IBM Security Zero Trust Blueprints

Secure the Hybrid Workforce

Tech Data

Today's Speakers & Agenda

Brett Scott | Tech Data
Director of Security Training and Enablement
Brett.Scott@techdata.com

- What is Zero Trust?
- Why Zero Trust to Secure the Hybrid Workforce?

Jason Keenaghan | IBM
Zero Trust Strategy Leader
jkeenagh@us.ibm.com

- Challenges to Secure the Hybrid Workforce.
- IBM Zero Trust Blueprint to Secure the Hybrid Workforce.


Tech Data
CYBER RANGE
Zero Trust Experience
Do not trust anything inside or outside network perimeters

Participant Experience

- The principle steps necessary to protect applications, systems and controls
- The importance of privileges in extending access for users, systems, and applications
- How to define and implement governance and policies for your Zero Trust framework
- Design and implement monitors to sustain your Zero Trust

Pillars of Security

- *Workforce Security*
- *Device Security*
- *Workload Security*
- *Network Security*
- *Data Security*
- *Visibility & Analytics*
- *Automation & Orchestration*

Workforce Security

Device Security

Workload Security

Network Security

Data Security

Analytics

Orchestration

The Why Behind Zero Trust

- Organizations can no longer focus exclusively on external cybersecurity defenses
  - Strategies must:
    - Accept the realities of breaches
    - Malicious insiders
    - Embedded backdoors in technologies from the supply chain
    - Compromised vendor/customer/contractor/partner networks and systems
    - Security realities when utilizing cloud providers and third-party services
  - Methodologies must:
    - Adapt to a "security over time strategy" rather than just a real-time window
    - Include recurring audits of applications/devices/logs
    - A long-term data logging strategy facilitating audits
    - Limiting network access

The Why Behind Zero Trust

In a traditional castle-and-moat security approach, organizations focus on defending their perimeters and assume that every user inside a network is trustworthy and cleared for access.

The vulnerability with this approach is that once an attacker or unauthorized user gains access to a network, that individual has easy access to everything inside the network.

In the zero-trust model, no user is trusted, whether inside or outside of the network. The zero-trust model operates on the principle of 'never trust, always verify'.

Expecting the perimeter to prevent intrusions has proven to be impossible to date. The consensus is that organizations should assume breaches and focus on detection and most importantly limiting access to organization assets.

Zero Trust

- A security concept centered on the belief that organizations should not automatically trust anything inside or outside its perimeters.
- Instead they must verify anything and everything trying to connect to its systems before granting access.
- The philosophy behind a zero-trust network assumes that there are attackers both inside and outside of the network, so no users or machines should be automatically trusted.

The What Behind Zero Trust

No automatic trust

- Instead organizations must verify anything and everything trying to connect to its systems before granting access.

Remote workers add a new risk factor

- Compromised at home
- Return to Office bringing infections

Zero Trust

Principles of zero trust networks

Principle: Least privilege access

- Giving users only as much access as they need, like an army general giving soldiers information on a need-to-know basis.
  - This minimizes each user's exposure to sensitive parts of the network.

Principle: Micro-segmentation

- The practice of breaking up security perimeters into small zones to maintain separate access for separate parts of the network.
  - For example, a network with files living in a single data center that utilizes micro segmentation may contain dozens of separate, secure zones.
  - A person or program with access to one of those zones will not be able to access any of the other zones without separate authorization.

Device Security

Network Security

Workforce Security

Principle: Multi-factor authentication

- MFA simply means requiring more than one piece of evidence to authenticate a user:
  - Just entering the right password is not enough to gain access.
  - A commonly seen application of MFA is the two-factor authentication (2FA) used on popular online platforms
    - In addition to entering a password, users who enable 2FA for these services must also enter a code sent to another device, such as a mobile phone, thus providing two pieces of evidence that they are who they claim to be.
  - Not only does my user know their password, they must also have their mobile phone/email account.
    - Something you know and something you have.

Data Security

Network Security

Workforce Security

Principle: Device knowledge and control

- How many different devices are trying to access your organization's networks?
  - Are the devices cloned?
- Ensure that every device is authorized.
  - Just being on the network is not authorization
  - This further minimizes the attack surface of the network.

Analytics

Device Security

Network Security

Principle: Detection

Assume	Detect	Notify
Assume the perimeter is breached	Detect malicious activity	Utilize notification or orchestration/automation to address detected issues/events

Orchestration

Analytics

Zero Trust

How to achieve an effective zero trust enterprise

The How of Zero Trust

- Micro segmentation
- Evaluations on access – access control
  - Who – user, machine, application
  - Where – location
  - What - data
- Least privilege access
  - user, systems, and applications
- Internal access controls
  - Firewalls
  - MFA
  - Time based limitations

Network Security

Data Security | Analytics

Data Security | Workforce Security

Network Security | Device Security

The How of Zero Trust

- Identity and Access Management – IAM
  - Management, auditing, and logging of user identities and access
  - Heuristics and behavioral profiling for anomaly detection
- Orchestration / automation
  - Leverage automation and orchestration to reduce human workloads
- Analytics
  - Set baselines for "normal" network/system operation
  - Detect anomalies and notify/orchestrate
- Encryption
  - Both at rest and in transit

Workforce Security

Orchestration

Network Security

Analytics

Workforce Security

Workload Security

Data Security

The How of Zero Trust

- Scoring and auditing
  - Leveraging analytics, automated auditing, and heuristic behavior-based anomaly detection
- File system permissions
  - Not just servers, workstations too
- Governance policies
  - Giving users the least amount of access needed to accomplish a specific task
  - No general access
  - Short term privileged access

Analytics

Workforce Security

Data Security

Data Security

Device Security

The How of Zero Trust

- Stranger Danger
  - All new things are untrusted and must be explicitly allowed access
  - Cloned devices detected and BOTH lose privileged access
  - Probing activity on internal network access points is alerted or orchestrated remediation
  - Network port controls
    - Lobby
    - Shipping dock
    - Remote buildings on campus

Implementing Zero Trust

Section 2 - Practical steps

Practical Zero Trust: IAM/ACL

- Manage Identities and access
  - MFA/2FA
  - Use encryption where possible
    - In transit
    - At rest)
  - Periodic reviews of access and privilege
    - As often as possible
    - Quarterly at a minimum
  - Key based access / authentication for API access
    - Notification on key based failures

Workforce Security

Workload Security

Network Security

Data Security

Workload Security

Practical Zero Trust: IAM/ACL

- Create access groups
  - Administrative access
    - limit and use sparingly only as needed
  - Operational management
    - Limit access times
    - Recurring audits
  - Reporting
    - Events
    - Anomalies
  - Transactional
    - Administrative power-ups
      - Lose functional capabilities during privileged access forcing users to return to lower privileged access

Workforce Security

Network Security

Analytics

Network Security

Practical Zero Trust: IAM users/groups

- Configure access groups and their access
  - Map the transaction flows
  - Identify least privilege for data access and configure data access accounts
  - File systems
  - Least privilege for each access type

Workforce Security

Device Security

Data Security

Practical Zero Trust: micro-segments

- Construct a limited microsegment
  - Software defined networking
  - Mini firewalls
  - Utilize/develop limitation to data access through service layers
    - API
    - Json
    - Web Services
  - When do users need to add/edit/delete?

Network Security

Data Security

Practical Zero Trust: analytics

- Create analytics and monitors
  - Transactional
    - Furrier transforms
    - Boundry exceptions
  - Security Incident and Event management (SIEM) feed
    - Fuse/correlate events
    - Notify and/or orchestrate
  - Authentications – successful and failed
  - Mini firewalls looking for and alerting on non-authorized ports, protocols, and probes

Analytics

Workload Security

Analytics

Network Security

Practical Zero Trust: policy/governance

- Policy and governance
  - Clearly document and define the systems and access
  - Create additions to the incident response plan

