



Discover, Analyze, Remediate

An aerial photograph of the Burj Khalifa in Dubai, United Arab Emirates. The skyscraper is the central focus, rising vertically from a dense urban landscape. The surrounding area includes other high-rise buildings, a large artificial lake with a green island, and various infrastructure like roads and parking lots. The sky is a clear, pale blue with some light clouds. The overall scene is a high-angle, wide-area shot of a modern city.

The Nanjgel Cyber Security Framework

Jude Pereira
Managing Director
Nanjgel Solutions FZ-LLC

Our Focus: Solving Wicked Hard Problems



COUNTER-TERRORISM

Quick Reaction Capabilities

CYBER

Mission Grade Cyber Defense

Secure Cloud Computing

Cyber Network Operations -
Operations, Development, Training

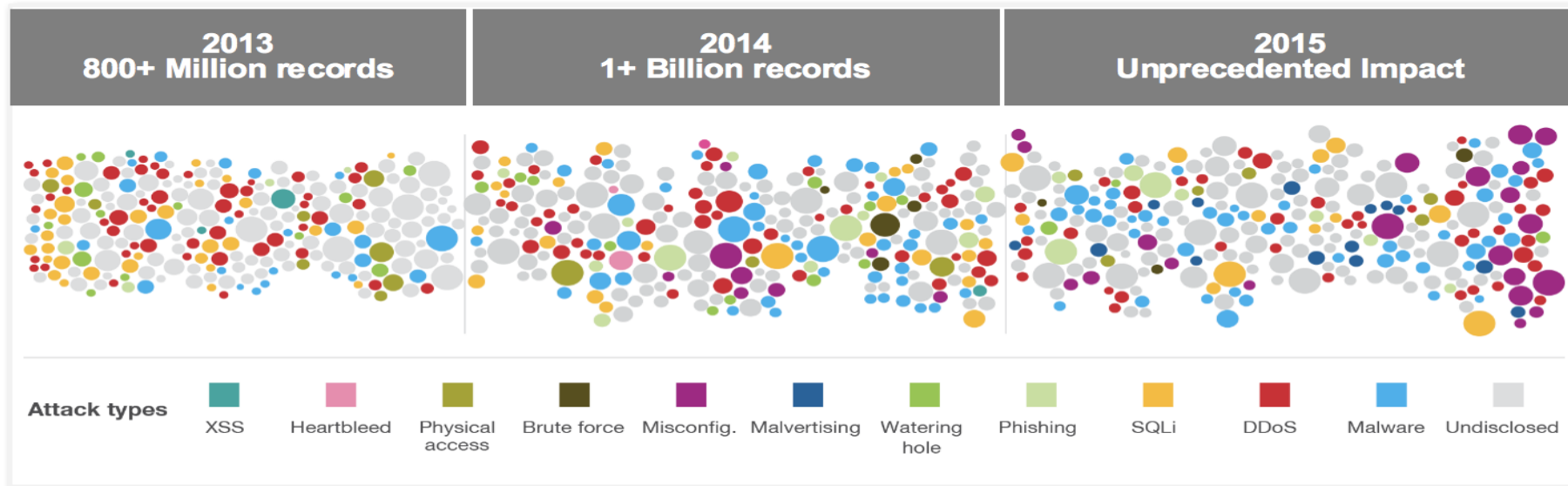
GEOSPATIAL

Geospatial Data
Management & Analysis

Geospatial Data Collection

Sensor Development & Integration

Attackers break through conventional safeguards every day



average time to detect APTs

256 days

average cost of a U.S. data breach

\$6.5M

We are in an era of continuous breaches

2013

Operational
Sophistication

**Year of the
Security Breach**

2014

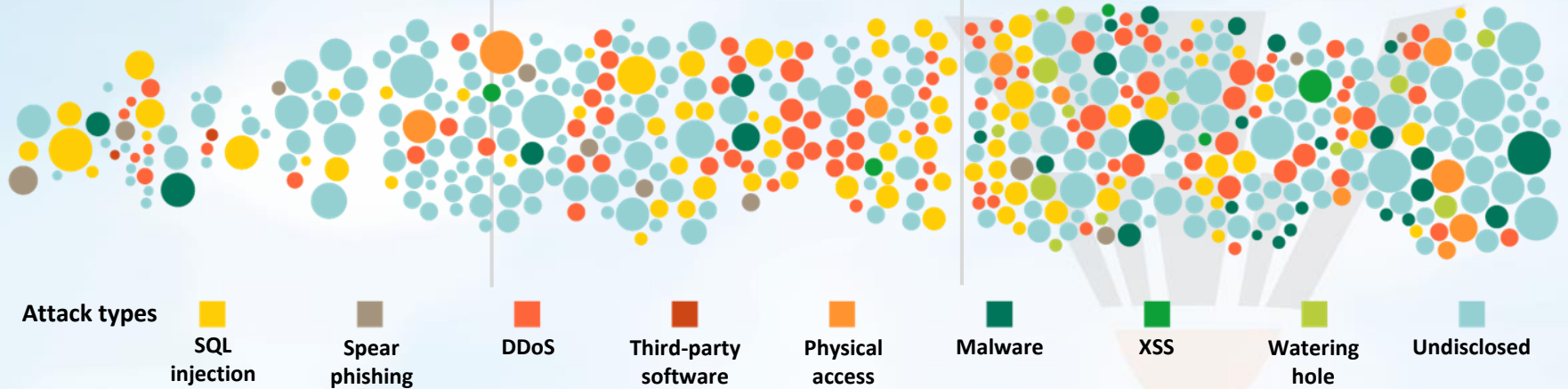
Near Daily Leaks
of Sensitive Data

40% increase
in reported data
breaches and incidents

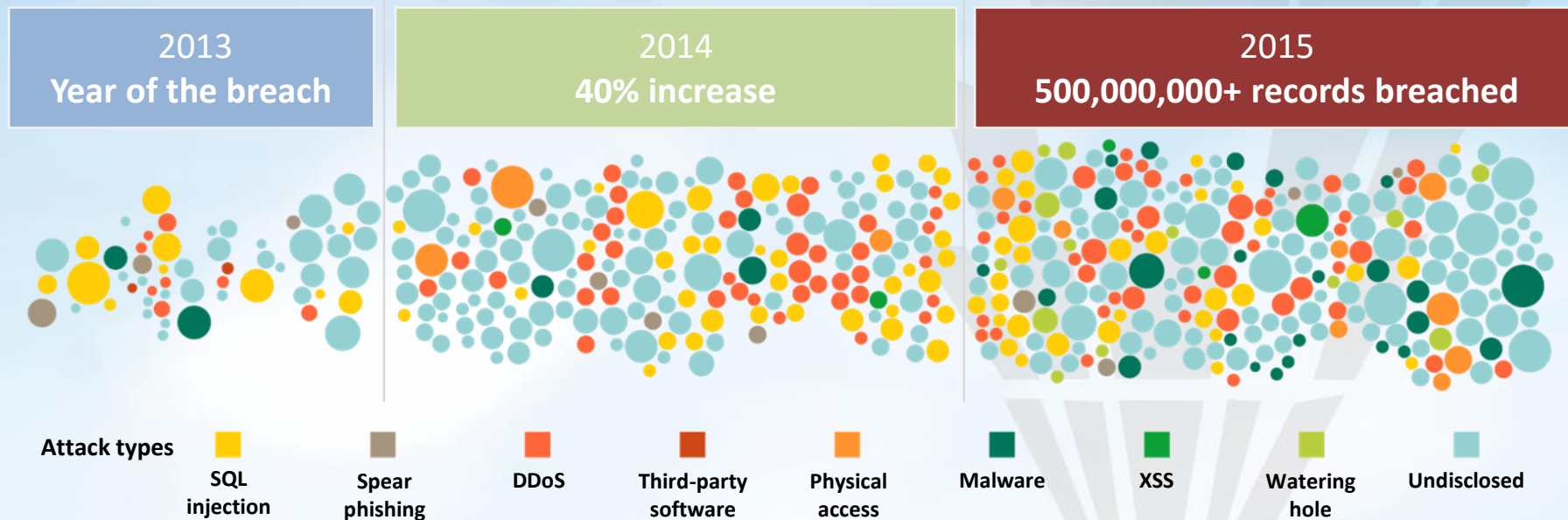
2015

Relentless Use
of Multiple Methods

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



The era of continuous breaches carry on...



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

Innovative technology changes everything



1 trillion
connected
objects



Social
business



Cloud and
virtualization



1 billion mobile
workers



Bring your
own IT

PARADIGM SHIFT

In Crime



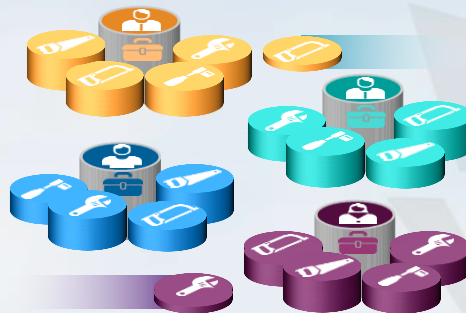
Today's challenges

Escalating Attacks



- Increasingly sophisticated attack methods
- Disappearing perimeters
- Accelerating security breaches

Increasing Complexity



- Constantly changing infrastructure
- Too many products from multiple vendors; costly to configure and manage
- Inadequate and ineffective tools

Resource Constraints



- Struggling security teams
- Too much data with limited manpower and skills to manage it all
