IBM Security Zero Trust Blueprints

Secure the Journey to Cloud

TechData

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*
- *Cloud / Hybrid Cloud Security*

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 everything before trying to connect to its systems before granting access.

New risk: Remote workers, cloud, hybrid

- 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

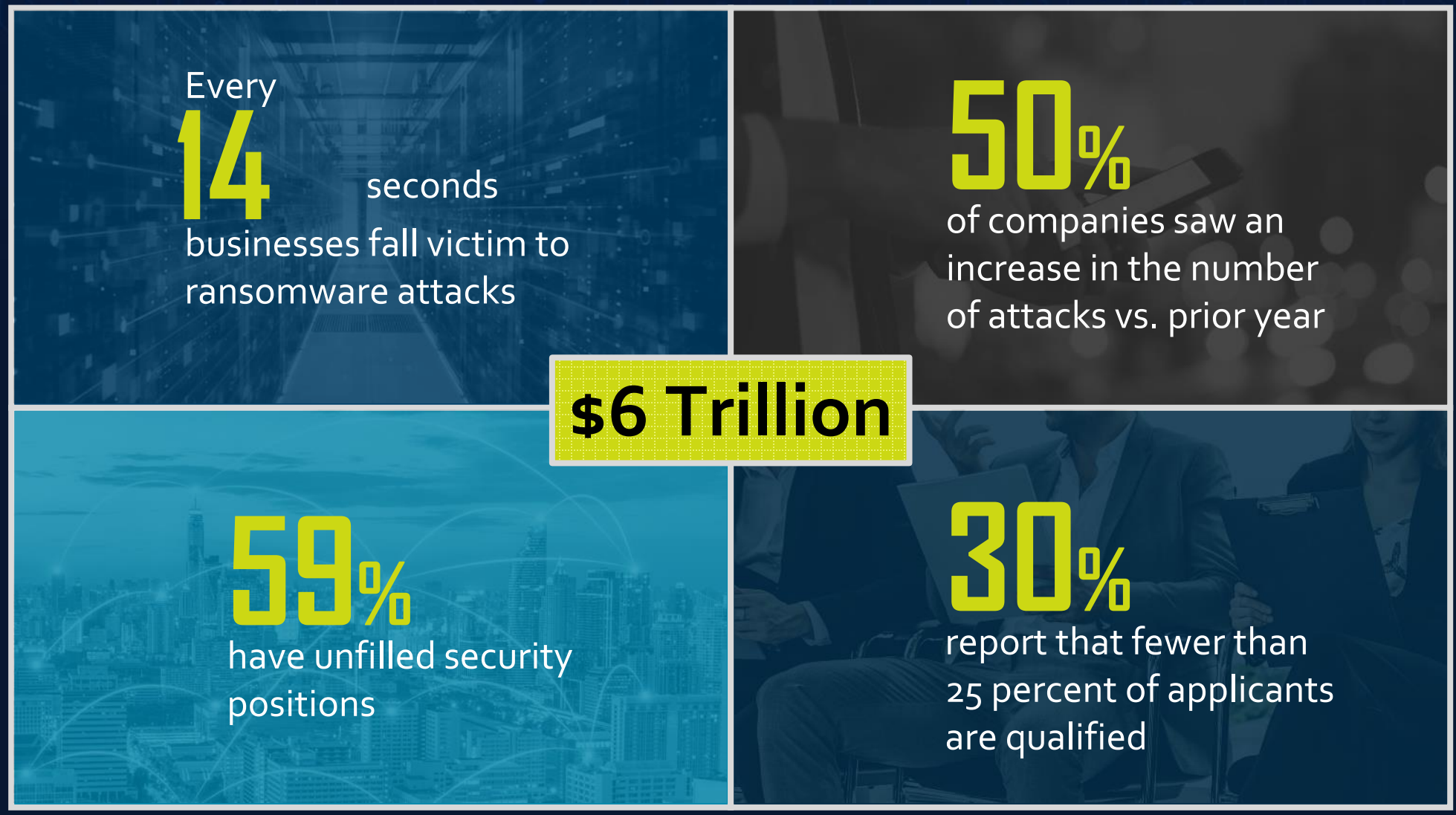
Next steps: Zero Trust

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

Protect the Hybrid Cloud

Reimagine your hybrid cloud security with zero trust in action

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

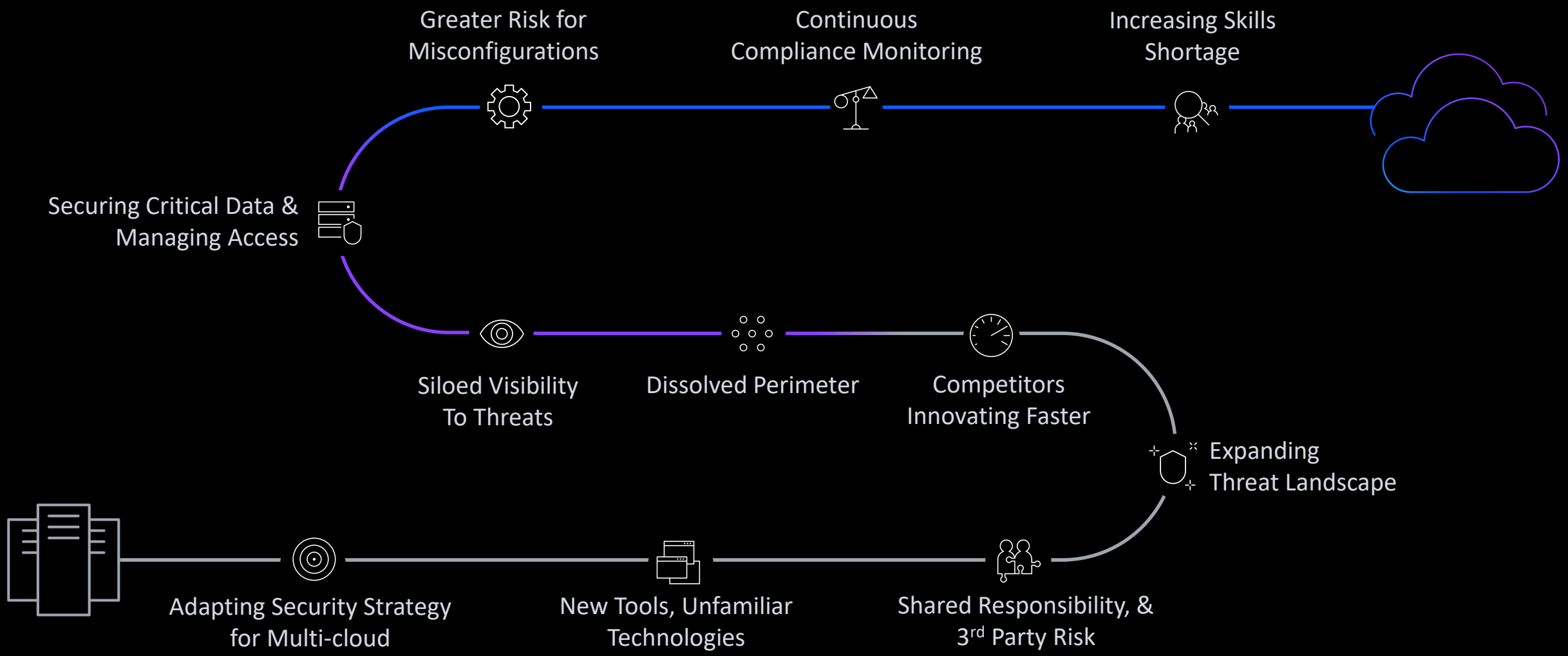
Eliminate VPNs

Provide passwordless experiences

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

- Mauricio Guerra, CISO, Dow Chemical

This digital transformation is creating many new security challenges.



The shift to Cloud requires a shift from

Static, network-based perimeters

to

dynamic, Zero Trust principles focused on users, assets, & resources

Modernizing applications to accelerate client value and differentiate the client experience

Exposure to threats from misconfigured / unsecured PaaS & container environments

Lateral movement and unauthorized access to critical corporate assets