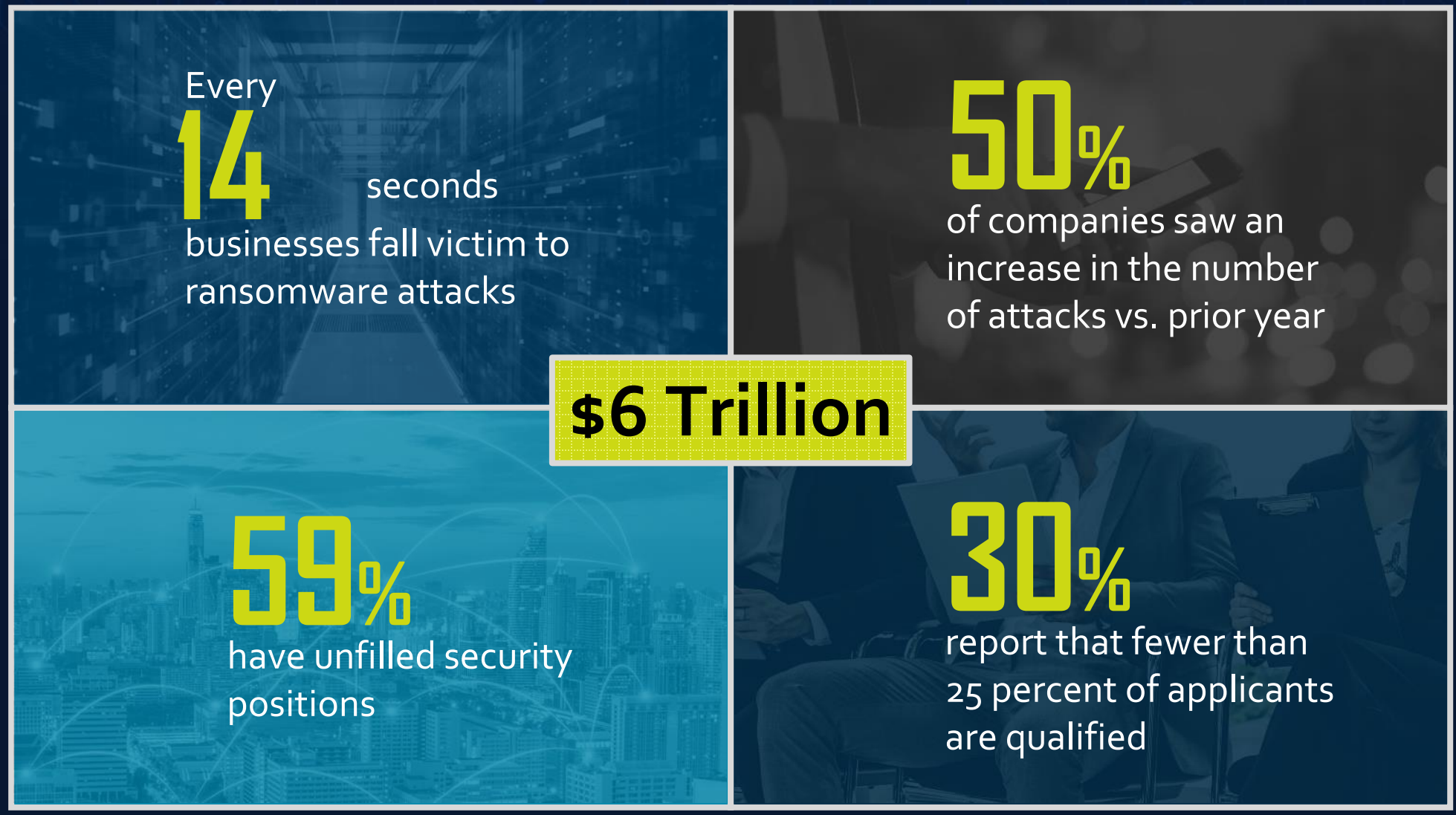
Next steps: Zero Trust

Bringing it all home

Tech Data Cyber Range

The first of its kind in the distribution industry

Cyber Crime is Everywhere… cyber skills are not



Source: ISACA State of Cybersecurity Report, 2019 Annual Cybercrime Report, Forbes

Training using multiple forms of on-prem & cloud-based learning courses

Demonstration of solutions using the best technology, proven processes, and most advanced techniques

Engagement with customers in an interactive learning environment that promotes security solution sales

Services augment the capabilities of our partners by leveraging Tech Data's professional and managed security services.

Tech Data Cyber Range

An interactive and immersive environment to train, demonstrate and engage partners and their customers using the best technologies, processes and most advanced techniques in cybersecurity

Engage with us today!

- Training
  - Incident response exercises, CNA, CND, DFIR, RedTeam/BlueTeam exercises, defense in depth, zero trust, and much more
- Demonstration
  - Technologies, methodologies, configurations, assessments, products, services
- Engagement
  - Events, social, conferences, workshop
- Services

cyberrange.techdata.com

cyberrange@techdata.com

Contact your Tech Data representative

Secure the Hybrid Workforce

Enable your anywhere workforce with everywhere security

Jason Keenaghan
Zero Trust Strategy Leader
jkeenagh@us.ibm.com
@jkeenagh
@jason-keenaghan

June 2021

IBM Security

IBM

Our customers are growing their business with a zero trust approach

Preserve customer privacy

Simplify and secure user onboarding

Manage user preferences and consent

Enforce privacy regulations controls

Reduce the risk of insider threat

Enforce least privilege access

Discover risky user behavior

Embed threat intelligence

Protect the hybrid cloud

Manage and control all accesses

Monitor cloud activity and configurations

Secure cloud native workload

Secure the hybrid workforce

Secure BYO and unmanaged devices

Eliminate VPNs

Provide passwordless experiences

"Zero trust helps us enable critical business capabilities while managing security"

- Mauricio Guerra, CISO, Dow Chemical

82%

of company leaders plan to allow employees to work remotely some of the time

47%

said they intend to allow employees to work remotely full time going forward

Source: Press Releases, ARLINGTON, Va., July 14, 2020, Gartner Survey Reveals 82% of Company Leaders Plan to Allow Employees to Work Remotely Some of the Time, Now Organizations Must Manage a More Complex, Hybrid Workforce

90%

of the polled IT leaders, from the manager level through the C-suite, believe remote workers are not secure

Source: OpenVPN, Remote Work Is the Future — But Is Your Organization Ready for It? March 28, 2021

Enabling a Hybrid Workforce Amplifies Threats Across the Ecosystem

End-users and their behavior expands attack-surface

Business & privileged users

Corporate-owned or BYOD

Anywhere network

Increased use of unmanaged unsecured BYOD

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

The 3 biggest challenges to secure the hybrid workforce

1. Virtual Private Networks (VPNs) introduce vulnerabilities (e.g., DDoS attacks, credential stuffing, lateral movement)

2. Phishing, smishing, and vishing attacks attempt to steal user credentials to gain access to critical resources

3. Unsafe browsing behaviors compromise endpoints and users outside of the workplace (e.g., infected sites, unapproved SaaS apps)

How can zero trust help?

Insights

Enable least privilege access by discovering and assessing risk across data, identity, endpoint, apps and infrastructure

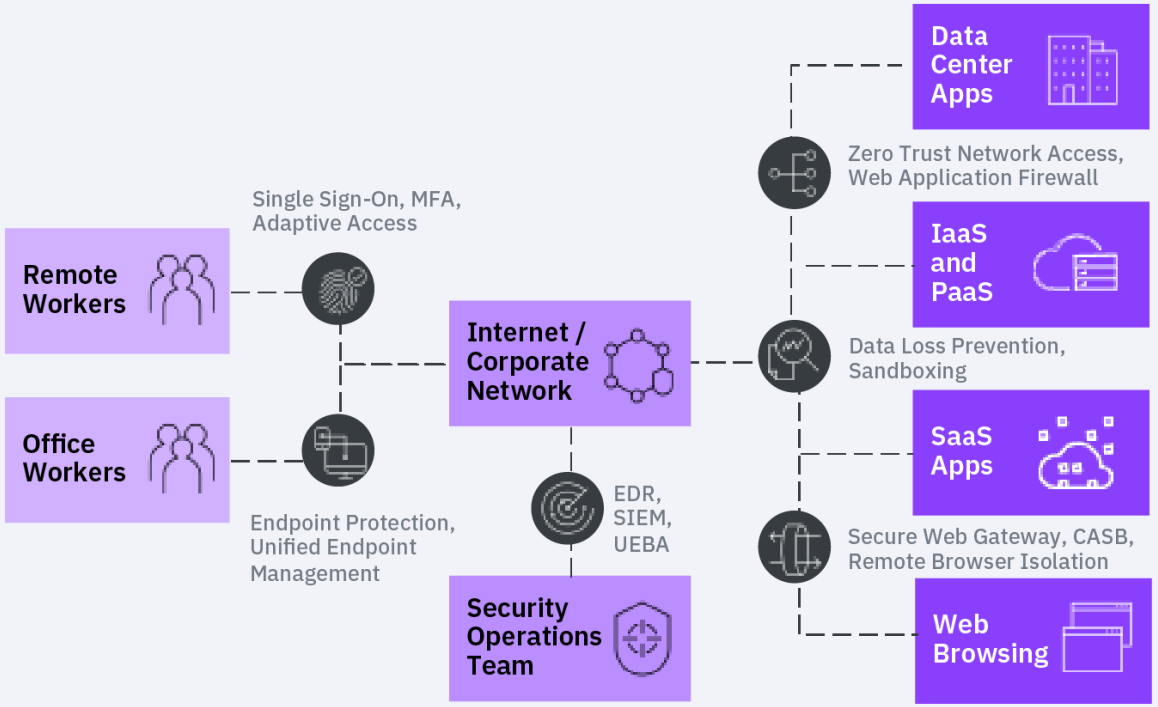
Enforcement

Continuous verification with context-aware access control to all apps, data, APIs, endpoints, and hybrid cloud resources

