Zero Trust in Hybrid Cloud and Multi Cloud Environments

Dominik Sowinski
Senior Cloud Security Consultant
Oct 2022

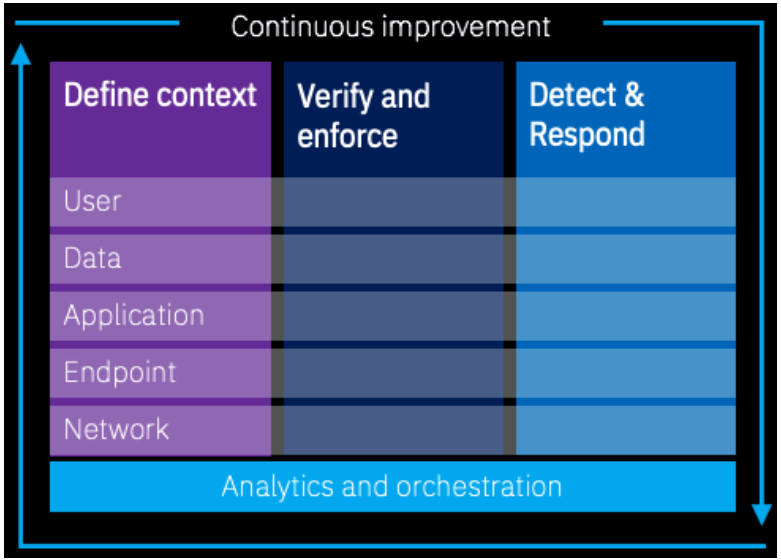
IBM Security / © 2022 IBM Corporation

What is Zero Trust?

NIST 800-207 Zero Trust Tenets

1. All data sources and computing services are considered resources.
2. All communication is secured regardless of network location.
3. Access to individual enterprise resources is granted on a per-session basis.
4. Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.
5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
7. The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

IBM Zero Trust Governance Model



IBM Security / © 2022 IBM Corporation

Agenda

- **Layered approach to Zero Trust in Hybrid Cloud and Multi Cloud**
- First Layer – Inter-Cloud
- Second Layer – Intra-Cloud
- Third Layer – Inter-Workloads
- Q&A

Zero Trust in Hybrid Cloud/MultiCloud – Which Layers have to be considered?

Address the Zero Trust solutions through a layered approach

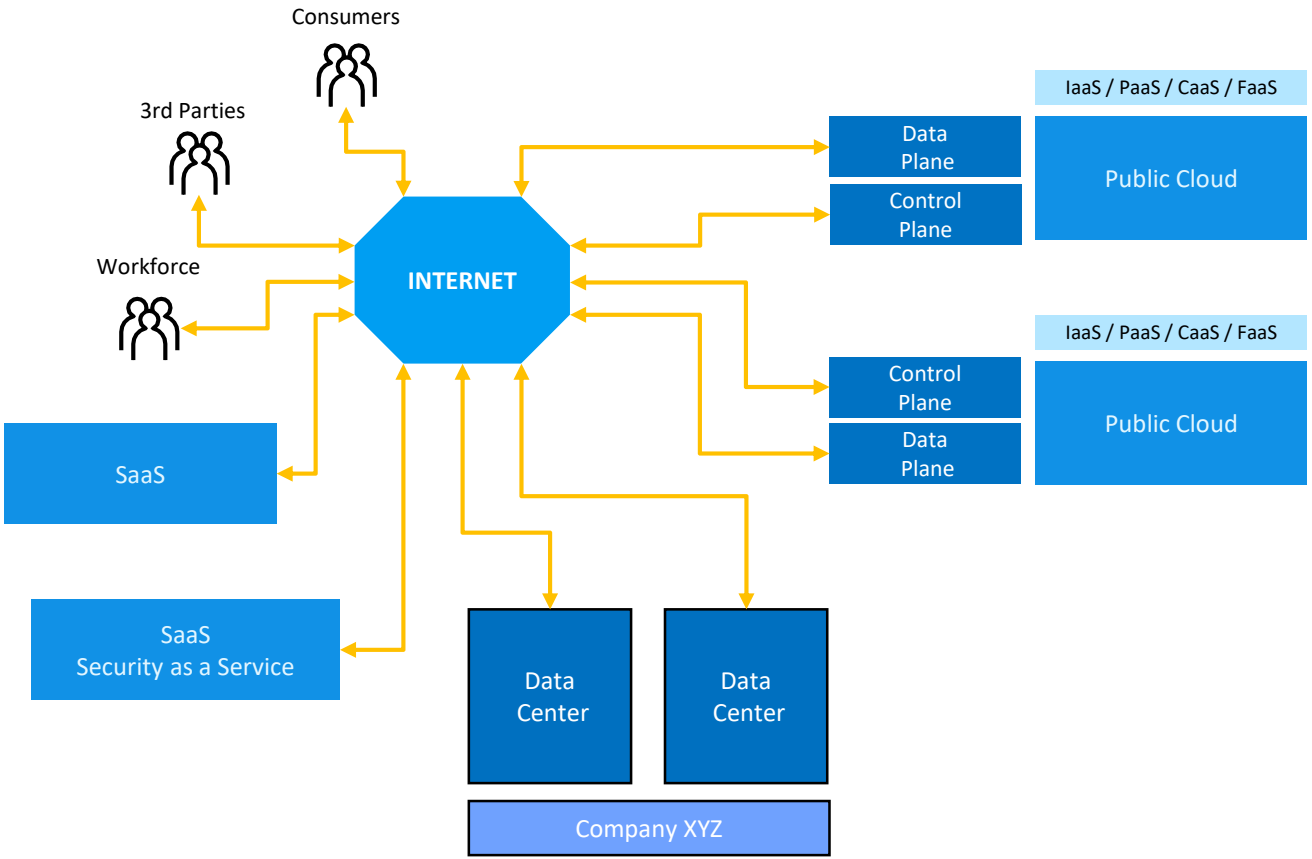
1) **inter-cloud**: apply zero trust based solutions cross cloud instances and data centers

2) **intra-cloud**: apply zero trust solutions within one cloud instance

3) **inter-workload**: apply zero trust solutions within a Kubernetes cluster and the workloads & services within that cluster*

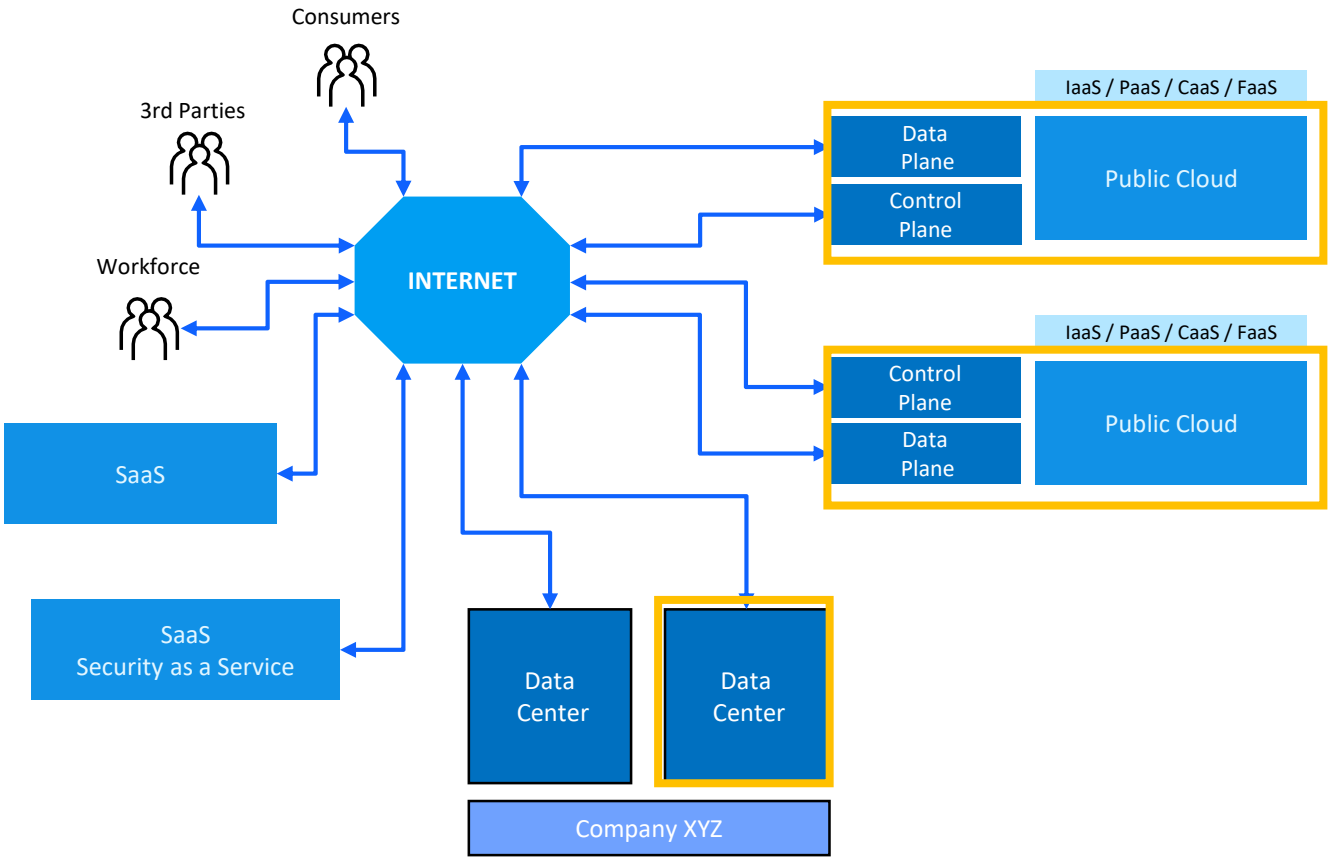
* Inter-workload might be across mutliple k8s clusters and thus even across cloud instances