Exposure of cloud credentials, API keys, and secrets from poor secure development practices

Using cloud applications to enable & optimize the business for speed, scale, & flexibility

Data loss via unsanctioned SaaS usage

Unauthorized access from compromised credentials & broad access controls

Migrating workloads for scalability, flexibility & resiliency

Lateral movement and unauthorized access to critical corporate assets

Exposure to threats via legacy secure connectivity practices that expose internal networks & introduce vulnerabilities

Exposure to threats from misconfigured / unsecured cloud workloads

Modernize data platform for more efficient & effective processing & utilization of data

Exposure to threats from misconfigured / unsecured Cloud services

Data loss from lack of visibility & control of data flow across hybrid environment

Unauthorized access or exfiltration of unsecured data from Insider Threats, compromised credentials, and external malicious actors

How can zero trust help?

Insights

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

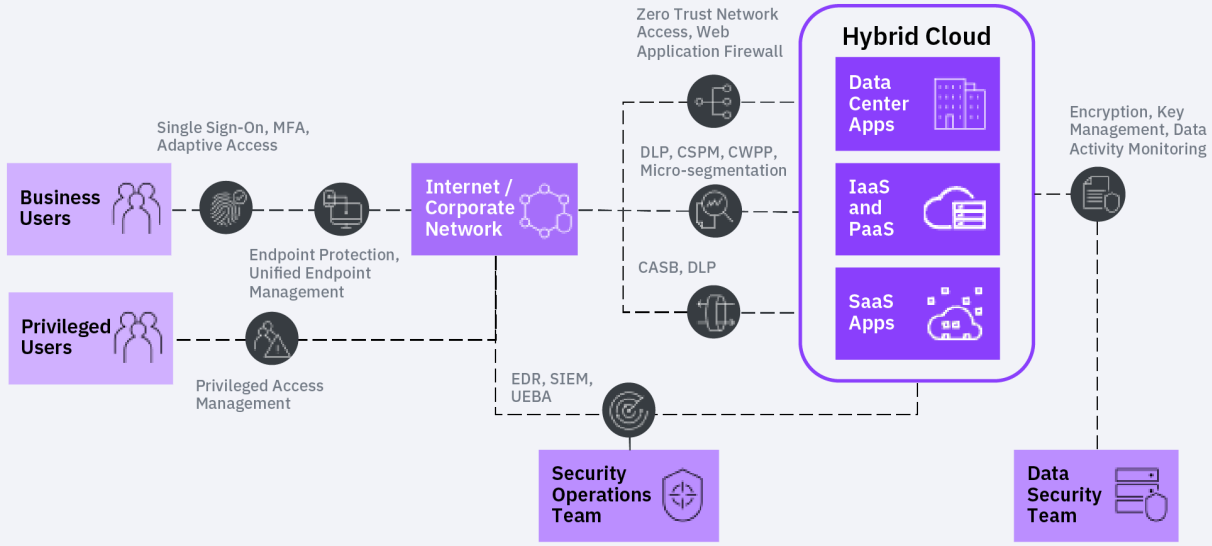
Enforcement

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

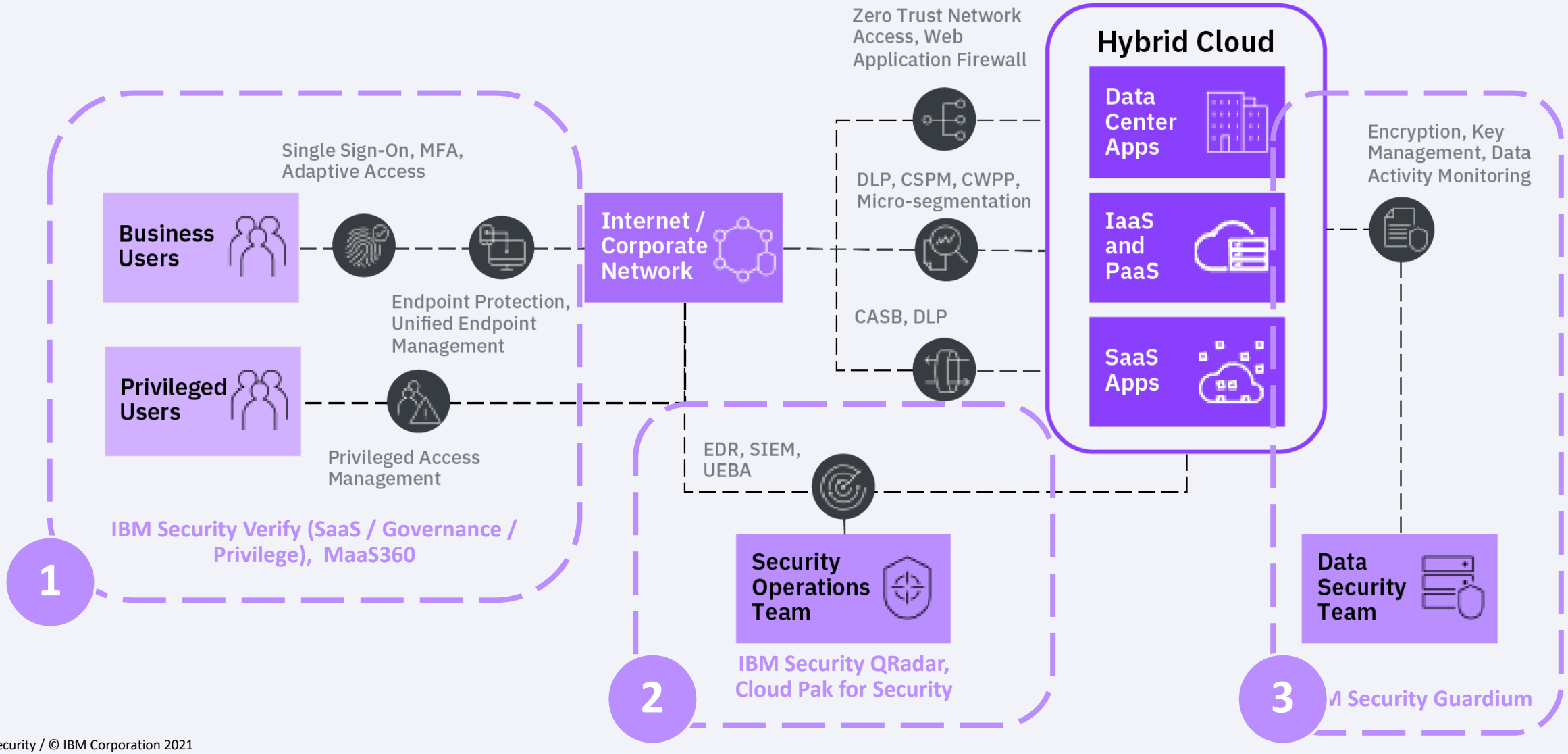
Zero Trust Solution Blueprint: *Protect the hybrid cloud*