Detection and Response

Assume breach and identify threats and automate responses that not only stop the immediate attack, but dynamically adapt access controls

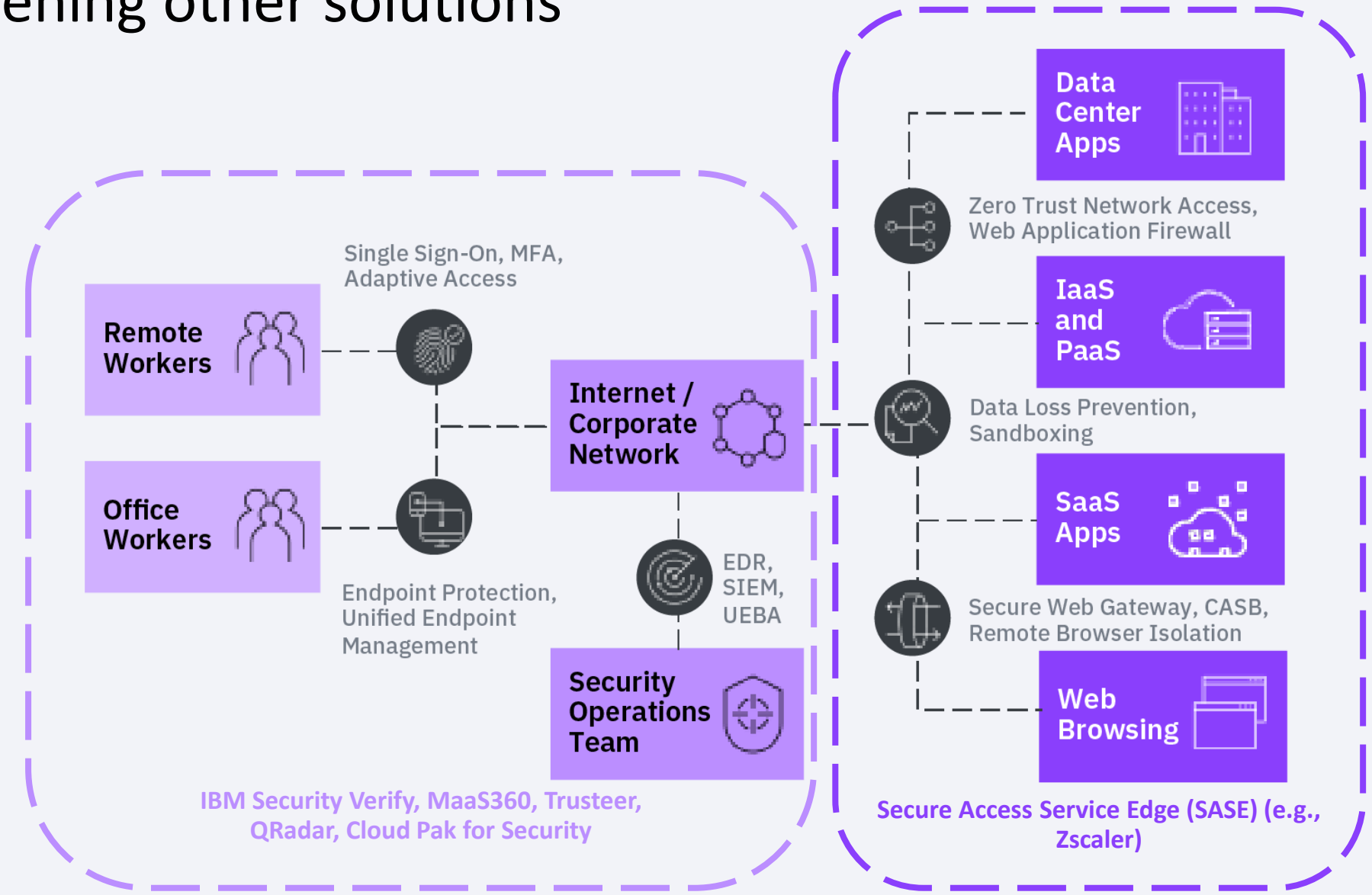
Zero Trust Solution Blueprint: *Secure the hybrid workforce*



	Replace VPNs to reduce network access risks	Protect employees from phishing attacks	Secure risky internet behavior
Get Insights			
Application Discovery	●	○	●
Unified Endpoint Management	○	●	○
Vulnerability Management	○	●	○
Enforce Protection			
Adaptive Access	●	●	○
Cloud Access Security Broker	○	○	●
Data Loss Prevention	○	○	●
E-mail Filtering	○	●	○
Endpoint Protection	○	●	○
Multi-factor Authentication	●	●	○
Remote Browser Isolation (RBI)	○	●	●
Sandbox	○	○	●
Zero Trust Network Access	●	○	○
Detect & Respond			
Endpoint Detection and Response	○	●	●
User and Entity Behavior Analytics	●	●	○
Extended Detection and Response	●	●	●

To put zero trust into action to secure the hybrid workforce you'll want to consider each of the critical capabilities indicated (●) for the specific security challenge you want to address.

IBM provides core capabilities to secure the hybrid workforce while strengthening other solutions



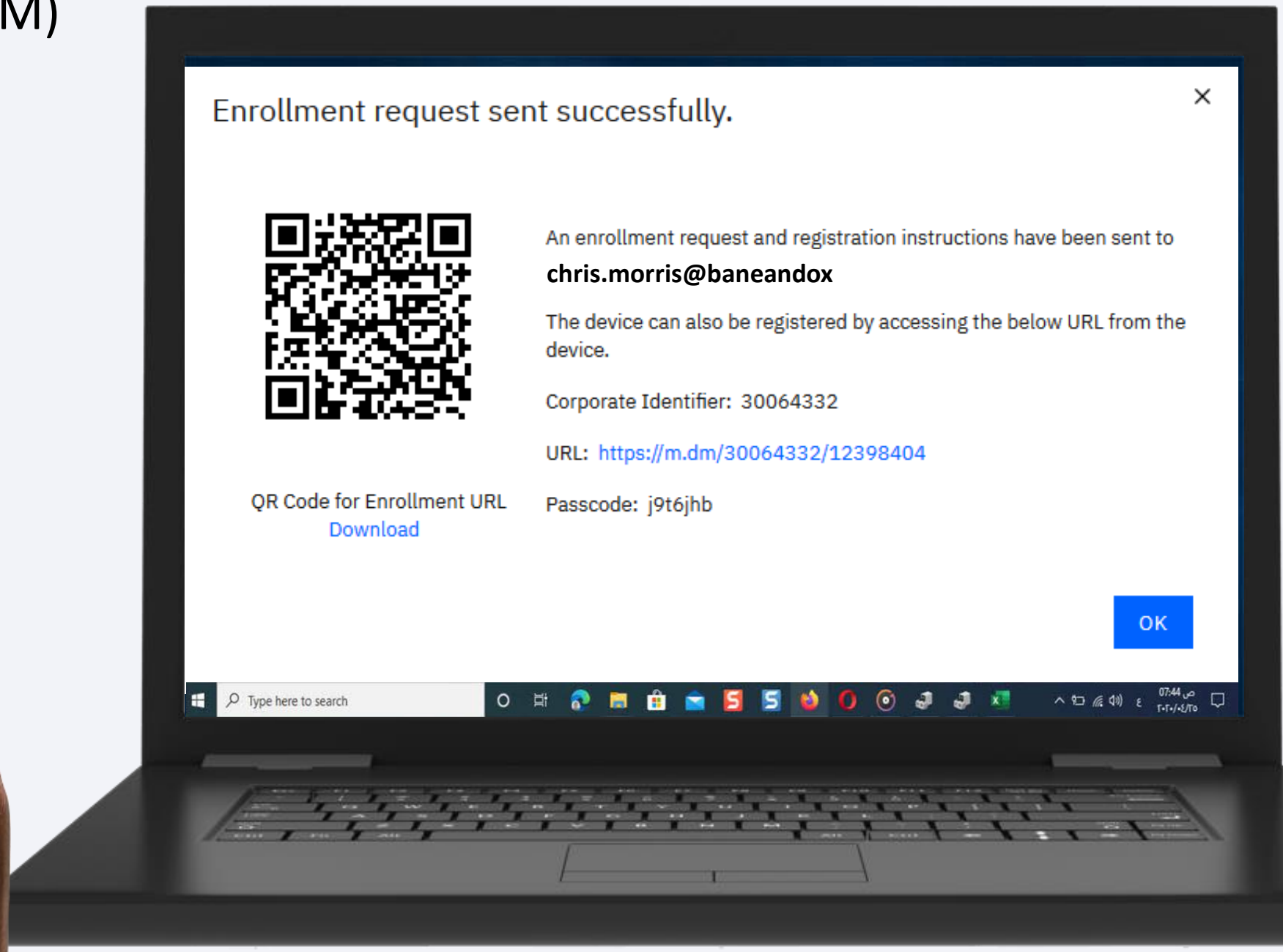
What does this look like in action?

