AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

SEC327-S

SPONSORED BY SOPHOS

AWS cybersecurity as a system

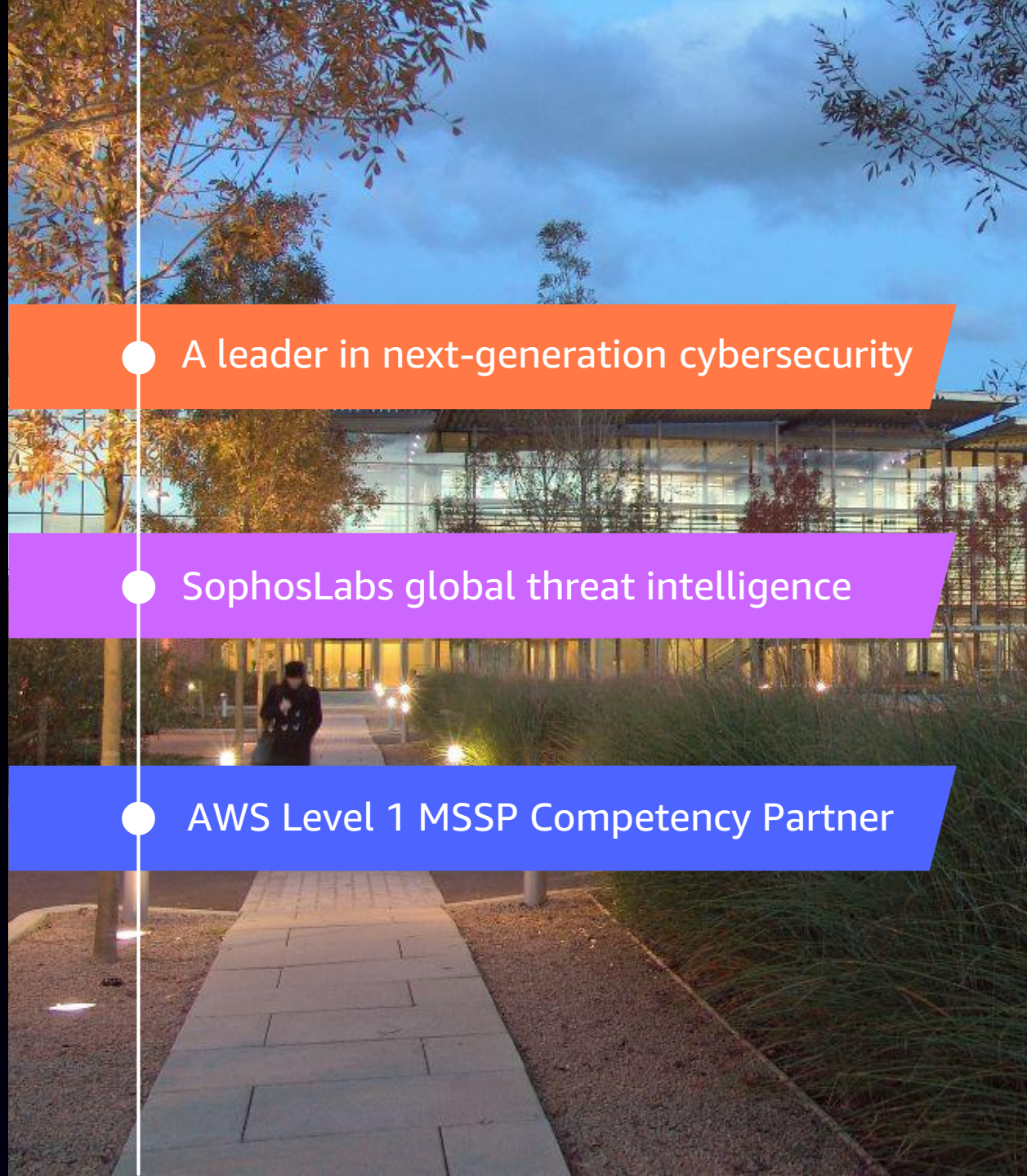
Marion Guerin
Alliance Lead for AWS
Sophos

Bill Prout
Director of Global Solutions Engineering
Sophos

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sophos

- Protecting over 100 million users from advanced cybersecurity vulnerabilities
- Adaptive cybersecurity system protecting workloads, data, apps, and access
- One of the world's largest and fastest-growing managed detection and response providers
- Global reach with products and 60,000 partners
- AWS Security Competency Partner
- AWS Level 1 Managed Security Service Provider Partner
- Available in AWS Marketplace

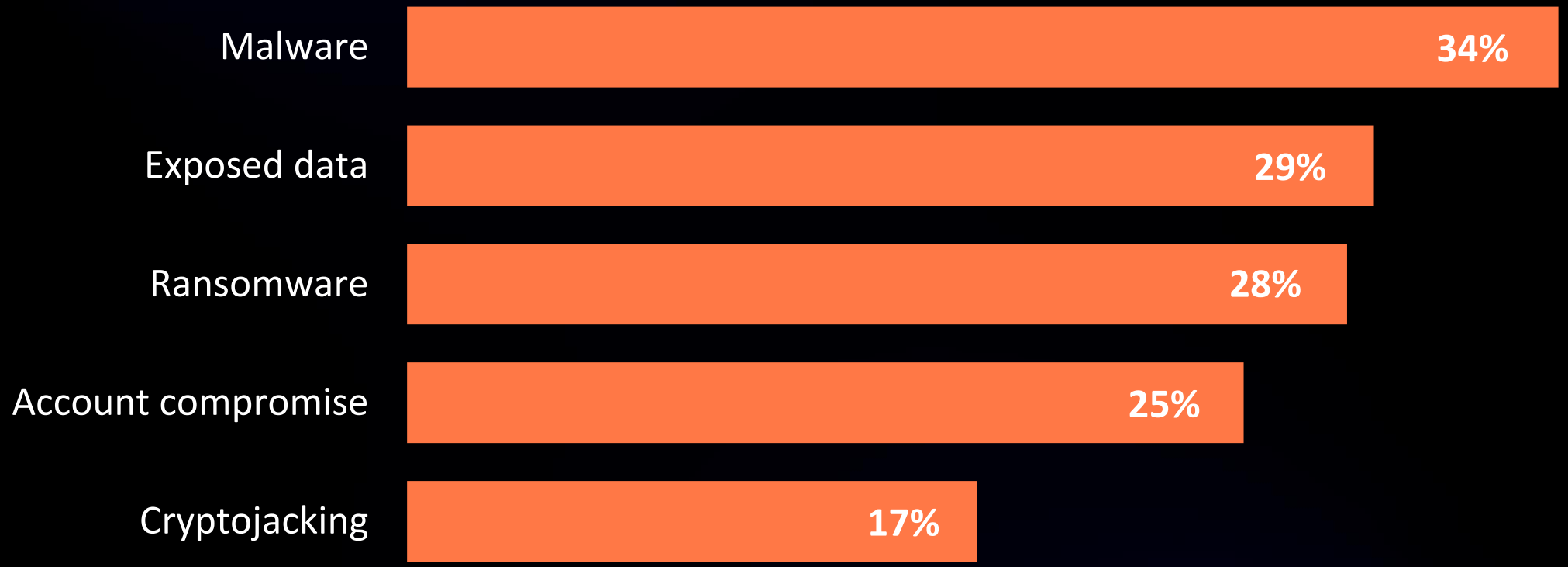


aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Securing organizations experiencing incidents