	Modernizing applications	Adopting SaaS applications	Migrating data and workloads to cloud
Get Insights			
Cyber Risk Management	●	●	●
Data Discovery & Classification	○	●	●
Offensive Testing	●	○	●
Vulnerability Management	●	○	●
Enforce Protection			
Activity Monitoring	●	○	●
Adaptive Access	●	●	●
Cloud Access Security Broker	○	●	○
Cloud Workload Protection	●	○	●
Data Encryption & Key Management	●	○	●
Data Loss Prevention	○	●	○
Microsegmentation	●	○	●
Multi-Factor Authentication	●	●	●
Privileged Access Management	●	●	●
Secure Access Service Edge	●	●	●
Detect & Respond			
Cloud Security Posture Management	●	○	●
Endpoint Detection and Response	●	●	●
Security Information and Event Management	●	●	●
Security Orchestration Automation and Response	●	●	●

To put zero trust into action to protect the hybrid cloud 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 cloud while strengthening other solutions



IBM Security Verify – Making identity consumable for all users

Extend embedded platform identity layers to deliver advanced functionality and a common experience for all developers, admins, and application users – from mainframe to multicloud

Authenticate and Secure App Workloads

- Strong 2FA (e.g., passwordless auth, mobile push, mobile native biometrics, FIDO2)
- Adaptive access (i.e., risk based auth)
- User consent management

Intelligent Governance
Provision | Certify | Analyze

Continuous Access Control
Authenticate | Authorize | Connect

Proactive Threat Mitigation
Monitor | Detect | Orchestrate

Govern and Administer Access

- Provisioning adapters
- Identity analytics
- Privileged user access (admins, developers, automation)
- Least privilege endpoint controls

IBM **Cloud**

IBM **Cloud Paks**
IBM **WebSphere Hybrid Edition**

3rd Party **Cloud Providers**

IBM **Z**

IBM QRadar and Cloud Pak for Security deliver continuous intelligence, analytics, & response