Insights & Enforcement

- MaaS360
- Verify SaaS
- Verify Adaptive Access

Unified endpoint management (UEM)

- Windows 10
- MDM - MaaS360
- SASE / ZTNA - Zscaler
- EDR - Cybereason



Unified endpoint management (UEM)

- Windows 10
- MDM - MaaS360
- SASE / ZTNA - Zscaler
- EDR - Cybereason

My apps

Add app +

What app are you looking for?

Sort by A-Z

- Arrow Insurance Company
- Citrix
- Credential Viewer
- ZScaler Internet Access
- Gold Finch
- Google Calendar
- Google Drive
- Google Sheets
- IBM Cloud App ID
- IBM Connections Meetings
- IBM Verify SDK
- IBM Verify SDK - Javascript
- IBM Verse
- JAMF Connect
- JWT Bearer exchange
- Keycloak

Catalog

My apps

What app are you looking for?

Sort by **A-Z**

Adobe Creative Cloud	Request access
Arrow Insurance Company	Added
Box	Request access
Citrix	Added
Credential Viewer	Added
Gmail (G Suite bundle)	Added
Gold Finch	Added
Google Calendar (G Suite bundle)	Added
Google Drive (G Suite bundle)	Added

IBM Security | App center | My requests

CC

Catalog

My apps

What app are you looking for?

Sort by A-Z

Adobe Creative Cloud — Request access

Arrow Insurance Company — Added

Box — Request access

Citrix — Added

Credential Viewer — Added

Gmail (G Suite bundle) — Added

Gold Finch — Added

Google Calendar (G Suite bundle) — Added

Google Drive (G Suite bundle) — Added

Request Access

Box

A cloud storage and file sharing service

Justification

Need to work our customers on the latest spreadsheets and sales documentation

Cancel | Submit

IBM Security | App center | My requests

CC

Profile & settings

Profile | **Security** | Privacy | SAML aliases

Security

Protect your account access with a strong password plus an additional verification method as well as recovery options if you get locked out.

IBM Verify

Christopher iPhone 12 Pro

Authenticator app

Enroll

Connect

Next, conne

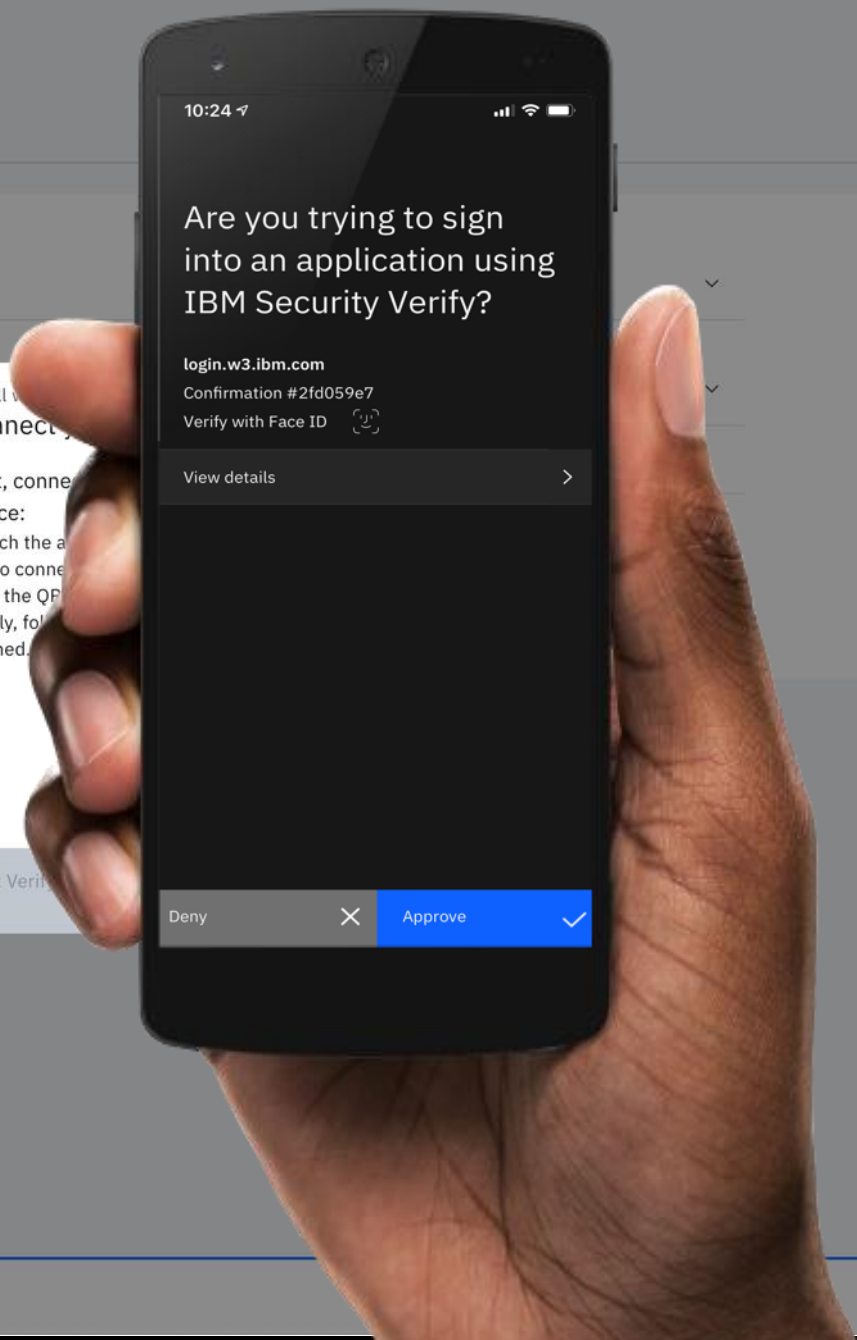
device:

1. Launch the a
2. Tap to conne
3. Scan the QR
4. Finally, fo

finished.

Cancel

Next: Verif



Sign in with B&Oid

Choose a Single-Sign On method.

B&O Credentials

Use your w3id and password

QR Code

Scan with IBM Verify mobile app.

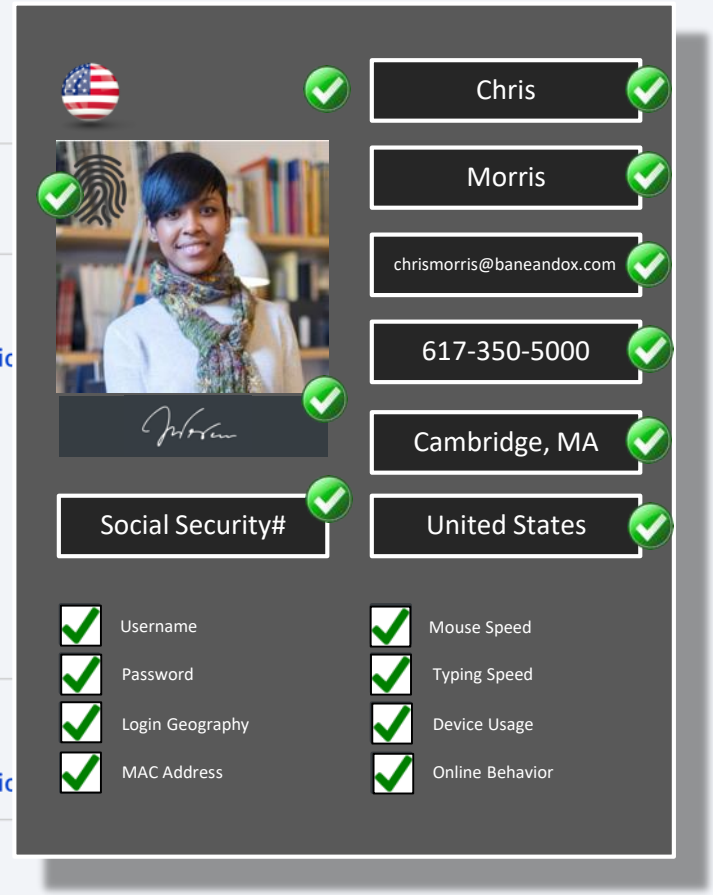
Note: Registration is required. View registration instructic

