CISO Story/Perspective: Practical Zero Trust and XDR

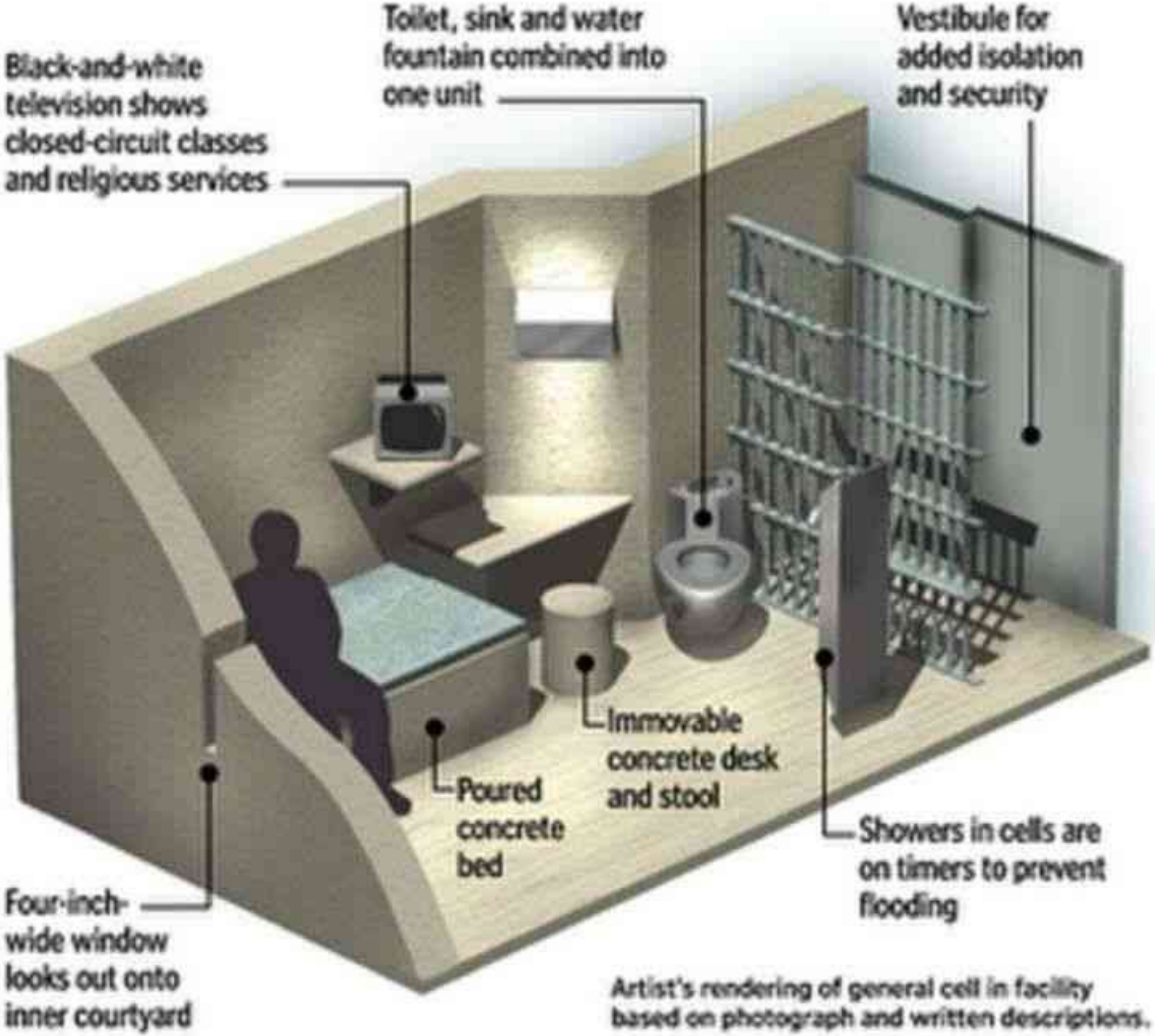
Chip Crane, CISSP
SC Upstate Regional VP InfraguardS
Americas Technical Security Leader
IBM Security
wcrane@us.ibm.com

DISCLAIMER:

1. If you, or the organization you represent, are experiencing a breach, immediate threat, high risk exposure, etc. consult me after this presentation.

2. I am very “zealous” about security, which I am suppressing for this presentation

3. “Discretion is the better part of valor”. Therefore, everything I say is “hypothetical”


Black-and-white television shows closed-circuit classes and religious services
Toilet, sink and water fountain combined into one unit
Vestibule for added isolation and security
Immovable concrete desk and stool
Poured concrete bed
Showers in cells are on timers to prevent flooding
Four-inch-wide window looks out onto inner courtyard

Artist's rendering of general cell in facility based on photograph and written descriptions.