70% OF ORGANIZATIONS HAVE HAD A PUBLIC CLOUD SECURITY EVENT IN THE LAST 12 MONTHS



Sources: Sophos State of Cloud Security 2020

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Ransomware by the numbers

59%

of attacks where data is encrypted involve data on the public cloud

$170K

was the average ransom paid in 2020

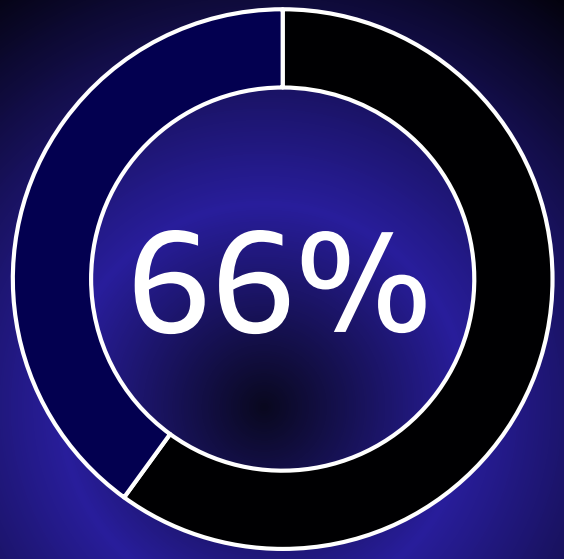
35%

of encrypted data was not recovered on average after the ransom was paid

Sources: Sophos, State of Ransomware, 2020 and 2021

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Shift your focus to protect your infrastructure



of security threats to public clouds are attributed to resource misconfigurations

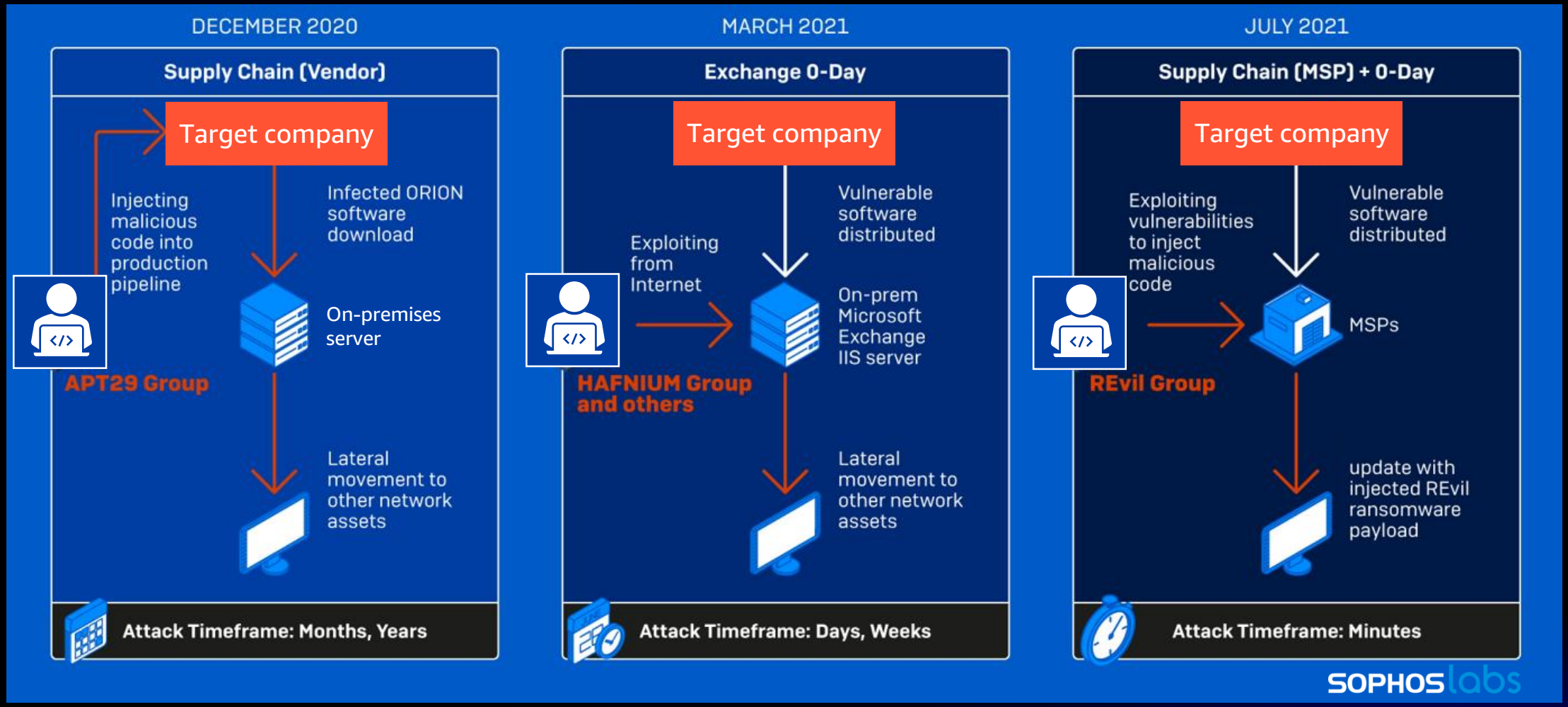


Source [66% of threats]: Sophos, State of Cloud Security, 2020
Source [Time to first authentication attempt]: Exposed: Cyberattacks on Cloud Honeypots, 2019

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Shift focus to proactive identification and response



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Introducing Celayix

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Celayix

VANCOUVER

- Thriving SaaS services business
- Established in 2000
- Powerful suite of AI-driven workforce management tools
- Leader in employee scheduling, time and attendance, and employee communication



aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Accelerated with AWS

- Use AWS managed services (database and containers)
- Expand market opportunities with SaaS
- Skill development and deployment automation



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Data security and uptime are paramount

CELAYIX RESPONSIBILITIES



CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION

SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)

NETWORKING TRAFFIC PROTECTION (ENCRYPTION INTEGRITY, IDENTITY)