First layer: Inter-cloud

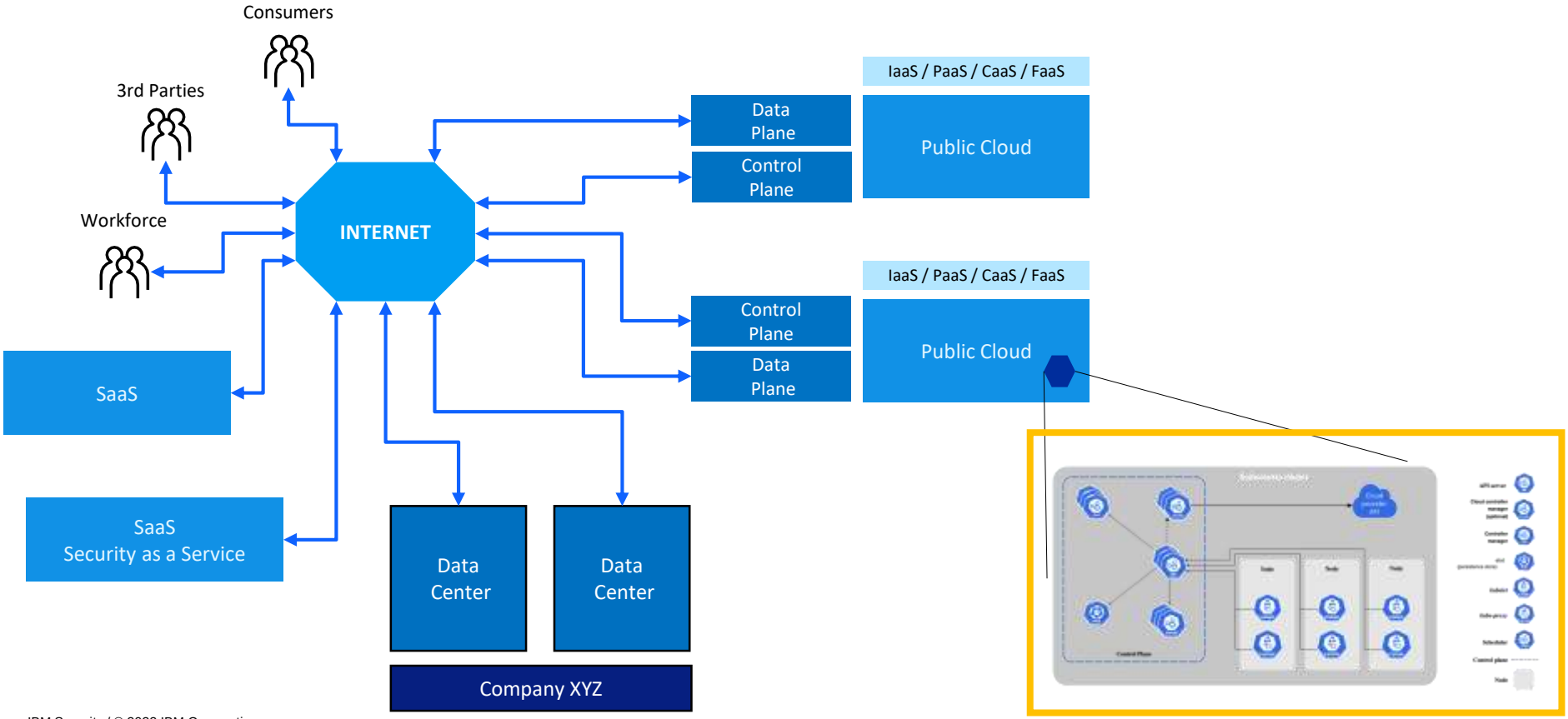


IBM Security / © 2022 IBM Corporation

Second layer: Intra-cloud



Third layer: inter-workload



IBM Security / © 2022 IBM Corporation

What are the risks specific to cloud?

Cloud Technical Risks to be addressed by the customer

- **Data and application layer risks**: includes poor access management, unsanctioned applications, open shares

- **Cloud deployment configuration risks**: wrong configuration exposes cloud resources on the data plane
- **Network layer risks**: wrong configuration of data plane network
- **Cloud workload risks**: incomplete hardening, unauthorized services running, unpatched vulnerabilities
- **Cloud interconnect risks**: poor integration between multiple cloud services leading to unauthorized access
- **Cloud management layer configuration risks** : Control Plane related risks; privileged users management and monitoring, unauthorized changes to Cloud deployments

IBM Security / © 2022 IBM Corporation

Cloud Technical Risks to be addressed by the customer

- **Data and application layer risks**: includes poor access management, unsanctioned applications, open shares
- **Cloud deployment configuration risks**: wrong configuration exposes cloud resources on the data plane
- **Network layer risks**: wrong configuration of data plane network
- **Cloud workload risks**: incomplete hardening, unauthorized services running, unpatched vulnerabilities
- **Cloud interconnect risks**: poor integration between multiple cloud services leading to unauthorized access
- **Cloud management layer configuration risks** : Control Plane related risks; privileged users management and monitoring, unauthorized changes to Cloud deployments

IBM Security / © 2022 IBM Corporation

Cloud Technical Risks to be addressed by the customer

- **Data and application layer risks**: includes poor access management, unsanctioned applications, open shares
- **Cloud deployment configuration risks**: wrong configuration exposes cloud resources on the data plane
- **Network layer risks**: wrong configuration of data plane network
- **Cloud workload risks**: incomplete hardening, unauthorized services running, unpatched vulnerabilities
- **Cloud interconnect risks**: poor integration between multiple cloud services leading to unauthorized access
- **Cloud management layer configuration risks** : Control Plane related risks; privileged users management and monitoring, unauthorized changes to Cloud deployments

IBM Security / © 2022 IBM Corporation

Cloud Technical Risks to be addressed by the customer

- **Data and application layer risks**: includes poor access management, unsanctioned applications, open shares
- **Cloud deployment configuration risks**: wrong configuration exposes cloud resources on the data plane
- **Network layer risks**: wrong configuration of data plane network
- **Cloud workload risks**: incomplete hardening, unauthorized services running, unpatched vulnerabilities
- **Cloud interconnect risks**: poor integration between multiple cloud services leading to unauthorized access
- **Cloud management layer configuration risks** : Control Plane related risks; privileged users management and monitoring, unauthorized changes to Cloud deployments

IBM Security / © 2022 IBM Corporation

Cloud Technical Risks to be addressed by the customer

- **Data and application layer risks**: includes poor access management, unsanctioned applications, open shares
- **Cloud deployment configuration risks**: wrong configuration exposes cloud resources on the data plane
- **Network layer risks**: wrong configuration of data plane network
- **Cloud workload risks**: incomplete hardening, unauthorized services running, unpatched vulnerabilities
- **Cloud interconnect risks**: poor integration between multiple cloud services leading to unauthorized access
- **Cloud management layer configuration risks** : Control Plane related risks; privileged users management and monitoring, unauthorized changes to Cloud deployments

IBM Security / © 2022 IBM Corporation

Cloud Technical Risks to be addressed by the customer

- **Data and application layer risks**: includes poor access management, unsanctioned applications, open shares
- **Cloud deployment configuration risks**: wrong configuration exposes cloud resources on the data plane
- **Network layer risks**: wrong configuration of data plane network
- **Cloud workload risks**: incomplete hardening, unauthorized services running, unpatched vulnerabilities
- **Cloud interconnect risks**: poor integration between multiple cloud services leading to unauthorized access
- **Cloud management layer configuration risks** : Control Plane related risks; privileged users management and monitoring, unauthorized changes to Cloud deployments

Cloud* Technical Risks to be addressed by the customer

- **Data and application layer risks**: includes poor access management, unsanctioned applications, open shares **=> Intra-Cloud**
- **Cloud deployment configuration risks**: wrong configuration exposes cloud resources on the data plane **=> Intra-Cloud**
- **Network layer risks**: wrong configuration of data plane network **=> Intra-Cloud**
- **Cloud workload risks**: incomplete hardening, unauthorized services running, unpatched vulnerabilities **=> Inter-Workload**
- **Cloud interconnect risks**: poor integration between multiple cloud services leading to unauthorized access **=> Inter-Cloud**
- **Cloud management layer configuration risks** : Control Plane related risks; privileged users management and monitoring, unauthorized changes to Cloud deployments **=> Intra-Cloud**

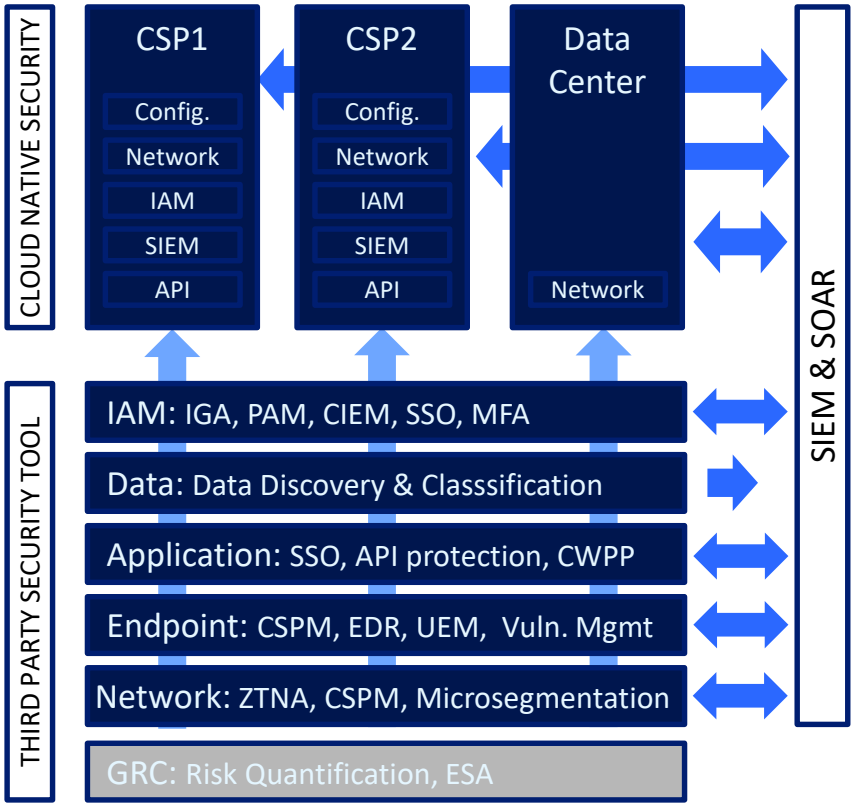
* Hybrid Cloud => add data center related risks: Network layer risks (lateral movement), Endpoint risks (vulnerabilities, configuration, malware), Data Risks (data profileration, data loss), Application (cumulation of access through the years, vulnerabilities,), ….