Organizations are undergoing rapid digital transformation

Shift to hybrid cloud

Infrastructure distributed across hybrid cloud, edge, IoT and OT

Remote workforce

Employees accessing data from anywhere, using any device

Regulatory and privacy demands

As data is shared, regulations and end-users demand more control

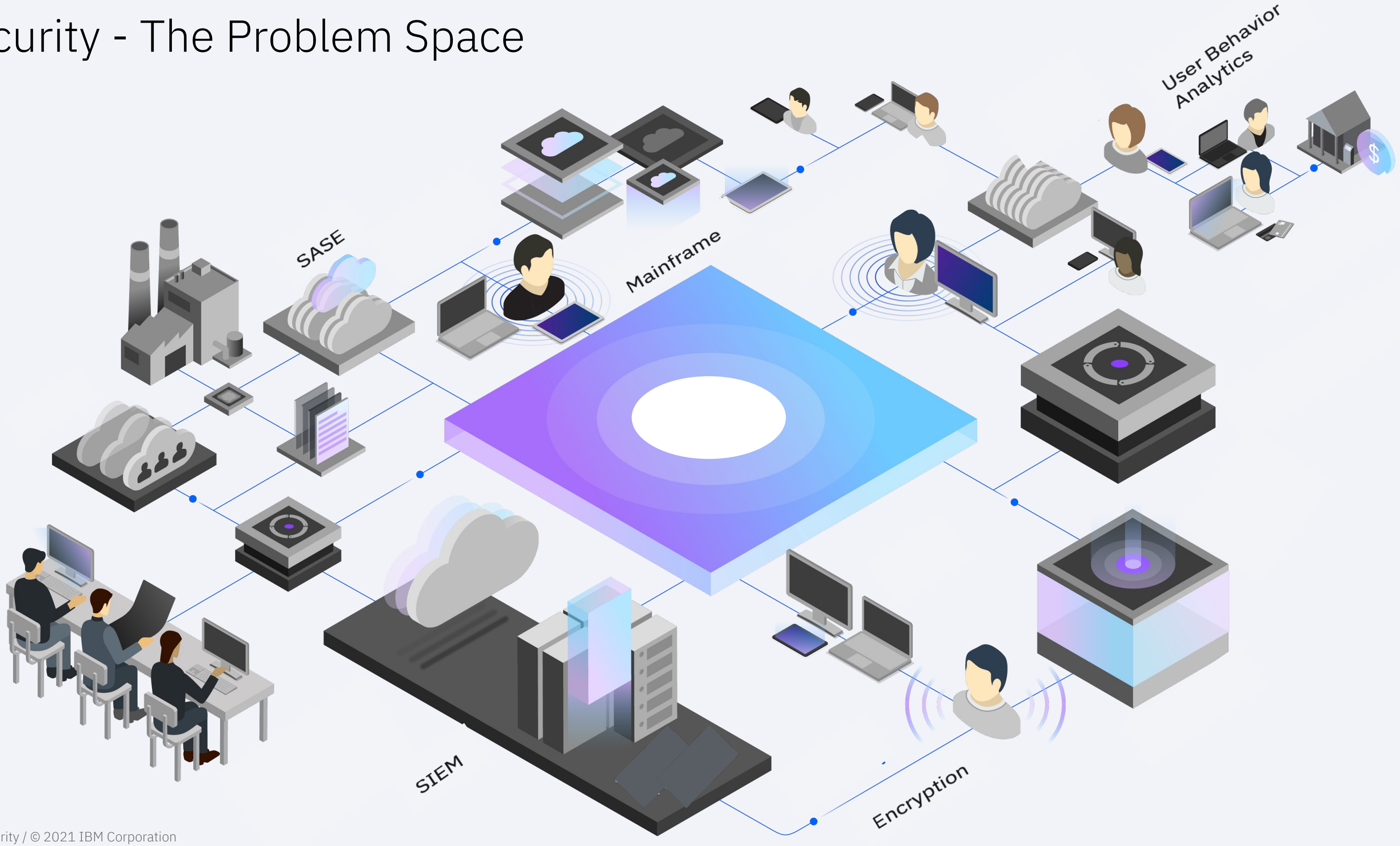
Evolving threats - Ransomware

Increasing ransomware and other sophisticated attacks

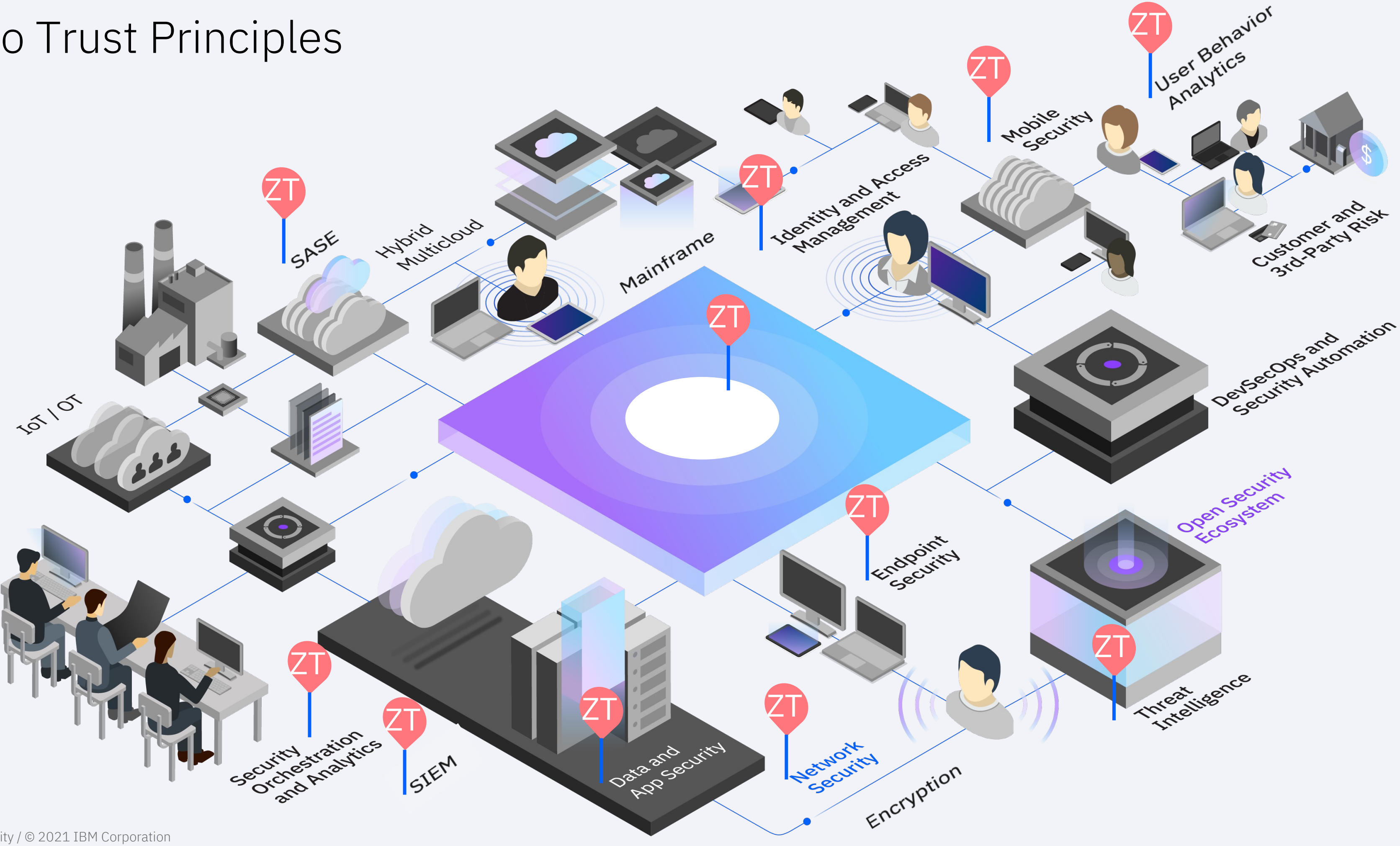
Building a SuperMax prison on a boat, that is trailered, being driven up a highway at 80 mph, crossing a mountain, in a snowstorm, with broken windshield wipers.

We have to take a practical approach without closing the business

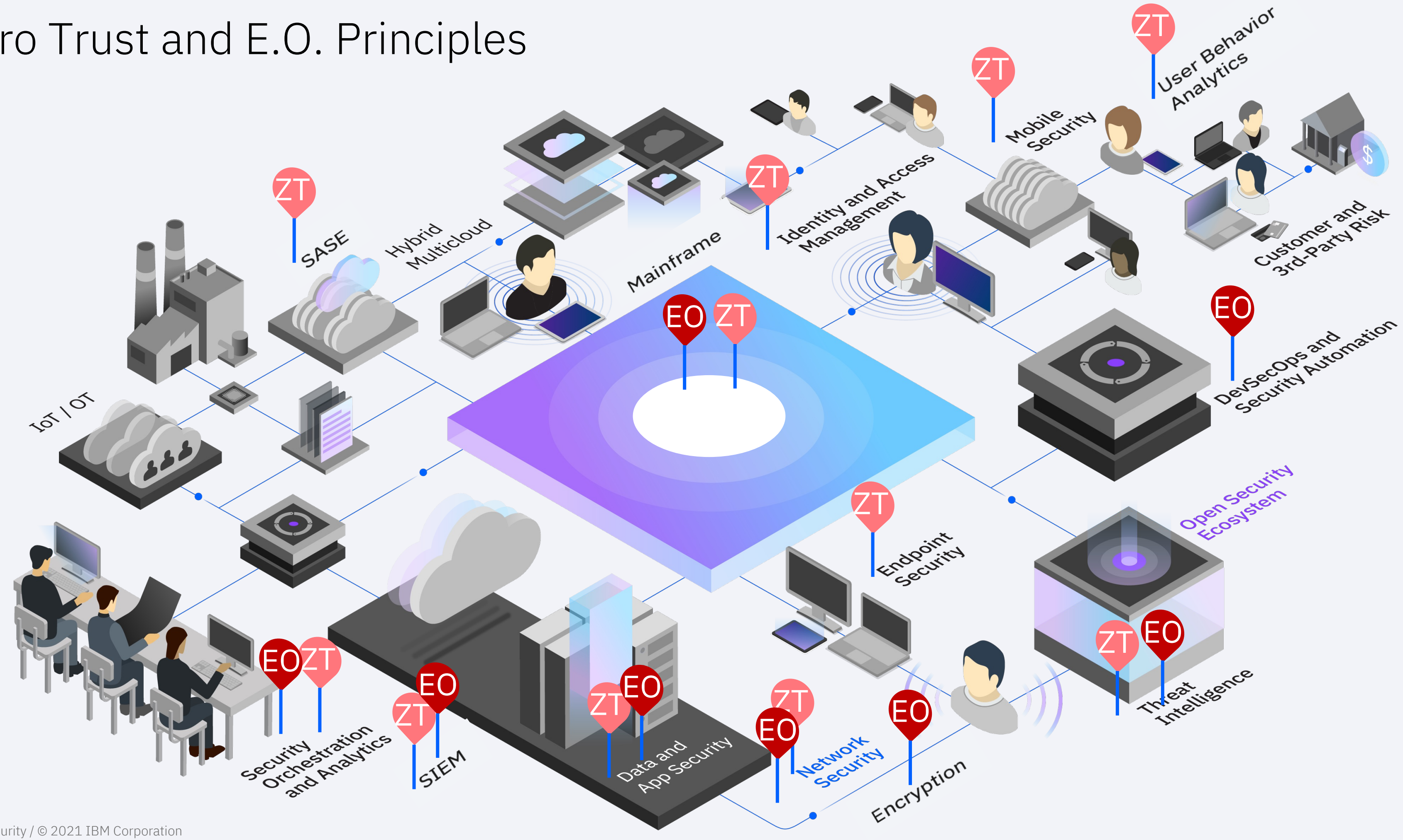
Security - The Problem Space



Zero Trust Principles



Zero Trust and E.O. Principles



Cyberattacks are the top cause of business disruption, with ransomware leading the way

$1.59M

portion of data breach costs attributable to lost business, including business disruption, system downtime, lost customers and reputation losses.[1]

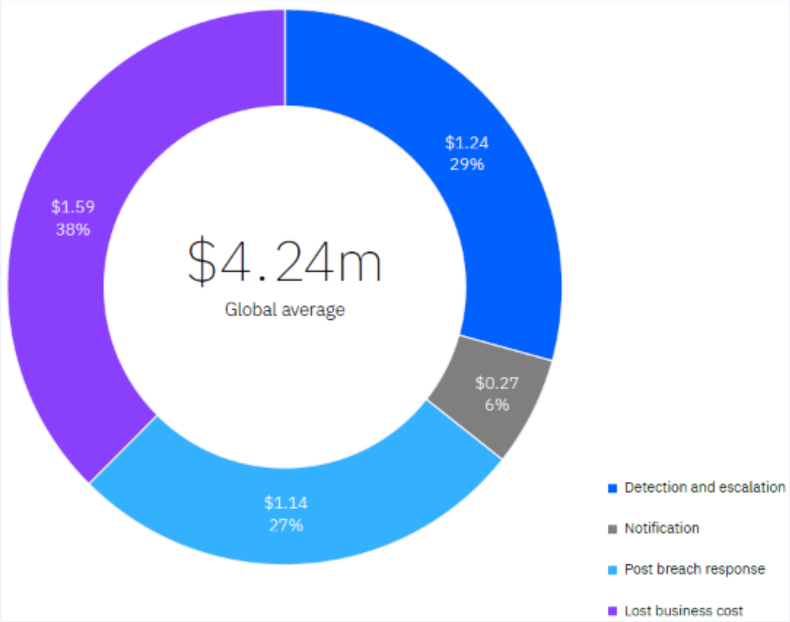
23%

of all security attacks in 2020 were the result of ransomware, up 15% from 2019.[2]

20%

Share of breaches initially caused by compromised credentials, the most common initial attack vector. [1]

Average cost of a data breach (38% from business disruption)



[1] IBM Security Cost of a Data Breach Report 2021
[2] IBM Security X-Force Threat Intelligence Index 2021

Unfortunately, not all attacks come from the outside

Anyone can be an insider

14%
Compromised users

23%
Malicious users

62%
Careless users

Insider threats are hard to contain

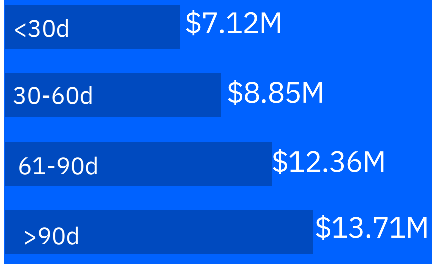
77
Average number of days to contain each insider threat incident

87%
Take 30+ days to contain

And it comes at a cost

$644K
Cost per insider threat incident

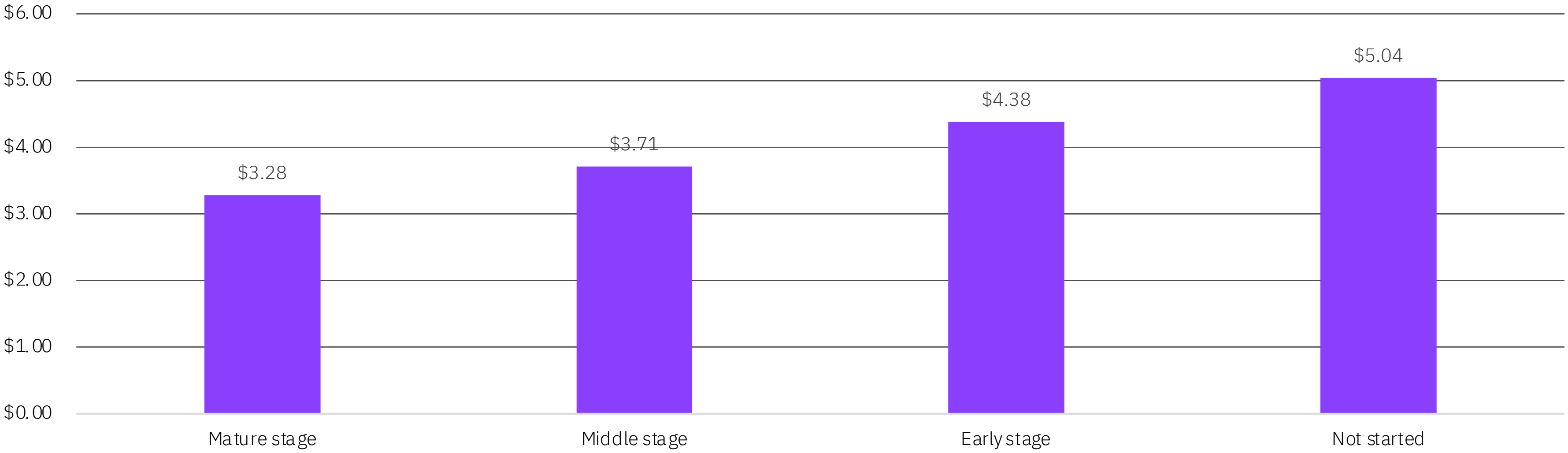
$11.5M
Average annual cost to respond to insider threats



Source: *2020 Cost of Insider Threats Global Report*, Ponemon Institute.