- Managing and monitoring increasing compliance demands

The Fact of Reality?

Security Intelligence and Vulnerability Management



Fraud



Identity & Access



Data



Applications



Network



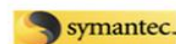
Endpoint



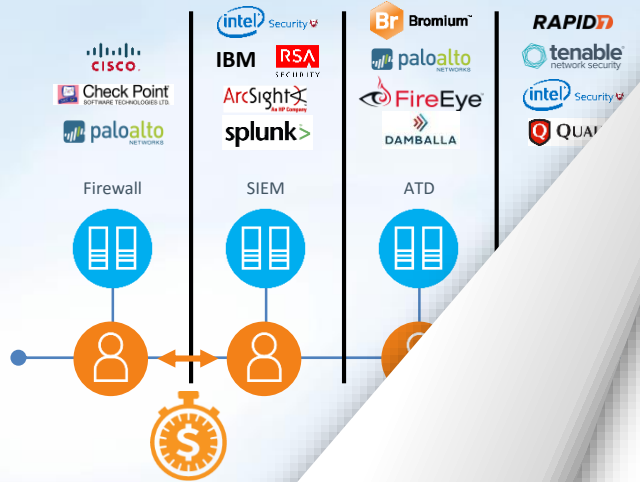
Mobile



Managed Security Services



IT Security Challenges



Human br

SecOp

Fragmented security lets attackers in

“70 to 90 percent of all malicious incidents could have been prevented or found sooner if existing logs and alerts had been monitored”

Verizon Data Breach Investigations Report

“Average time to contain a cyber attack is 31 days”

Ponemon Institute “2014 Global Report on the Cost of Cyber Crime”

Yesterday's practices are not working



\$3.5M+

Average cost
of a data breach



85 tools from

45 vendors

Your security team sees noise

We need a new approach – *The power to act* – at scale





Organizations Need to Speed Up Breach Detection

On average, organizations take **229 days** to detect a data breach, according to a recent study from a cybersecurity firm.

One reason for the lengthy detection time is two-thirds of organizations are told about a breach by a third party, rather than discovering it themselves.

Organizations looking to speed up breach detection on their own, rather than relying on others, need to improve their data analytics capabilities, prioritize the type of data they want to collect and analyze, and ensure they have appropriate staff who can take the time to review the data for suspicious activity.

By Jeffrey Roman, November 25, 2014.

Security Intelligence – Core Functionality for Cyber Security

Security Intelligence

-- noun

- 1. the real-time collection, normalization and analytics of the data generated by users, applications and infrastructure that impacts the IT security and risk posture of an enterprise*

Security Intelligence provides actionable and comprehensive insight for managing risks and threats from protection and detection through remediation

SECURITY INTELLIGENCE

Not because you think you know
everything without questioning,
but rather because you question
everything you think you know.



It's about discovering
what you did not know!!

