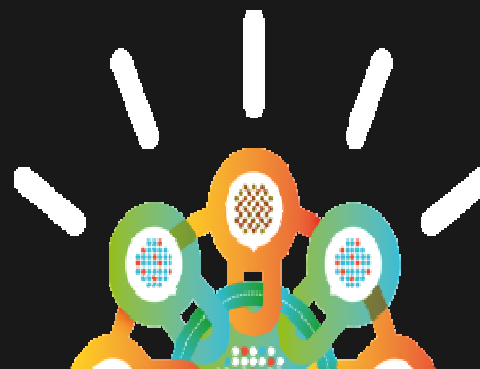
Discovered and enrolled **3,000 devices in under 5 minutes** each with ability to wipe the device if lost
Chemical company

Helping prevent user access to fraudulent websites for **thousands** of mobile customers
Large European bank



don't wait
for what
lies ahead

IBM Security Framework



Intelligence

Integration

Expertise



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.

Thank You

www.ibm.com/security

© Copyright IBM Corporation 2014. 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.