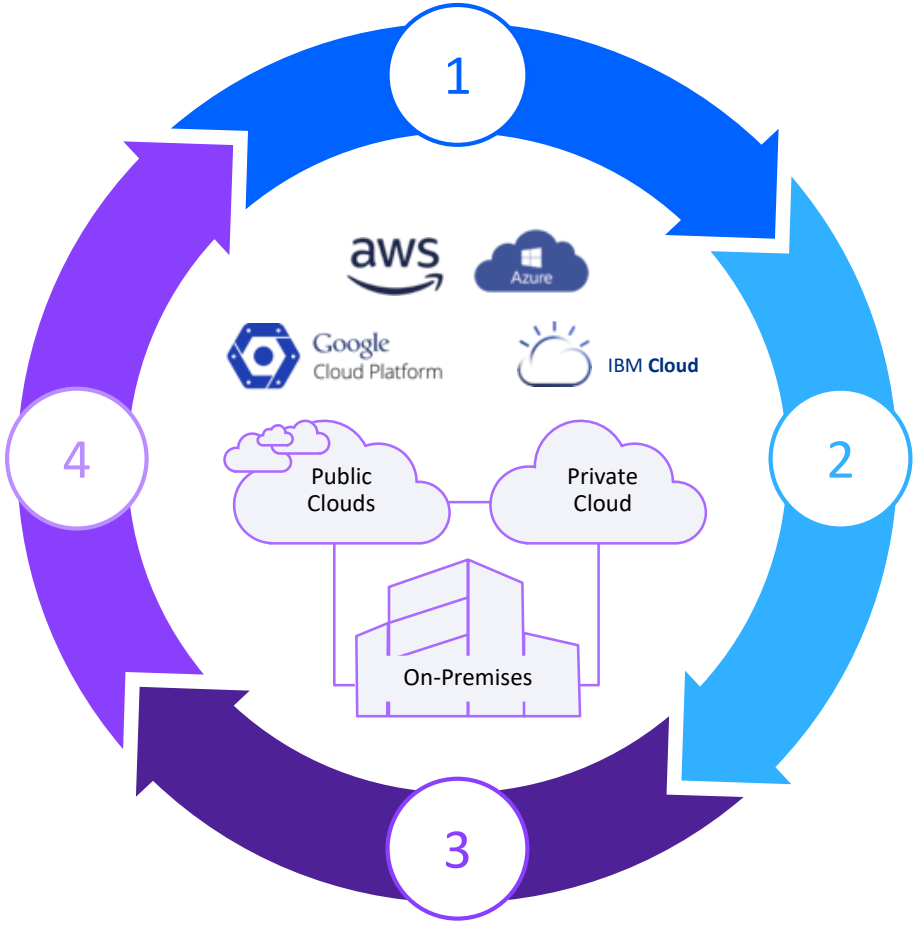
IBM Security

1 **Discover Cloud Footprint**
Identify cloud resources across the enterprise

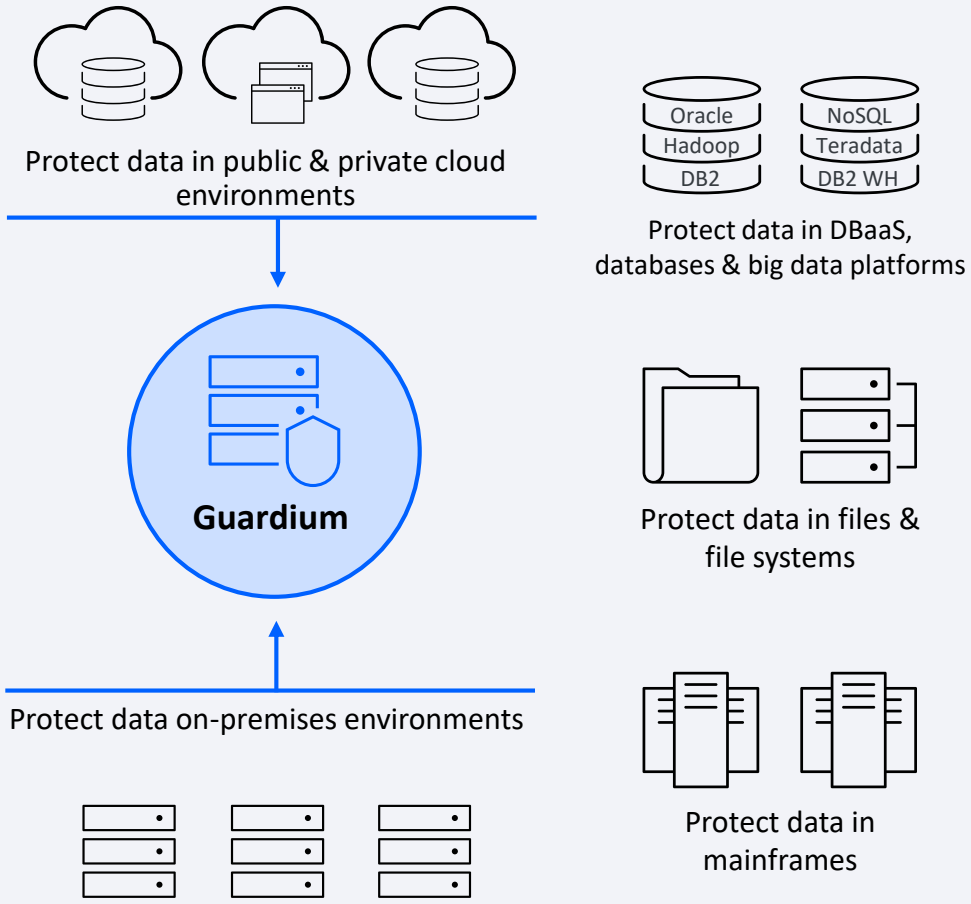
2 **Protect Business SaaS Apps**
Gain deep visibility into cloud applications

3 **Secure IaaS and PaaS**
Secure cloud infrastructure and identify threats with real-time security analytics

4 **Defend Cloud Workloads**
Ingest container-level telemetry and protect the application stack

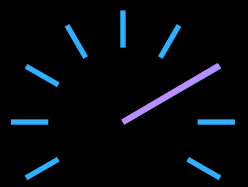


IBM Security Guardium & Cloud Pak for Security: Data security and compliance that support your hybrid cloud journey



- ✓ Simplifies compliance across cloud and on-premises data sources
- ✓ Provides deep data security capabilities:
  - Data discovery and classification
  - Flexible monitoring options of modern and legacy data sources
  - Dynamic data protection, separation of duties
  - Encryption
  - Vulnerability assessment
  - Risk management
  - Data security hub enhances threat detection and accelerated compliance
- ✓ Delivers hybrid multi-cloud data protection with holistic risk views and supports consistent data security policies across environments
- ✓ Broad platform support and massive scalability for the largest environments

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

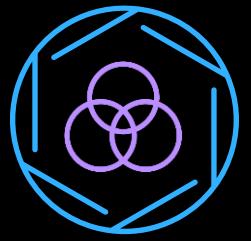


Industry Leading SW

- 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

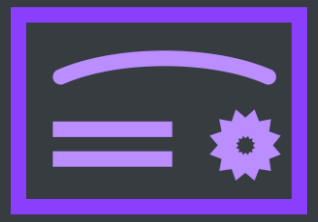
End to End Capability

- 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.)



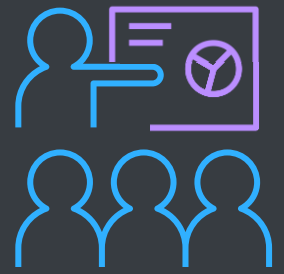
Zero Trust Certifications

- Official product administrator and specialist accreditation
- Demonstrate expertise in 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

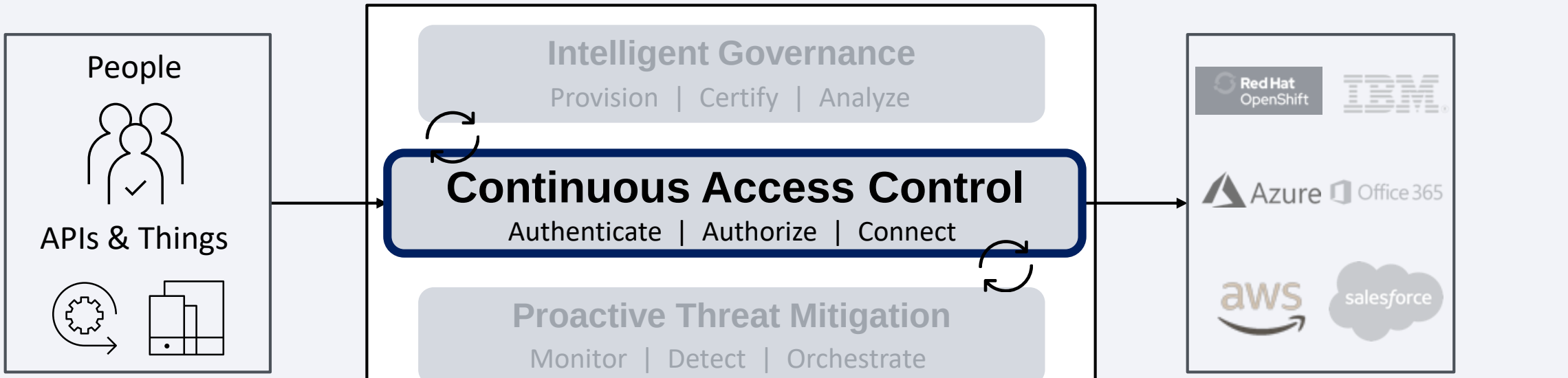
For Organizations

PROTECT THE HYBRID CLOUD

IBM Security Verify

Continuous Access Control

Adaptively enforce authentication and authorization policies, while delivering a frictionless experience for consumers, workforce, and privileged users