Our Approach

INTELLIGENCE

*Use insights
and analytics
to identify
outliers*

INTEGRATION

*Develop an integrated
approach to
stay ahead
of the threat*

INNOVATION

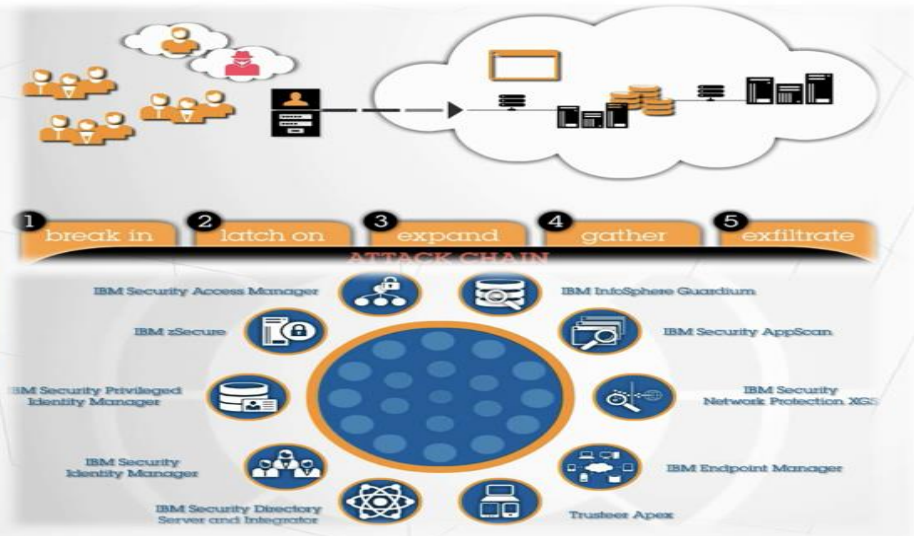
*Use cloud
and mobile
for better
security*

"More Context" means more Integration

- Security Systems solutions offer integration and interoperation, for the benefit of customers who need their security infrastructure to support relevant standards and integrate and interoperate for ease of operations and for broad span of coverage.

The value of Security Integrations:

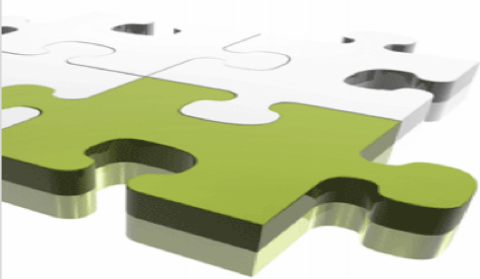
<http://youtu.be/kxBVAZ1Sxy8>



Integration” means easier & more comprehensive

Security skills and staffing continues to lag at enterprise organizations.

Data points to a pretty substantial skills gap:

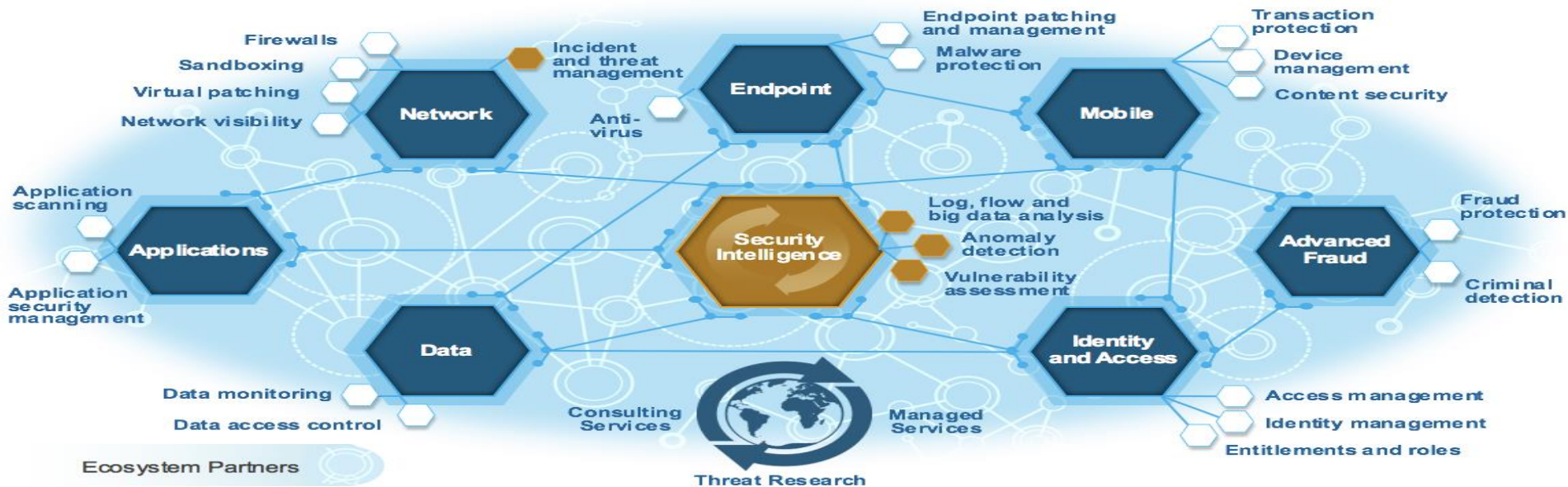


- 30% of organizations say that the network security skills of the infosec staff are inadequate in some, most, or all cases.
- 44% of organizations say that the number of networking/security staff with strong knowledge in both security and networking technology is inadequate in some, most, or all cases.
- 38% of organizations say that the ability of the security staff to keep up with network security changes is inadequate in some, most, or all cases.
- 37% of organizations say that the ability of the security staff to keep up with the threat landscape is inadequate in some, most, or all cases.
- 47% of organizations say that the number of employees dedicated to network security is inadequate in some, most, or all cases.