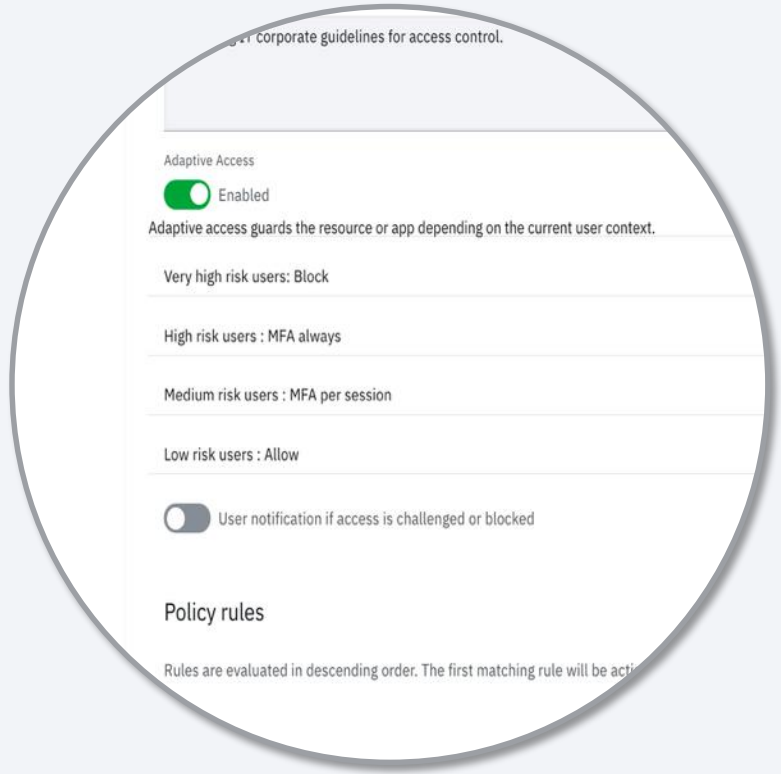
Security Key / Touch ID

Use a security key or biometrics to authenticate.

Note: Registration is required. View registration instructic

We're enhancing w3id. Learn more





Timestamp	User	Risk Level	Reason	Policy Action	Policy	Location	Device
March 24th	chris.morris	LOW	Access from device that passed MFA	Allow	Adaptive Access	Cambridge, MA	Windows 10
March 24th	chris.morris	MEDIUM	Access with a change in device attributes	MFA per session	Adaptive Access	Cambridge, MA	Windows 10

Detect & Respond

- Cloud Pak for Security
- QRadar with Watson SIEM
- SOAR Automation
- Breach Response

IBM MaaS360 | With Watson

Search for Devices, Users, Apps or Docs

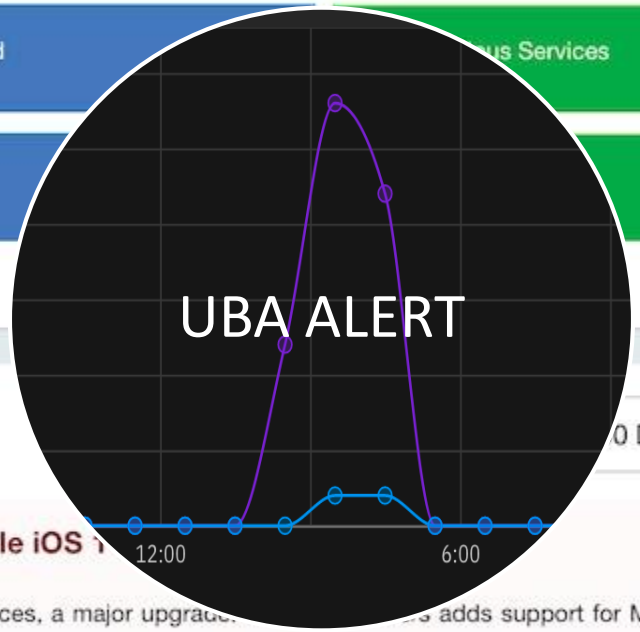
My Groups

HOME DEVICES USERS SECURITY APPS DOCS EXPENSE SCHOOLS REPORTS SETUP

My Alert Center

Last Analyzed: Thursday, June 7, 2018 11:55:15 AM EDT

4 Out of Policy Compliance	0 iOS in Supervised Mode	0 Jailbroken or Rooted
2 No Passcode	1 Recently Added	us Services
1 Location Service Disabled	0 Roaming	



My Advisor With Watson

Risk Exposure: 8 devices are missing the latest Apple iOS

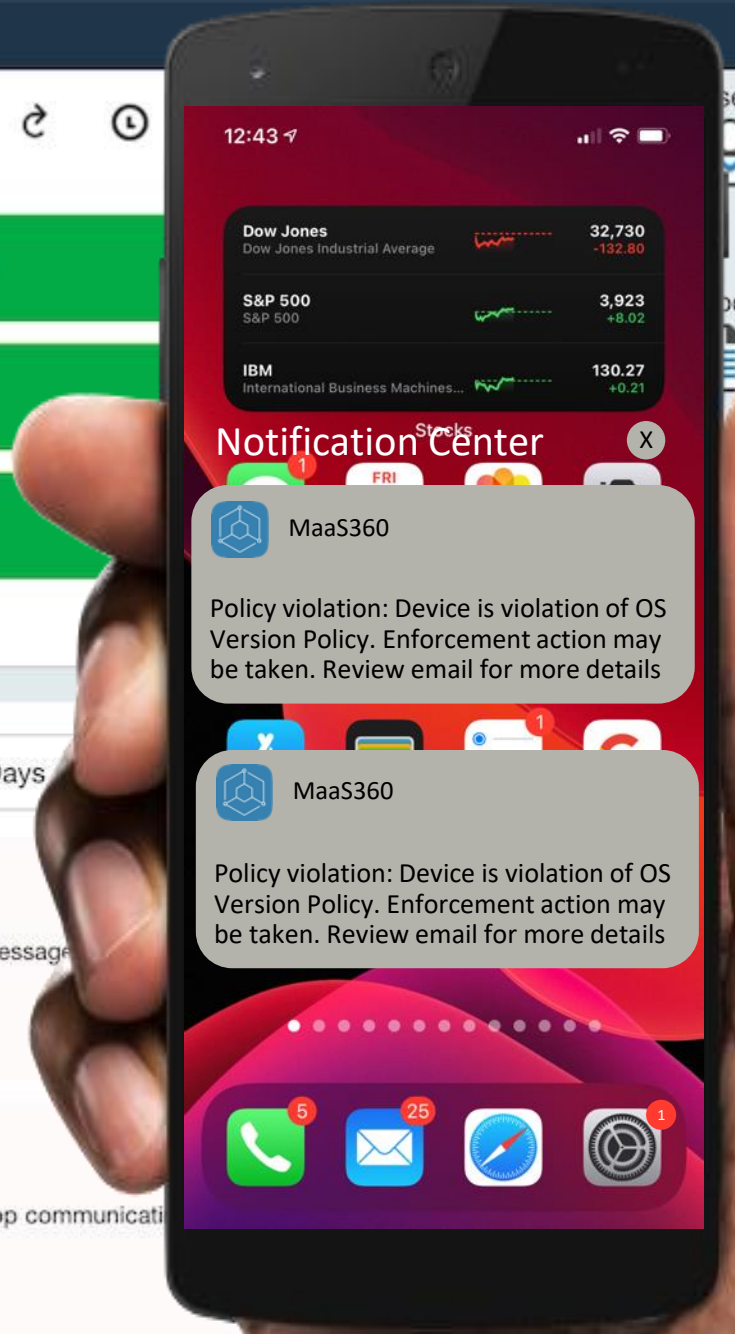
Apple has released iOS 11.4 for iPhone, iPad and iPod touch devices, a major upgrade. adds support for Message and other new exciting features along with several security fixes.

Learn more

Risk Exposure: Cloud Extender less than version 2.91 are impacted by TLS 1.0 deprecation

On June 25,2018 the MaaS360 Platform will deprecate support for TLS 1.0. Any Cloud Extenders less than version 2.91 will stop communicati to the MaaS360 Platform. Upgrade your Cloud Extender now.

Learn more



My applications

Data Explorer

Search and analyze all of your data from one unified UI.

Case Management

Collaborate with your team and track work in a centralized location.

Orchestration & Automation

User Behavior Analytics

Detect and analyze insider threats

Threat Intelligence Insights

Identify your most impactful threats with relevant threat intelligence

Threat Investigator [Preview]

Automatically investigate and prioritize cases.

Risk Manager

Visualize correlated security risks across domains

Threat intelligence report lookup

Search for IPs, URLs, file hashes, vulnerabilities, threats, malware...