https://aws.amazon.com/compliance/shared-responsibility-model

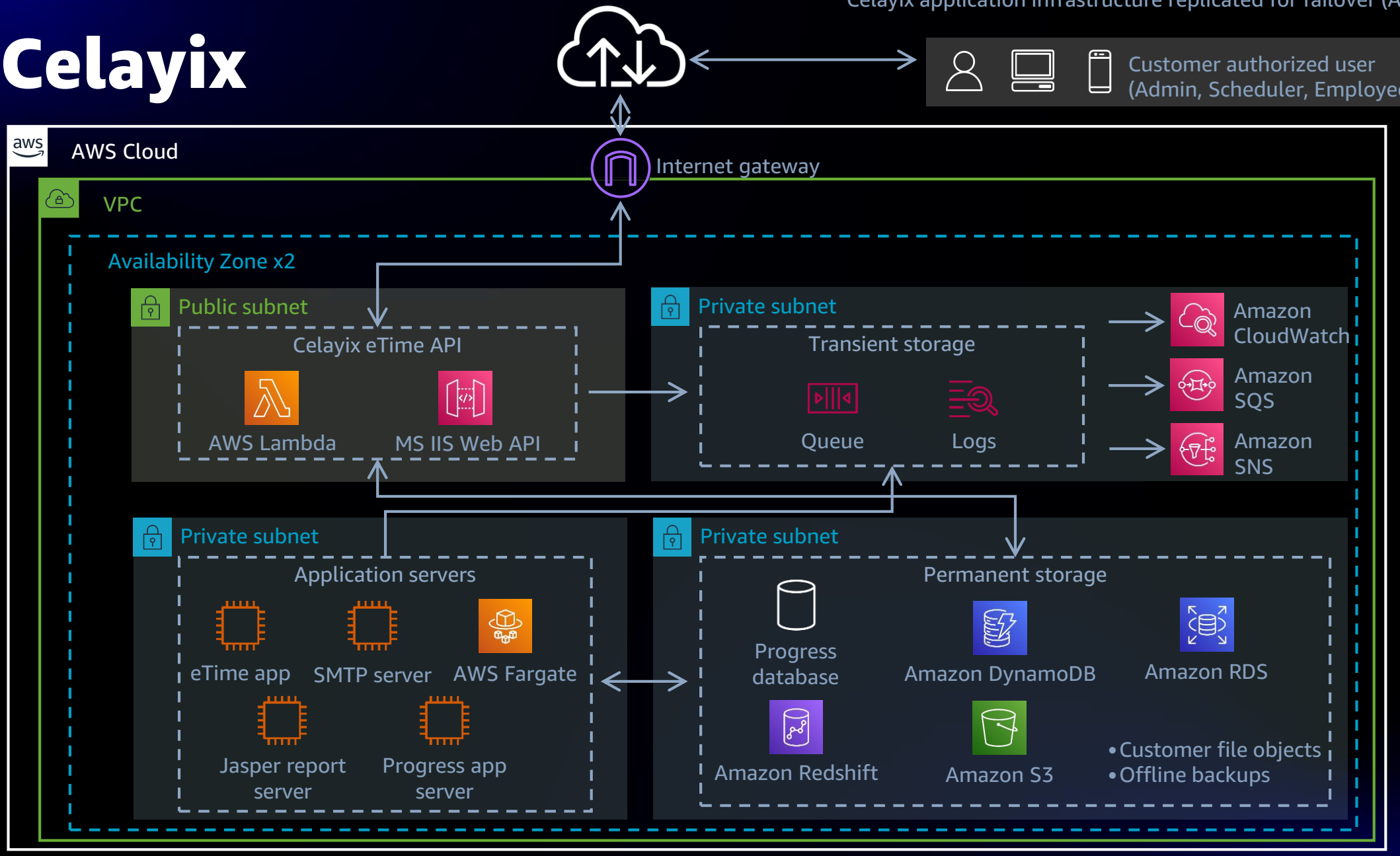
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Celayix architecture

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Celayix

Celayix application infrastructure replicated for failover (AWS CAN & VA Regions)



Amazon GuardDuty

AWS Identity and Access Management (IAM)

AWS Key Management Service (AWS KMS)

SOPHOS

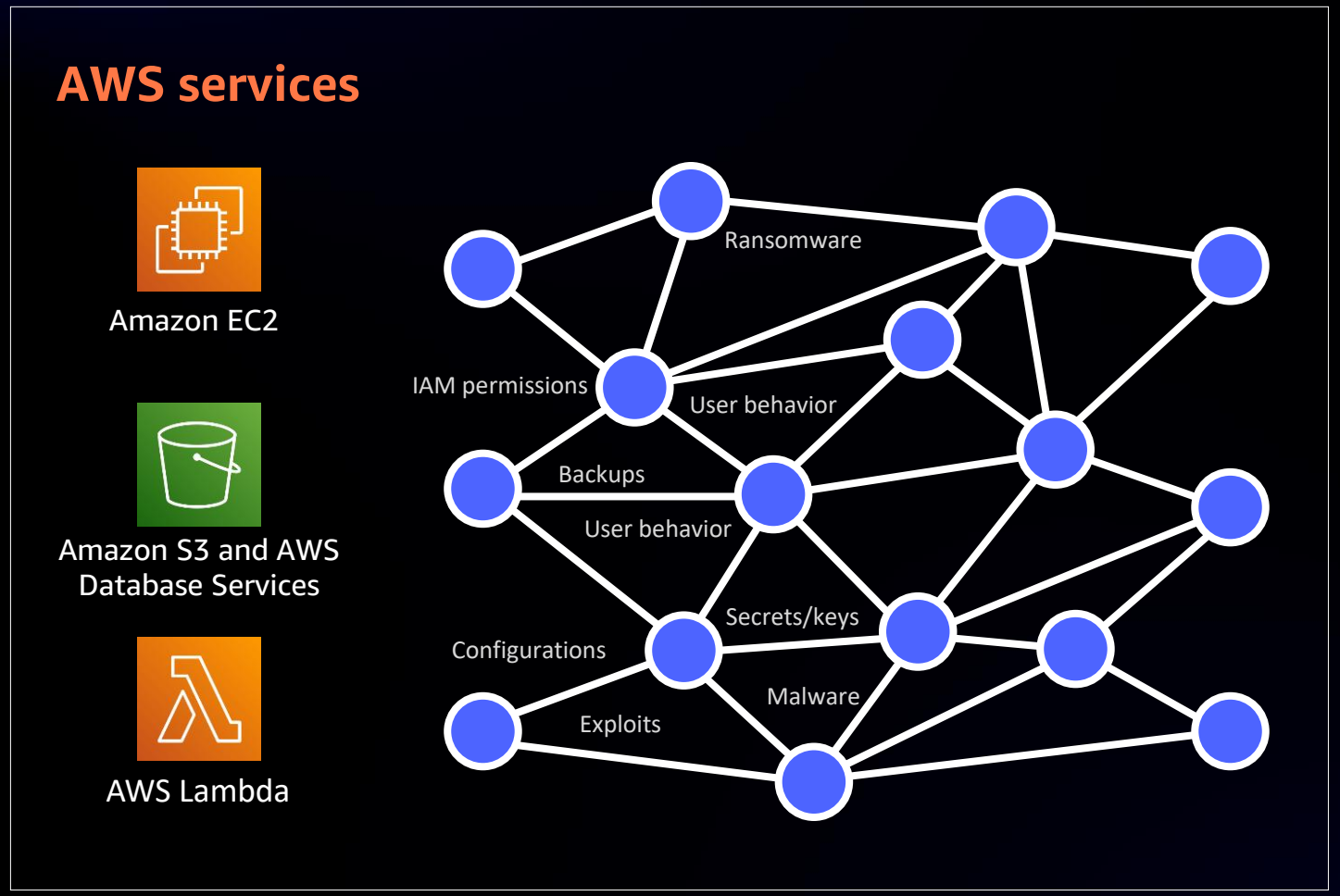
Sophos Cloud Optix (CSPM)

Sophos Intercept X for Server (CWPP)

Sophos Managed Threat Response

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scalable cloud services and protection