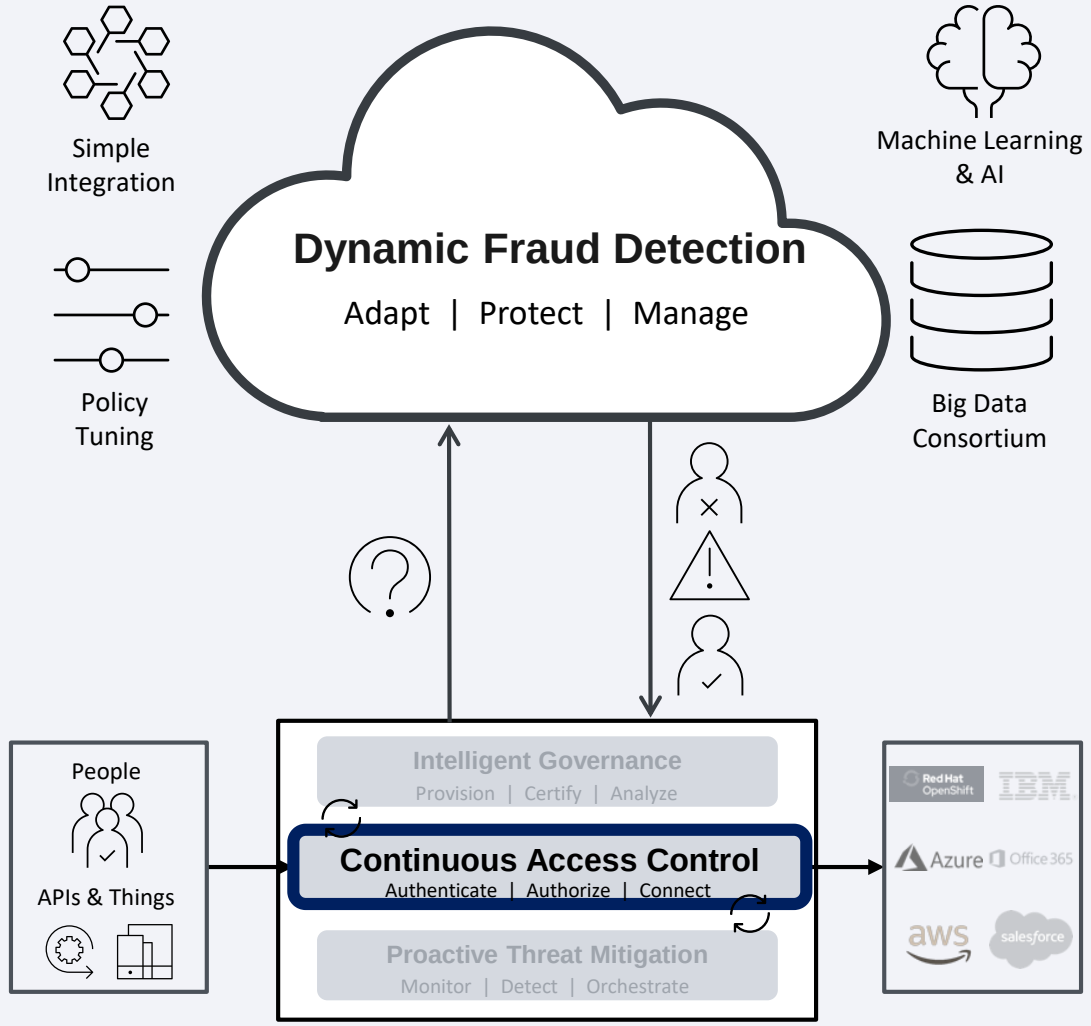


- Password-less & MFA
- Privacy & Consent Management
- Single Sign-On
- Protect Modern & Legacy Apps
- Native Developer Integrations
- Vault & Session Management

Leading fraud detection powers smarter access decisions

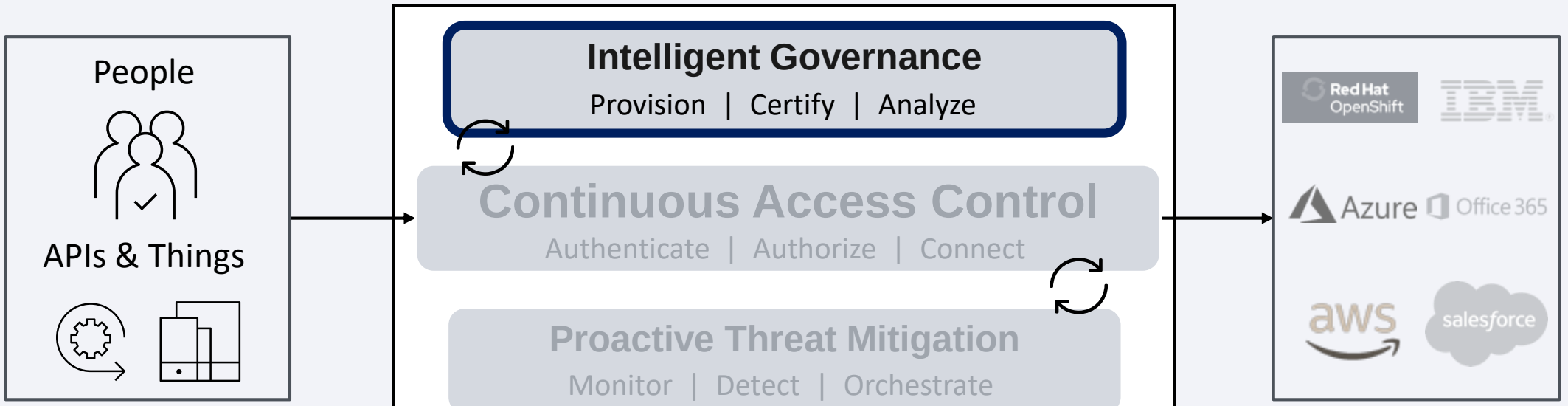
Enable business agility across all digital channels by knowing your users, delivering frictionless access, and securing critical assets with layered fraud detection