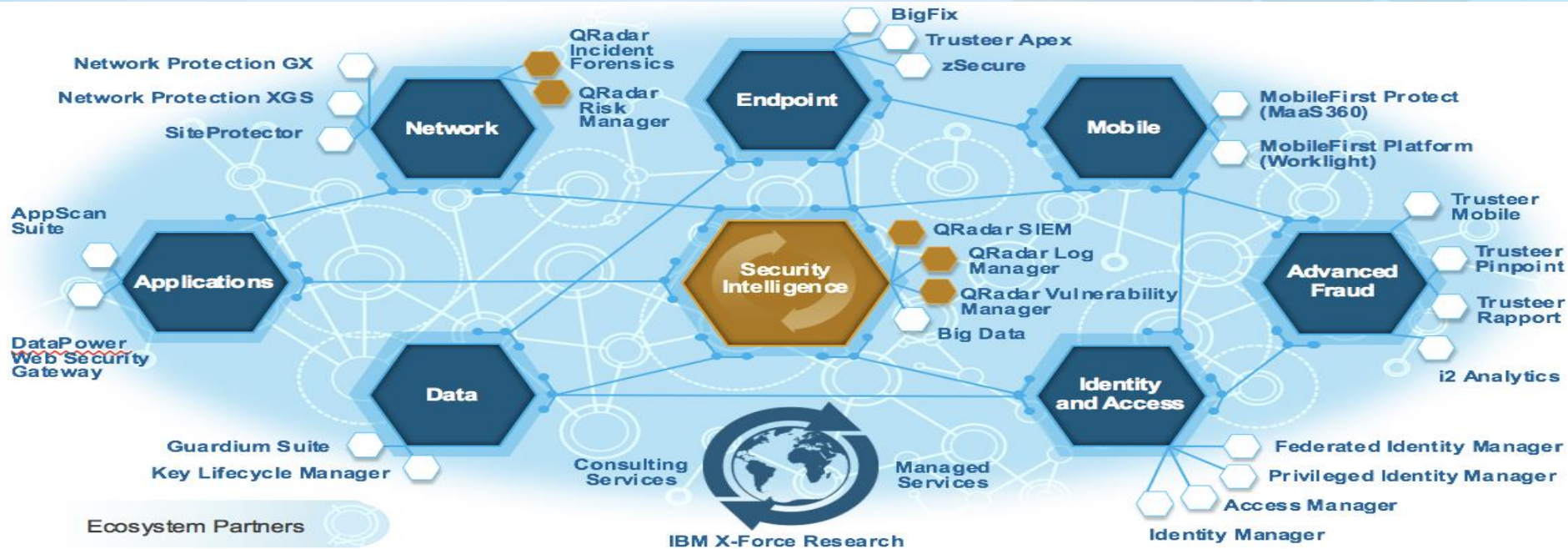
Large organizations have been segmenting networks, filtering packets, and managing firewalls, IDS/IPS, network proxies, and assorted gateways for years. In spite of this experience however, they remained under-skilled and understaffed and thus more vulnerable than they should be.

Establish Security as a System

Key integrated capabilities



Establish Security as an **Eco-System**



Our Methodology

Security Intelligence

Information and event management, Advanced correlation and deep analytics, External threat research

Cross-domain Analytics, Reporting, Forensics and Management Capabilities

ENHANCED
USER
SECURITY

DATA SECURITY

APPLICATION
SECURITY

ENDPOINT
SECURITY

NETWORK
SECURITY

What we need to do ?

- ▼ **Visibility**
Get full visibility into your Environment, Understand what is happening & what is not.
- ▼ **Detect**
External & Internal Threats, Vulnerabilities, User Activity, Loss of System and personal or sensitive Data.
- ▼ **Report**
Provide evidence in investigation, Historic & Real Time Data gathering.

What we **else** also do ?



Respond

Virtual Firewalling, Data Protection, Block Access, Turn off switch Port , Notification.



Remediate

Incident management, Open Trouble Ticket, Self Remediation, Integration with 3rd Party tools

SANS 20 CRITICAL CONTROLS

CIS Critical Security Controls

CSC 1

Inventory of Authorized and Unauthorized Devices

Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unwanted devices are found and prevented from gaining access.

CSC 2

Inventory of Authorized and Unauthorized Software

Actively manage (inventory, track, and correct) all software installed and not authorized, and unauthorized and unwanted software is found and prevented from installation or execution.

CSC 3

Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Establish, implement, and actively manage (track, report on, and correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attacks from exploiting vulnerable services and settings.

CSC 4

Continuous Vulnerability Assessment and Remediation

Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, and to remediate and minimize the window of opportunity for attackers.

CSC 5

Controlled Use of Administrative Privileges

Track, control, prevent, and correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

CSC 6

Maintenance, Monitoring, and Analysis of Audit Logs

Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

CSC 7

Email and Web Browser Protections

Minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and e-mail systems.

CSC 8

Malware Defenses

Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the rate of automation to enable rapid updating of defenses, data gathering, and corrective action.

CSC 9

Limitation and Control of Network Ports, Protocols, and Services

Manage (track, control, and correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.

CSC 10

Data Recovery Capability

Properly back up critical information with a proven methodology for timely recovery.

CSC 11

Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

Establish, implement, and actively manage (track, report on, and correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

CSC 12

Boundary Defense

Detect, prevent, and correct the flow of information transforming networks of different trust levels with a focus on security-damaging data.

CSC 13

Data Protection

Prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

CSC 14

Controlled Access Based on the Need to Know

Track, control, prevent, and correct access to critical assets (e.g., information, resources, systems) according to the formal determination of which person, computer, and application have a need and right to access those critical assets based on an approved classification.

CSC 15

Wireless Access Control

Track, control, prevent, and correct the security use of wireless local area networks (LANs), access points, and wireless client systems.

CSC 16

Account Monitoring and Control

Actively manage the life-cycle of system and application accounts — data creation, use, dormancy, deletion — in order to minimize opportunities for attackers to leverage them.

CSC 17

Security Skills Assessment and Appropriate Training to Fill Gaps

Identify the specific knowledge, skills, and abilities needed to support defense of the enterprise, develop and execute an integrated plan to assess, identify and remediate gaps, through policy, organizational planning, training, and awareness programs for all functional roles in the organization.

CSC 18

Application Software Security

Manage the security life-cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

CSC 19

Incident Response and Management

Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plan, defined roles, training, communications, management oversight).

CSC 20

Penetration Tests and Red Team Exercises

Test the overall strength of an organization's defenses (technology, process, and people) by simulating the objectives and actions of an attacker.

The CIS Critical Security Controls as the Basis for Cybersecurity Audits

Daily headlines of significant cyber news items with their associated effects on consumers and citizens have generated an outcry from the public and lawmakers to demand better performance in cybersecurity for enterprises in every industry. Societal and government directives have been enacted to the problem but we are far from the most part, still largely unaware of how best to protect their IT and sensitive data.