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

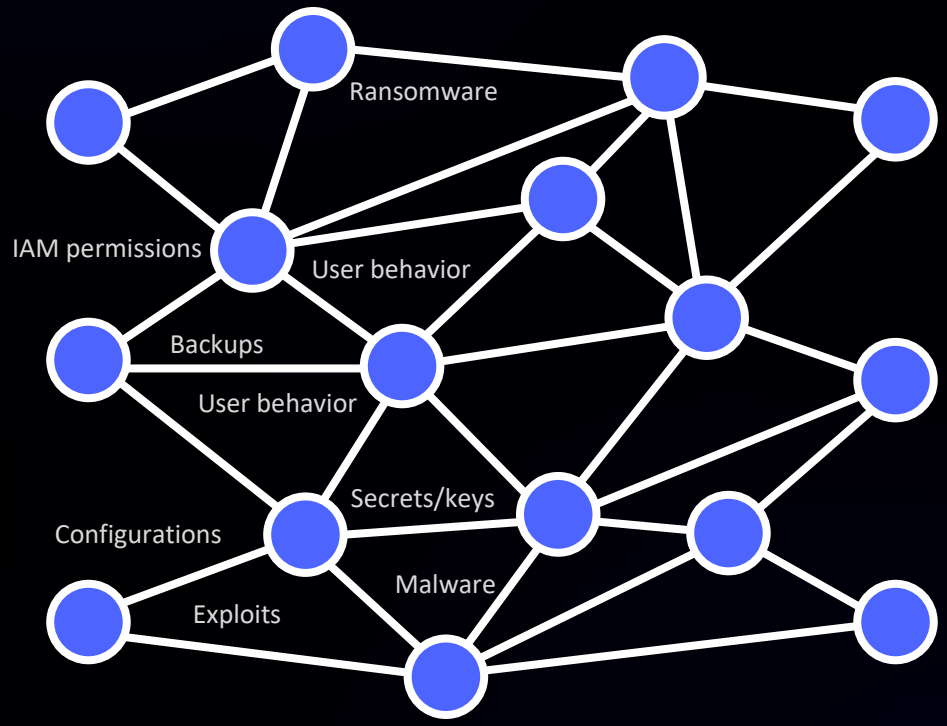
Scalable cloud services and protection

AWS services

Amazon EC2

Amazon S3 and AWS Database Services

AWS Lambda



Sophos solutions

Sophos Cloud Optix (CSPM)

Sophos Intercept X for Server (CWPP)

Sophos Managed Threat Response (MDR)

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The Celayix approach to cybersecurity

EMBRACE AND EXTEND AWS CLOUD TOOLS

Cloud security best practices

Design environments to meet best-practice standards with visibility and tools to maintain them

Latest cybersecurity intelligence

Gain the benefit of threat intelligence at scale with AI, keeping security tools lightweight while preventing potential concerns

24/7 threat monitoring and response

Increase team efficiency with monitoring via managed services and be able to respond to threats sooner



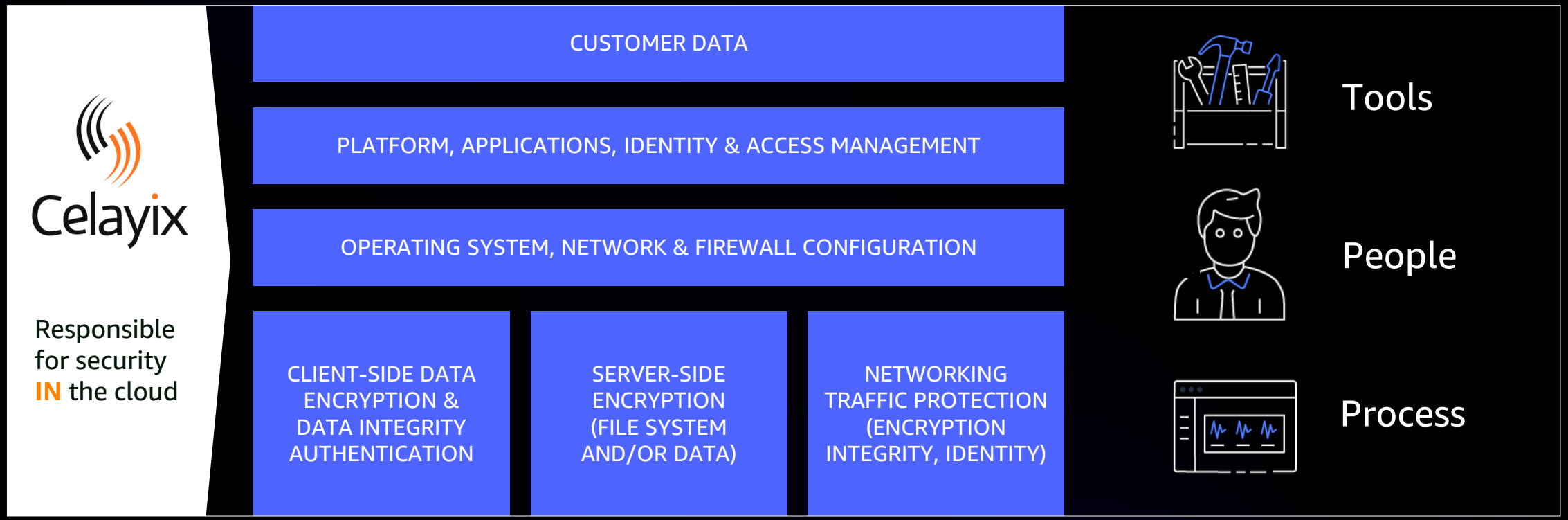
aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Realizing Celayix's cybersecurity goals

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Operationalizing security in the cloud



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sophos as an AWS Partner

aws partner network | competency
level 1 MSSP

aws marketplace

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Ten AWS Level 1 Managed Security Services

AWS.AMAZON.COM/MSSP

1. **AWS infrastructure vulnerability scanning**
   Routine scanning of AWS infrastructure resources for known software vulnerabilities
2. **AWS resource inventory visibility**
   Continuous scanning and reporting on all AWS resources and their configurations
3. **AWS security best-practices monitoring**
   Tracking and detecting possible misconfigurations of AWS resources
4. **AWS compliance monitoring**
   Monitoring compliance standards such as CIS AWS Foundations Benchmark, PCI DSS, HIPAA
5. **Monitor and triage security events**
   Triaging security events and providing recommended remediation guidance
6. **24/7 incident alerting and response**
   Offering expert guidance on recommended remediation steps 24/7
7. **Distributed Denial of Service (DDoS) mitigation**
   Reducing risk of availability and financial or security impacts to applications
8. **Managed intrusion prevention system (IPS)**
   Defending against known threat patterns to increase overall security posture
9. **Managed detection and response (MDR)** Experts working to continuously detect, investigate, and remove threats
10. **Managed web application firewall (AWS WAF)**
    Protecting web-facing applications and APIs against common exploits

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The way you want cloud security to work

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sophos threat protection

aws marketplace

24/7 THREAT PROTECTION, MONITORING, AND RESPONSE PACKAGE

One cybersecurity package

The Sophos package – Products and services

CO	Svr	Fw	Ep	MTR
Cloud Optix Cloud Security Posture Mgmt.	Intercept X for Server CWPP XDR	Firewall Network and App Security	Intercept X for Endpoint Endpoint XDR	MTR Managed Threat Response Service

100% control

- Deployment and configuration by Sophos MSP partner or your in-house team
- Always backed by Sophos Managed Threat Response service experts