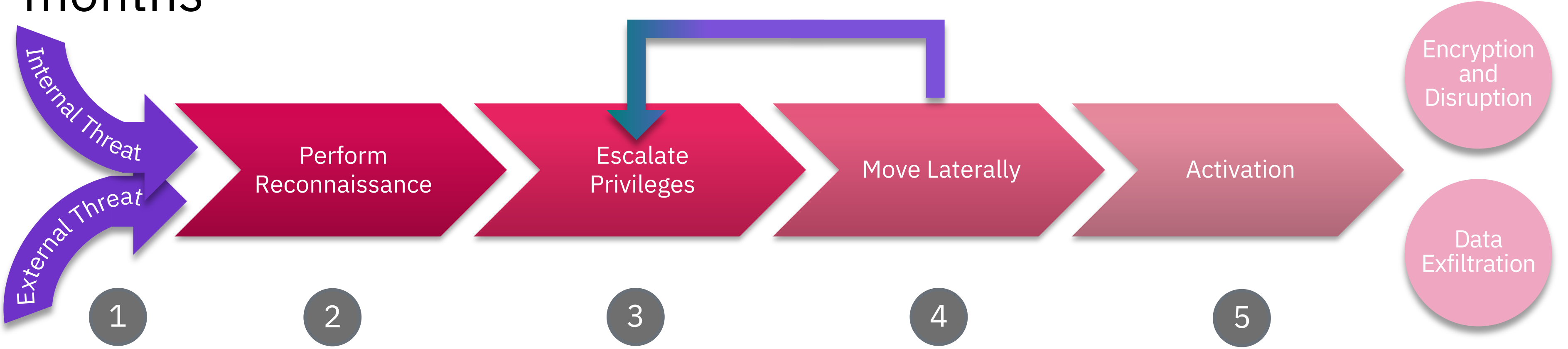
Average total cost of a breach by the state of **zero trust** deployment

Measured in US$ millions



Source: 2021 Cost of a Data Breach Report, Ponemon Institute

Ransomware, insider threats, and other persistent attacks are highly sophisticated and can go undetected for weeks or months



Internal Threat

External Threat

Perform Reconnaissance

Escalate Privileges

Move Laterally

Activation

Encryption and Disruption

Data Exfiltration

1

Phishing / spear phishing

Malware downloaded

2

Scan networks

Infiltrate on-prem & cloud

Resist detection & removal

Link command & control

3

Access privileged accounts

Leverage admin rights

4

Identify additional targets

Self propagation

5

Encrypt files & databases

Locate & encrypt backups

Exfiltrate high-value data

Example Targets

Crown Jewels

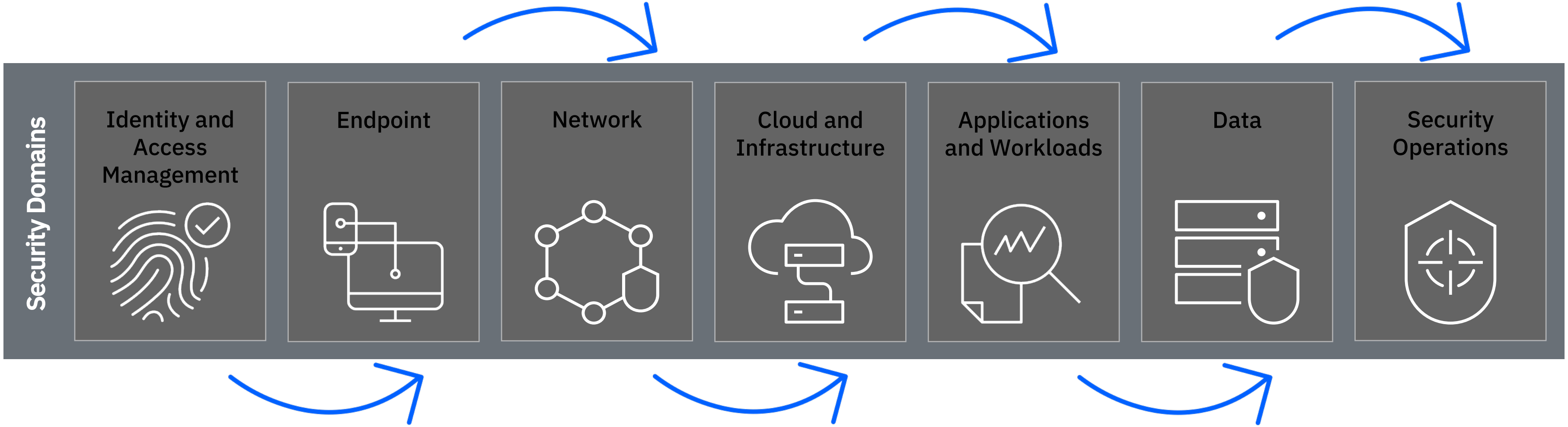
Intellectual Property

PII

POS and OT

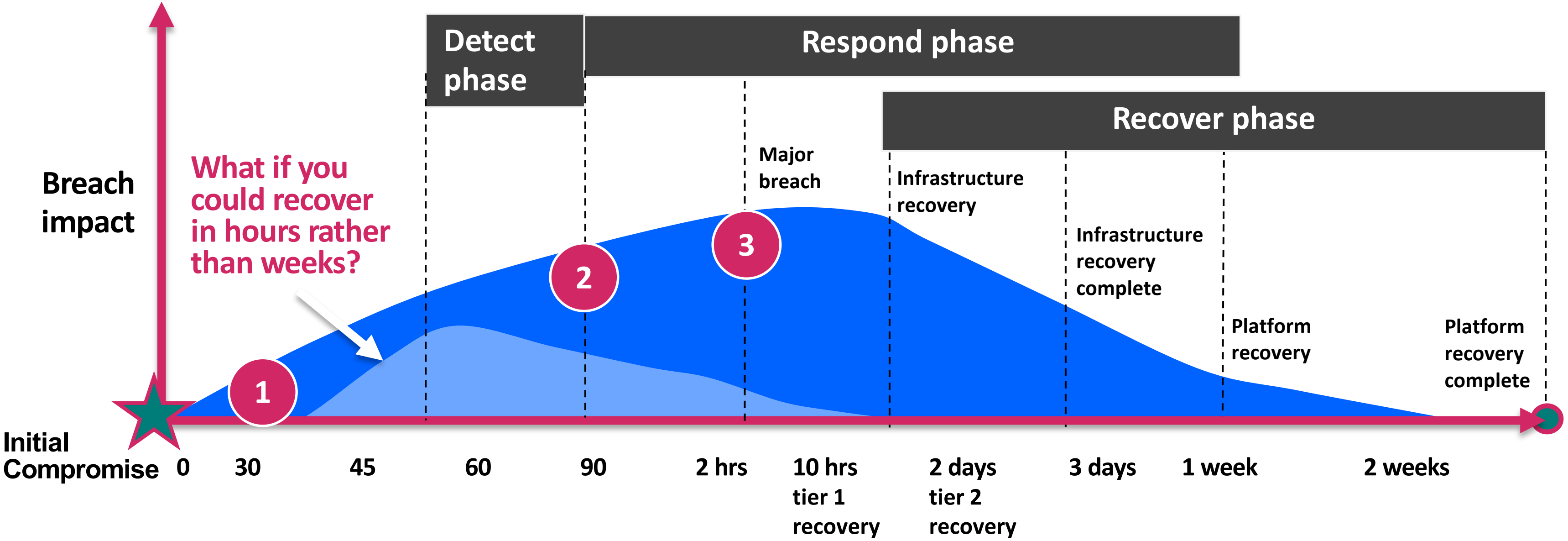
Understanding the attack chain is critical for preparation, protection, and prevention

…However, no single tool can holistically solve the challenge of business disruption.



It demands open integration across security domains.

How quickly you can move from detection to recovery can be the difference between a minor incident and a major breach



1 Corruption of data occurs – but not yet detected

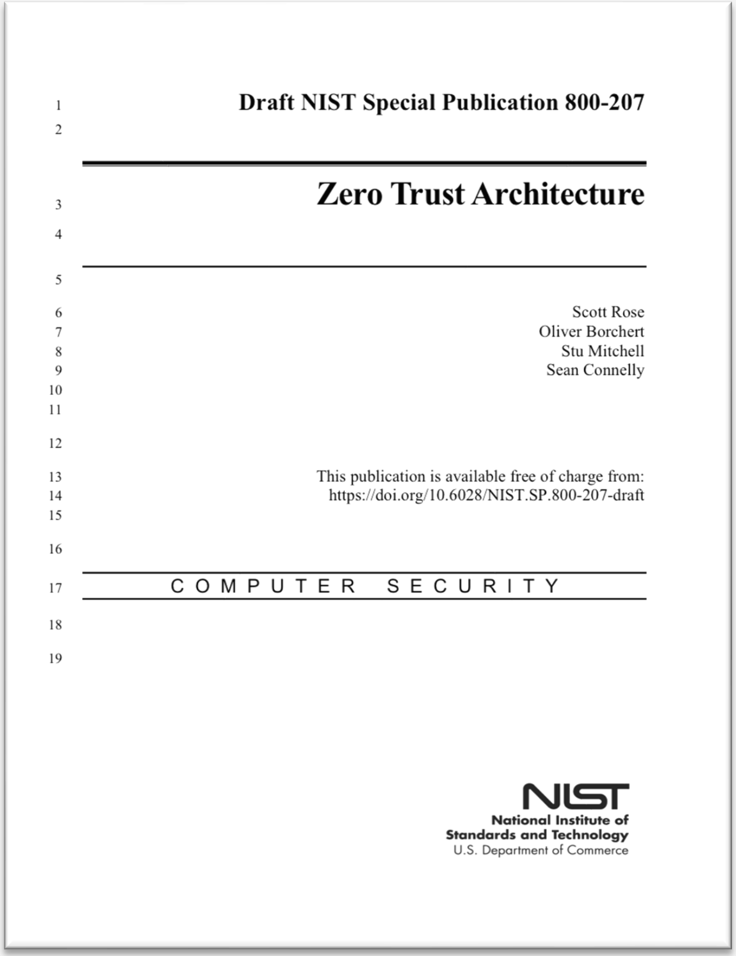
2 Without proper data resilience, corruption is detected much later and has a greater chance to spread

3 It takes even longer to identify all impacted data once the corruption has spread within the enterprise

What is Zero Trust?