IBM Security / © 2022 IBM Corporation

Agenda

- Layered approach to Zero Trust in Hybrid Cloud and Multi Cloud
- **First Layer – Inter-Cloud**
- Second Layer – Intra-Cloud
- Third Layer – Inter-Workloads
- Q&A

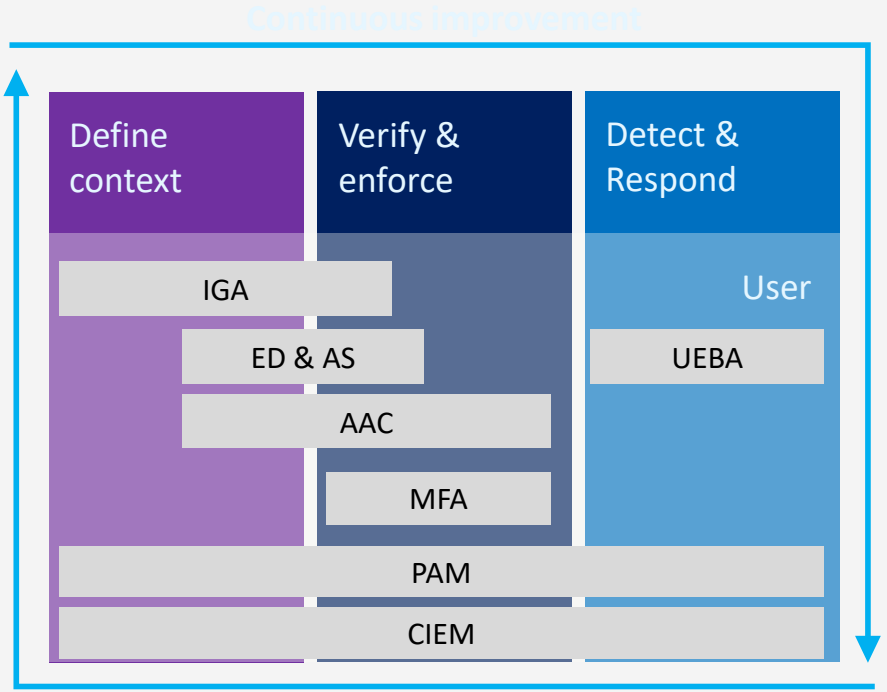
Types of security capabilities deployed at the inter-cloud level



IBM Security / © 2022 IBM Corporation

Inter-Cloud – IAM – Zero Trust Focus

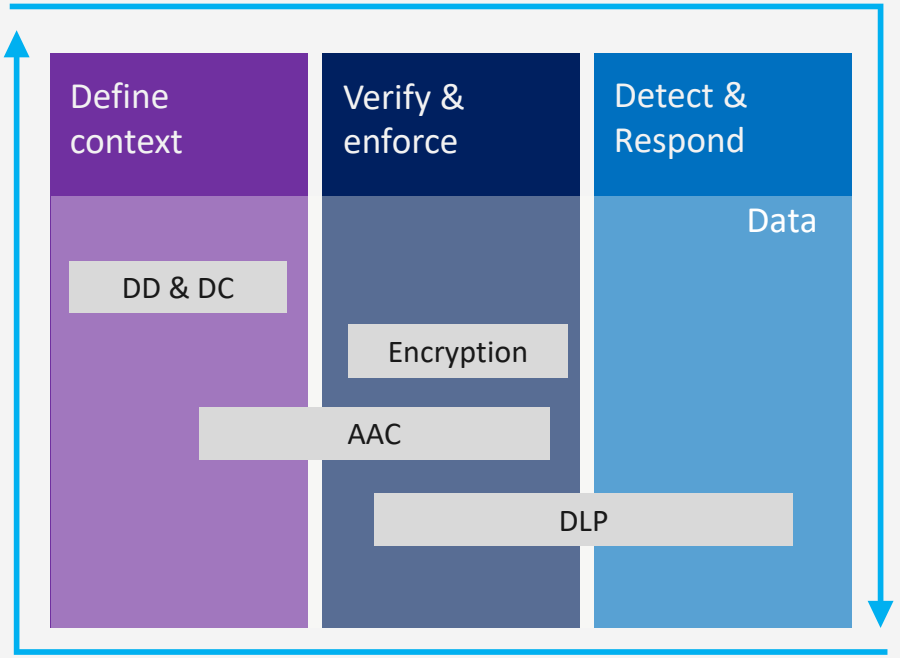
- IAM are the most typical cross-cloud capabilities
- Do expect a mix of On Premise, SaaS and Cloud Native IAM capabilities
- Typical cross cloud IAM capabilities
  - Enterprise Directory (ED)
  - Authentication Service (AS) (+Federation)
  - Provisioning Accounts (IGA)
  - Group/Role membership (IGA / RBAC)
  - Privileged Access Management (PAM)
- Zero Trust Focus areas for IAM
  - Least Privilege
  - JIT (Privileged) Access to resources
  - Adaptive Access Control (AAC) with MFA
  - Continuous Authentication
  - Secrets Management
  - Cloud Infrastructure Entitlement Management (CIEM)



IBM Security / © 2022 IBM Corporation

Inter-Cloud – Data – Zero Trust Focus

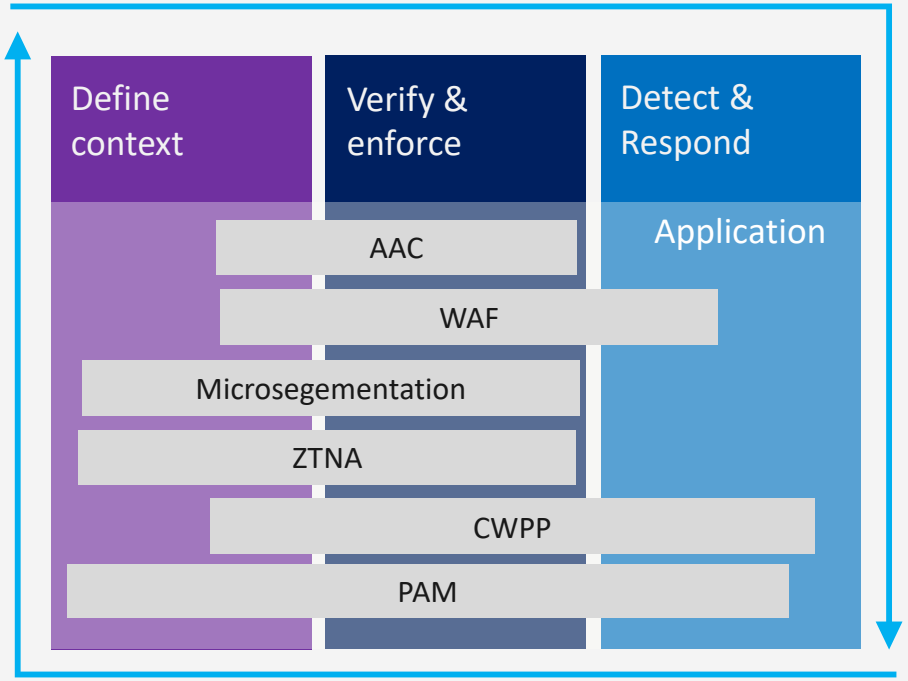
- Typical Data Security topics are:
  - Data Discovery (DD)
  - Data Classification & Labelling (DC)
  - Protection (Access Control & Encryption)
  - Data Loss Prevention (DLP)
  - Lifecycle Management
- Zero Trust Focus areas for Data Security are
  - All security measures are there to protect data…but some specific ones are:
    - Encryption in Transit & At Rest
    - Automation for classification & labelling
    - Data classification is taken in account for adaptive access control
    - Monitoring of Data usage to detect anomalies => Data Loss Prevention



IBM Security / © 2022 IBM Corporation

Inter-Cloud – Application* – Zero Trust Focus

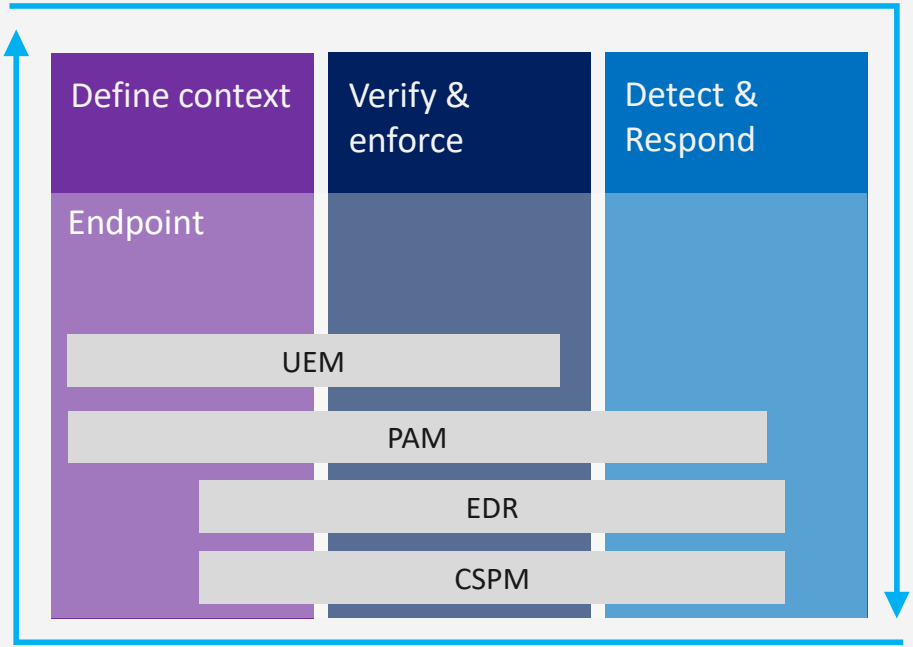
- Typical Application Security topics are:
  - Access Control / SSO
  - Web Application Firewall (WAF)
  - Network Segmentation
  - API Protection
  - Vulnerability Management
- Zero Trust Focus areas for Application Security are:
  - Microsegementation by grouping applications/workloads
  - Zero Trust Network Access (session based access)
  - Adaptive Access Control (ingration with AAC solution for application authentication)
  - JIT Privileged Access
  - WAF
  - Cloud Workload Protection Platform (CWPP)