- **Modernize any access management solution** and allow it to adapt with comprehensive fraud detection that can assess risk based on the identity, device, environment, resource, and behavior
- **Protect emerging access channels** like APIs, IoT, and chat sessions in addition to traditional web and mobile apps to deliver a consistent omnichannel experience
- **Leverage expertise from professional fraud researchers** to stay ahead of emerging threats with out-of-the-box risk detection policies, self-service policy tuning, and the option for full-service policy customization



Intelligent Governance

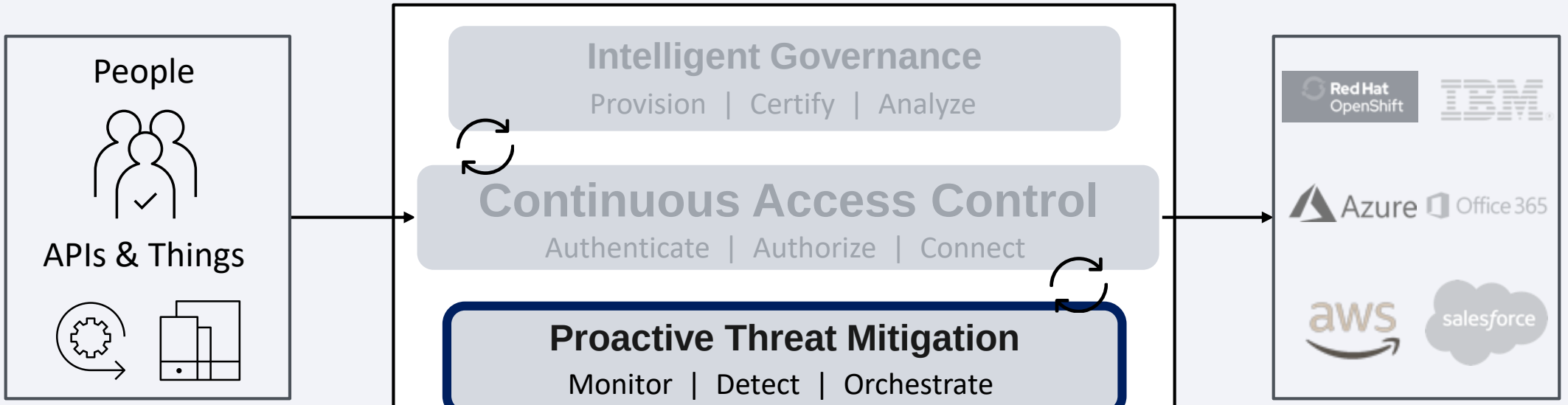
Govern all digital identities, from business to privileged users, with risk-aware compliance and actionable intelligence



- User Lifecycle Management
- Govern Privileged Users & Data
- PAM Reporting & Attestations
- Cloud & On-prem Provisioning
- Risk-Based Certifications
- Business Activity Models

Proactive Threat Mitigation

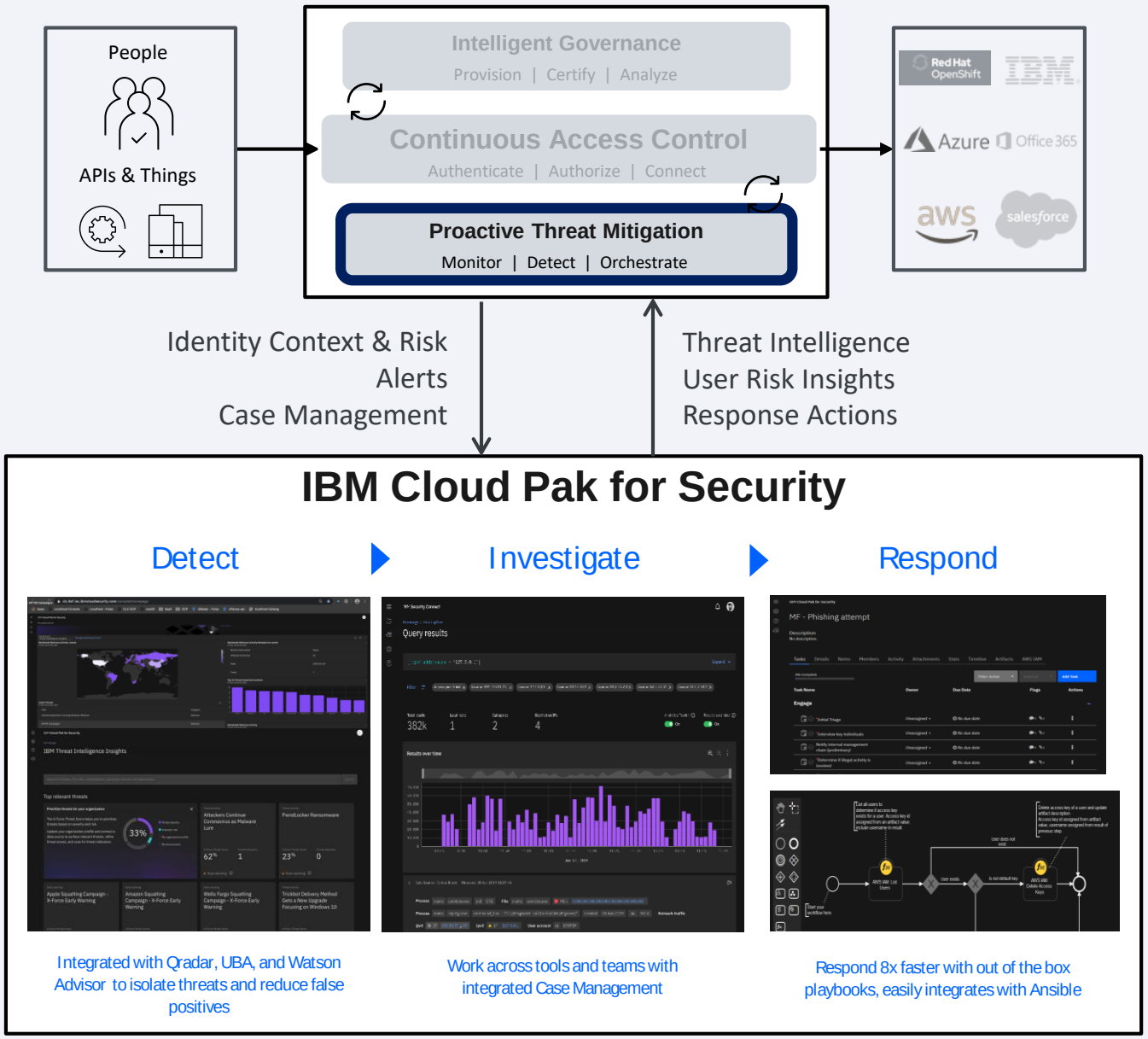
Integrate identity into the broader security ecosystem in order to more effectively adapt to emerging internal and external threats



