Secure your endpoints with AI-powered, automated security from IBM Security ReaQta

Bri Belicic

Worldwide GTM Program Manager
AWS Marketplace, IBM Security

Senthil Nagaraj

AWS Solutions Architect

Chase Singleton

IBM EDR Specialist

Mitch Lukaart

IBM EDR Specialist & Security Engineer

IBM Security

Agenda

- AWS and IBM: *Better Together*
- AWS Perspective on EDR
- Customer Challenges with Endpoint Security
- EDR with AWS Integrations
- ReaQta Demo
- IBM Security on AWS Marketplace

IBM Software and Services on AWS

IBM is strategically partnering with AWS

aws PARTNER Premier Tier Services

- L1 MSSP Services Competency
- Security Services Competency
- Security Software Competency

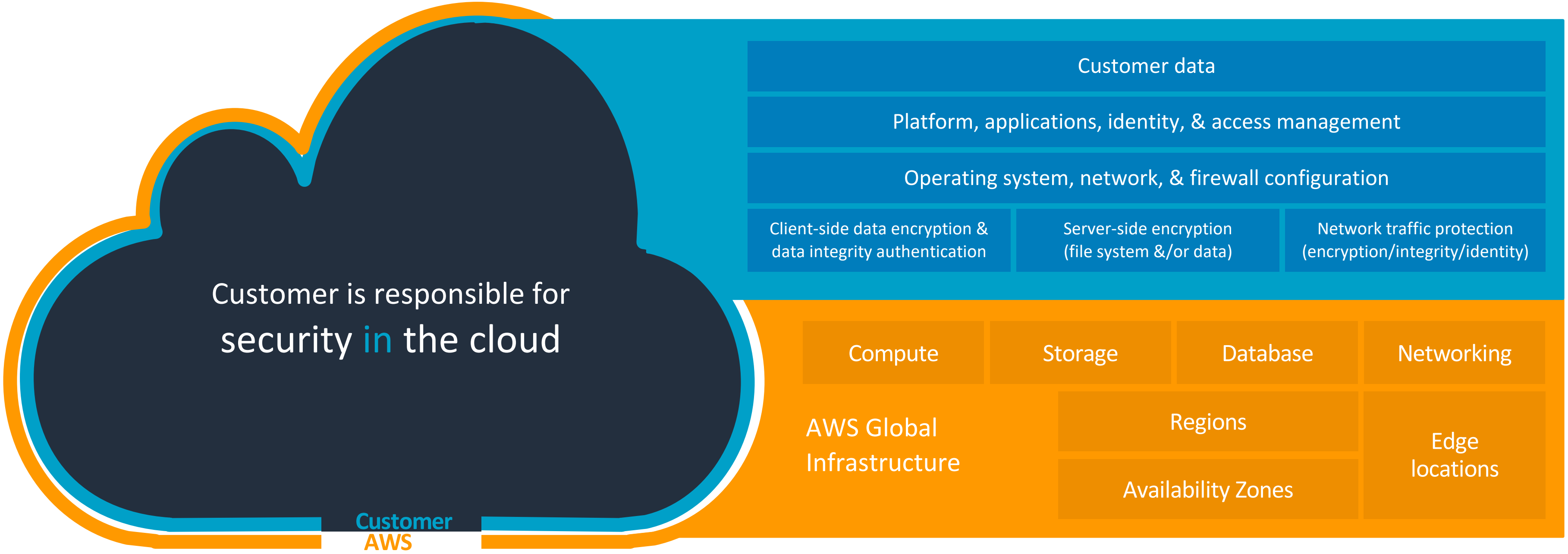
Strategic Collaboration agreement for IBM SaaS on AWS *signed*

- ✓ IBM Security
- ✓ IBM Data & AI
- ✓ IBM Automation
- ✓ IBM Sustainability
- ✓ IBM Storage

IBM Security

- Largest enterprise cybersecurity provider
- Leader in 15 security market segments
- 5,500+ security experts in 130 countries
- 20+ security acquisitions
- 70B+ security events monitored per day
- 9 global security centers
- 3 Security Competencies with AWS
- 21 IBM Security Software listings on the AWS Marketplace
- 11 IBM Security Services listings on the AWS Marketplace

Shared security responsibilities on AWS



Customer is responsible for
security in the cloud

Customer data

Platform, applications, identity, & access management

Operating system, network, & firewall configuration

Client-side data encryption & data integrity authentication

Server-side encryption (file system &/or data)

Network traffic protection (encryption/integrity/identity)