IBM Security / © 2022 IBM Corporation

Inter-Cloud – Endpoint – Zero Trust Focus

- Typical Endpoint Security topics are:
  - Anti-Malware
  - Endpoint Detection & Response (EDR)
  - Unified Endpoint Management
    - Configuration & Hardening
    - Patching
    - Software Installation
  - Vulnerability Management
- Zero Trust Focus areas for Endpoint Security are
  - Cloud Security Posture Management*
  - Endpoint Detection & Response (EDR)
  - JIT Privileged Access

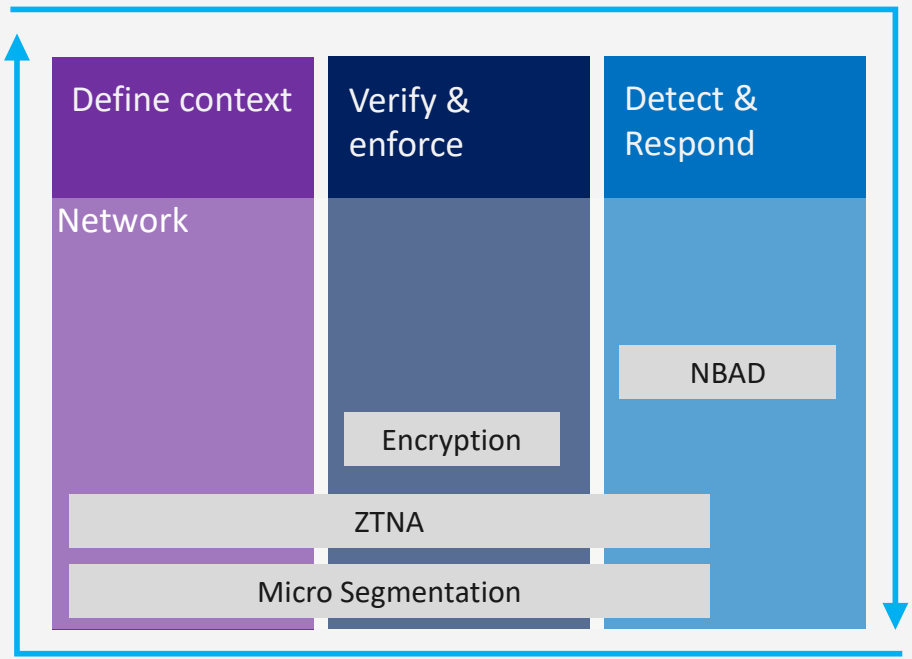


* CSPM goes broader than the typical endpoints like VMs, it also takes care of Cloud resources and configuration in general

IBM Security / © 2022 IBM Corporation

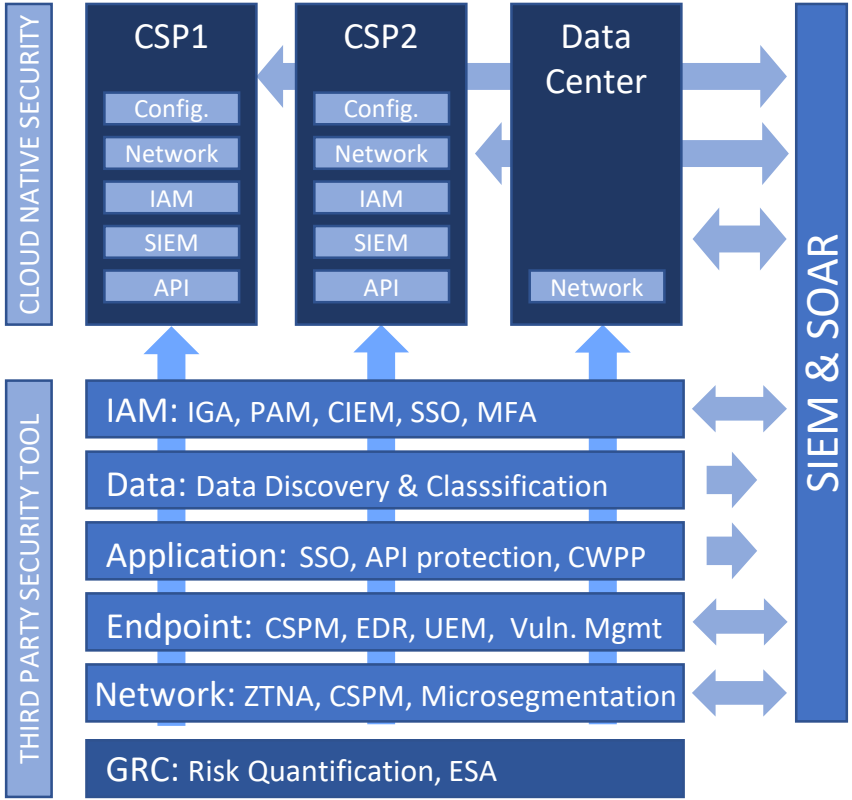
Inter-Cloud – Network – Zero Trust Focus

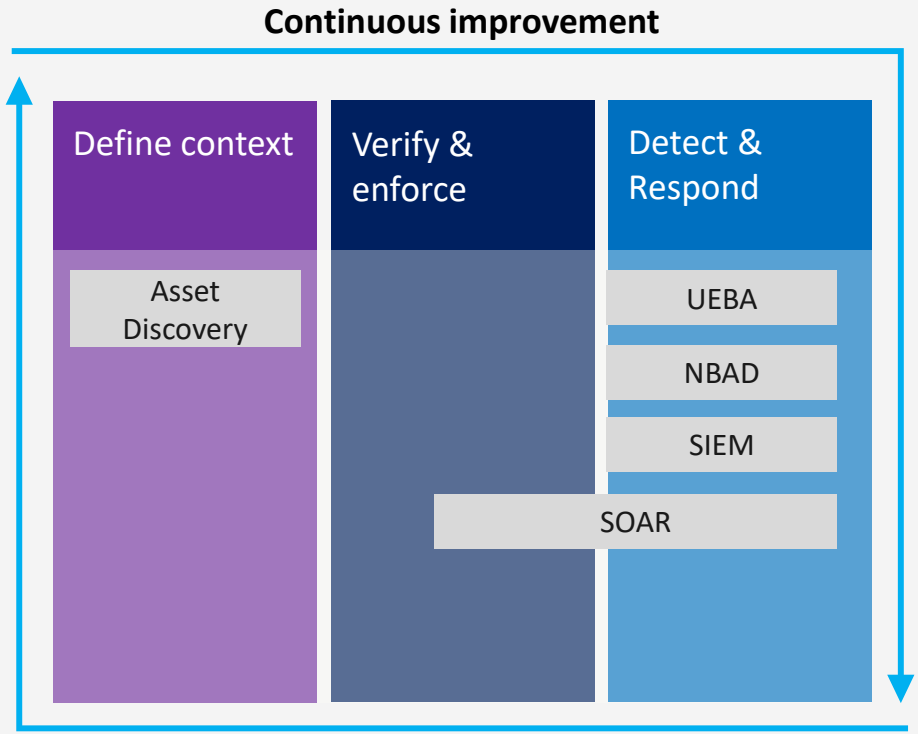
- Typical Network Security topics are:
  - Firewall
  - Encryption
  - Intrusion Detection/Protection (IDPS)
  - Segmentation
  - Network Behavior Anomaly Detection (NBDAD)
- Zero Trust Focus areas for Network Security are
  - Microsegmentation
  - Zero Trust Network Access (ZTNA*)
  - Encryption (mutual TLS)
  - Cloud Traffic Monitoring (part of CSPM)



* ZTNA is mostly delivered as a key component of a Secure Access Service Edge (SASE) solution

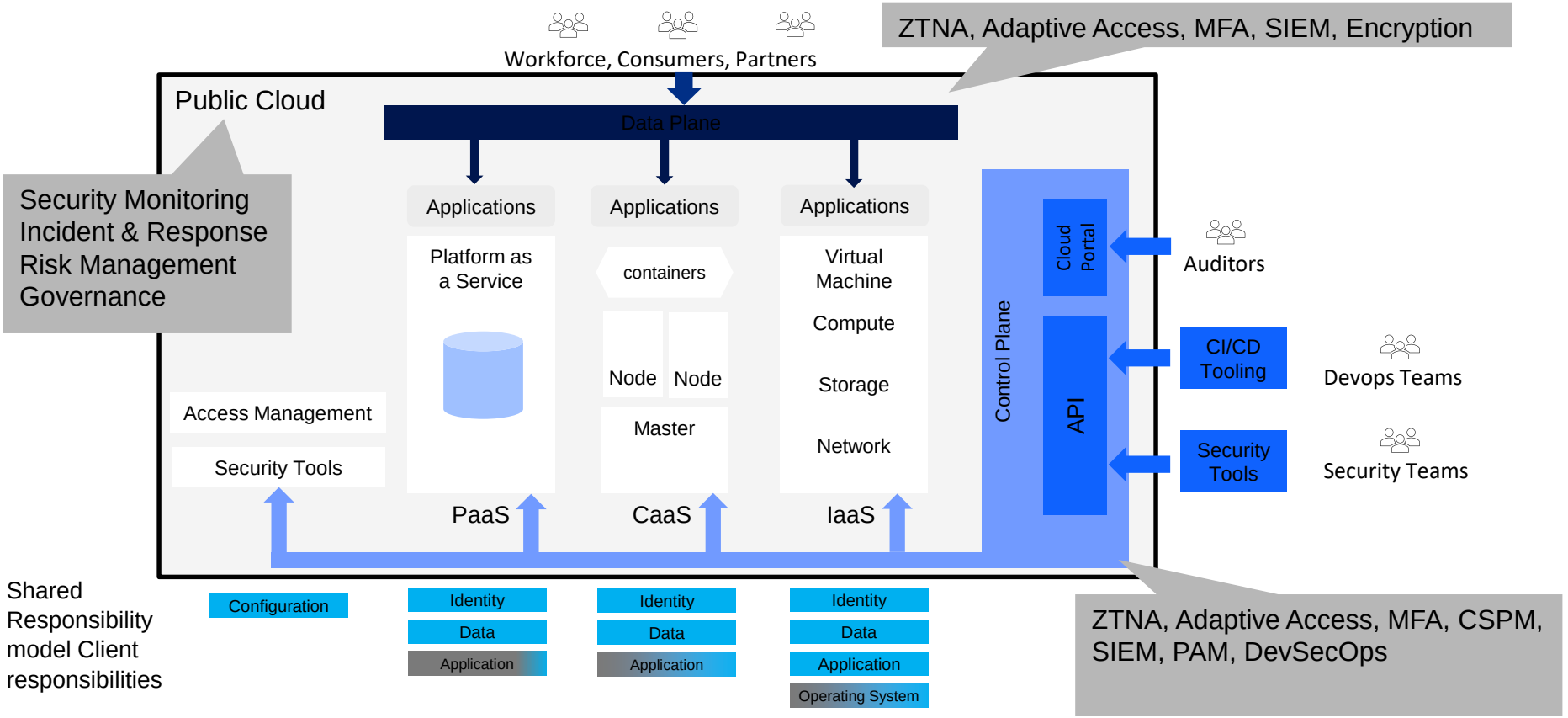
Inter-Cloud – SIEM & SOAR – Zero Trust Focus