The Joint Task Force Cyber Security Office of the Center for Internet Security (CIS) frequently meets with CEOs and CIOs of major companies and government organizations who are grappling with the cybersecurity problem. As the former Deputy Secretary and Chief Operating Officer for the Department of Homeland Security, Jim Underbrink understands the challenges facing leaders who must make tough choices about how to allocate resources to cybersecurity. The problem has shifted from a traditional technology and product view of security to also include the executive's view of the risk to the business. Therefore our solutions (both as individual enterprises and as communities) must bridge this gap in a manner that can be openly described, assessed, shared and negotiated.

The CIS Critical Security Controls provide a highly practical and useful framework for every organization to use for both implementation and assessment. Because the Controls are developed by the community and based on actual threat data, they are an authoritative, industry-friendly and vendor-neutral approach to assessment and building of security.

Getting Started: Ask and Answer Key Questions

- What am I trying to protect? Create a prioritized list of business or mission-critical processes and inventory the controls, assets that risk to these processes. This information will be critical for creating a baseline of your current security posture against the CIS Critical Security Controls.
- Where are my gaps? For each business or mission-critical asset, compare existing security controls against the CIS Critical Security Controls, indicating the sub-controls that the existing controls already meet and those they do not meet.
- What are my priorities? Create a prioritized list of business or mission-critical assets and controls that need to be implemented to meet the Top 5 Controls and develop a strategic plan to implement the other Controls.
- Where can I automate? As you plan your implementation of the Controls, focus on opportunities to create security capabilities that can be integrated and automated using tools that remove skilled security and administrative staff from the work. The Controls were written to be automated. The goal is to have the system respond rapidly and efficiently deliver accurate, timely and actionable information to the system administrator and others who can take proactive steps to detect threats.
- How can my vendor partners help? Some vendor solutions significantly improve and automate implementation of the CIS Critical Security Controls in terms of continuous monitoring and mitigation. Contact your current vendors to see how they can support your implementation of the CIS Critical Security Controls and compare their solutions with other vendor products.

SANS

PRESENTS

CIS Critical Security Controls

Since its release in February 2011, the NIST Framework for Improving Critical Infrastructure Cybersecurity (CIS) has become a major part of the national conversation about cybersecurity for the critical infrastructure and beyond. (The Center for Internet Security was an active participant in the development of the NIST Framework and the CIS Critical Security Controls are cited as one of the "reference materials" that can be used to develop a security implementation.)

The Framework provides a way to organize, conduct and drive planning on security goals and improvements for individual enterprises and across sectors of enterprise. But it does not include any specific risk management process, or specify any priority of action. These decisions and judgments are left to the adapter to manage for their specific situation and context.

CIS believes that this task is beyond the ability or resources of most enterprises to do effectively or efficiently. This approach doesn't recognize the interdependency that every enterprise has with its many partners. A community-link approach for considering attacks that

The CIS Critical Security Controls for Effective Cyber Defense Now

The CIS Critical Security Controls are a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive and dangerous attacks. A primary benefit of the Controls is that they prioritize and focus a smaller number of actions with high pay-off results. The Controls are effective because they are derived from the most common attacks that are occurring in the leading threat reports and vetted across a very broad community of security and industry practitioners. They were created by the people who have attacked you, while they are attacking you, and they are the response organizations — to answer the question, "what do we need to do to stop known attacks?" That group of organizations took the time to look at the top 100 attacks and the top 100 vulnerabilities and what it is that the Controls are updated based on new attacks that are identified and analyzed by groups from Verizon to Symantec to the Control.

In addition to being grounded in current attack data, the Controls align with numerous other frameworks, such as PCI DSS, ISO 27001, US CIS Center for Internet Security, NIST SP 800-133, and the NIST Framework. The Controls don't try to replace these other frameworks but they are frequently used by enterprises to make sense of other frameworks. The Controls are a highly practical approach to providing the overarching security strategy for an enterprise. Further, since a program for cyber security is a plan and operations, the Controls can also be used with the Critical Security Controls Measurement Campaign to assess the effectiveness of the organization's security efforts.

The Controls save the best-in-class threat data and transform it into actionable guidance to improve individual and collective security in cyberspace. Too often in cyberspace it is the "bad guy" are better organized and collaborate more closely than the "good guys". The Controls provide a means to turn that around.

The CIS Critical Security Controls are the Core of the NIST Cybersecurity Framework

Since its release in February 2011, the NIST Framework for Improving Critical Infrastructure Cybersecurity (CIS) has become a major part of the national conversation about cybersecurity for the critical infrastructure and beyond. (The Center for Internet Security was an active participant in the development of the NIST Framework and the CIS Critical Security Controls are cited as one of the "reference materials" that can be used to develop a security implementation.)

The Framework provides a way to organize, conduct and drive planning on security goals and improvements for individual enterprises and across sectors of enterprise. But it does not include any specific risk management process, or specify any priority of action. These decisions and judgments are left to the adapter to manage for their specific situation and context.

CIS believes that this task is beyond the ability or resources of most enterprises to do effectively or efficiently. This approach doesn't recognize the interdependency that every enterprise has with its many partners. A community-link approach for considering attacks that

A Case Study in Auditing the CIS Critical Controls at the U.S. Federal Reserve

The U.S. Federal Reserve audit currently covers a wide range of critical functions representing each of the 12 regional Reserve Banks. In recognizing the unique and pervasive nature of cybersecurity risk, the collection of internal auditors used a highly coordinated approach to assess and report on the CIS Critical Security Controls. The audit findings were used to inform the Reserve Banks' risk management efforts as well as the consideration of control effectiveness as demonstrated in previous audits organized by the Controls, in business operations, and in the Reserve Banks' risk management efforts.

Cybersecurity risk spans across all business and IT areas and risks for individual Reserve Banks may vary. Since the Controls are set forth in priority order, they provide a strong starting point for prioritizing audit coverage. The Controls provide a clear framework for effectively managing and improving the effectiveness of internal auditors and information security officers. This combination of prioritization and clear risk knowledge supports an effective baseline of cybersecurity audit coverage against the CIS Critical Security Controls.