Zero Trust is the term for an evolving set of network **security paradigms** that:

- move network defenses **from wide network perimeters** to **narrowly focusing** on **individual** or **small groups** of resources.
- **no implicit trust granted to systems based on their physical or network location** (i.e., local area networks vs. the Internet).
- access to data resources is granted **when the resource is required**
- authentication (both user and device) is performed **before the connection is established**.



Draft NIST Special Publication 800-207

Zero Trust Architecture

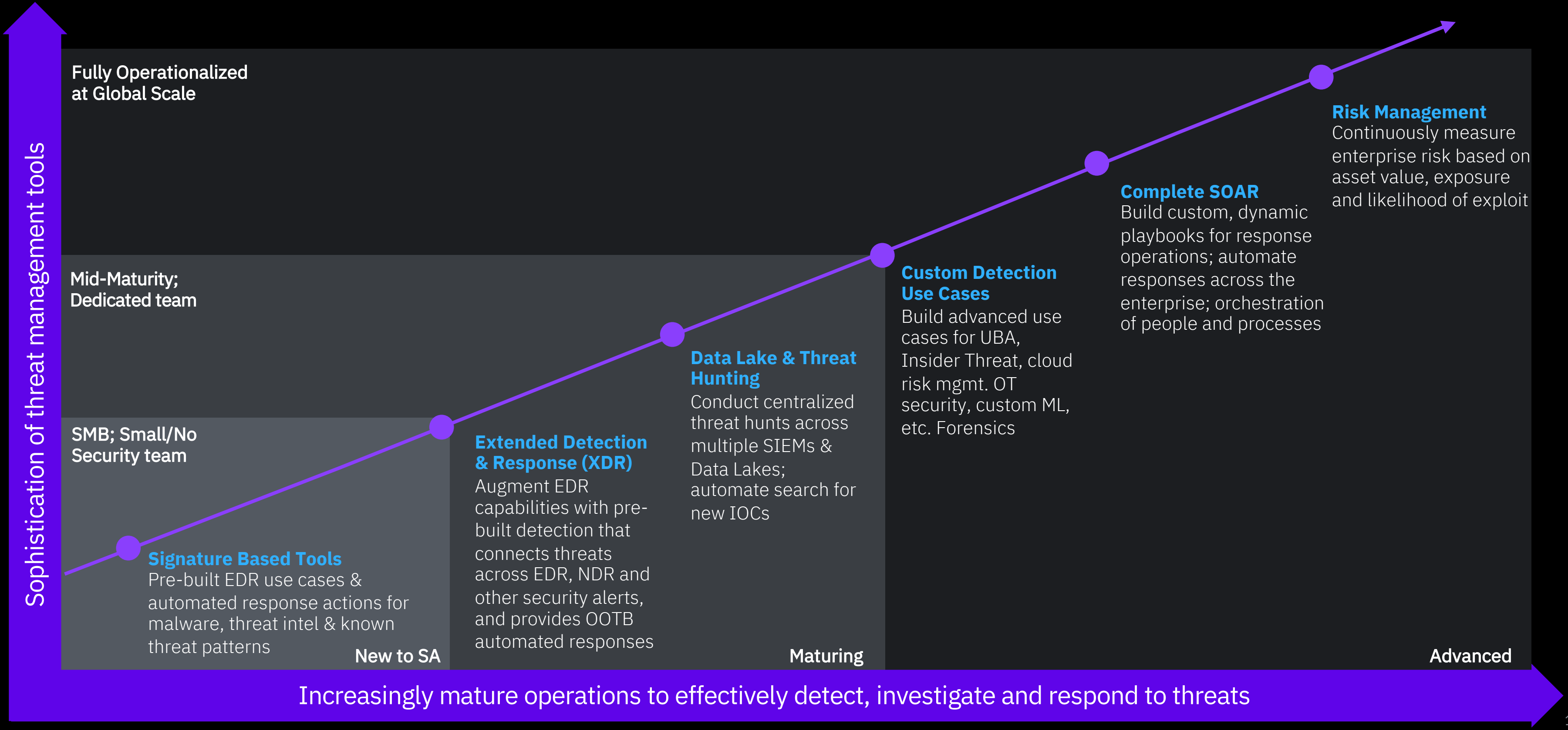
Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207-draft

COMPUTER SECURITY

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Capability Maturity Model (CMM) applied to Threat Detection & Response



Sophistication of threat management tools

Fully Operationalized at Global Scale

Mid-Maturity; Dedicated team

SMB; Small/No Security team

Signature Based Tools
Pre-built EDR use cases & automated response actions for malware, threat intel & known threat patterns

Extended Detection & Response (XDR)
Augment EDR capabilities with pre-built detection that connects threats across EDR, NDR and other security alerts, and provides OOTB automated responses

Data Lake & Threat Hunting
Conduct centralized threat hunts across multiple SIEMs & Data Lakes; automate search for new IOCs

Custom Detection Use Cases
Build advanced use cases for UBA, Insider Threat, cloud risk mgmt. OT security, custom ML, etc. Forensics

Complete SOAR
Build custom, dynamic playbooks for response operations; automate responses across the enterprise; orchestration of people and processes

Risk Management
Continuously measure enterprise risk based on asset value, exposure and likelihood of exploit

New to SA

Maturing

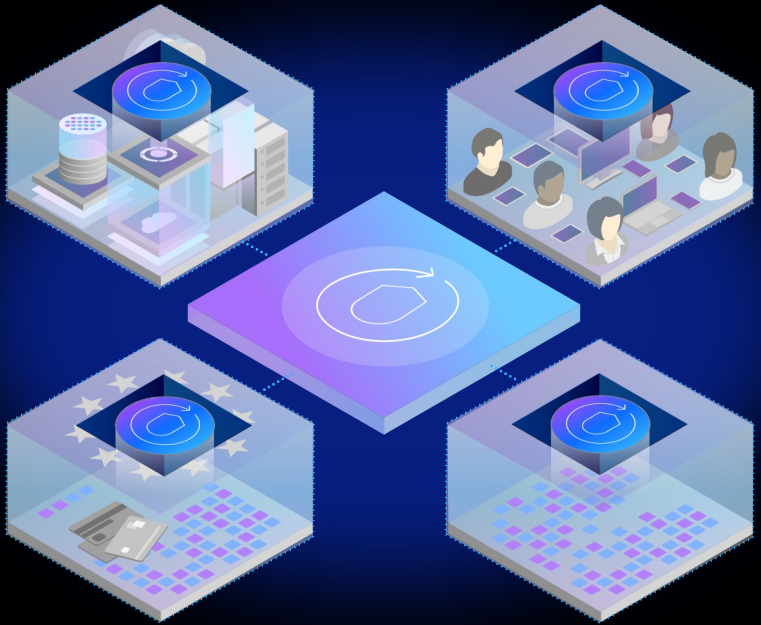
Advanced

Increasingly mature operations to effectively detect, investigate and respond to threats

A modern and practical zero trust approach is needed to advance the business

A zero trust approach to...

- Strategically Assume breach
- Establish least privilege
- Verify continuously
- Perimeter based controls should be viewed as just data points



Delivers real business outcomes

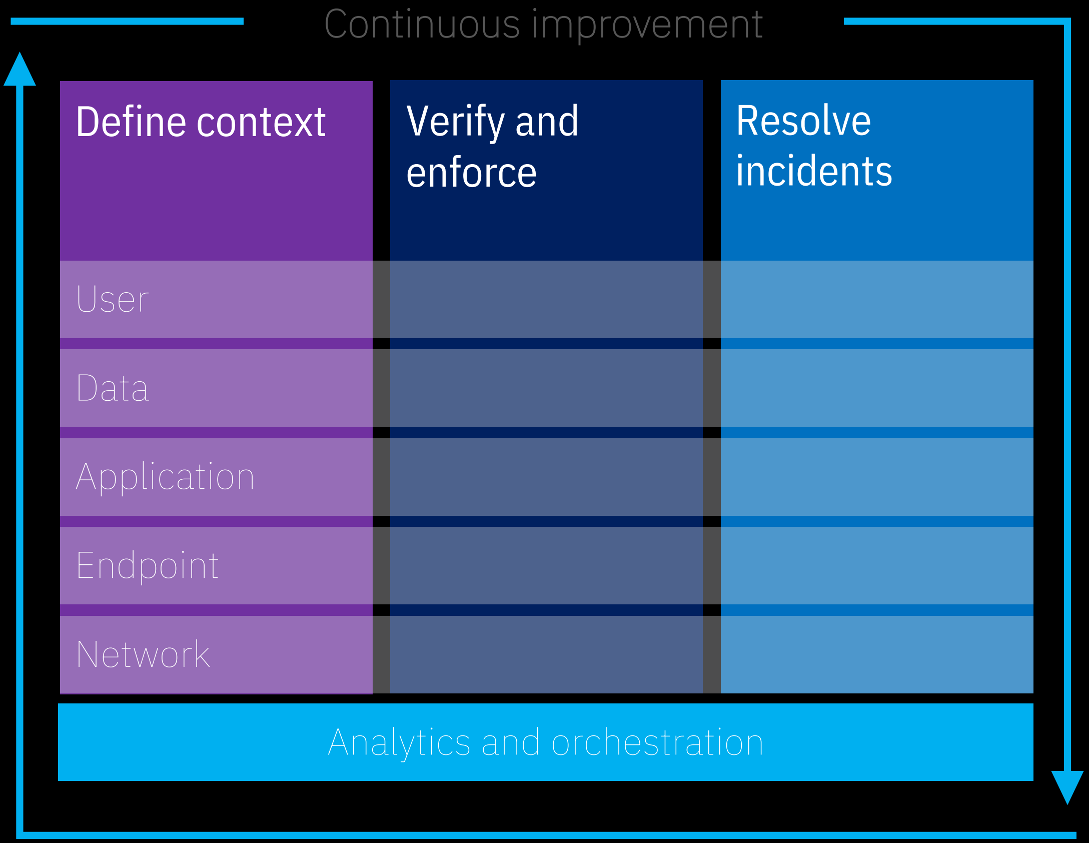
- Faster cloud adoption
- More productive employees
- Improve business continuity
- Build trust and improve customer experience

Context is Essential For Zero Trust

Enabling the **right user**
to have the **right access**
to the **right data**

under the **right conditions**

What does zero trust success look like in practice?