IBM Security / © 2022 IBM Corporation

Three areas where Zero Trust can be applied

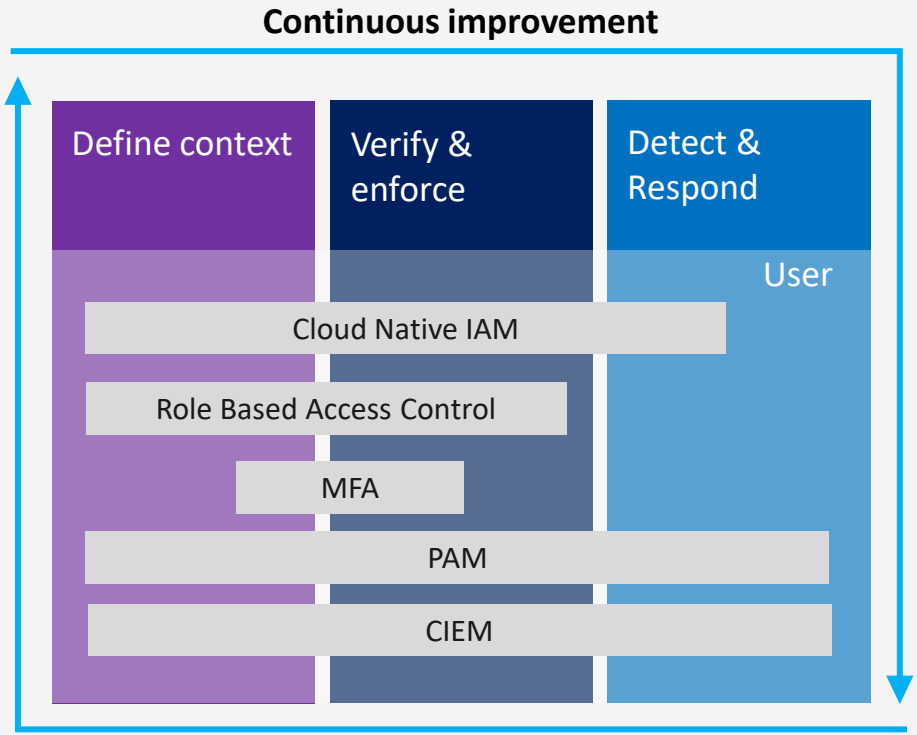


IBM Security / © 2022 IBM Corporation

Intra-Cloud – IAM – Zero Trust Focus

- Data Plane related IAM
  - Consumer IAM (Business Driven)
  - Workforce RBAC (IT Driven)
  - Adaptive Access Control
  - MFA
- Control Plane related IAM
  - CIEM
  - (JIT) Privilged Access Management (PAM)
  - Access Management to API
  - Temporary & automated permissions to deploy resources (Native IAM controls to manage CI/CD pipeline permissions)

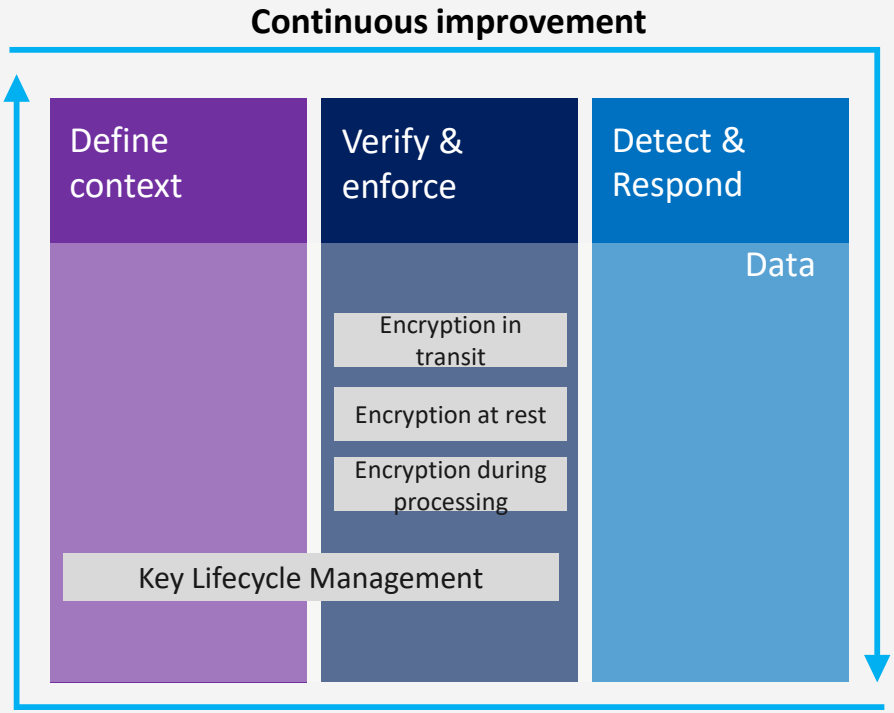
Note : Identity based networking or segmentation is about creating an unique identity per workload/system communicating over the network



IBM Security / © 2022 IBM Corporation

Intra-Cloud – Data – Zero Trust Focus

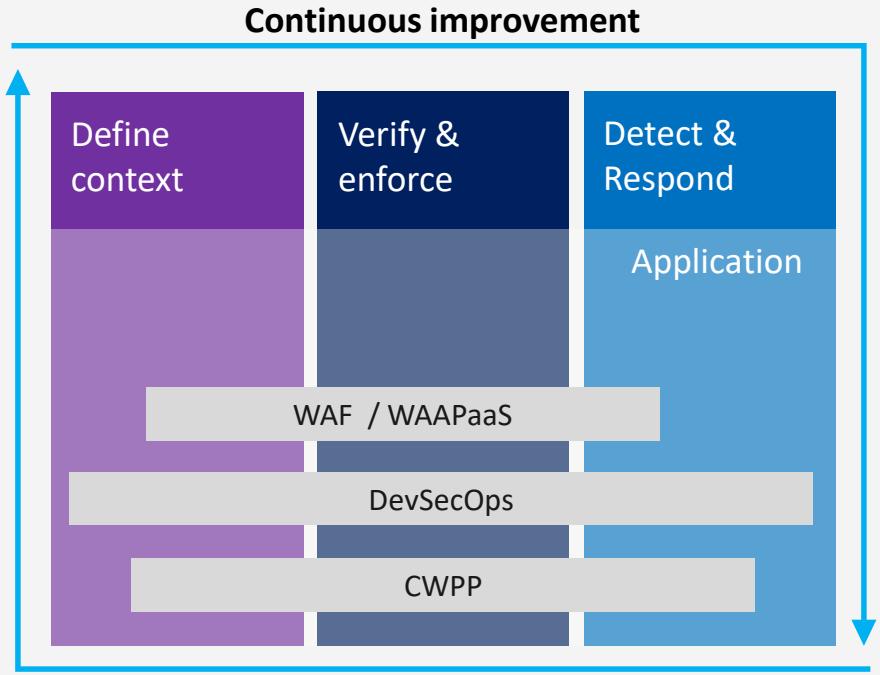
- Data Plane
  - Data Discovery (DD)
  - Data Classification & Labelling (DC)
  - Protection (Access Control & Encryption)
  - Data Loss Prevention (DLP)
  - Data Lifecycle Management
  - Confidential Computing
- Control Plane
  - Confidential Computing



IBM Security / © 2022 IBM Corporation

Intra-Cloud – Application – Zero Trust Focus

- Data Plane related
  - Application based Segmentation (see network)
  - Cloud Native Application Protection
  - Public API Protection
  - Web Application Firewall
- Control Plane related
  - DevSecOps*
    - Source Code scanning (Quality Gate)
    - Web Application scanning (Quality Gate + operations)
    - Vulnerability Management (Quality Gate + operations)
    - DevOps permissions (people & tools)
  - Workload Protection (container, see further)



*DevSecOps : should be intercloud as well, it depends, if the client adheres to IBM Hybrid Cloud strategy it could be more easily set-up as inter-cloud approach. If multi-cloud has been set-up ad-hoc , typically DevSecOps might have to be set up per Cloud provider type

IBM Security / © 2022 IBM Corporation

Agenda

- Layered approach to Zero Trust in Hybrid Cloud and Multi Cloud
- First Layer – Inter-Cloud
- Second Layer – Intra-Cloud
- **Third Layer – Inter-Workloads**
- Q&A

Inter-Workload

- Both Container based solutions and services mesh based solutions are environment on their own with their own capabilities and constraints
- New and existing (security) solutions are in continuous evolution
- These environments have their own Control & Data Plane and for both Zero Trust approaches are needed
- All domains from the Zero Trust Governance model have to be addressed in this environment
- A lot of good solutions both COTS and Open Source