As part of management's layered control framework, Fed management assigns an overall maturity score of fed Controls organized by the Controls. Lower assigned maturity scores drive stronger investment and management attention. This aligns the cybersecurity risk focus between management and the internal audit, and improves organizational conversations about relative control effectiveness. It is increasingly apparent that cybersecurity risk isn't just an IT risk — it is an enterprise-wide business risk that requires broad awareness and coordination. The Controls provide a common framework for both management and auditors for the assessment and management of cybersecurity risk. 9000 A Federal Reserve Bank of Richmond.

The National Campaign for Cyber Hygiene

The National Campaign for Cyber Hygiene was developed to provide a plain-language, accessible, and low-cost foundation for implementing the CIS Critical Security Controls. Although the Controls already simplify the challenges of cyber defense by creating community priorities and actions, many enterprises are still struggling.

The Campaign starts with a few basic questions that every corporate and government leader ought to be able to answer:

- Do we know what is connected to our systems and networks? (CSC 1)
- Do we know what software is running (or trying to run) on our systems and networks? (CSC 2)
- Are we continuously managing our systems using "known" and configured software? (CSC 3)
- Do we have continuously logging and managing "known bad" software? (CSC 4)
- Are we aware of the people who have the administrative privileges to change, bypass, or override our security settings? (CSC 5)

These questions, and the actions required to answer them, are represented in plain language by the Top 5 Priority of the Campaign. The Campaign provides a clear framework for both management and auditors for the assessment and management of cybersecurity risk. 9000 A Federal Reserve Bank of Richmond.

The Configuration Benchmarks Community

The Center for Internet Security (CIS) develops and distributes secure configuration benchmarks and automated configuration assessment tools, and centers security software products designed to help organizations improve their security posture. The internationally recognized benchmarks are developed through an open consensus-based process and are aligned with the CIS Critical Security Controls. Cybersecurity and industry professionals from around the world volunteer to participate in CIS's open security benchmark development community. These volunteers, known as the Configuration Benchmarks Community, are responsible for identifying, creating, and updating benchmarks against the benchmarks, and monitor security improvements over time. For more information on CIS-CAT or CIS Benchmark membership visit cisbenchmarks.com.

Security through Collaboration

The Center for Internet Security (CIS) is a not-for-profit organization that is dedicated to enhancing the security of the critical infrastructure and beyond. CIS is a community of security professionals, government and government practitioners. CIS combats existing cybersecurity challenges on a global scale and helps organizations adopt key practices to achieve immediate and effective defenses against cyber attacks. CIS is home to the Multi-State Information Sharing and Analysis Center (ISAC) Benchmarks and CIS Critical Security Controls. To learn more about cybersecurity or follow us at CISecurity.org.

Where to Learn More

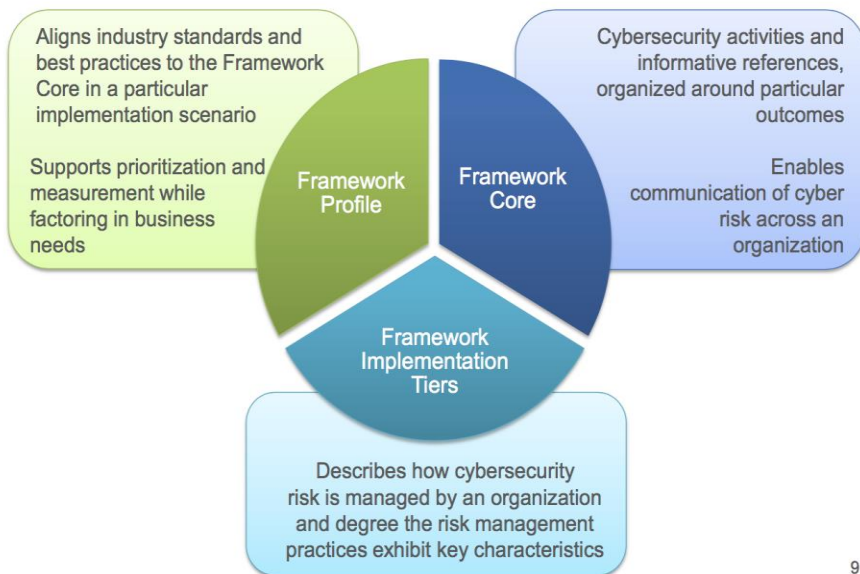
Here are some additional resources for effective planning and implementation of the CIS Critical Security Controls

1) SANS courses on planning and implementing the CIS Critical Security Controls include:

- SEC440: Critical Security Controls Planning, Implementing and Auditing**
This course helps you master specific, proven techniques and tools needed to implement and audit the CIS Critical Security Controls as described by the Center for Internet Security. SEC440 does not contain any risks. It is a hands-on course for those looking for the CIS Critical Security Controls. www.sans.org/courses/critical-security-controls-planning-implementing-auditing
- SEC564: Implementing and Auditing the CIS Critical Security Controls – In-Depth**
This course shows security professionals how to implement the controls in an existing network through cost-effective automation. For auditors, CIOs, and risk officers, the course is the best way