Continuous improvement

Define context	Verify and enforce	Resolve incidents
User		
Data		
Application		
Endpoint		
Network		

Analytics and orchestration

Zero Trust

Capability Model

ZERO TRUST

CORE PILLARS

CORE CAPABILITIES

DATA	DEVICE & ENDPOINT	NETWORK & ENVIRONMENT	APPLICATION & WORKLOAD	USER	VISIBILITY & ANALYTICS	AUTOMATION & ORCHESTRATION
Data Loss Prevention	Device Authorization	API Integration	DevSecOps	User Authentication	Discovery & Baselining	API Standards
Data Classification	HW & SW Inventory	Fully Encrypted Traffic	Application Delivery	User Authorization	Machine Learning	Incident Response
Metadata Mgmt.	Cloud-based Baseline Enforcement	Common Service Access	Micro Segmentation	Cybersecurity Access Policy	Advanced Threat Protection	Artificial Intelligence
Data Encryption	Compliance Enforcement	Network Segmentation	Application Segmentation	Privilege Access Mgmt.	Monitoring and Auditing	Security Orchestration, Automation & Response (SOAR)
Data Segmentation	Device Authentication	Cloud Access Security Broker (CASB)	Software Chain Supply	Single Identity Platform	Risk Evaluation & Dynamic Risk Scoring	
Dynamic Data Masking (DDM)	Cloud-based Software Deployment & Mgmt.	Software Defined Networking (SDN)	Software Defined Compute	MFA	Security and Information Event Management (SIEM)	
Fully-automated Data Tagging via ML/AI	Intelligence for Endpoint Response	Software Defined Perimeter *(Access to Apps and Data)*	Application Approved/ Prohibited List	In-session Monitoring		
Data Rights Management (DRM)		Application Proxy	Application Visibility & Access *(Anytime, Anywhere)*	ABAC		
				Key Mgmt.		
				Transparent Authentication		

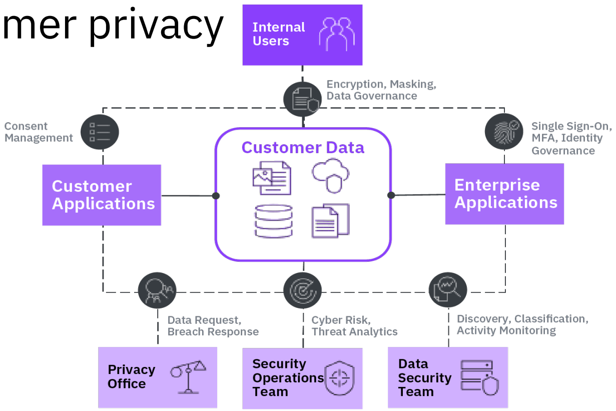
Threat Score, Risk Score, Target Valuation, Triage Priority, and Compliance Score (snapshots & trend)

FCEB Framework (when available); Periodic review updates within 360 days; system wide data/system/software/user/log provenance (origin)

GOVERNANCE

Zero Trust Solution Blueprints – Security Use Case Driven

Preserve customer privacy



Internal Users

Encryption, Masking, Data Governance

Consent Management

Single Sign-On, MFA, Identity Governance

Customer Applications

Customer Data

Enterprise Applications

Data Request, Breach Response

Cyber Risk, Threat Analytics

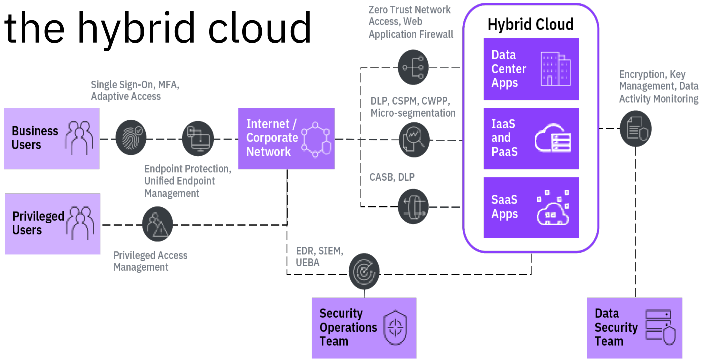
Discovery, Classification, Activity Monitoring

Privacy Office

Security Operations Team

Data Security Team

Protect the hybrid cloud



Zero Trust Network Access, Web Application Firewall

Hybrid Cloud

Data Center Apps

IaaS and PaaS

SaaS Apps

Single Sign-On, MFA, Adaptive Access

DLP, CSPM, CWPP, Micro-segmentation

Encryption, Key Management, Data Activity Monitoring

Business Users

Internet / Corporate Network

Endpoint Protection, Unified Endpoint Management

CASB, DLP

Privileged Users

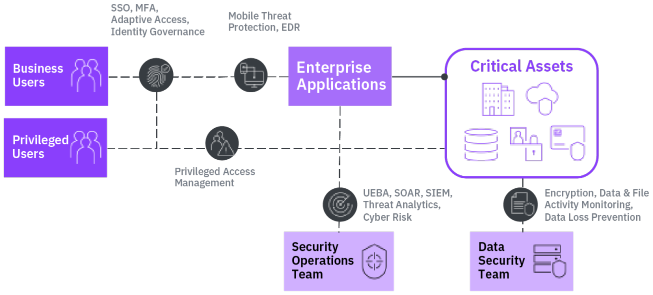
Privileged Access Management

EDR, SIEM, UEBA

Security Operations Team

Data Security Team

Reduce the risk of insider threats



SSO, MFA, Adaptive Access, Identity Governance

Mobile Threat Protection, EDR

Business Users

Enterprise Applications

Critical Assets

Privileged Users

Privileged Access Management

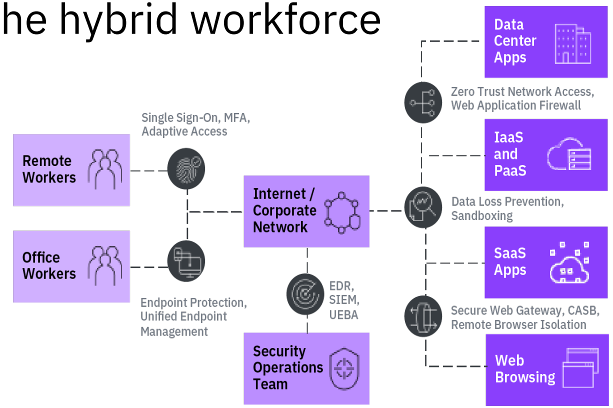
UEBA, SOAR, SIEM, Threat Analytics, Cyber Risk

Encryption, Data & File Activity Monitoring, Data Loss Prevention

Security Operations Team

Data Security Team

Secure the hybrid workforce



Data Center Apps

Zero Trust Network Access, Web Application Firewall

Single Sign-On, MFA, Adaptive Access

IaaS and PaaS

Remote Workers

Internet / Corporate Network

Data Loss Prevention, Sandboxing

Office Workers

SaaS Apps

EDR, SIEM, UEBA

Endpoint Protection, Unified Endpoint Management

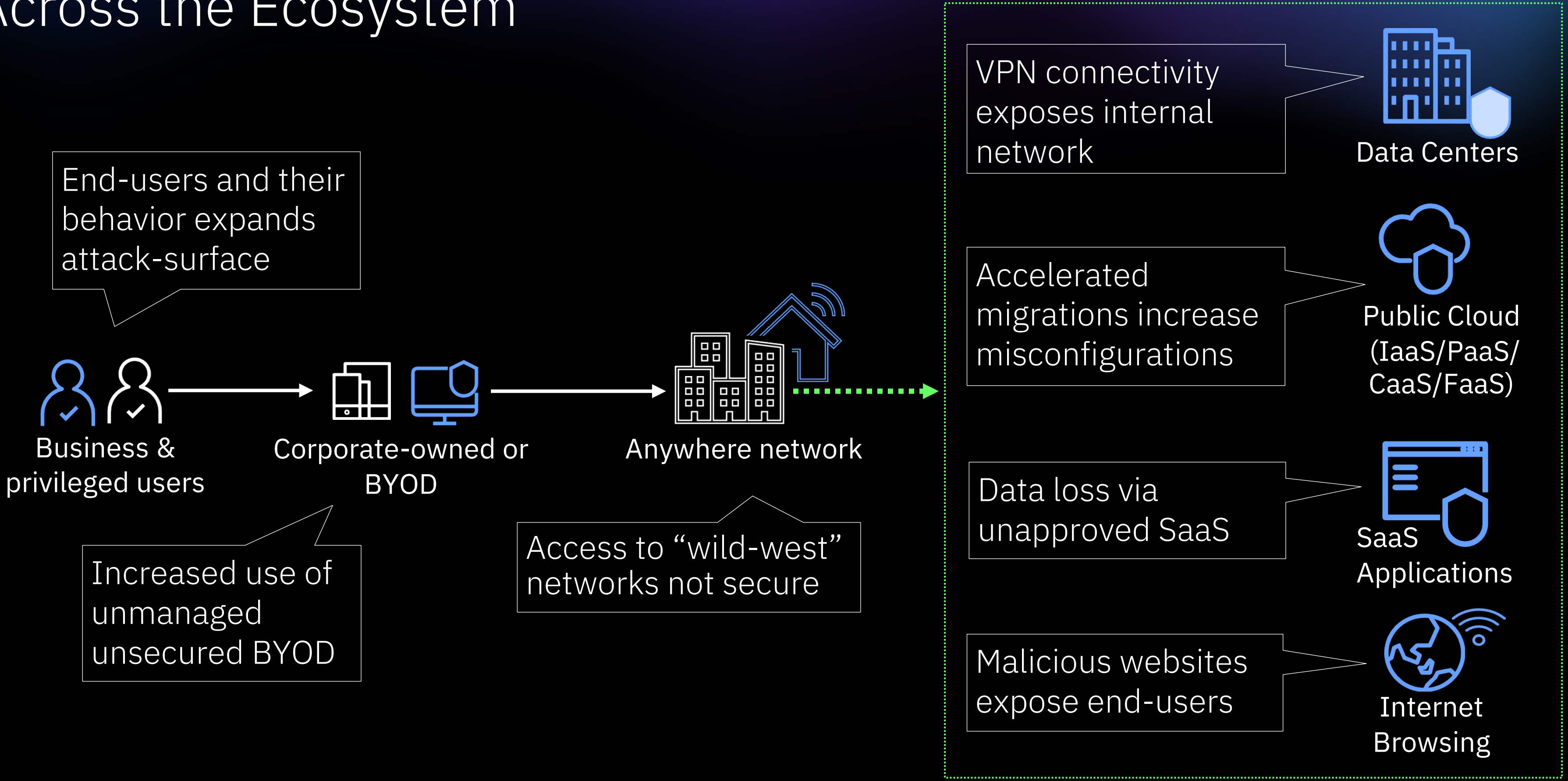
Secure Web Gateway, CASB, Remote Browser Isolation

Security Operations Team

Web Browsing

Zero Trust Hybrid Workforce Use Case

Increasing Remote-Work Footprint Amplifies Threats Across the Ecosystem



End-users and their behavior expands attack-surface

Business & privileged users

Corporate-owned or BYOD

Increased use of unmanaged unsecured BYOD

Anywhere network

Access to “wild-west” networks not secure

VPN connectivity exposes internal network

Data Centers

Accelerated migrations increase misconfigurations

Public Cloud (IaaS/PaaS/ CaaS/FaaS)