IBM Security / © 2022 IBM Corporation

Inter-Workload – Network – Zero Trust Focus

Microsegmentation – in container environment, two examples

Tetrate Service Bridge

https://www.tetrate.io/tetrate-service-bridge/

Calico Cloud & Calico Enterprise

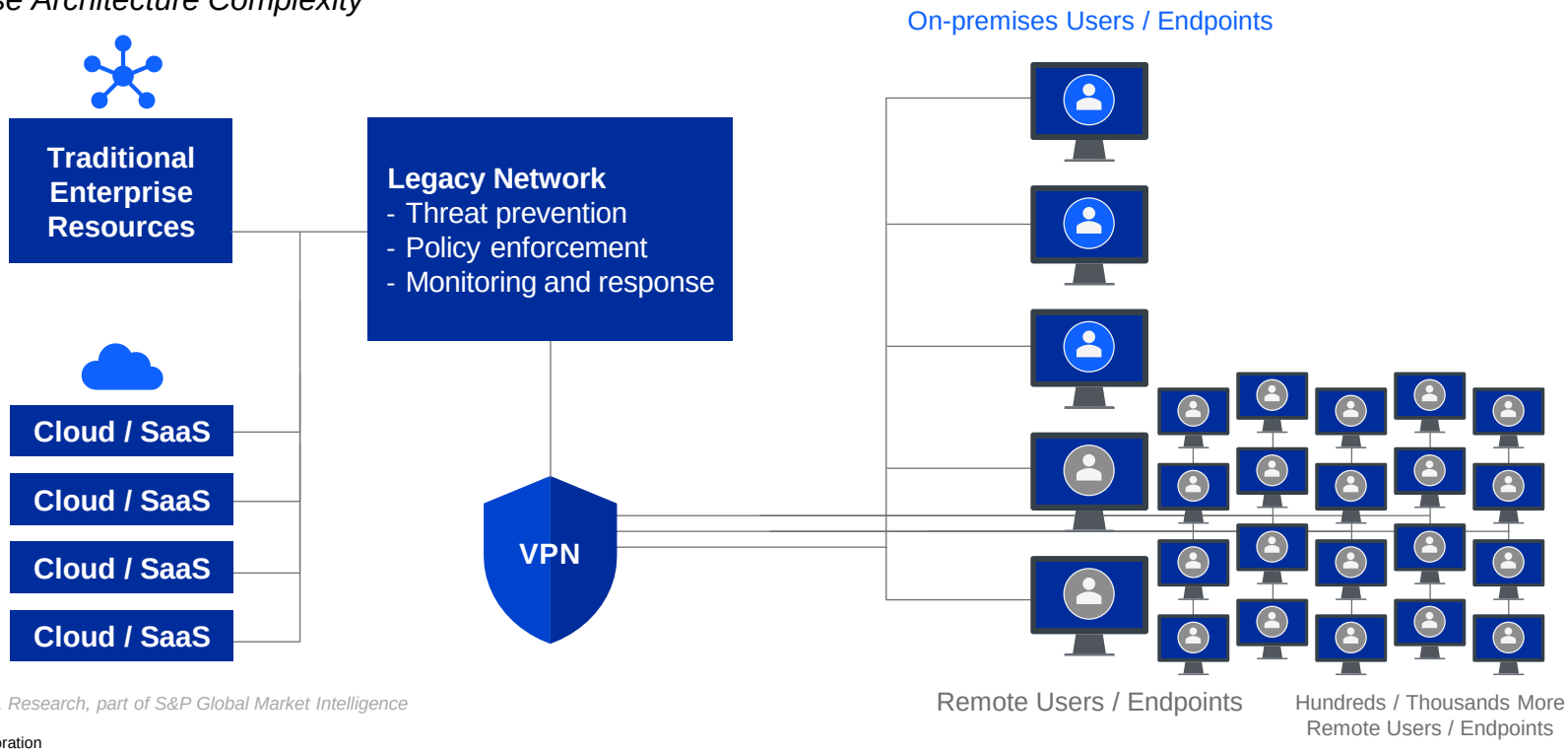
https://www.tigera.io/tigera-products/cloud-microsegmentation/

IBM Security Services Internal Use Only / © IBM Corporation 2021

Example: Endpoint Detection – Inter-Cloud/Inter-Workload Layer

A global pandemic, coupled with the rise of ransomware and move to Zero Trust, forced enterprises to rethink security

Current Enterprise Architecture Complexity



Source: Scott Crawford, 451 Research, part of S&P Global Market Intelligence

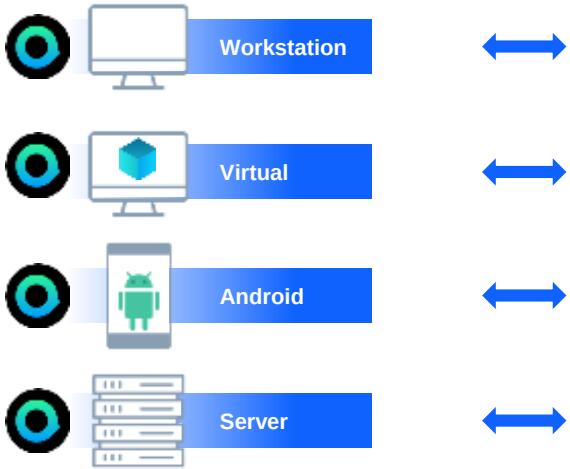
IBM Security / © 2022 IBM Corporation

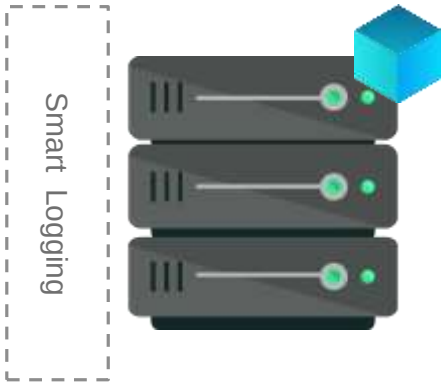
Inter Workload Protection – Endpoint – Example IBM ReaQta

Endpoint AI & NanoOS
Real-Time Coverage

Infrastructural AI
Data Collection & Behavioral Analysis

Single Console
Optimized Remediation Workflow



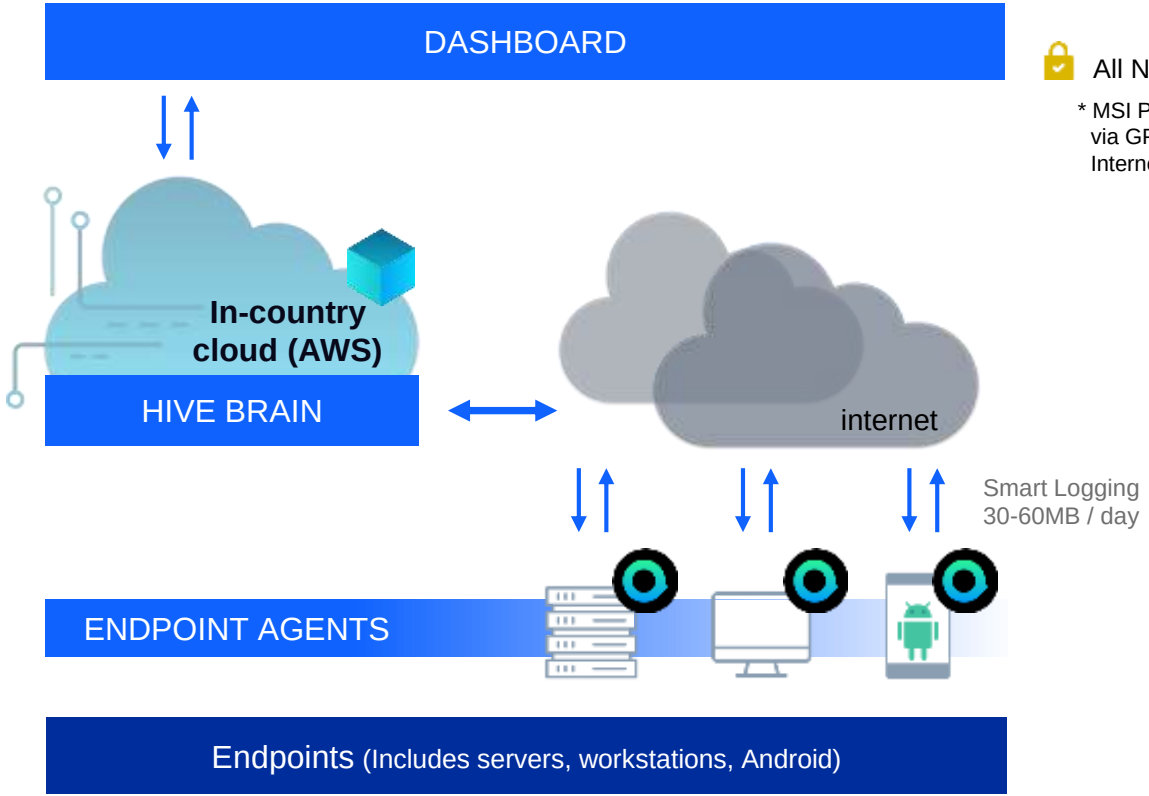


ENDPOINT AGENT

HIVE BRAIN

DASHBOARD

Cloud deployment



ReaQta in review

NANO OS
Live-Hypervisor based monitoring

Undetectable by Design

ADVANCED THREAT HUNTING
DeStra (Detection Strategy) scripting

Customized Threat Hunting

CYBER ASSISTANT
One-shot learning system

Can Help Reduce
False Positives by 80%+

Q&A

IBM Security / © 2022 IBM Corporation

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube.com/ibmsecurity

© Copyright IBM Corporation 2021. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty, of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