Customer

AWS

Compute

Storage

Database

Networking

AWS Global Infrastructure

Regions

Availability Zones

Edge locations

AWS is responsible for
security of the cloud

Endpoint security perspective

Detect

Correlate

Integrate

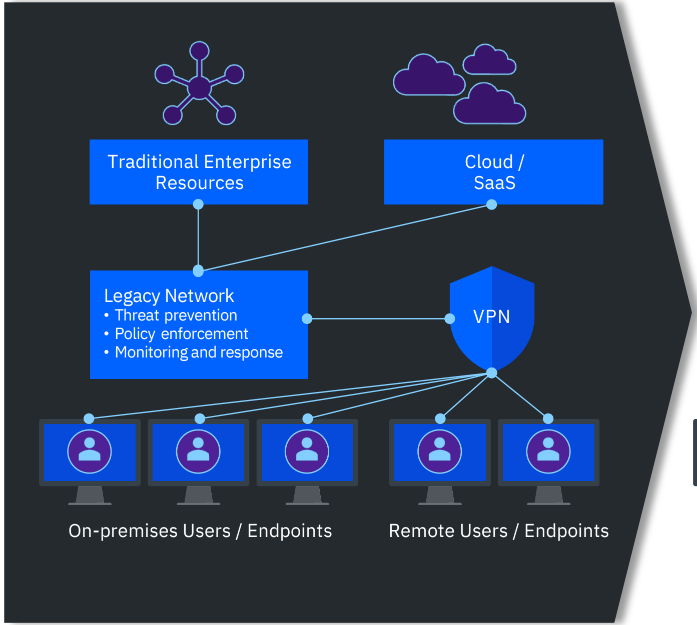
Observe

Investigate

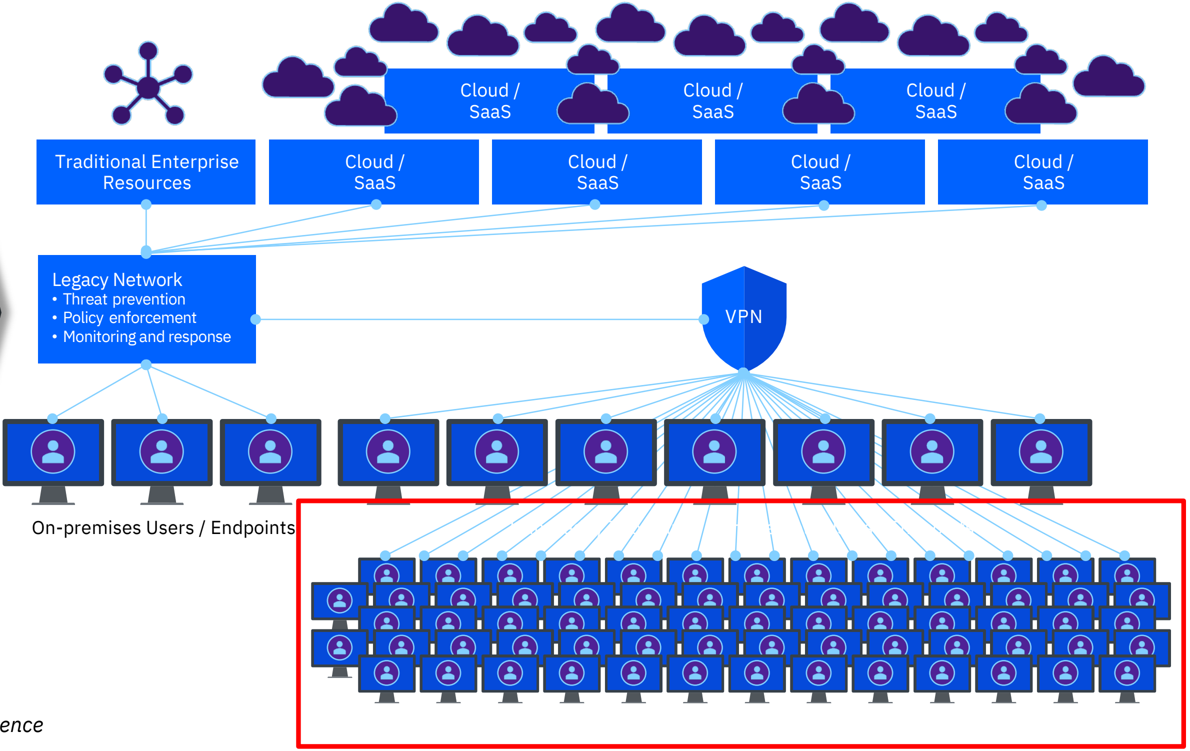
Remediate

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

Previous Enterprise Architectures



Current Enterprise Architecture Complexity



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

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

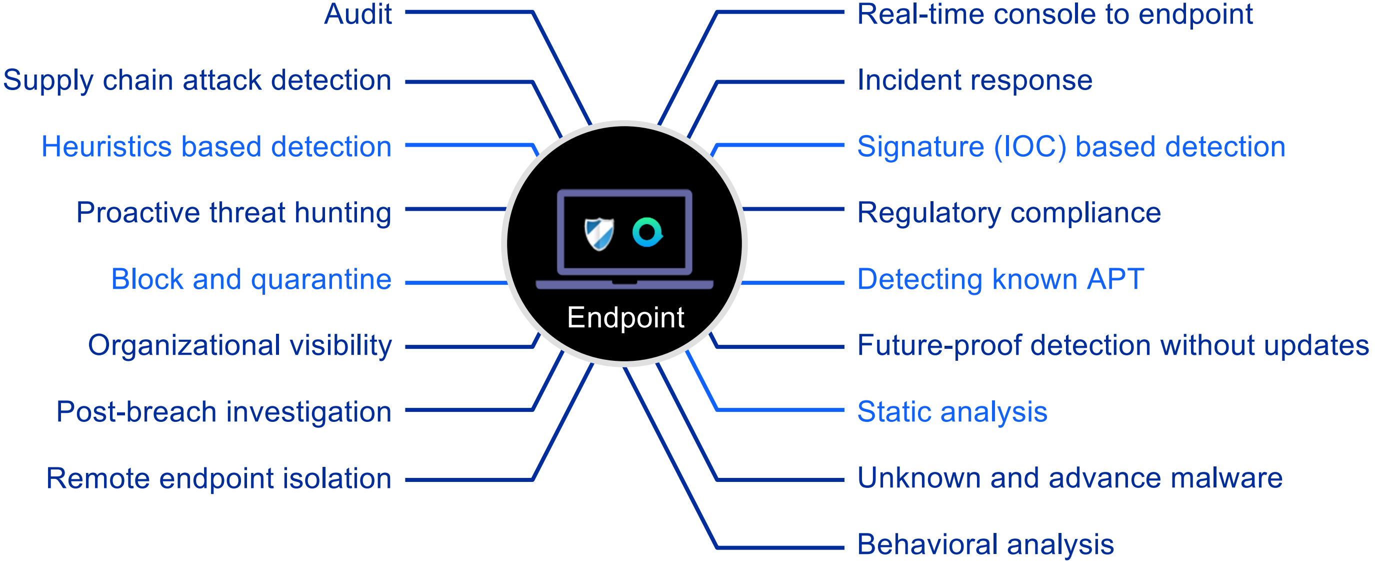
Multiple deployment options

Works in connected and air-gapped environments

Why Endpoint Detection & Response?

ANTI VIRUS + **BEST-IN-CLASS EDR**

- **Basic Protection**
- **Behavioral Analysis**
- **Threat Hunting**
- **Risk and Compliance**
- **CERT**
- **IT Audit**



Audit

Supply chain attack detection

Heuristics based detection

Proactive threat hunting

Block and quarantine

Organizational visibility

Post-breach investigation

Remote endpoint isolation

Real-time console to endpoint

Incident response

Signature (IOC) based detection

Regulatory compliance

Detecting known APT

Future-proof detection without updates

Static analysis

Unknown and advance malware

Behavioral analysis

What makes ReaQta a different endpoint protection solution?