Search

Trending reports

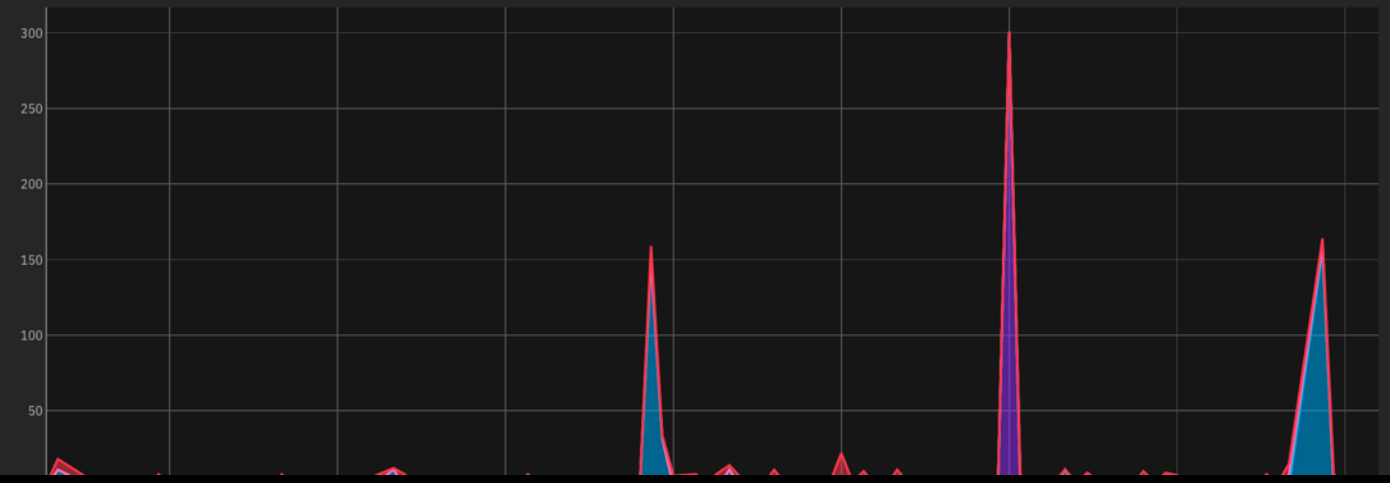
IP	45.146.165.157	IP	107.189.8.176
URL	gen.lib.rus.ec	IP	194.165.16.77
URL	r3.o.lencr.org		

Dashboard

SOC Analyst Custom Dashboard

Top 10 log sources by event count

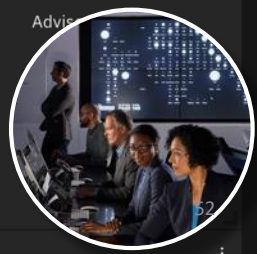
A few seconds ago



Latest Threats

A few seconds ago

Title	Category
Windows Safe Mode Unsafe From REvil	Advisory
Bank of America Squatting Campaign	Early Warning
ITG14 Shift To Ransomware With New TTPs	Advis
Hive0097 Activity Update - March 2021	
macOS Adware in Rust	



Open Cases by Type

UBA Overview

All users

Search for users

Next refresh: 4:12

Reset layout

Monitored users	High risk users	Users discovered from events	Users imported from directory	Active analytics
41	2	36	5	Rules: 162 of 208
	5% of monitored users	88% of monitored users	Import not configured	Machine learning

Monitored users

Username	Recent risk	Overall risk
chris.morris	225	2.4M
BILL	225	14K
tom_wilson	0	217.2
BADGUY	0	98.63
jblack	0	76.47
POCTEST	0	16.42
DALE	0	16.42
APPUSER	0	16.25
com.ibm.guardium.jd...	0	5.97
thaverford	0	5.97

View all 41 users

Recent offenses

Offense #63 (Case #2123) — updated 14 hours ago
User: jblack
Description: IP ip WebVPN session started.
Event count: 7 Flow count: 0 Magnitude: 4/10

Offense #62 (Case #2118) — updated 4 days ago
User: :SC=COMPANY
Description: Sensitive Objects - Alert preceded by DML
Event count: 2 Flow count: 0 Magnitude: 5/10

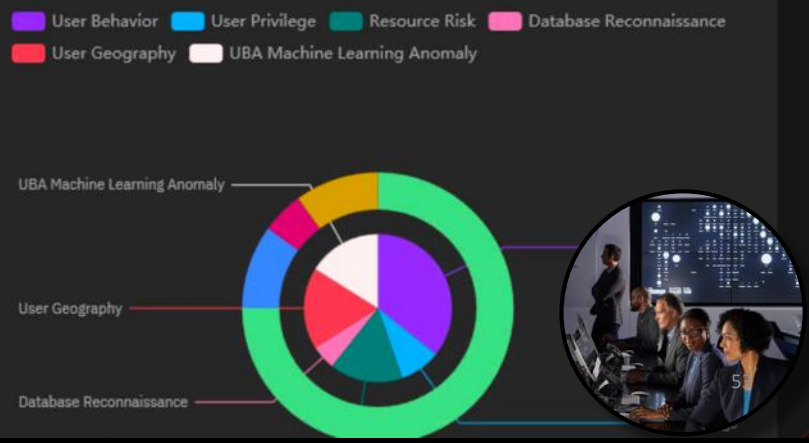
Offense #61 (Case #2119) — updated 4 days ago
User: :SC=optim
Description: Sensitive Objects - Alert preceded by DML
Event count: 1 Flow count: 0 Magnitude: 5/10

Offense #60 (Case #2120) — updated 4 days ago
User: POLLY
Description: Sensitive Objects - Alert preceded by DML
Event count: 13 Flow count: 0 Magnitude: 5/10

System score

Dec 2 - Dec 12

Risk category breakdown (Last hour)



Merger and Acquisition

Sales Department

Cases

Create case +

Filters

Initial (8)

2171
QRadar ID 1 , Case Created from UBA - BILL

A1 Time open: 0 days 20 hrs 49 mins
Created by: Integration key for QRadar

UBA

Extra information

2170
QRadar ID 31 , Sensitive Objects - Alert preceded by DML - KEN

A1 Time open: 1 days 0 hrs 37 mins
Created by: Integration key for QRadar

UBA

Extra information

2168
QRadar ID 28 , X-Force Premium: Internal Host Communication with Malicious IP containing ICMP.Destination-Unreachable - 161.156.185.184

A1 Time open: 2 days 0 hrs 31 mins
Created by: Integration key for QRadar

UBA

Extra information

Engage (1)

2129
SolarWinds Orion Compromise Information

I Time open: 1 months 19 days 1 hrs 14 mins
Created by: isc-demo

Malware

Extra information

Detect/Analyze (1)

2111
Ocacle Customer Data Large Transfer

I Time open: 2 months 24 days 20 hrs 3 mins
Created by: isc-demo

Lost storage device / media

Extra information

Respond (2)

2154
APT41 Dual Espionage and Cyber Crime Operation

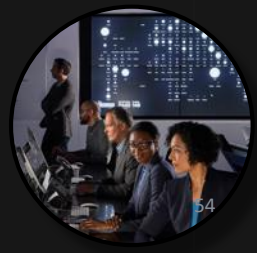
I Time open: 11 days 5 hrs 36 mins
Created by: isc-demo

Extra information

2153
NCAS Malware Analysis Report AR21-039A - SUNBURST

I Time open: 13 days 14 hrs 38 mins
Created by: isc-demo

Extra information



QRadar ID 79 , FWUC1 Customer 2 RSS Taxii Suspected Connecti...

Actions

Description

30 events in 2 categories: FWUC1 Customer 2 RSS Taxii Suspected Connection to BotNet Host preceded by FWUC1 RSS Taxii Suspected Connection to BotNet Host containing Session Allowed

Details | Tasks | Notes | Members | News Feed | Attachments | Stats | Timeline | Artifacts | Asset Database | QRadar | Firewall Rules | Firewall Configuration Changes | MITRE ATT@CK | Service Now | Report

Add Artifact | Table | Graph

Value: All | Type: All | Date Created: All | Has Attachment: All | More...

Columns Search...

Related I...	Type	Value	Created By	Created	Last Modified	Description	Actions
4	Port	443	app_fn_qradar_integration_exe_fn_qradar_integration	12/09/2020 11:24	12/09/2020 11:24	Destinatio...	
5	Port	3868	app_fn_qradar_integration_exe_fn_qradar_integration	12/09/2020 11:24	12/09/2020 11:24	Source Port	
0	IP Address: Source	172.18.4.204	qradar_app	12/09/2020 11:21	12/09/2020 11:21	QRadar Of...	