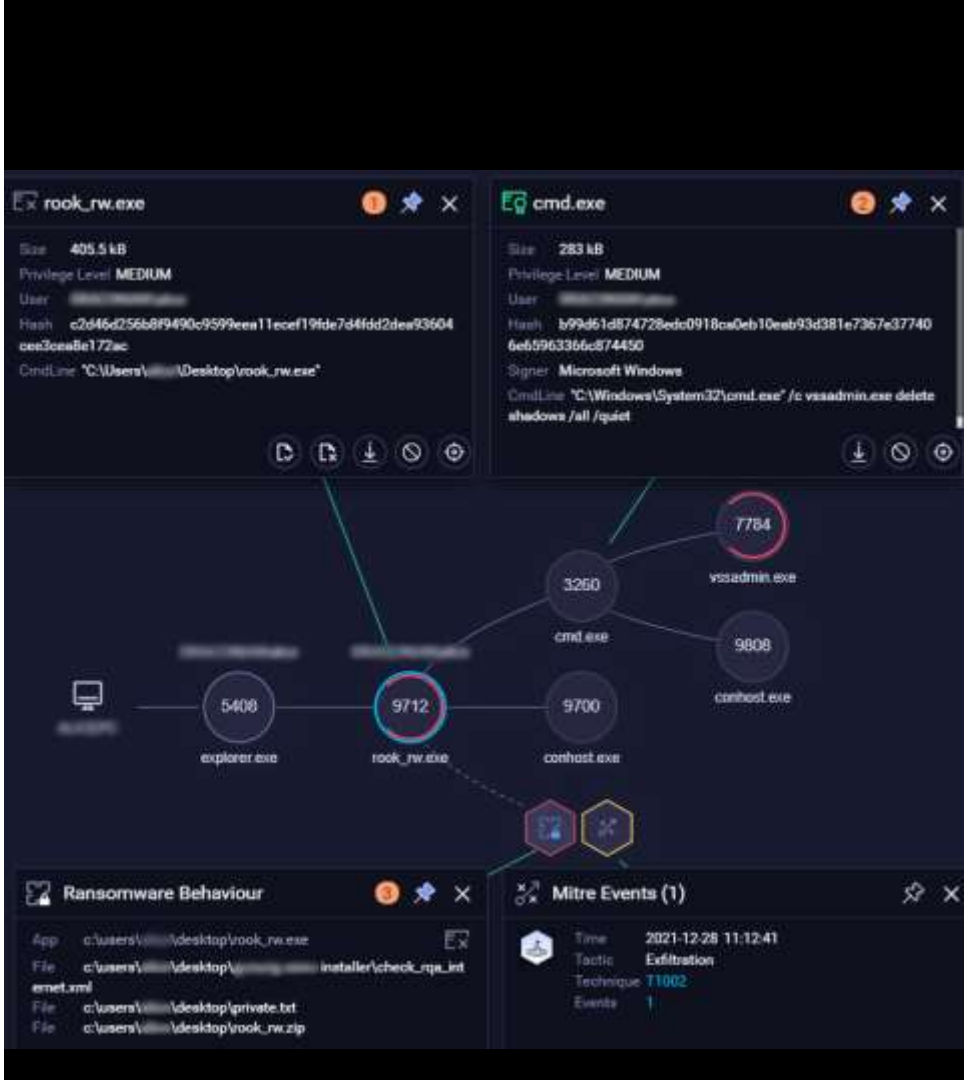
Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or 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.

ReaQta in action: Early detection of ransomware

By leveraging AI and automation directly on the endpoint, ReaQta helped detect Rook Ransomware (RaaS) and actively mitigate in near real-time

Key capabilities

- Detects unknown ransomware variants using a behavioral engine
- Analyzes file activities and access, if an encryption attempt is detected and the process chain is suspicious, the process is blocked, and the encrypted files are restored in real-time



IBM Security / © 2022 IBM Corporation

ReaQta in review

NANO OS
Live-Hypervisor based monitoring

Undetectable by Design

ADVANCED THREAT HUNTING
DeStra (Detection Strategy) scripting

Customized Threat Hunting

CYBER ASSISTANT
One-shot learning system

Can Help Reduce
False Positives by 80%+

Backup

Resources

IBM Internal

ZT landing page https://ibm.seismic.com/Link/Content/DCrUUI-8P1gUCvd1UWDJqlmA
L100 ZT training https://lr-sellers.yourlearning.ibm.com/#/Security/course/6880/details
ZTAS https://w3.ibm.com/w3publisher/cis-knowledge-hub/zero-trust-acceleration-services

IBM Public

https://www.ibm.com/security/zero-trust
https://www.ibm.com/security/services/zero-trust-acceleration
https://securityintelligence.com/?s=Zero+Trust

Extra Information on Zero Trust

IBM Cloud Blueprint talk on Zero Trust
https://w3.ibm.com/w3publisher/blueprint-talks/cloud/cloud-security-compliance-capabilities

Microsoft Zero Trust Reference Architecture
https://docs.microsoft.com/en-us/security/cybersecurity-reference-architecture/mcra

Gartner Report “How to Protect Your Clouds With CSPM, CWPP, CNAPP and CASB” (link via https://w3.ibm.com/marketing/bluemine/)
https://ibm.northernlight.com/document.php?docid=IA20210510200000060&datasource=IBM&caller=resultslist

IBM Security Services Internal Use Only / © IBM Corporation 2021

Resources (continued)

Additional Lecture on Zero Trust or topics addressed in this presentation
Zero Trust & CIEM https://cloudknox.io/zero-trust-model-in-the-cloud/
Data in Cloud & ZT https://cyral.com/blog/getting-started-with-zero-trust-for-the-data-cloud/
Secure data with Zero Trust https://docs.microsoft.com/en-us/security/zero-trust/data
Application & Zero Trust https://www.f5.com/services/resources/use-cases/zero-trust-in-an-application-centric-world
API Security and Zero Trust https://salt.security/blog/mythbusters-api-edition-zero-trust-and-its-limitations-for-api-security
Zero Trust Network https://www.kuppingercole.com/insights/zero-trust#Chapter3
DevSecOps https://www.beyondtrust.com/blog/entry/devops-security-best-practices
IAM and Zero Trust https://thycotic.com/company/blog/2019/09/26/zero-trust/
DevSecOps Metrics https://tech.gsa.gov/guides/dev_sec_ops_guide/
Zero Trust at AWS https://aws.amazon.com/security/zero-trust/
Azure Control Plane Security https://docs.microsoft.com/en-us/azure/architecture/framework/security/design-identity-control-plane
Google Cloud IAM overview https://cloud.google.com/iam
AWS Data Plane IAM https://aws.amazon.com/identity/
AWS Security Strategy https://www.sans.org/reading-room/whitepapers/analyst/build-security-posture-strategy-control-plane-assets-aws-cloud-40260
Zero Trust Strategy https://searchsecurity.techtarget.com/tip/Planning-a-zero-trust-strategy-in-6-steps
Emerging Technologies: Top Trends in Security for 2021 https://www.gartner.com/document/4001838
Confidential Computing https://www.ibm.com/cloud/confidential-computing
Zero Trust Workbook for Sentinel https://techcommunity.microsoft.com/t5/public-sector-blog/announcing-the-azure-sentinel-zero-trust-tic3-0-workbook/ba-p/2313761
Hashicorp Zero Trust solutions https://www.hashicorp.com/solutions/zero-trust-security
Zero Trust in k8s https://itnext.io/two-quick-ways-to-apply-zero-trust-to-kubernetes-79764dd420bf
Tetrate Service Bridge https://www.tetrate.io/tetrate-service-bridge/
Calico https://www.tigera.io/tigera-products/cloud-microsegmentation/
Zero Trust network in k8s https://www.stackrox.com/wiki/zero-trust-networks-in-kubernetes-cloud-native-applications/

IBM Security Services Internal Use Only / © IBM Corporation 2021

Endpoint security: more timely, more challenges

- Traditional approaches rely on finding what's known (known signatures), but attackers target unknown (fileless/ransomware)
- Poor visibility and zero-day attacks
- Attackers are "living off the land" (manipulating legitimate software and files to disguise their presence)
- A rise in—and complexity of—malicious and automated cyber activity, most of which originates at the endpoint
- Inexperienced, new and fatigued analysts who struggle with complex tooling, alert overload and time-consuming investigations

"Endpoint security continues to be one of the most requested core topic coverage areas... because the endpoint is often a target of attack, attacks becoming more sophisticated, and endpoints getting more and more diversified."

Gartner, Guide to Endpoint Security Concepts, Dec. 2020

IBM acquired ReaQta, a leading European AI-based endpoint security provider

ReaQta's endpoint security solutions leverage AI to help automatically identify and manage threats

Endpoint Detection & Response

ReaQta unifies detection, response, and automated hunting

NANO OS
Live-hypervisor based monitoring

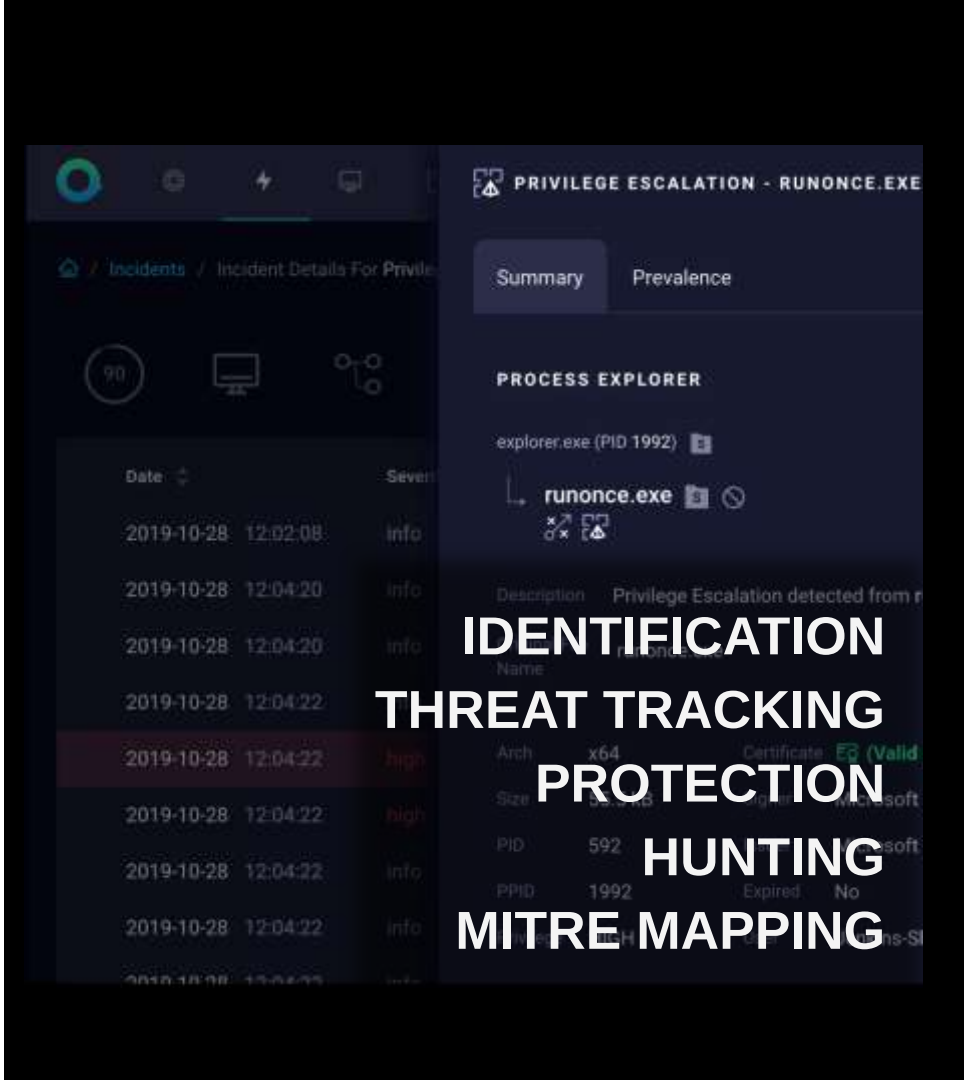
AI-Driven Threat Hunting
Data-mining to find advanced threats