NIST – CYBER SECURITY FRAMEWORK

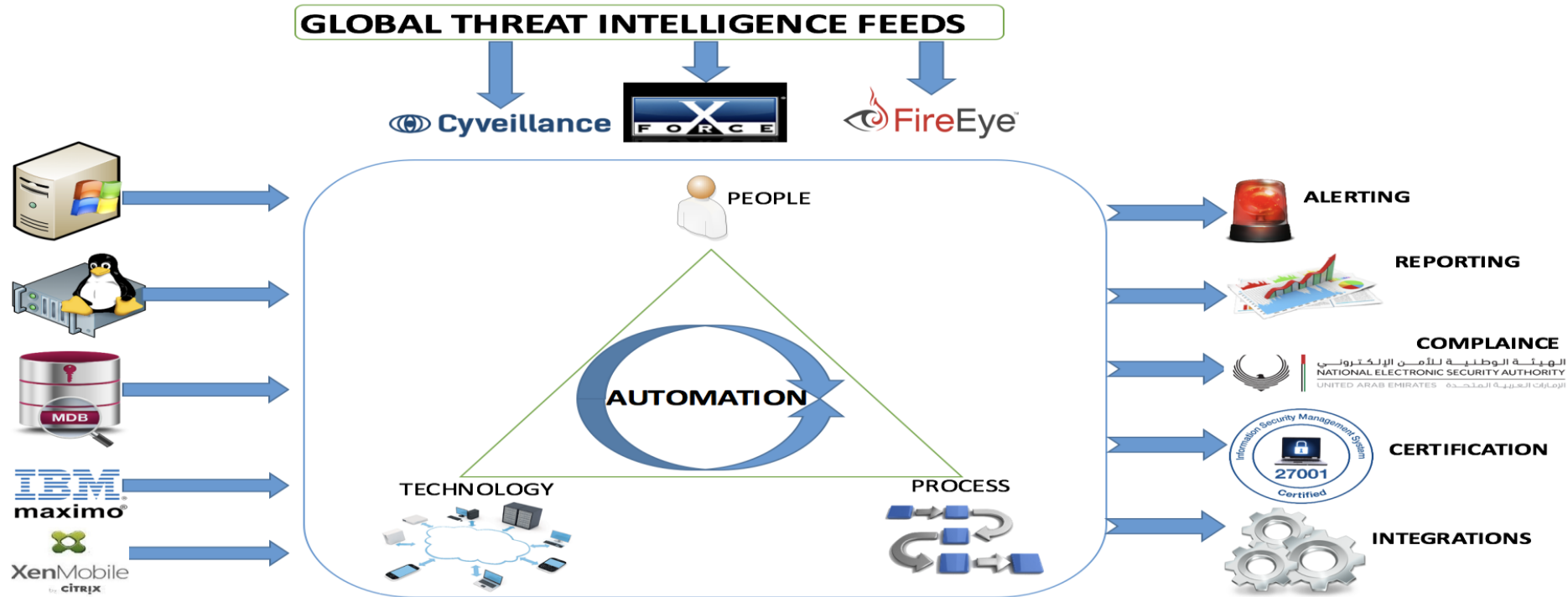
Framework Components



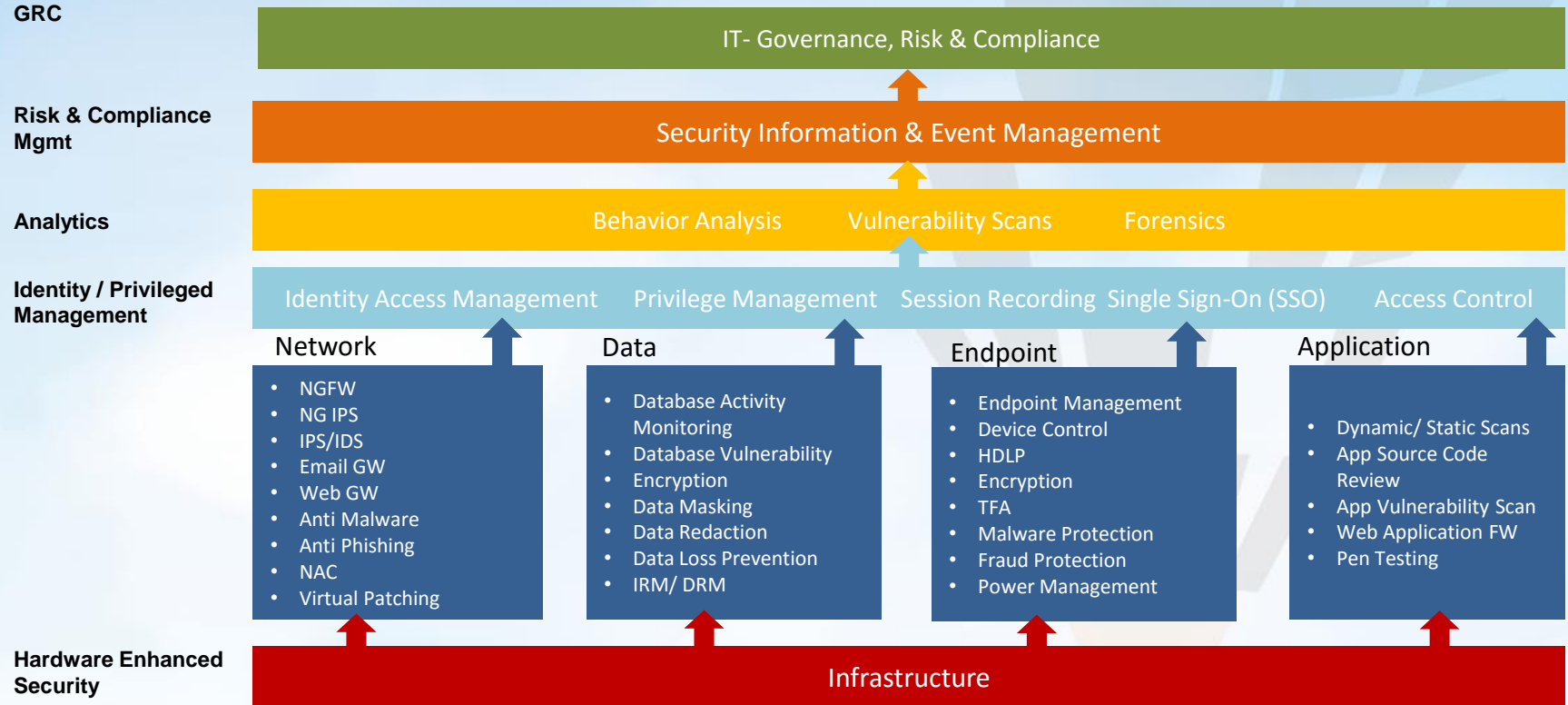
9

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

NANJGEL AUTOMATED CYBER SECURITY FRAMEWORK



Automated Framework Architecture



Cyber Analytics – Using IBM QRadar

Security Intelligence Solutions

QRadar Log Manager

QRadar SIEM

QRadar Risk Manager

QRadar Vulnerability Manager

QRadar Incident Forensics

Reporting Engine

Workflow

Rules Engine

Real-Time Viewer

Analytics Engine

Warehouse

Archival

Normalization

Security Intelligence Operating System (SIOS)