Unlock value in cloud services

Required AWS services

- AWS CloudTrail
- Amazon GuardDuty
- AWS Security Hub

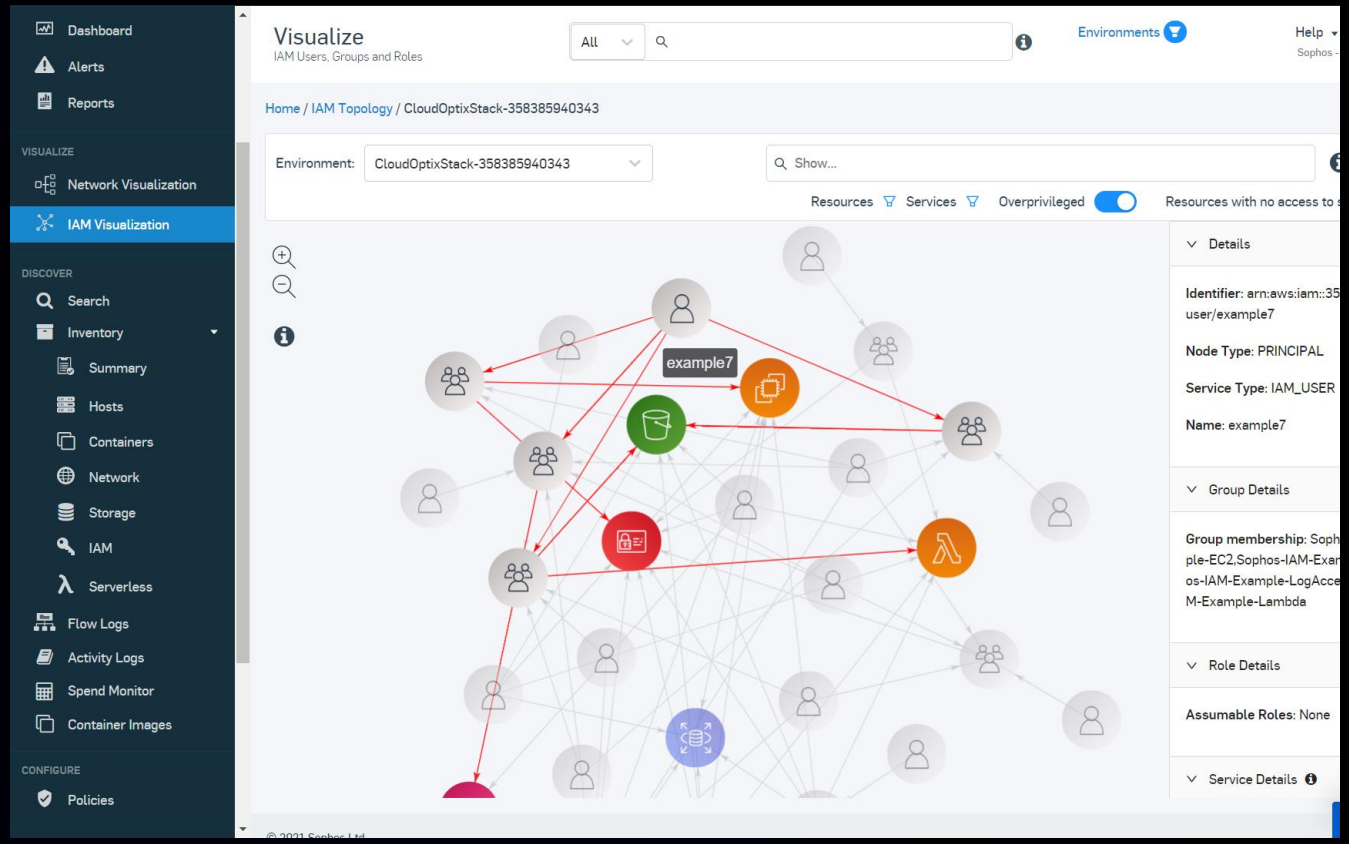
Web: sophos.com/aws-mssp
AWS Marketplace: https://soph.so/aws-mssp

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Proactively prevent vulnerabilities

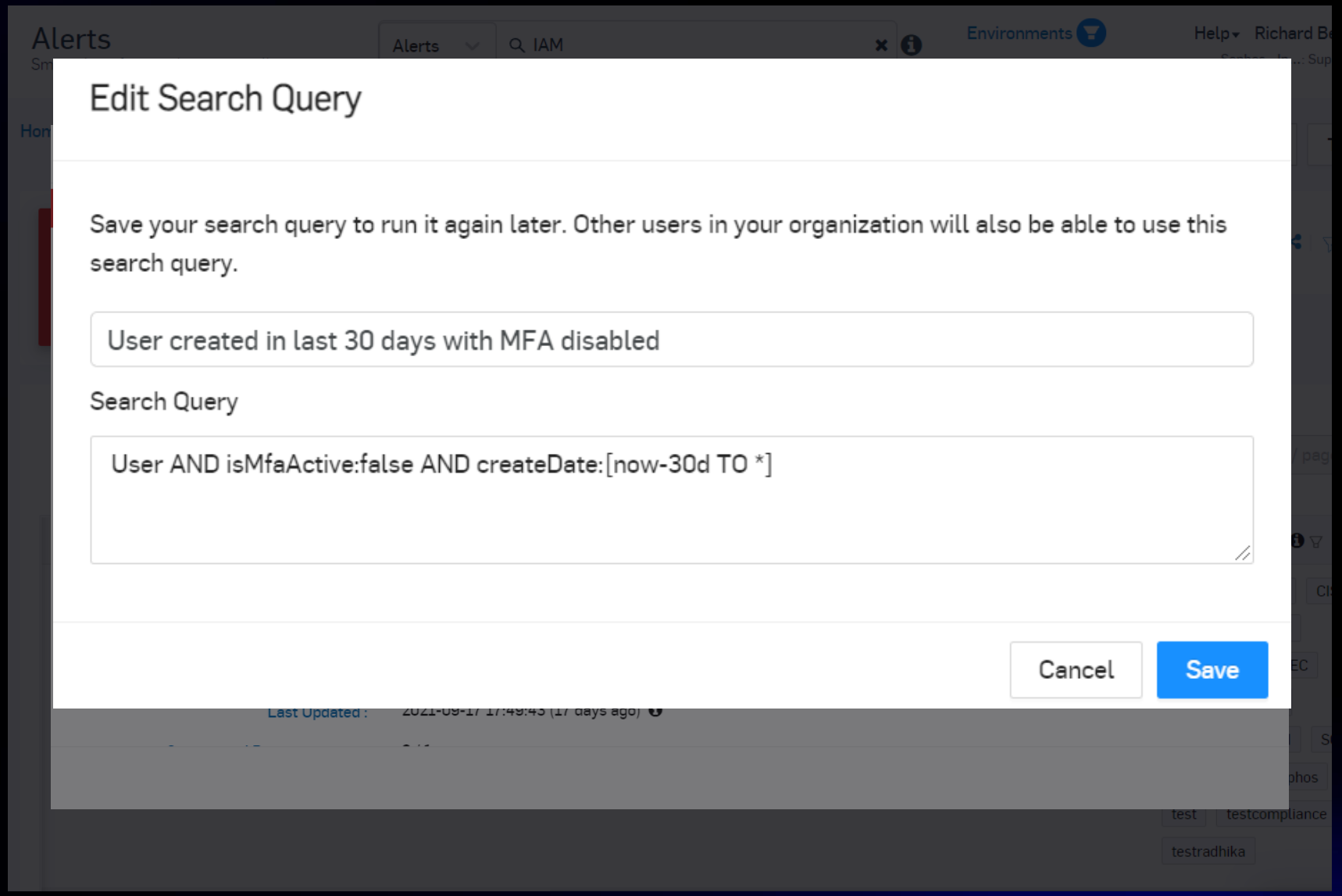
- Visualize networks and resources
- Run detailed security and compliance assessments with custom policies
- Benefit from risk-based prioritization of cloud provider security alerts with guided remediation
- Scan container image registries and infrastructure-as-code templates
- Monitor IAM roles for overprivileged access and more