Managed Detection and Response (MDR) Services

24x7x365 Essential MDR service

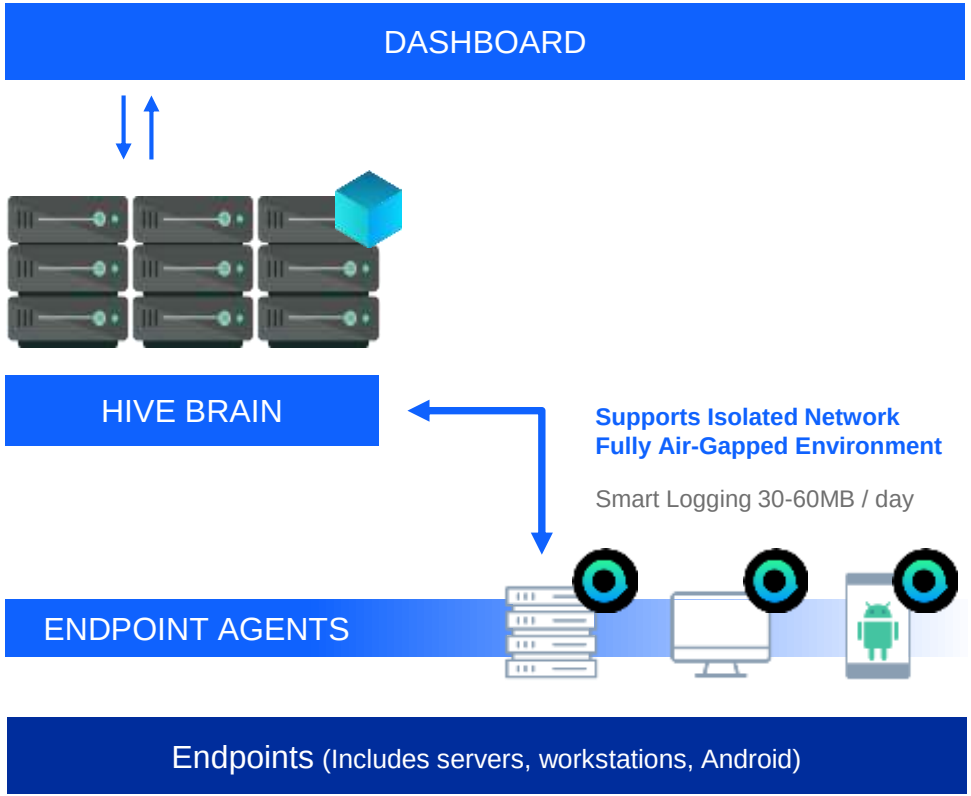
Single Agent, Multiple Deployment Options

Runs on desktop, server, cloud and mobile operating systems, deploys as SaaS, on-premises or in air-gapped environments



IBM Security / © 2022 IBM Corporation

On-prem deployment



All Network Traffic

* MSI Package Deployment via GPO (15Mb) with no Internet required

How organizations can modernize endpoint detection & response

Behavioral Analytics

Must move beyond signature-based detections

AI & Automation

Autonomous response capabilities

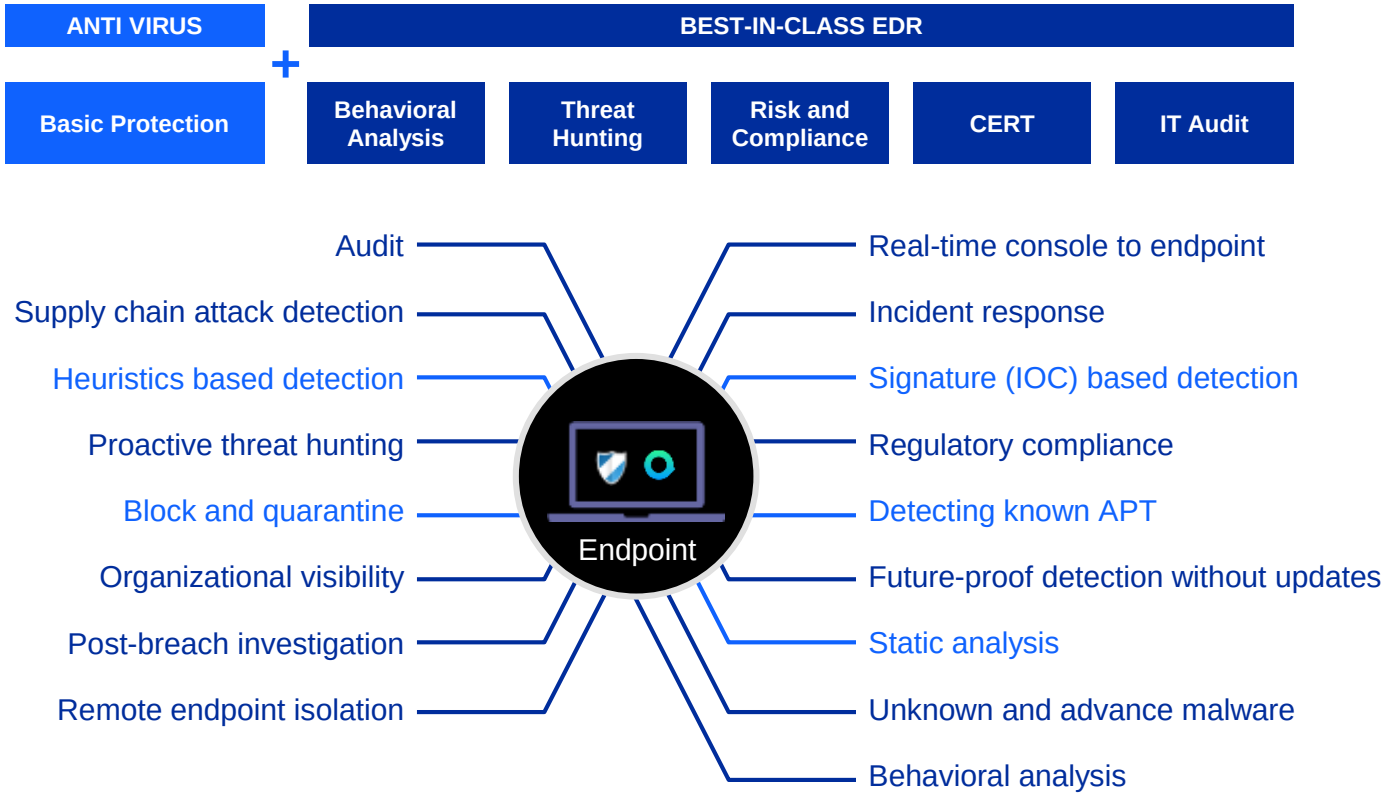
Easy UI

Easy to use visual workflow, and integrated analytics and response workflow

Multiple deployment options

Works in connected and air-gapped environments

Why Endpoint Detection & Response?



What makes ReaQta a different endpoint protection solution?

Undetectable by Design

NANO OS
Live-Hypervisor based monitoring

- Monitors the Operating System (OS) from the outside (Ring-1)
- Offers broad visibility and insight over application's life
- Designed to be invisible to malware
- Proprietary detection of high-level malicious behaviors:
  - Keylogging, Dynamic Impersonation, Credential Harvesting, Kernel Exploits, Screen captures

Customized Threat Hunting

ADVANCED THREAT HUNTING
DeStra (Detection Strategy) scripting

- Easily create customed detection & response used cases
- Beyond "out of the box" models—to address compliance or company-specific requirements
- Deploy across the organization within minutes, without intervention or downtime
- MITRE ATT&CK mapping

Can Help Reduce False Positives by 80%+

CYBER ASSISTANT
One-shot learning system

- Automatically learns from analyst past decisions and takes actions
- Can help free up time for analysts to focus on higher level tasks
- Available for single customers or for multi-tenant MSSPs
- Guided and autonomous remediation simplifies and speeds response

2022 MITRE Engenuity ATT&CK® Evaluations

100% detection coverage across the cyber kill chain

No configuration changes during the entire evaluation

100% of detections done in real-time without delays

All ransomware actions detected

Stops the latest advanced threats out of the box

UI allows analysts to keep up with the speed of real-time detection

Log data only increases when it matters

Is MDR right for you?

Common pain points

- Too many tools and alerts to adequately reduce mean time to resolution (MTTR) and improve productivity
- Cybersecurity skills gaps are increasing with lack of experienced security professionals to handle sophisticated and advanced threats
- Meeting compliance and regulatory requirements – regulations aren’t just for the financial services and healthcare industries
- Lack of visibility into your environment

How organizations can modernize endpoint detection & response

24/7/365 monitoring

Today's cyber threats require a complete understanding of your environment in order to detect the most minute anomalies. We provide 24/7 monitoring, tracking and resolve critical alerts while keeping you always up to date.

Zero downtime

We contain and remediate threats as soon as they're detected – minimizing your business risk and reducing damages and interruption of services.

AI-powered cyber defense

With both artificial intelligence and our team's deep experience in intelligence and analysis, we help you to identify and track even the most sophisticated actors and run advanced threat hunting campaigns.

Deep threat portfolio

We can extend your protection and recovery through our extensive catalogue (Advisory, Systems Integration, Managed Security Services).