- Continuous IT Asset Discovery
- Centralized Policy Definitions
- Enforce Privileged ID Controls
- Integration to Next Gen SOC
- UEBA Anomaly Detection
- Automate Identity Response

Embed Identity into Threat Management Workflow

- **Gain complete insights** with a unified console that provides analytics across IBM and 3rd party security tools, data, and clouds
- **Act faster** with AI and automation, simplify operations and streamline response, to save time and lower risk
- **Modernize your architecture** and run anywhere with open, multicloud platform that gives you flexibility, extensibility and avoids lock-in



PROTECT THE HYBRID CLOUD

IBM Security QRadar
IBM Cloud Pak for Security

Discover cloud application usage across the enterprise

- Uncover and control Shadow IT
- Automatically discover hybrid multicloud data and assets
- Gain actionable insights to automate offense triage
- Apply business context to security data

- Enforce security policies using IBM X-Force Threat Intelligence
- Safeguard data and intellectual property
- Minimize enterprise risk through real-time classification

IBM QRadar
Cloud Discovery

#1 SIEM for
Advanced Threat Defense

- Gartner

Gain deep visibility into cloud applications

- Obtain actionable insights into offenses, network data, threats, and malicious behavior in your SaaS applications
- Overcome SaaS provider lack of transparency
- Protect your sensitive data from insider threats
- Combat phishing attempts and credential compromise

- Reduce the risk of data exfiltration and unauthorized file access
- Seamless data protection across multiple SaaS applications including:
  - Microsoft Office 365
  - Salesforce.com
  - G Suite Apps

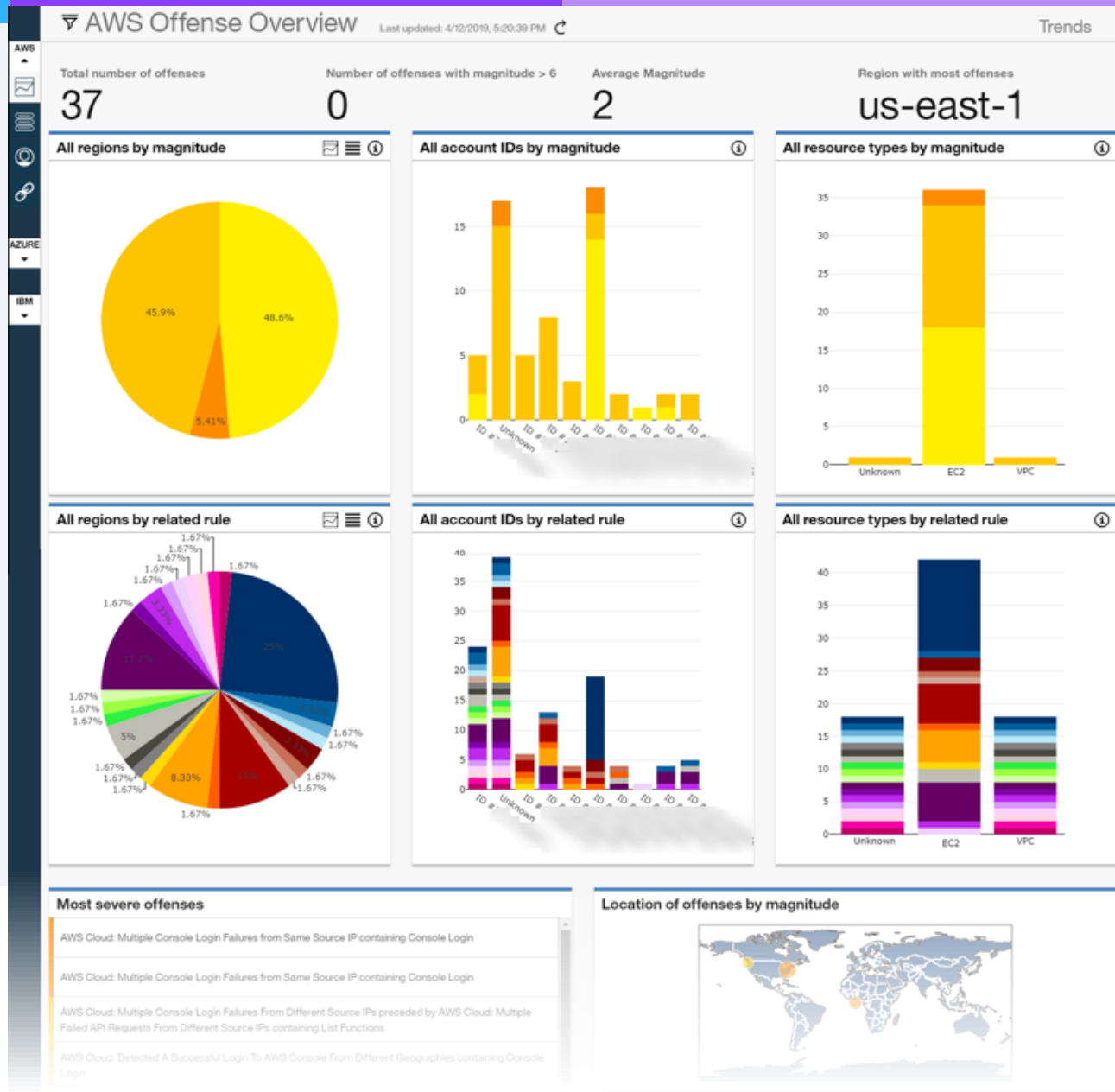
IBM QRadar for SaaS

Secure cloud workloads and identify threats

Simplify Cloud Security

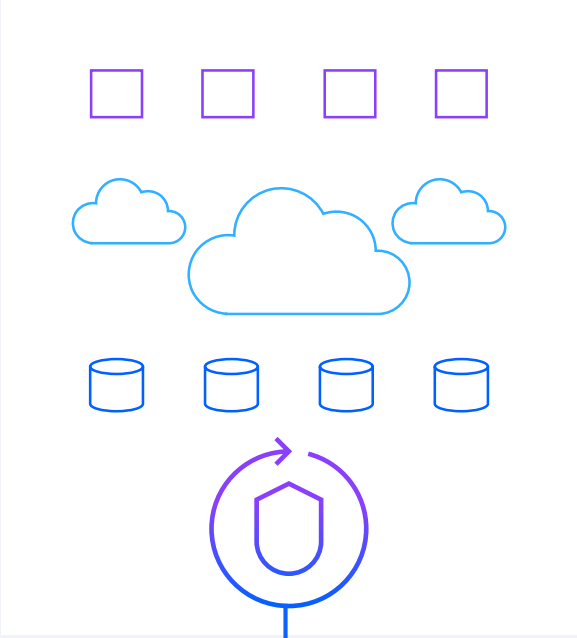
> "QRadar Cloud Visibility and the latest out-of-the-box AWS integrations introduced automation and drastically reduced the time it took us to connect our 100+ AWS accounts to QRadar. This made it easy to consume both events and network flow traffic from our AWS environment."
>
> - Large US-based Insurance Company