Items per page 25 | 1-3 of 3 items

- Add artifact to Splunk ES
- Add to QRadar Reference Set
- Ansible Tower Run Job - Artifact
- Ansible: Add NAT CheckPoint Rule
- Ansible: Create New CheckPoint Access Rule
- Checkpoint add
- Checkpoint remove
- Delete from QRadar Reference Set
- Find All QRadar Reference Sets
- Find in QRadar Reference Set
- Panorama Block IP Address
- Panorama Block Traffic
- Panorama Unblock IP Address
- QRadar Add to Reference Set
- QRadar Ariel Query
- QRadar Move from Sample Blocked to Sample Suspected
- Query Asset DB
- Search Splunk ES for an artifact
- Run Query in Data Explorer

Summary

ID	2211
Phase	Complete
Priority	
Severity	High
Magnitude	7
Customer	B
Customer Risk Appetite	20
Analyst Intervention Required	Yes
ThreatCo Risk Score	–
Date Created	12/09/2020 11:21
Date Occurred	12/09/2020 08:56
Date Discovered	12/09/2020 08:56
Date Determined	12/09/2020 08:56
Was personal information or personal data involved?	Unknown
Incident Type	UCFW1 - TI IOCs

SLA (In Minutes)

SLA Target	30
SLA Status	Achieved
Duration	7

People

Created By	qradar_app
Owner	L1
Members	*There are no members.*

Related Incidents

#2210 QRadar ID 76 , FWUC1 RSS Taxii S...
#2198 QRadar ID 73 , FWUC1 RSS Taxii S...

QRadar ID 79 , FWUC1 Customer 2 RSS Taxii Suspected Connecti...

Actions

- Ansible Tower List Job Templates
- Ansible Tower List Jobs
- Ansible Tower Run an Ad Hoc Command
- Ansible Tower Run Job - Incident
- Automation: Decision Engines WF
- Create Jira Issue
- MITRE: Get Groups per Technique
- MITRE: Get Groups using all Techniques
- MITRE: Get Tactic information
- MITRE: Get Technique information
- MITRE: Get Technique's Software
- Post an Incident to Microsoft Teams
- Search QRadar for offense id
- Send Incident Email HTML
- Send Incident Email Text
- ServiceNow: Close Record [Incident]
- Symantec EDR - Get Blacklist information
- Symantec EDR - Get Endpoints status summary
- Symantec EDR - Get Groups information
- Test CMDB Query
- Test Config Analysis
- Test Firewall Workflow
- Update Splunk ES notable event

- Action Status
- Workflow Status
- Close Case
- Delete Case

Description

30 events in 2 categories: FWUC1 Customer 2 RSS Taxii Suspected Connection to BotNet Host preceded by FWUC1 RSS Taxii Suspected Connection to BotNet Host containing Session Allowed

Details | Tasks | Notes | Members | News Feed | Attachments | Stats | Timeline | Artifacts | Asset Database | QRadar | Firewall Rules | Firewall Configuration Changes

MITRE ATT@CK | Service Now | Report

Edit

Basic Details

Name	QRadar ID 79 , FWUC1 Customer 2 RSS Taxii Suspected Connection to BotNet Host preceded by FWUC1 RSS Taxii Suspected Connection to BotNet Host containing Session Allowed - 172.18.4.204
MITRE ATT&CK Technique ID	–
Description	30 events in 2 categories: FWUC1 Customer 2 RSS Taxii Suspected Connection to BotNet Host preceded by FWUC1 RSS Taxii Suspected Connection to BotNet Host containing Session Allowed
Customer	B
Magnitude	7
Incident Type	UCFW1 - TI IOCs
NIST Attack Vectors	–
Incident Disposition	Unconfirmed
Phase	Complete
Resolution	–
Resolution Summary	–
Owner	L1
Created By	qradar_app

Date and Location

Date Created	12/09/2020 11:21
Date Occurred	12/09/2020 08:56:23
Date Discovered	12/09/2020 08:56:23
Address	75 Binney Street
City	Cambridge
Country/Region	United States
State	Massachusetts
Zip Code	02142

Implications

Summary

ID	22
Phase	Co
Priority	
Severity	Hi
Magnitude	7
Customer	B
Customer Risk Appetite	20
Analyst Intervention Required	Ye
ThreatCo Risk Score	–
Date Created	12
Date Occurred	12
Date Discovered	12
Date Determined	12
Was personal information or personal data involved?	Ur
Incident Type	U

SLA (In Minute

SLA Target	30
SLA Status	Achieved
Duration	7

People

Created By	qradar_app
Owner	L1
Members	*There are no members.*

Related Incidents

#2210 QRadar ID 76 , FWUC1 RSS Taxii S...

Describe the Incident
Date and Location
Implications
Privacy
Team Formation
Regulators
Record Count
Data Types
Europe Breach Risk Assessment
Create

Regulators

Organizational Rules
- [x] Data Breach Best Practices

U.S. States and Territories
Select only those state regulators that are applicable to this specific incident.

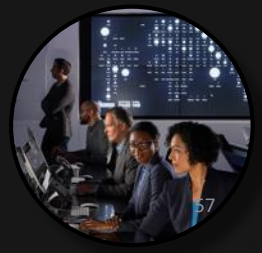
- [x] Alabama
- [ ] Alaska
- [ ] Arizona
- [ ] Arkansas
- [x] California
- [ ] Colorado
- [x] Connecticut
- [ ] Delaware
- [x] District of Columbia
- [x] Florida
- [ ] Georgia
- [ ] Guam
- [x] Hawaii
- [ ] Idaho
- [ ] Illinois
- [ ] Indiana
- [ ] Iowa
- [ ] Kansas
- [ ] Kentucky
- [ ] Louisiana
- [ ] Maine
- [ ] Maryland
- [x] Massachusetts
- [ ] Michigan
- [ ] Minnesota
- [ ] Mississippi
- [ ] Missouri
- [ ] Montana
- [ ] Nebraska
- [ ] Nevada
- [ ] New Hampshire
- [ ] New Jersey
- [ ] New Mexico
- [x] New York
- [ ] North Carolina
- [ ] North Dakota
- [ ] Ohio
- [ ] Oklahoma
- [ ] Oregon
- [x] Pennsylvania
- [ ] Puerto Rico
- [ ] Rhode Island

Canada Special Regulators
Select only those provinces in which the corporate establishment or data processing was material to this specific incident.

- [x] Alberta (Health)
- [x] Manitoba (Health)
- [x] New Brunswick (Health)
- [x] Newfoundland and Labrador (Health)
- [x] Ontario (Health)

Europe
Please select the competent national supervisory authority, or in the case of a cross-border breach, the lead authority (which is not necessarily where the affected data subjects are located or where the breach has taken place). For controllers not established in the EU, subject to GDPR, select the location of your designated representative. For guidelines on identifying a controller or processor's lead supervisory authority, click here. If there is any doubt as to the location of the lead supervisory authority then, at a minimum, select the location where the breach has taken place.

- [ ] Austria
- [x] Belgium
- [ ] Bulgaria
- [ ] Croatia
- [ ] Cyprus
- [ ] Czech Republic
- [ ] Denmark
- [ ] Estonia
- [x] Finland
- [ ] France
- [ ] Germany
- [ ] Gibraltar
- [x] Greece
- [ ] Guernsey
- [ ] Hungary
- [ ] Iceland
- [x] Ireland
- [ ] Isle of Man
- [ ] Italy
- [ ] Jersey
- [ ] Latvia
- [ ] Liechtenstein
- [ ] Lithuania
- [ ] Luxembourg
- [ ] Malta
- [ ] Moldova
- [x] Netherlands
- [ ] North Macedonia
- [x] Norway
- [x] Poland

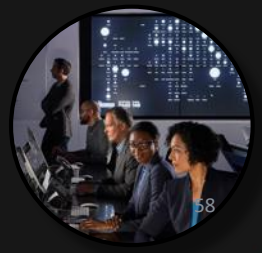


Describe the Incident
Date and Location
Implications
Privacy
Team Formation
Regulators
Record Count
Data Types
Europe Breach Risk Assessment
Create