Undetectable by Design

NANO OS
Live-Hypervisor based monitoring

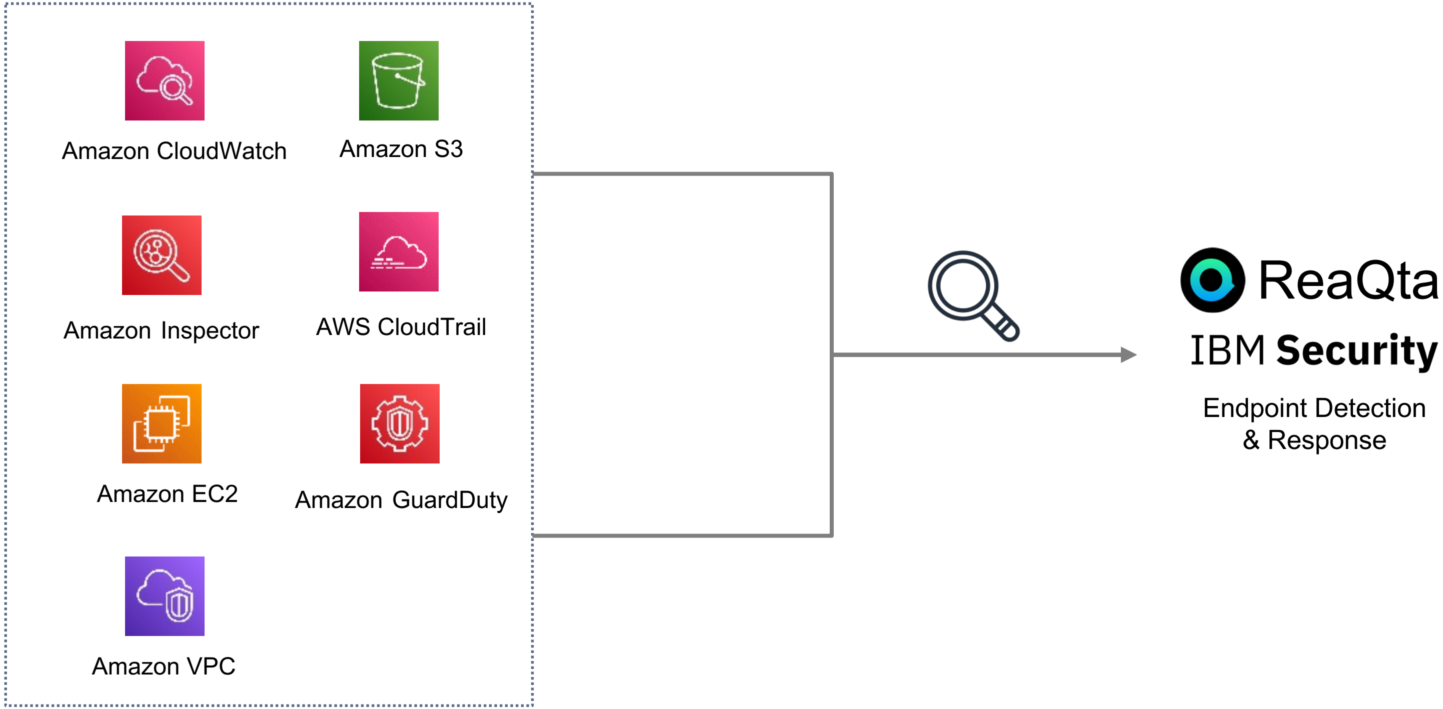
Customized Threat Hunting

ADVANCED THREAT HUNTING
DeStra (Detection Strategy) scripting

Can Help Reduce False Positives by 80%+

CYBER ASSISTANT
One-shot learning system

IBM Security ReaQta with AWS Integrations



Amazon CloudWatch

Amazon S3

Amazon Inspector

AWS CloudTrail

Amazon EC2

Amazon GuardDuty

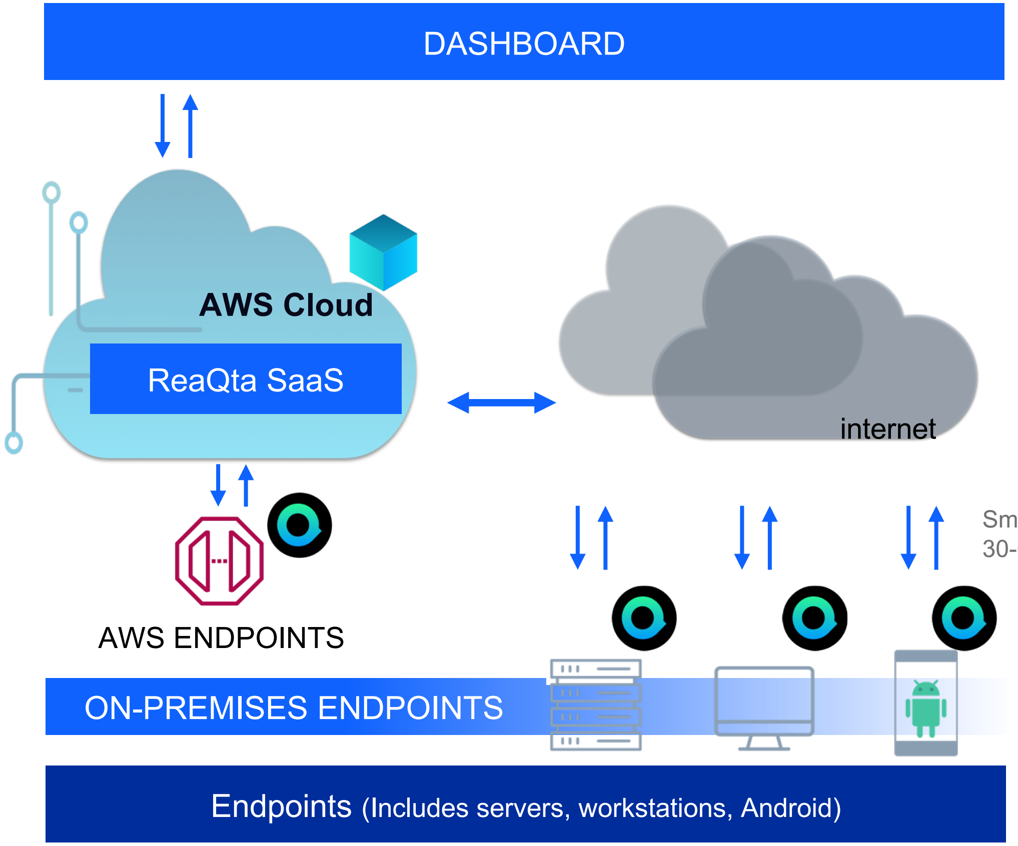
Amazon VPC

ReaQta

IBM **Security**

Endpoint Detection
& Response

AWS Cloud deployment

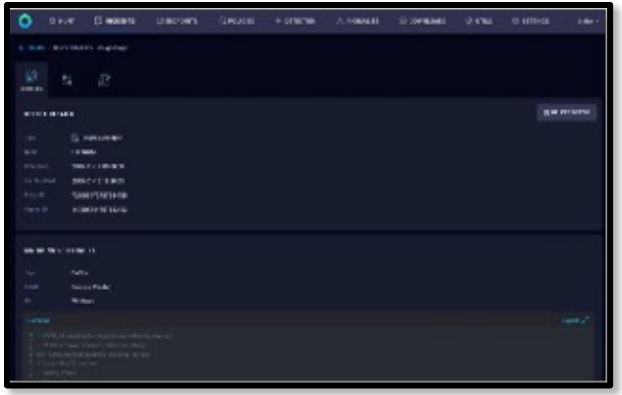


🔒 All Network Traffic

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

Smart Logging
30-60MB / day

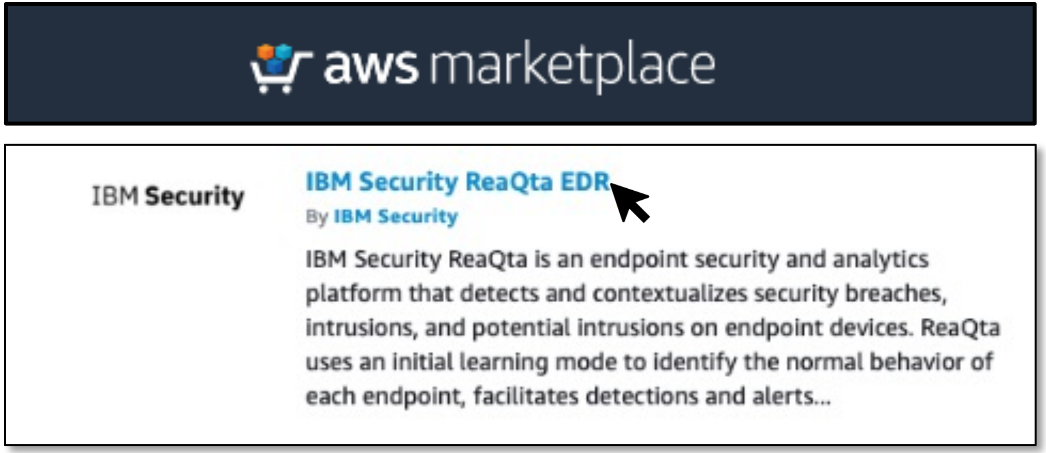
Demo



Available on AWS Marketplace

Benefits Purchasing on AWS Marketplace

- Marketplace purchases qualify against customer EDP
- Existing IBM clients can bring their IBM Software licenses to AWS Marketplace BYOL listings and purchase their AWS services
- Smoother deployment experience with clients - Access technical expertise through AWS Partner Solution Architects dedicated to IBM
- Marketplace offers clients one stop shopping and consolidated billing



IBM Security ReaQta EDR

By IBM Security

IBM Security ReaQta is an endpoint security and analytics platform that detects and contextualizes security breaches, intrusions, and potential intrusions on endpoint devices. ReaQta uses an initial learning mode to identify the normal behavior of each endpoint, facilitates detections and alerts...

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube.com/ibmsecurity

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.