- Quickly detect and prevent cloud misconfigurations
- Gain deep visibility across IaaS environments including AWS, Azure, and IBM Cloud
- Consume cloud threats via a single pane of glass
- Clearly visualize cloud network traffic in real-time



IBM QRadar
Cloud Visibility

Ingest container-level telemetry and protect the application stack



Defend containers with real-time threat detection

- Gain visibility into container-based applications
- Discover indicators of container compromise and credential vulnerabilities
- Elevate threat hunting

- Prevent container breakout to safeguard applications
- Identify anomalous authentication and privilege escalation
- Detect indicators of insider threats or active data exfiltration

Red Hat OpenShift

Red Hat Enterprise Linux

Twistlock A PALO ALTO NETWORKS® COMPANY

aqua

Sysdig

IBM QRadar Container Security

PROTECT THE HYBRID CLOUD

IBM Security Guardium

Guardium: A unified data security solution

Securing hybrid multicloud environments with Guardium Data Protection

Dynamic

Active & passive monitoring for 30+ cloud-native data sources

- Agentless
- Agent-based

Minimize security blind spots and take real-time action with blocking and redaction*

Store data security and audit data to meet retention requirements and uncover unknown threats

* Agent-based

Orchestrated

Centralized policy enforcement and management across hybrid multi clouds

Automate compliance workflows for audit reviews and approvals

Orchestrate remediation and response with IT and SecOps tools

- ServiceNow, Splunk, QRadar, Resilient, and more

Modern

Uses cloud-native and containerized technology

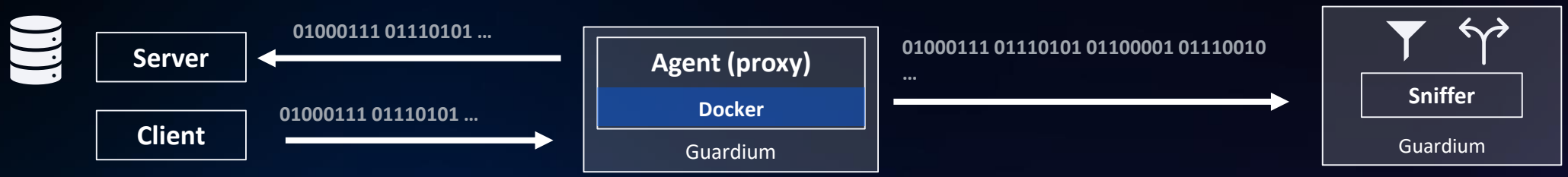
Simplify and streamline deployment with cloud management frameworks, such as Kubernetes and OpenShift

Elastic, scalable and resilient

Supporting flexible monitoring using modern architectures

Real-time protection for mission critical on-premises data sources: Agents (STAPs)

Real-time protection for mission critical data sources in the cloud: Proxy-based Agents (E-TAPs)



Agentless audit support for on-premises or cloud-based data sources: Universal Connectors

Call to Action

Next Steps

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

Tech Data IBM Security Brand Team

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

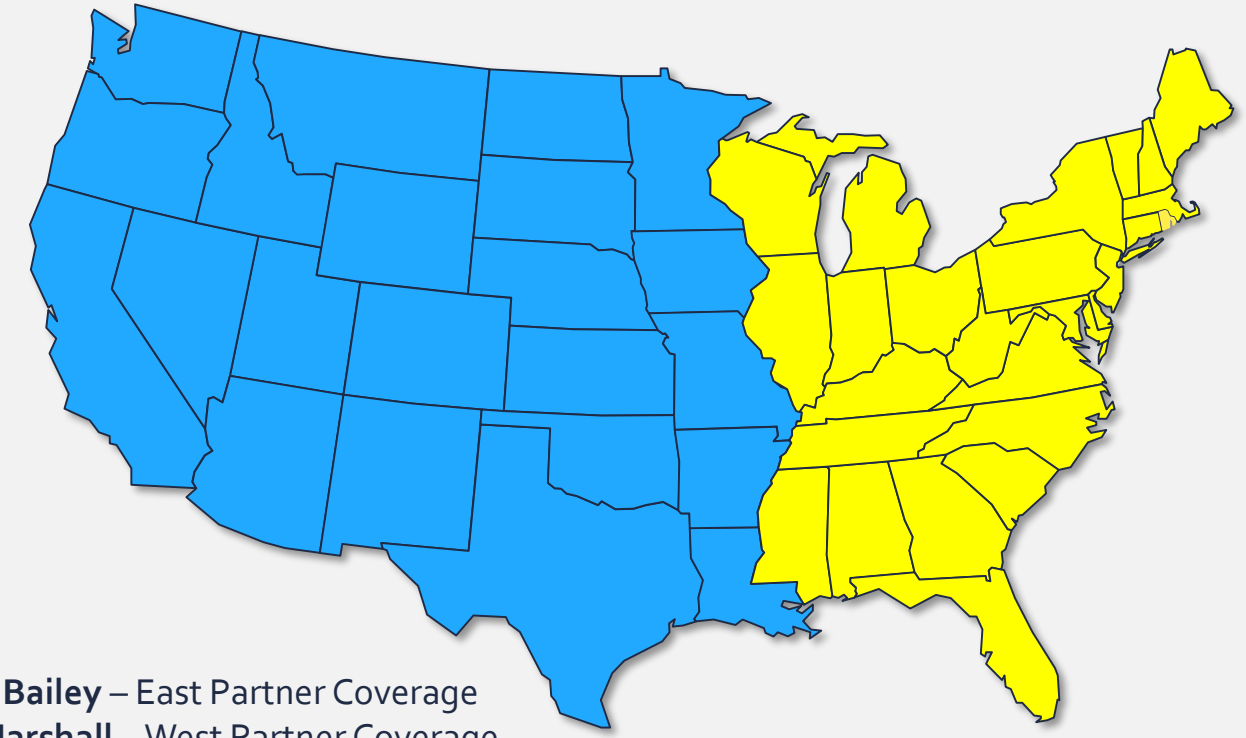
Rick Marshall
Business Development Executive
Location – Tempe, Arizona
(480) 254-4420
Rick.Marshall@Techdata.com

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!