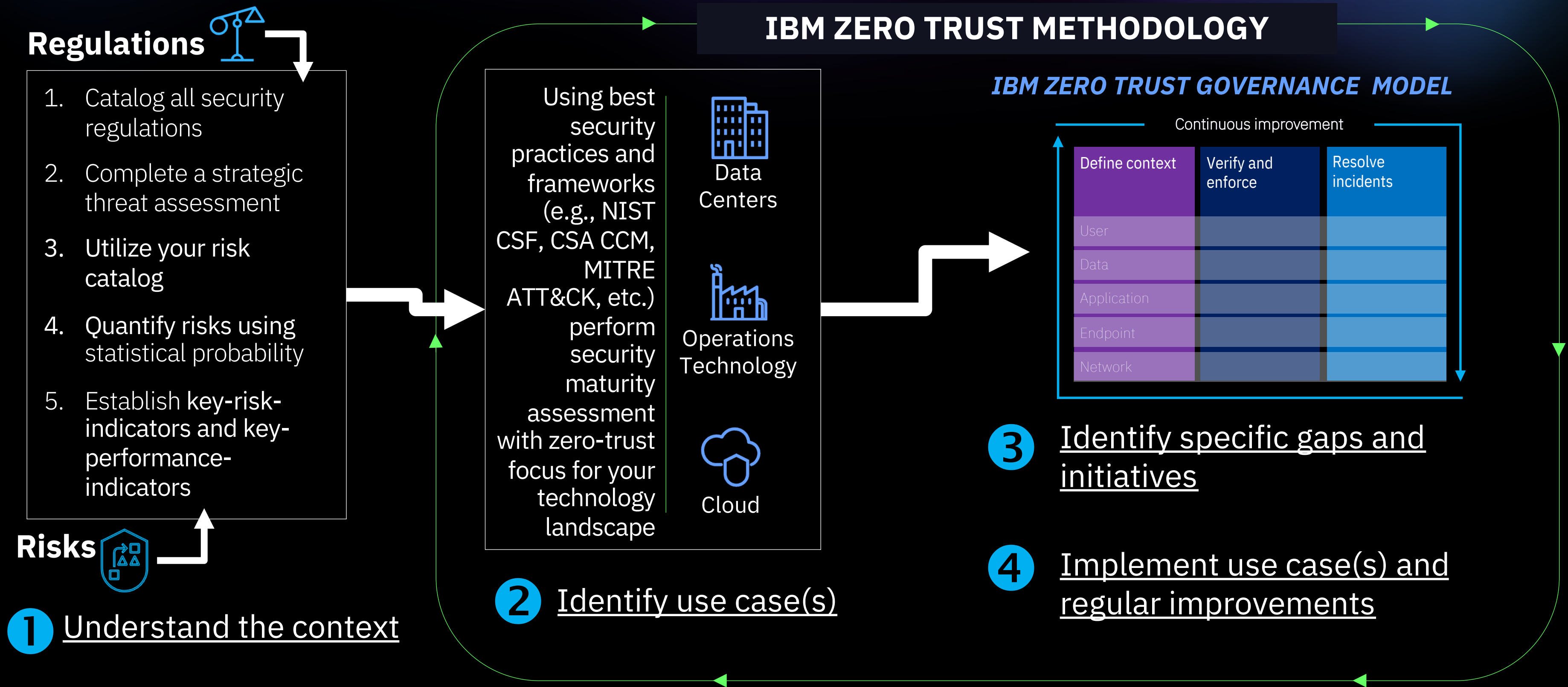
Data loss via unapproved SaaS

SaaS Applications

Malicious websites expose end-users

Internet Browsing

Mitigate Risks with Zero Trust as the Guiding Principle



Regulations

1. Catalog all security regulations
2. Complete a strategic threat assessment
3. Utilize your risk catalog
4. Quantify risks using statistical probability
5. Establish key-risk-indicators and key-performance-indicators

Risks

1 Understand the context

IBM ZERO TRUST METHODOLOGY

Using best security practices and frameworks (e.g., NIST CSF, CSA CCM, MITRE ATT&CK, etc.) perform security maturity assessment with zero-trust focus for your technology landscape

2 Identify use case(s)

IBM ZERO TRUST GOVERNANCE MODEL

Continuous improvement

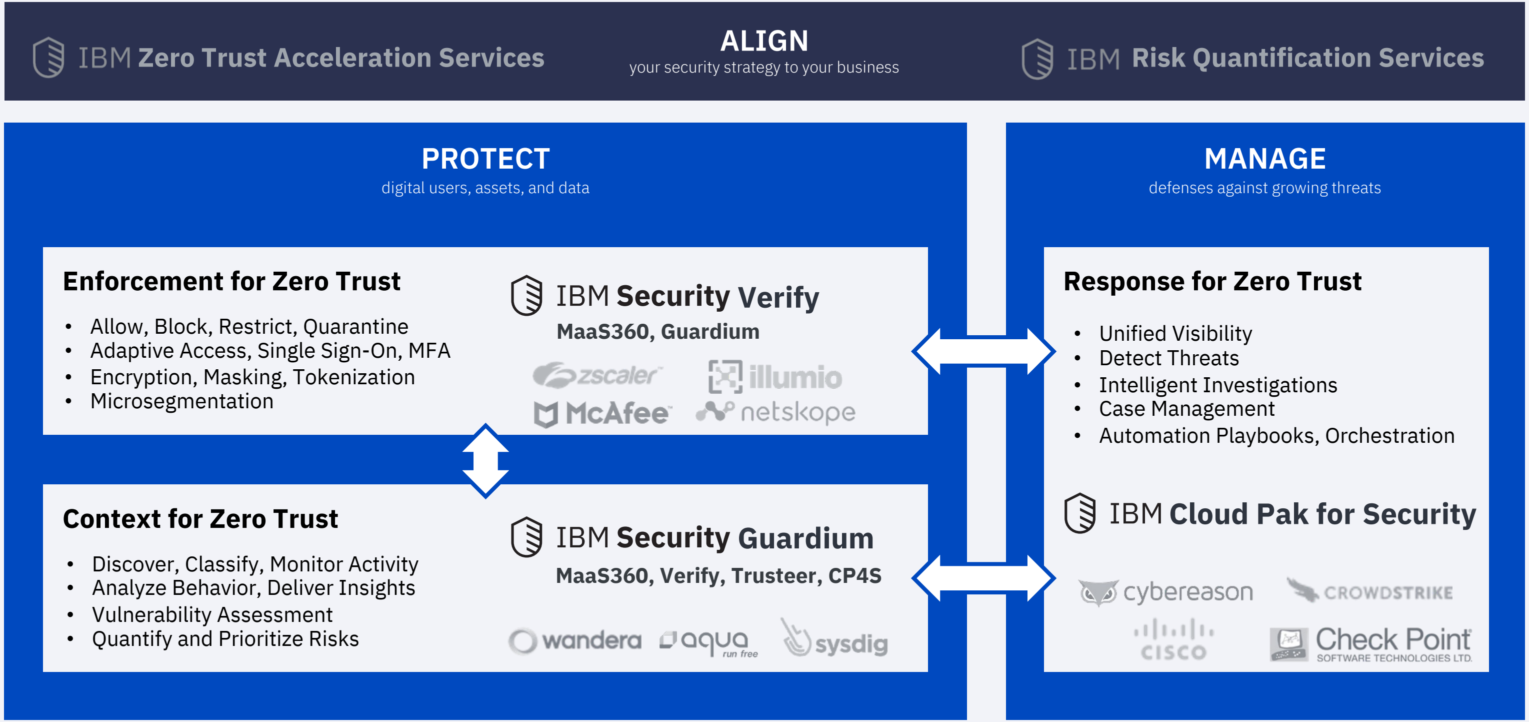
Define context	Verify and enforce	Resolve incidents
User		
Data		
Application		
Endpoint		
Network		

3 Identify specific gaps and initiatives

4 Implement use case(s) and regular improvements

IBM Security's Zero Trust Solutions

Enabling the right user - under the right conditions - to have the right access - to the right data



IBM **Zero Trust Acceleration Services**

ALIGN
your security strategy to your business

IBM **Risk Quantification Services**

PROTECT
digital users, assets, and data

Enforcement for Zero Trust

- Allow, Block, Restrict, Quarantine
- Adaptive Access, Single Sign-On, MFA
- Encryption, Masking, Tokenization
- Microsegmentation

IBM **Security Verify**
MaaS360, Guardium

zscaler illumio McAfee netskope

Context for Zero Trust

- Discover, Classify, Monitor Activity
- Analyze Behavior, Deliver Insights
- Vulnerability Assessment
- Quantify and Prioritize Risks

IBM **Security Guardium**
MaaS360, Verify, Trusteer, CP4S

wandera aqua run free sysdig

MANAGE
defenses against growing threats

Response for Zero Trust

- Unified Visibility
- Detect Threats
- Intelligent Investigations
- Case Management
- Automation Playbooks, Orchestration

IBM **Cloud Pak for Security**

cybereason CROWDSTRIKE CISCO Check Point SOFTWARE TECHNOLOGIES LTD.

Note: Vendors depicted are representative only and does not indicate a specific relationship or agreement at this time

Emerge Smarter: Zero Trust Framing & Discovery

An interactive virtual session that helps you understand and prioritize strategic Zero Trust initiatives.

The details

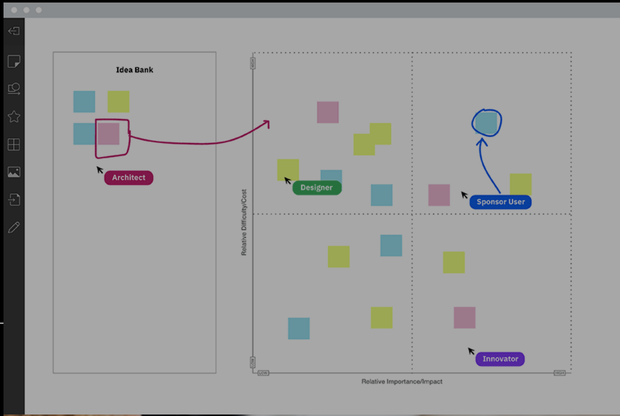
IBM subject matter experts will help you modernize your security program to uncover hidden threats faster, make more informed, risk-based decisions, close technology and skills gaps, and prioritize your team's time.