Correlation

- Logs/events
- Flows
- IP reputation
- Geographic location

Activity baselining and anomaly detection

- User activity
- Database activity
- Application activity
- Network activity

Offense identification

- Credibility
- Severity
- Relevance

True offense

Suspected incidents

Extensive data sources



Deep intelligence



Exceptionally accurate and actionable insight

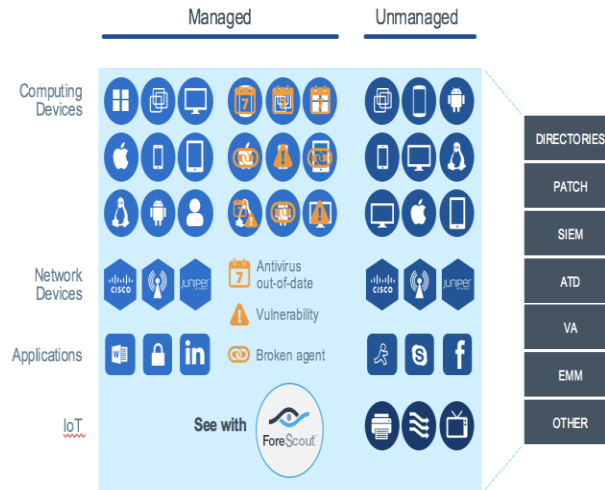
Cyber Security Automation – EVAS – ForeScout

See

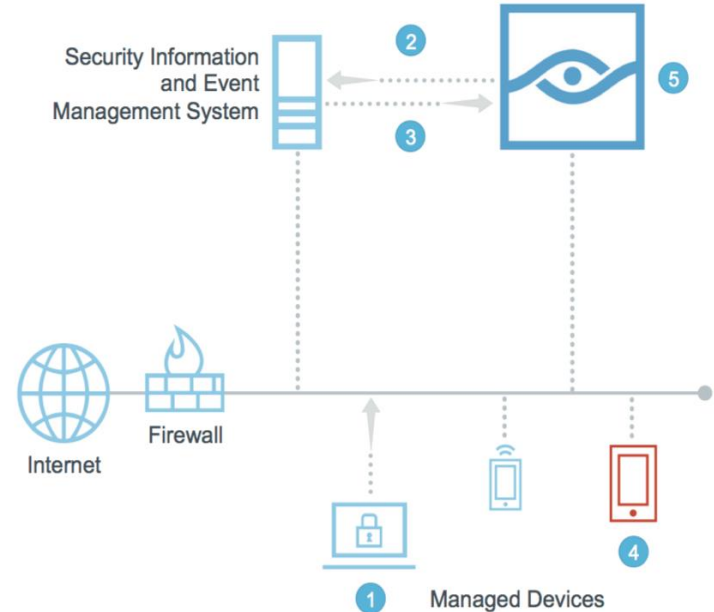


AGENTLESS

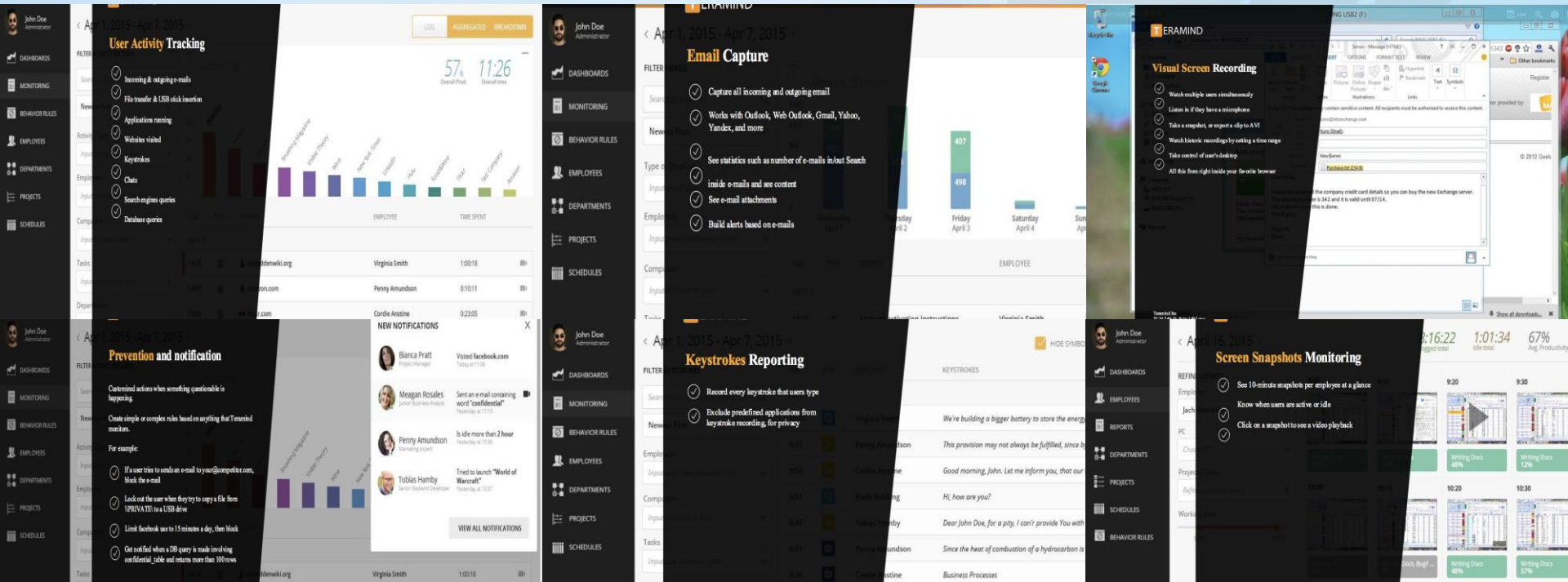
CONTINUOUS



ForeScout CounterACT®



Automated End User Risk Analysis



Automated Global Threat Intelligence

LookingGlass monitors the broadest possible set of sources to maximize detection and speed



Anti-Phishing
Take down
Service



Anti Spoofing
DMARC
Email Service



C-Level
ID Theft
Fraud
Detection



Social Media
Monitoring
Facebook,
Twitter etc



Domain
Name
Registrations
and "Go
Live" Alerts



Patented Site-
Seal Early-
Detection
System

About Us

Established in **2005**
providing IT
Security
Solutions

We lead the
way in a
different
approach to
information
security

Presence in **Middle
East , Europe &
India** with over **12
strategic partners
& alliances**

Long standing
**customer
relationships**
across all
verticals

We provide next
generation IT
solutions for
secured business
operations