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Quickly find IAM roles without MFA

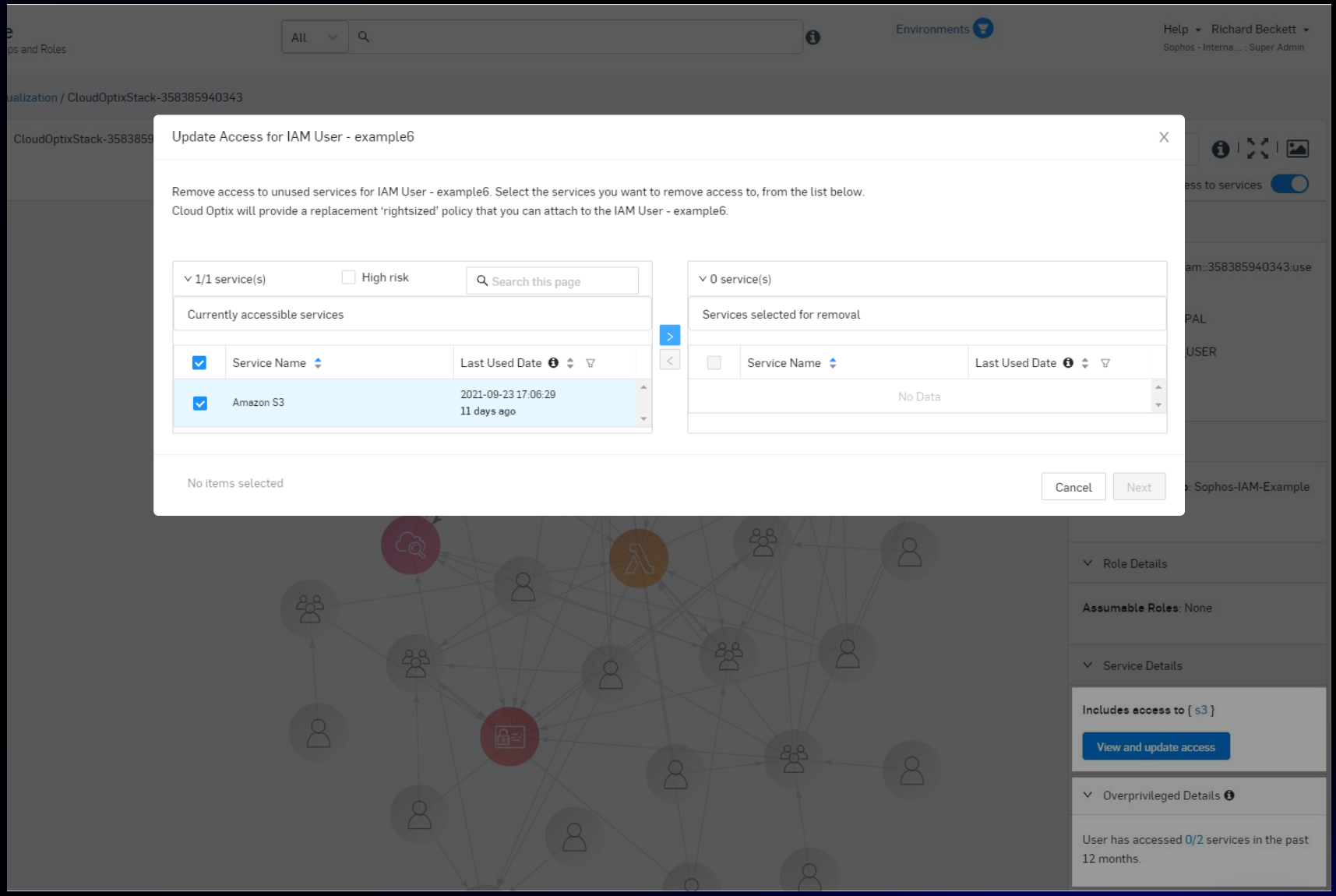
1. Inventory visibility
2. IAM roles
3. MFA disabled
4. Proactive alerts
5. Added context



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The end of overprivileged access

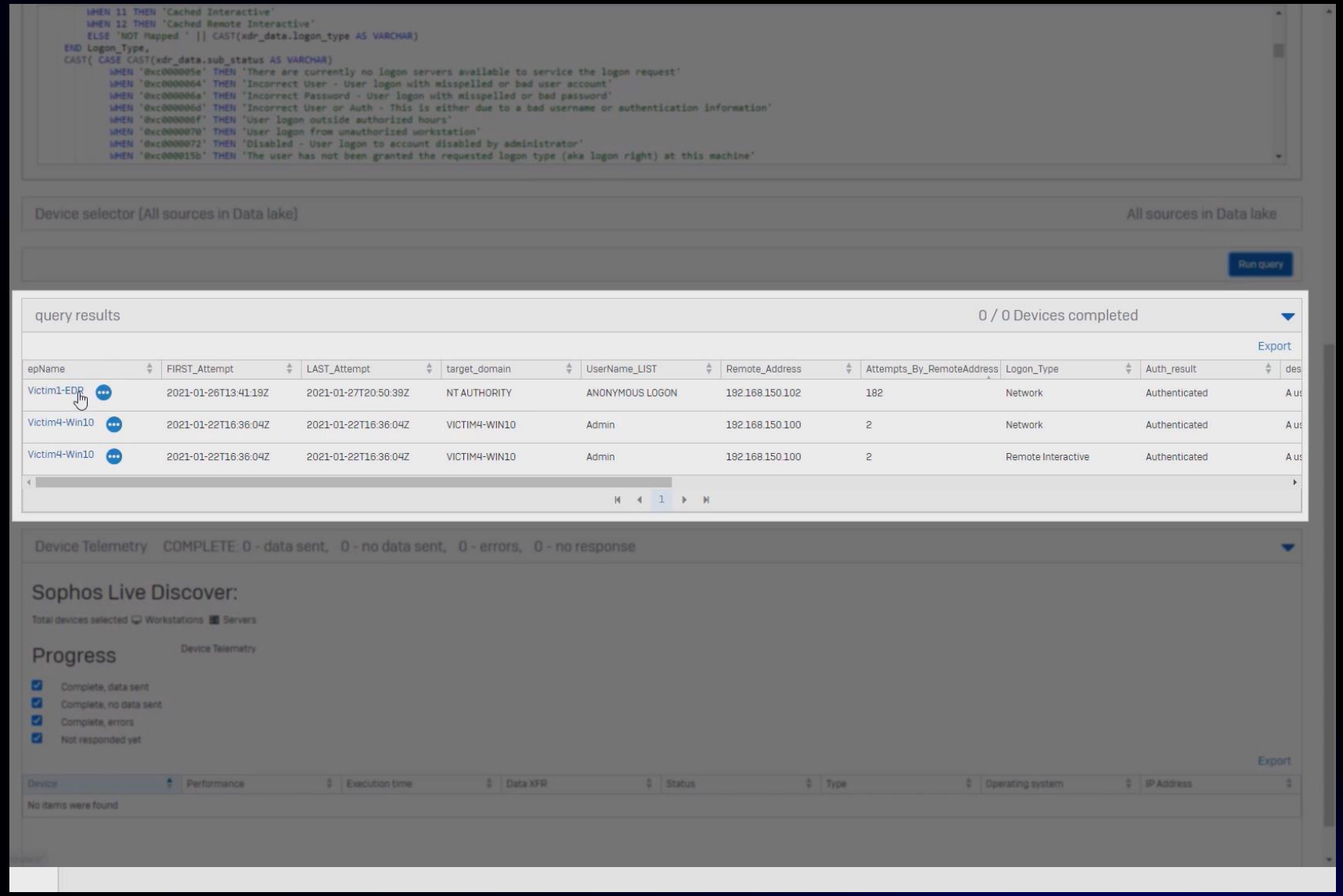
1. Visualize IAM relationships
2. Review access pathways
3. Identify over-privileged access
4. Right-size IAM policies