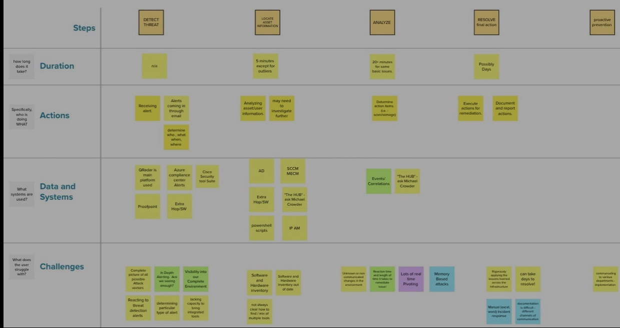
Obtain a strategic view of Zero Trust architectures

Align stakeholders around the most urgent and impactful Zero Trust goals

Gain insight on your critical resources and how to best apply a Zero Trust approach

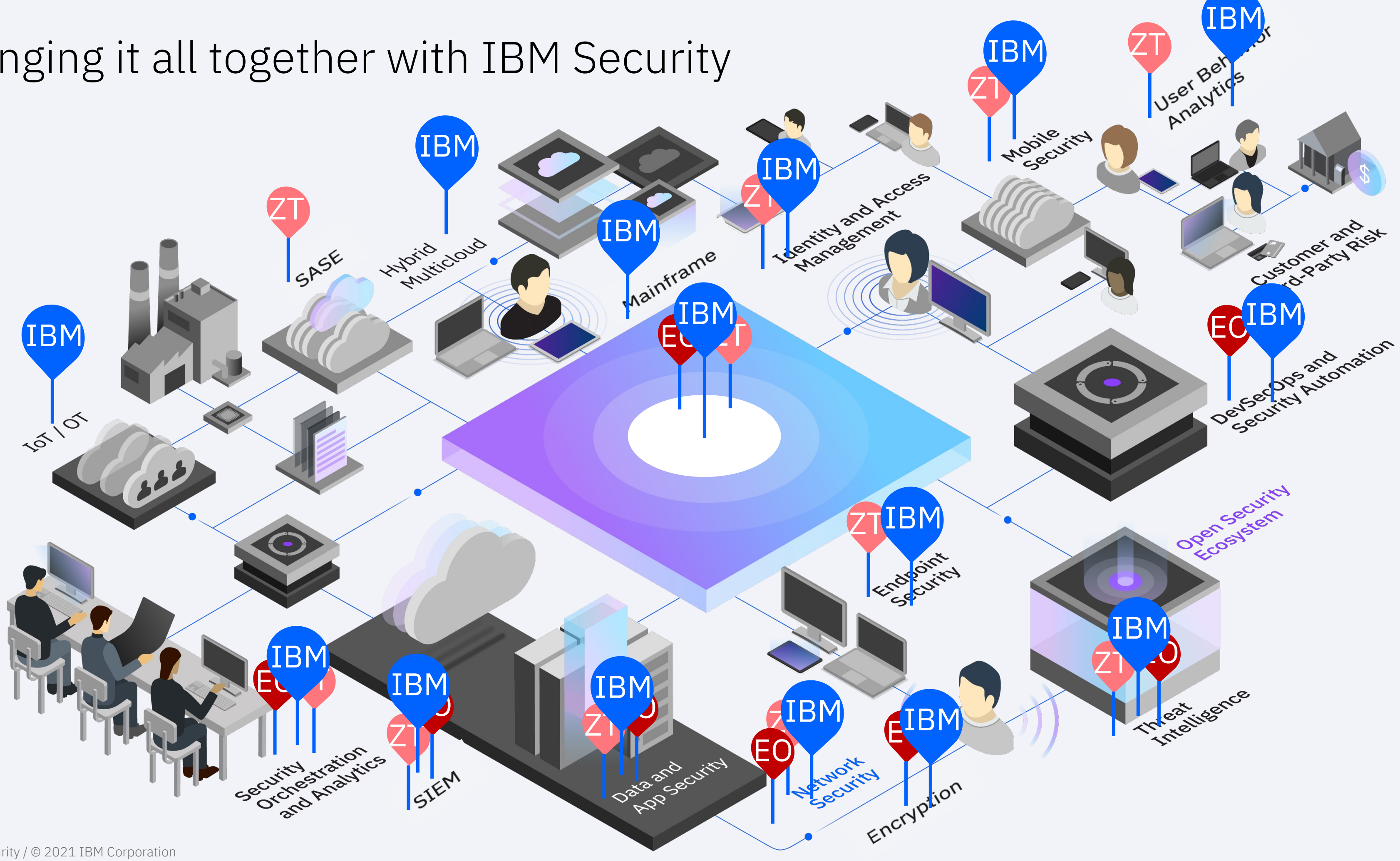
Identify zero trust initiatives based on your business needs





	Steps	DETECT THREAT	LOCATE ASSET INFORMATION	ANALYZE	RESOLVE final action	proactive prevention
how long does it take?	Duration	n/a	5 minutes except for outliers	20+ minutes for some basic issues.	Possibly Days	
Specifically, who is doing WHAT	Actions	Receiving alert. Alerts coming in through email determine who , what when, where	Analyzing asset/user information. may need to investigate further	Determine action items. (i.e. - scan/reimage)	Execute actions for remediation. Document and report actions.	
What systems are used?	Data and Systems	QRadar is main platform used Azure compliance center Alerts Cisco Security tool Suite Proofpoint Extra Hop/SW	AD SCCM MECM Extra Hop/SW "The HUB" - ask Michael Crowder powershell scripts IP AM	Events/ Correlations "The HUB" - ask Michael Crowder		
What does the user struggle with?	Challenges	Complete picture of all possible Attack vectors In Depth Alerting. Are we seeing enough? Visibility into our Complete Environment Reacting to threat detection alerts determining particular type of alert lacking capacity to bring integrated tools	Software and Hardware inventory Software and Hardware inventory out of date not always clear how to find / mix of multiple tools	Unknown or non communicated changes in the environment Reaction time and length of time it takes to remediate issue/ Lots of real time Pivoting Memory Based attacks	Rigorously applying the lessons learned across the Infrastructure can take days to resolve! Manual (excel, word) incident response documentation is difficult - different channels of communication	communicating to various departments - implementation

Bringing it all together with IBM Security



IBM XDR Solution

Obstacles to streamlined threat management

Visibility

- Data ingestion
- No common framework
- Unified on-premise, SaaS and Cloud

Detection

- Cutting through the noise
- Tuning false positives
- Building detection content

Investigations

- Triage time
- Expert insights
- Multiple places to investigate

Response

- Automation and playbooks
- People and processes
- Navigate legal and regulatory compliance

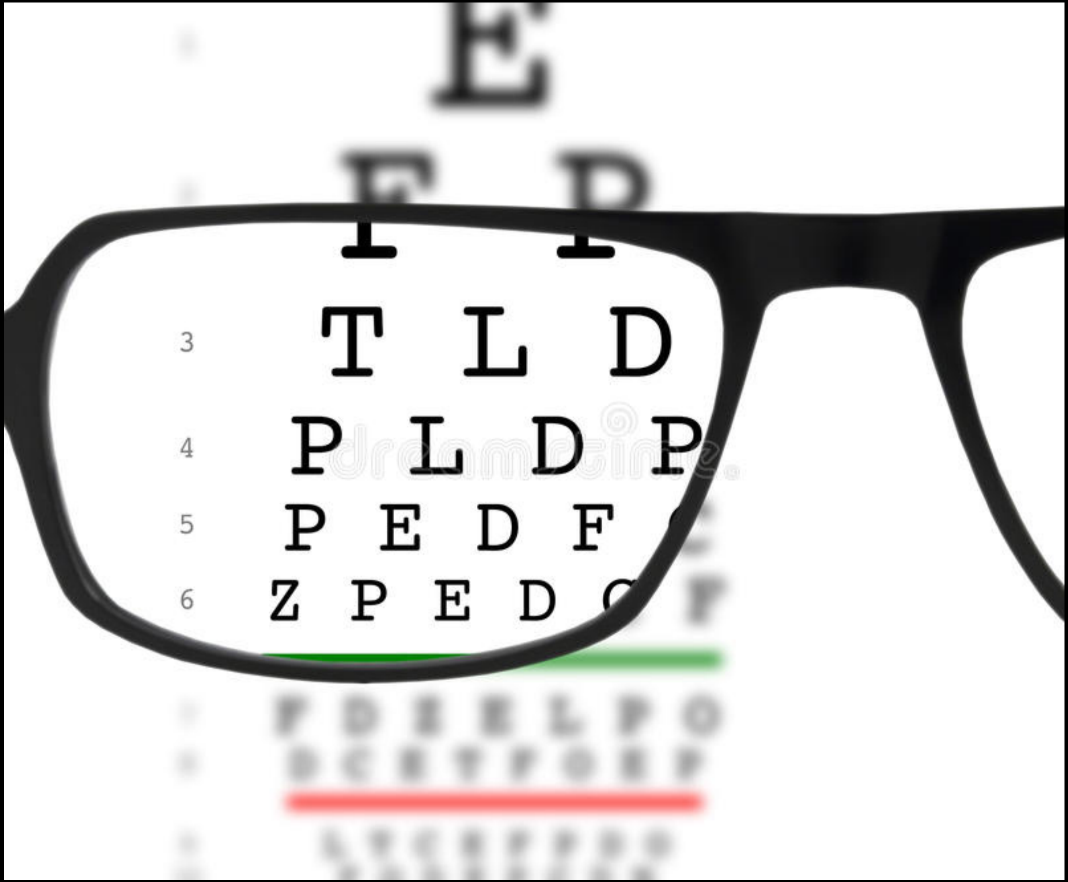
Ima

Advanced Attacks and Analyst Overload

What Analysts Need:

Streamlined

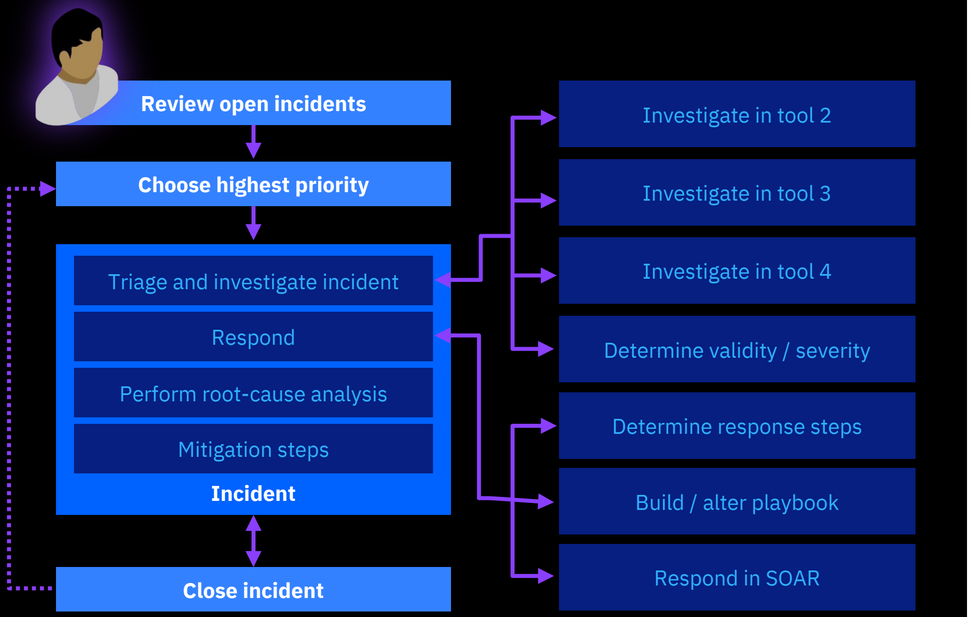
- ➢ Detection
- ➢ Triage
- ➢ Response



Vision and Focus

BEFORE

Security analysts typical workflow complexity



Review open incidents

Choose highest priority

Triage and investigate incident

Respond

Perform root-cause analysis

Mitigation steps

Incident

Close incident

Investigate in tool 2

Investigate in tool 3

Investigate in tool 4

Determine validity / severity

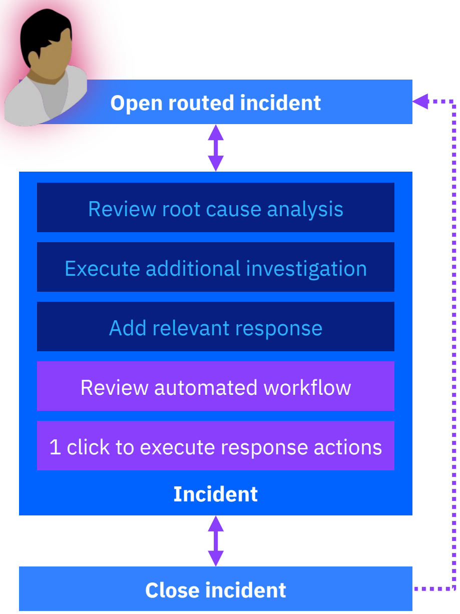
Determine response steps

Build / alter playbook

Respond in SOAR

AFTER

Simplified workflow using QRadar XDR



Open routed incident

Review root cause analysis

Execute additional investigation

Add relevant response

Review automated workflow

1 click to execute response actions

Incident

Close incident

- Fewer, more accurate alerts with an open scalable approach
- Leverage existing tools and avoid vendor lock in
- Streamlined workflow, reduced manual effort thanks to automation
- Pre-built detection and response so teams can protect your organization, even without deep security expertise

Source: Forrester Report, Adapt Or Die: XDR Is On A Collision Course With SIEM And SOAR, April 2021

IBM Security QRadar XDR, an Open, Connected Approach

Connected - Integration with Existing Tools or IBM’s

The industry’s largest Open XDR ecosystem can integrate your EDR, SIEM, NDR, SOAR and Threat Intelligence, while leaving data where it is for a complete XDR approach

Unified - Single User Experience across Tools & Teams

Simple XDR workflows, co-designed with experts, help speed up alert triage, threat hunting, investigation and response

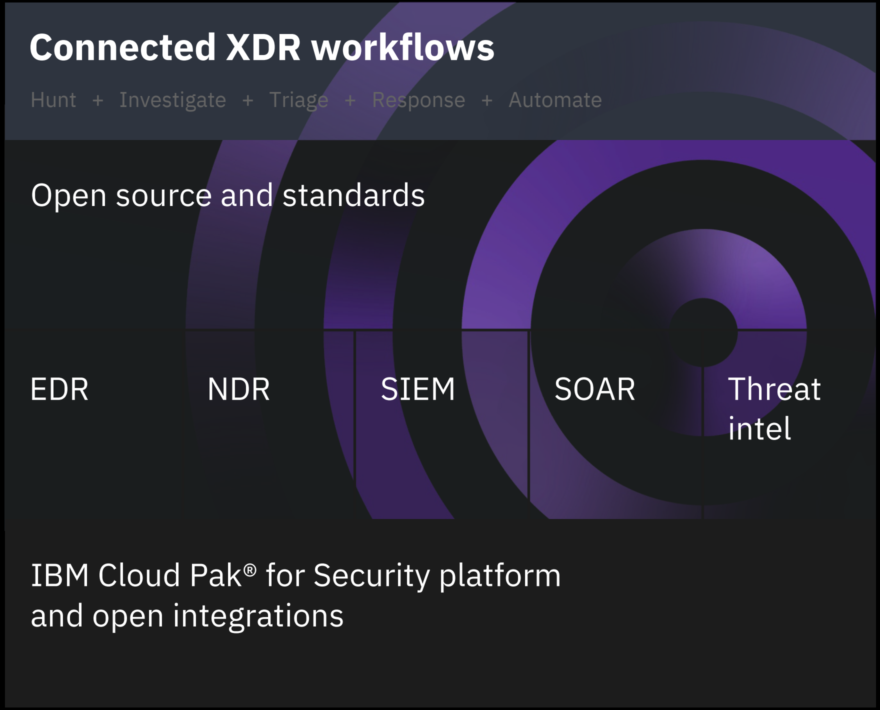
Intelligent - AI Built for Analyst Productivity

Automate the work of enriching, correlating, and investigating threats with purpose-built AI and pre-built playbooks, including automated root cause analysis and MITRE ATT&CK mapping

Open – Adaptable Architecture to Help Avoid Lock-In

Built on IBM Cloud Pak for Security for deployment on premises or on cloud, and ready for use by security service providers

IBM Security QRadar XDR



Connected XDR workflows

Hunt + Investigate + Triage + Response + Automate

Open source and standards

EDR

NDR

SIEM

SOAR

Threat intel

IBM Cloud Pak® for Security platform and open integrations

IBM Security QRadar XDR, an Open, Connected Approach

IBM Security QRadar XDR

NEW

IBM Security QRadar XDR Connect

Connect your tools and automate your SOC using IBM and open third-party integrations

Open Source and Standards

EDR

NEW

REAQTA

cybereason

CROWDSTRIKE

vmware Carbon Black

TREND MICRO

Windows Defender

More EDR Integrations

SIEM

IBM Security QRadar SIEM

splunk>

Azure Sentinel

MICRO FOCUS ArcSight

Elastic Search

NDR

IBM Security QRadar NDR

DARKTRACE

ExtraHop

IronNet Cybersecurity

Vectra

SOAR

IBM Security QRadar SOAR

paloalto NETWORKS

splunk> phantom

servicenow

SWIMLANE

Requires QRadar SIEM to integrate with QRadar XDR Connect

Threat Intel

IBM Security X-Force

Alien Vault

CISCO

MANDIANT A FireEye Company

MAXMIND

REVERSING LABS

SANS

THREATQUOTIENT

VirusTotal

More Threat Intelligence Integrations

Open Integrations

aws

Microsoft Azure

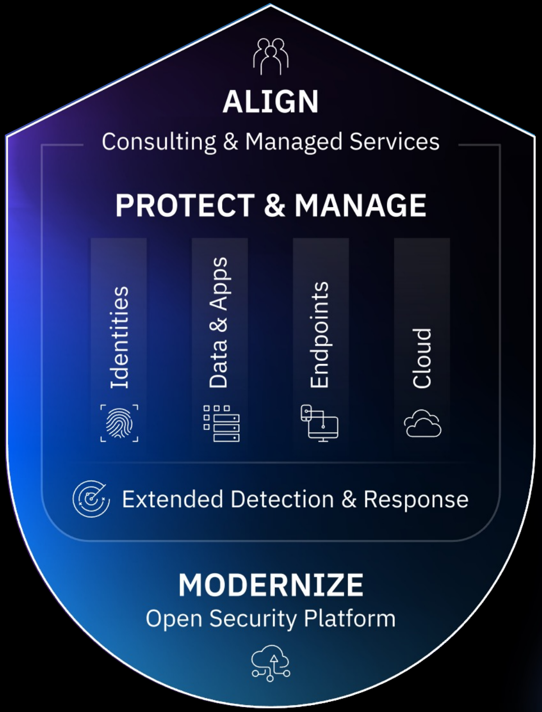
MySql

BIGFIX

tenable

Many More Open Integrations

IBM Security Shield



ALIGN your security strategy to your business

PROTECT identities, data, apps, endpoints, and cloud

MANAGE defenses against growing threats

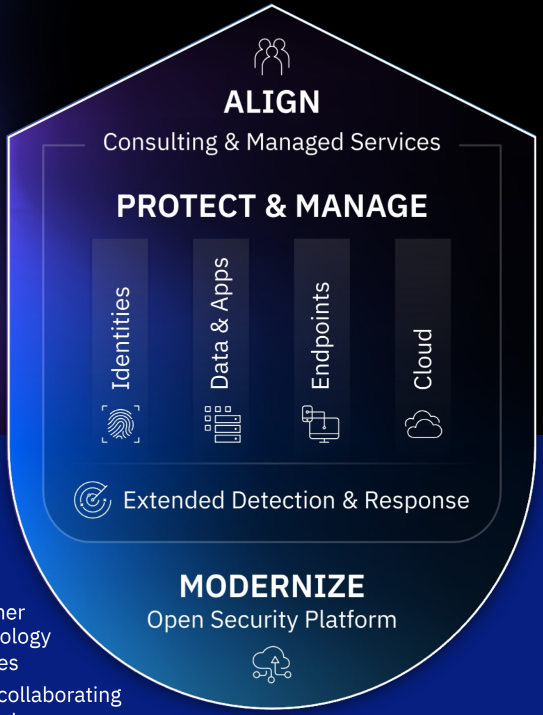
MODERNIZE your security architecture with an open platform

We put security everywhere, so your business can thrive anywhere

Overcome security challenges...	Protect the hybrid cloud	Secure the future of work	Reduce the risk of ransomware and business disruption	Preserve customer privacy
Using a Zero Trust strategy to...	Establish least privilege	Verify continuously	Assume breach	
To deliver real business outcomes	Faster cloud adoption	More productive employees	Improve business continuity	Build trust and improve customer experience

IBM Security Shield

An open and unified approach to Zero Trust that puts security everywhere, so your business can thrive anywhere



Driven by Foundational Differentiation

Leadership and expertise

- Largest enterprise security products and services provider
- Proven leadership across 15 security segments
- Analyze 3 trillion MBs of data for 15K+ clients

AI embedded across our entire portfolio

- Analytics and deep learning for proactive protection
- Machine learning for more accurate detection
- Automation and analysis for faster response

Open platform

- IBM Cloud Pak for Security to connect your disparate tools
- Leading open-source technology for security interoperability and collaboration via the Open Cybersecurity Alliance

Largest ecosystem

- Thousands of partner integrations, technology and service alliances
- 750K active users collaborating via X-Force App Exchange
- Quad9 partnership to discover and protect against threats

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube.com/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.

IBM **Security**

When you interact with IBM, this serves as your authorization to CISO Executive Network or its vendor to provide your contact information to IBM in order for IBM to follow up on y our interaction. IBM's use of your contact information is governed by the IBM Privacy Policy.

IBM