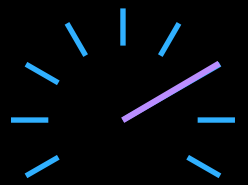
Previous
Next

Data Types

- [x] **Contact Information**
  - [x] First Name
  - [x] First Initial
  - [x] Middle Name
  - [x] Last Name
  - [x] Address
  - [x] Email Address
  - [x] Phone Number
- [x] **Personal Information**
  - [x] Birth Certificate
  - [x] Date of Birth
  - [x] Driver's License Number
  - [x] Marital Status
  - [x] Marriage Certificate
  - [x] Occupation
  - [x] Passport Number
  - [x] SSN or SIN
  - [x] Last Four Digits of SSN
- [x] **Identification Data**
  - [x] Employee ID Number
  - [x] ID Theft Protection PIN Issued by US IRS
  - [x] Military ID Number
  - [x] Personal Identification
  - [x] State ID Number
  - [x] Student ID Number
  - [x] Tax ID Number
  - [x] Tribal ID Number
- [ ] **Financial Information**
  - [ ] Account Password / Access Code (Financial)
  - [ ] Bank Account Number
  - [ ] Bank Routing Number
  - [ ] Brokerage Account Data
  - [ ] Financial Account Number
  - [ ] Income Tax Withheld
  - [ ] Online Username (Financial)
  - [ ] Other Personal Financial Information
  - [ ] Payment Card Mag Strip Data
  - [ ] Personal ID for Financial Accounts
  - [ ] Tax Information
  - [ ] Third-Party Account Information
- [x] **Credit Card Data**
  - [x] Credit Card CVV Code
  - [x] Credit Card Expiration Date
- [ ] **Medical Information**
  - [ ] Diagnostic Information
  - [ ] Medical History
  - [ ] Medical Treatment
  - [ ] Mental Condition
  - [ ] Organ Donor Information
- [x] **Health-Related Information**
  - [x] Healthcare Payment, Eligibility or Entitlement Information
  - [x] Healthcare Provider
  - [x] Health Insurance Identification Number
  - [x] Health Insurance Policy Number
  - [x] Health Insurer ID
  - [x] Medical Registration Information
  - [x] Medicare Number
  - [x] Personal Health Record (Electronic)
  - [x] Substitute Decision Maker
- [ ] **Other Data**
  - [ ] Account Password / Access Code (Non-Financial)
  - [ ] Biometric Data
  - [ ] CPNI/Communications Data
  - [ ] Digitized / Electronic Signature
  - [ ] Educational Records
  - [ ] Fingerprint
  - [ ] Genetic Information
  - [ ] Insurance Policy Number (Non-Health)
  - [ ] License Information and Status
  - [ ] License Plate Information
  - [ ] Online Username (Non-Financial)
  - [ ] Parent's Legal Surname Prior to Marriage
  - [ ] Security Question and Answer
  - [ ] Work-Related Evaluations
- [ ] **Special Categories**
  - [ ] Criminal Activities
  - [ ] Graphic, Photographic or Acoustic
  - [ ] Other Information Relating to an Identified or Identifiable Person
  - [ ] Political Opinions
  - [ ] Racial/Ethnic Origin
  - [ ] Religious or Philosophical Beliefs
  - [ ] Sex Life/Orientation
  - [ ] Trade Union Membership



IBM's approach is best positioned to deliver on the Zero Trust value proposition

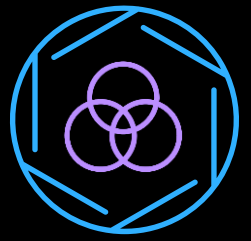


Industry Leading SW

- Industry leading Data Security, Threat Management and IAM tools
- Modern SW built for cloud-native and hybrid environments

Open Platform

- Cloud Pak for Security built on OpenShift
- Flexibility to deploy on-prem or across cloud environments
- Interoperability with existing security tools



Technology Ecosystem

- Leverage strategic alliances and partnerships to complement IBM technology and enable zero-trust use cases

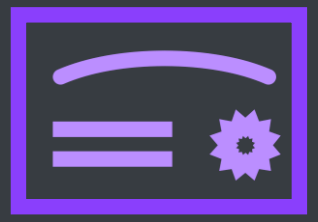
End to End Capability

- With the technology ecosystem, IBM offers an end-to-end security technology portfolio to enable a Zero Trust approach
- Integrated Zero Trust Framework

How to Get Started? IBM has several assets and initiatives to help you get started with Zero Trust

Zero Trust Badges

- Foundational courses and training across a variety of skills (sales, solution domains, etc)



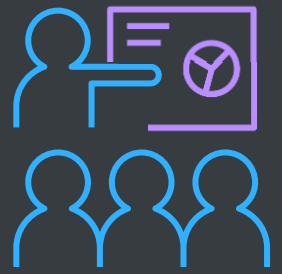
Zero Trust Certifications

- Official product administrator and specialist accreditation
- Demonstrate expertise in related IBM technologies and solutions

For Individuals

Zero Trust Competency

- Recognition for IBM partners who demonstrate technical proficiency and proven success in delivering zero trust value to customers



Zero Trust Workshop

- Workshop for BPs with IBM Security experts
- Prepare BPs to deliver a ZT engagement with customers

For Organizations

Call to Action

Next Steps

- Presentation Recording and Deck
- Webinar Survey
- Sign up for remaining sessions!
  Click here to register
- Schedule a follow up:
  - Deep Dive
  - Demo
  - Zero Trust Client Review

TechData

Tech Data IBM Security Brand Team

Karen Bailey
Business Development Executive
Location – Alpharetta, Georgia
(678) 642-3446
Karen.Bailey@techdata.com

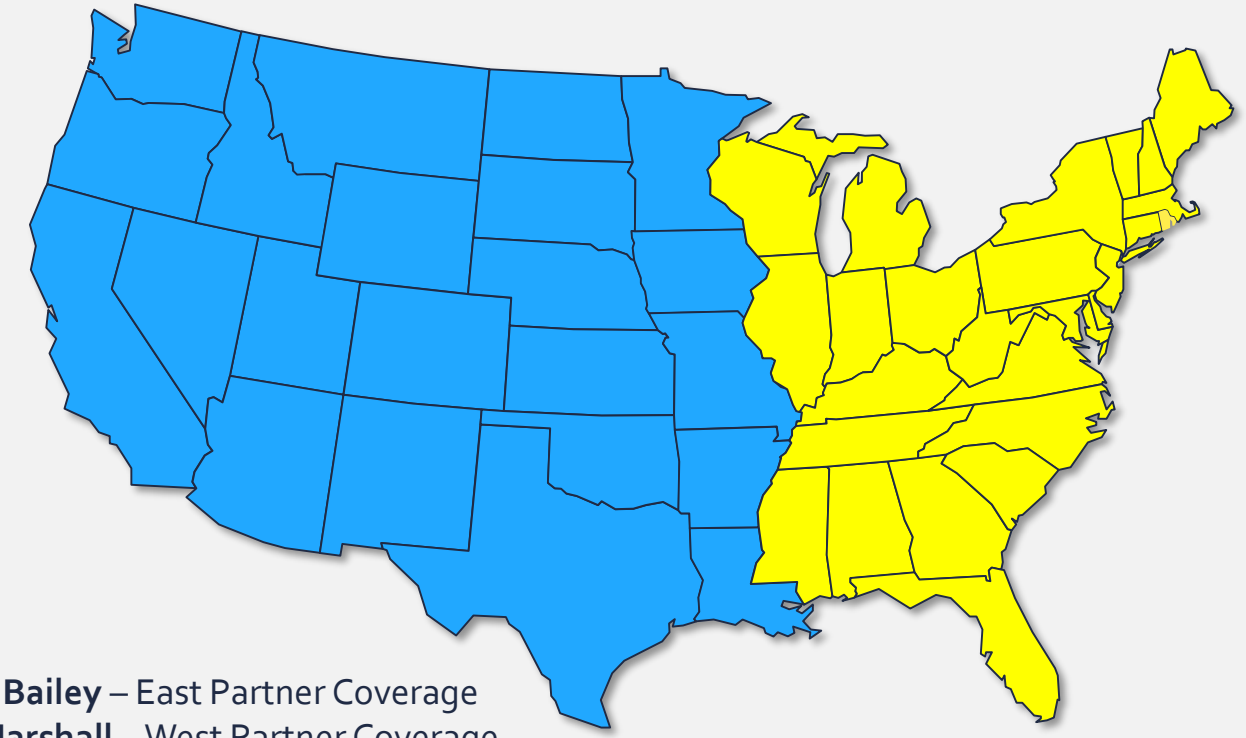
Rick Marshall
Business Development Executive
Location – Tempe, Arizona
(480) 254-4420
Rick.Marshall@Techdata.com

Marshall Hall
Field Solutions Architect, IBM Automation, Red Hat, & *Security*
Location – Bryon, Georgia
(478) 845-9239
Marshall.Hall@techdata.com

Jay Stephens
Field Solutions Architect
Location – San Antonio, Texas
(210) 771-2400
Jay.Stephens@techdata.com

Antonio Ruiz
IBM Vendor Business Executive
Location – San Antonio, Texas
(210) 683-2290
Antonio.Ruiz@techdata.com

Business Development Executive Team Partner Coverage



Karen Bailey – East Partner Coverage
Rick Marshall – West Partner Coverage

Thank you!