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Identify and investigate RDP exposures

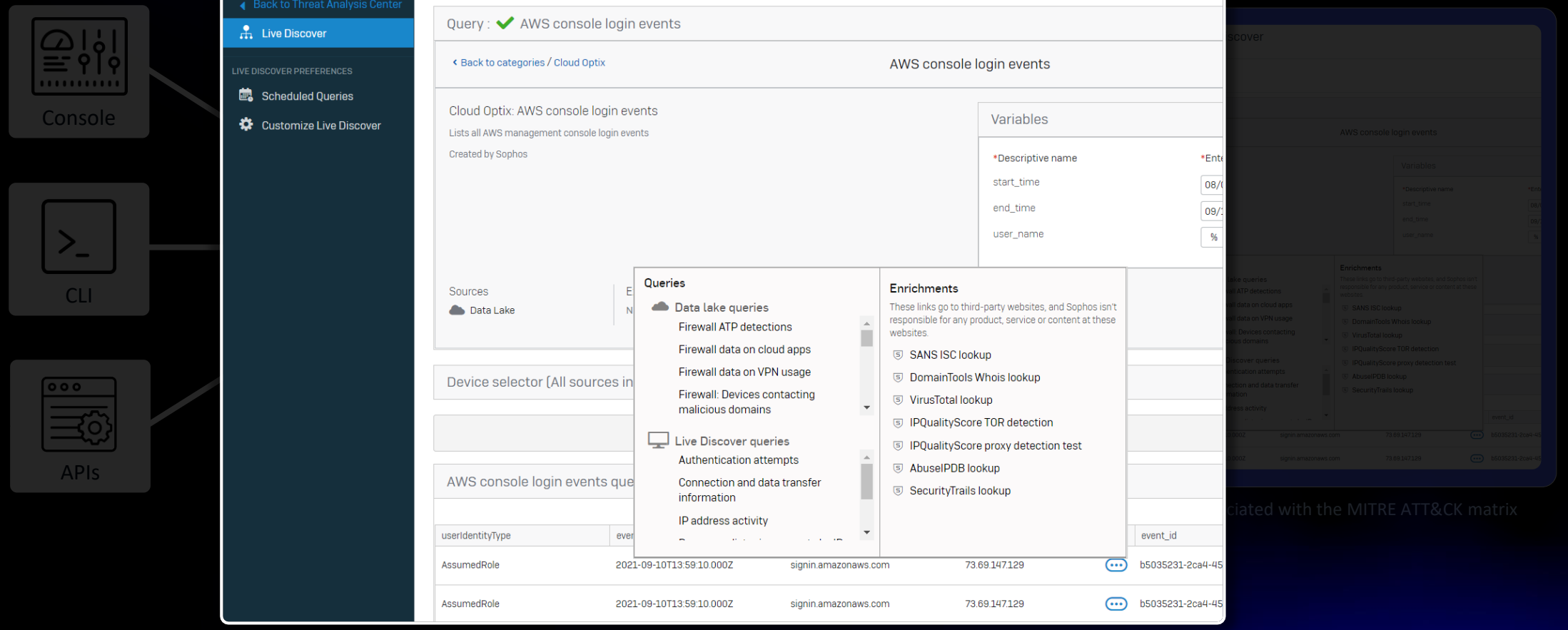
1. Setup RDP for EC2 instances
2. Alert to exposed ports
3. Add context with XDR
4. Search auth attempts
5. Find successful attempts



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS CloudTrail analysis and risk prioritization

IMPROVING THREAT DETECTION AND RESPONSE IN AWS WITH SOPHOS XDR

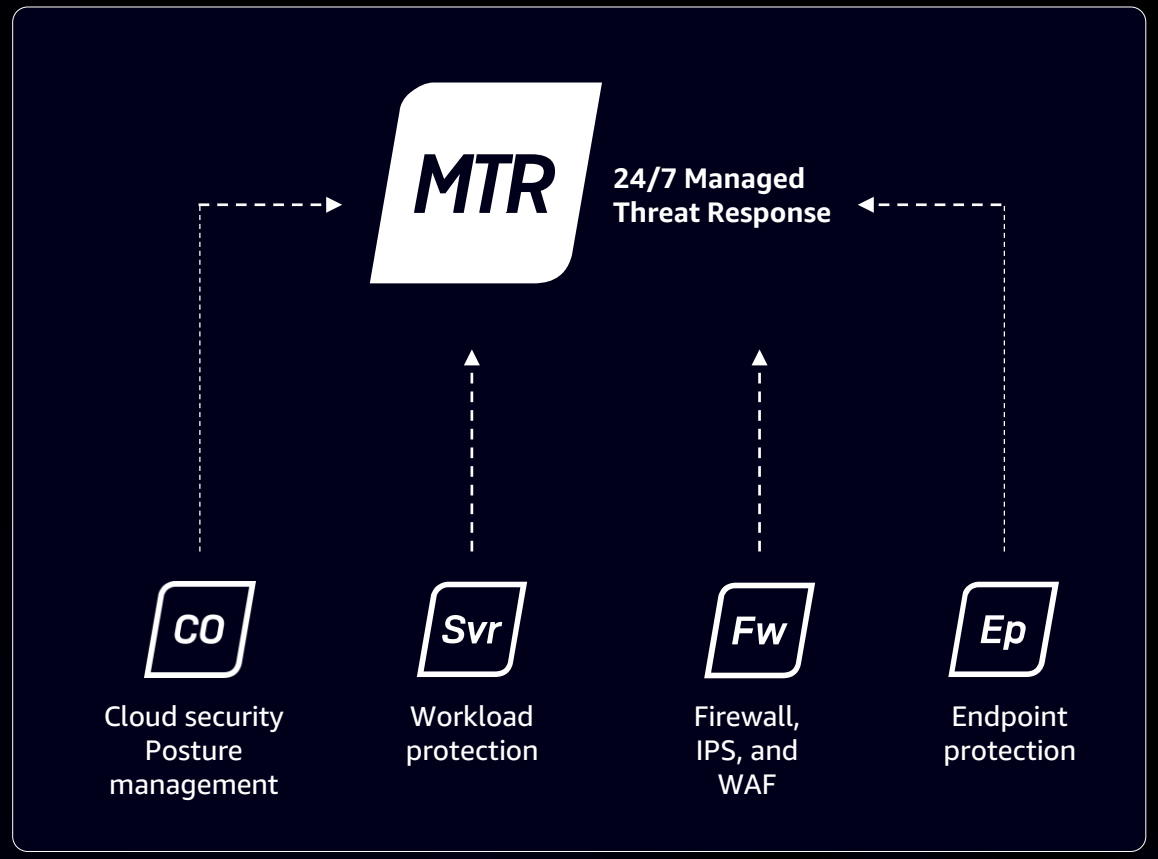


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

24/7 monitoring and response

SOPHOS MANAGED THREAT RESPONSE

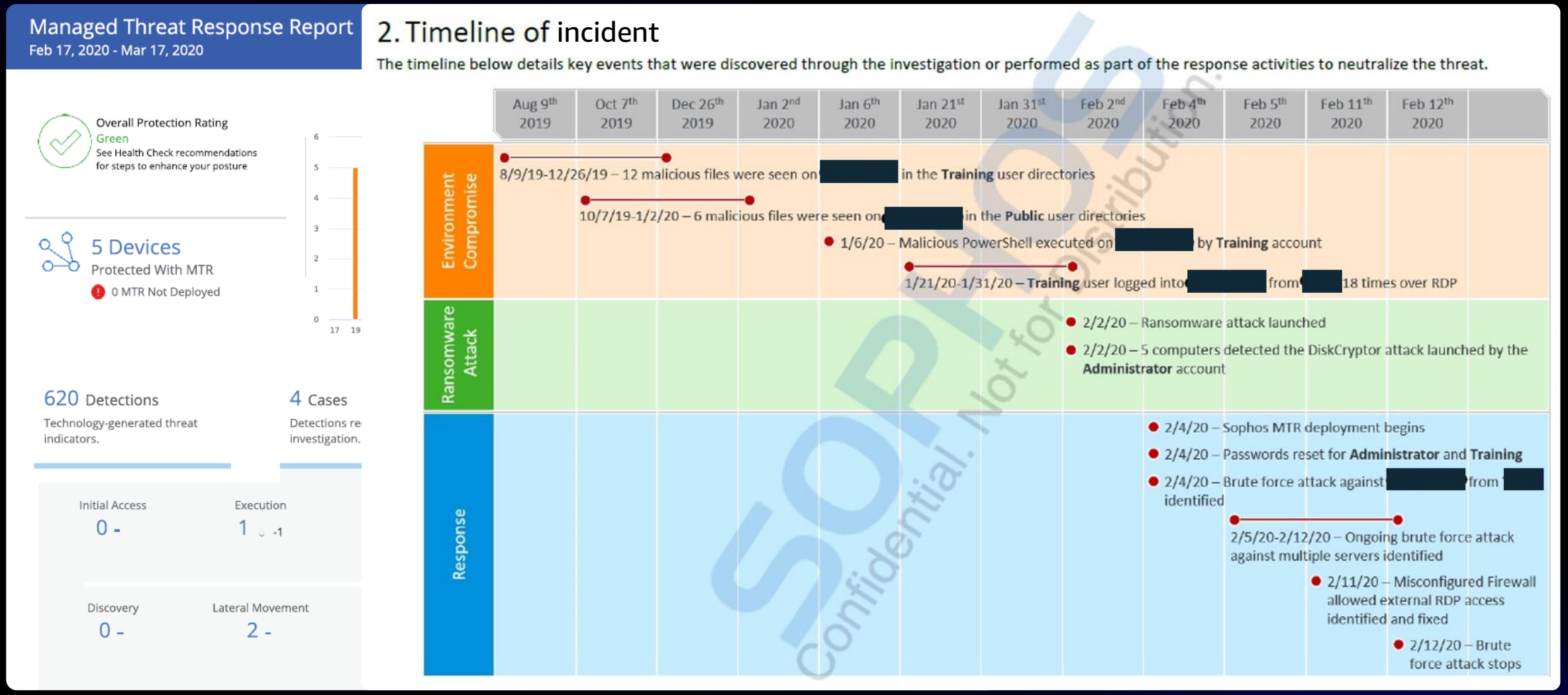
- Security experts monitor your cloud environment 24/7
- Sophos aggregates cross-environment data sources
- Response includes CSPM, cloud workload protection, firewall, and endpoint
- Actionable threat intelligence is programmatically served to analysts
- Sophos provides the ability to deliver integrated enterprise-wide prevention, detection, and response 24/7



aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

MTR report and timeline of incident



Managed Threat Response Report
Feb 17, 2020 - Mar 17, 2020

Overall Protection Rating
Green
See Health Check recommendations for steps to enhance your posture

5 Devices
Protected With MTR
0 MTR Not Deployed

620 Detections
Technology-generated threat indicators.

4 Cases
Detections re
investigation.

Initial Access 0 -
Execution 1 -1
Discovery 0 -
Lateral Movement 2 -

2. Timeline of incident

The timeline below details key events that were discovered through the investigation or performed as part of the response activities to neutralize the threat.

Aug 9th 2019 | Oct 7th 2019 | Dec 26th 2019 | Jan 2nd 2020 | Jan 6th 2020 | Jan 21st 2020 | Jan 31st 2020 | Feb 2nd 2020 | Feb 4th 2020 | Feb 5th 2020 | Feb 11th 2020 | Feb 12th 2020

Environment Compromise

- 8/9/19-12/26/19 – 12 malicious files were seen on [redacted] in the **Training** user directories
- 10/7/19-1/2/20 – 6 malicious files were seen on [redacted] in the **Public** user directories
- 1/6/20 – Malicious PowerShell executed on [redacted] by **Training** account
- 1/21/20-1/31/20 – **Training** user logged into [redacted] from [redacted] 18 times over RDP

Ransomware Attack

- 2/2/20 – Ransomware attack launched
- 2/2/20 – 5 computers detected the DiskCryptor attack launched by the **Administrator** account

Response

- 2/4/20 – Sophos MTR deployment begins
- 2/4/20 – Passwords reset for **Administrator** and **Training**
- 2/4/20 – Brute force attack against [redacted] from [redacted] identified
- 2/5/20-2/12/20 – Ongoing brute force attack against multiple servers identified
- 2/11/20 – Misconfigured Firewall allowed external RDP access identified and fixed
- 2/12/20 – Brute force attack stops

SOPHOS Confidential. Not for distribution.

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

“Sophos is there 24/7 so my team doesn’t need to be.”

Dinesh Adithan

Celayix Director of Software Engineering

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Why it’s important

Resources

Monitoring environments 24/7 for suspicious behavior and threats is unrealistic for many organizations

Skills

Proper configuration of cloud environments needed to optimize security and compliance posture

Budgets

Purchasing Sophos in AWS Marketplace can help customers’ IT budgets go further

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Next steps

One-minute infographic

Recap and share the key topics discussed today with our one-minute session infographic

Download infographic
https://soph.so/one-minute-mssp

Discover Sophos solutions

Discover the Sophos cloud security portfolio in AWS Marketplace

AWS Marketplace
https://soph.so/aws-mssp

Visit our booth

Get connected with a Sophos expert to help solve your business challenges

Booth 263

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Public Cloud Team

publiccloud@sophos.com

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.