SANS
The Most Trusted Source for Information
Security Training, Certification, and Research

Analyst Program

SANS 2024 Multicloud Survey

Securing Multiple Clouds Amid Constant Changes

Sponsored by Corelight, Fortinet, Infoblox, Microsoft, Tenable

Today’s Speakers

- Kenneth Hartman, Certified Instructor, *SANS*
- Simon Vernon, Certified Instructor, *SANS*
- Christina DePinto, Product Marketing Manager, *Tenable*
- Bob Hansmann, Sr. Product Marketing Manager – Security, *Infoblox*
- Ashish Malpani, Head of Product Marketing, *Corelight*
- Tamer Salman, Partner Director of Research, *Microsoft*
- Aidan Walden, Global Director, Cloud DevOps, Architecture & Engineering, *Fortinet*
- Oz Wilder, Partner Director of PM, *Microsoft*

slack

Join the SANS Analyst Program Slack Workspace

https://sansurl.com/forums

#00-help **–** Having technical difficulties? Let us know here, we’re ready to help!

# discussion **–** Chat with our SANS authors, sponsor speakers and fellow attendees to discuss presentations and post questions!

Code of Conduct

SANS strives to create an atmosphere of learning, growth, and community. We value the participation and input, in this event and in the industry, of people of all genders, sexual identities, cultural and socioeconomic backgrounds, races, ethnicities, nationalities, religions, and ages.

Please support this atmosphere with respectful behavior and speech. This applies to all online interactions including the event Slack channel and in Zoom.

If you witness or experience anything contrary to these guidelines, please tell us at: analyst@sans.org

Today’s Agenda

- Survey Key Findings and Insights – Kenneth Hartman and Simon Vernon
- Gain Control of Multicloud Complexity - Ashish Malpani
- Fortinet Presentation - Aidan Walden
- SANS 2024 Multicloud Survey: An Infoblox Perspective - Bob Hansmann
- Panel Discussion 1
- SANS Multicloud Security Defender for Cloud - Tamer Salman and Oz Wilder
- Becoming a Cloud Security Expert with CNAPP - Christina DePinto
- Panel Discussion 2

Questions or Comments?

Connect with Kenneth Hartman,
Certified Instructor, SANS

Connect with Simon Vernon,
Certified Instructor, SANS

For General Event Discussion:
#discussion

Executive Summary

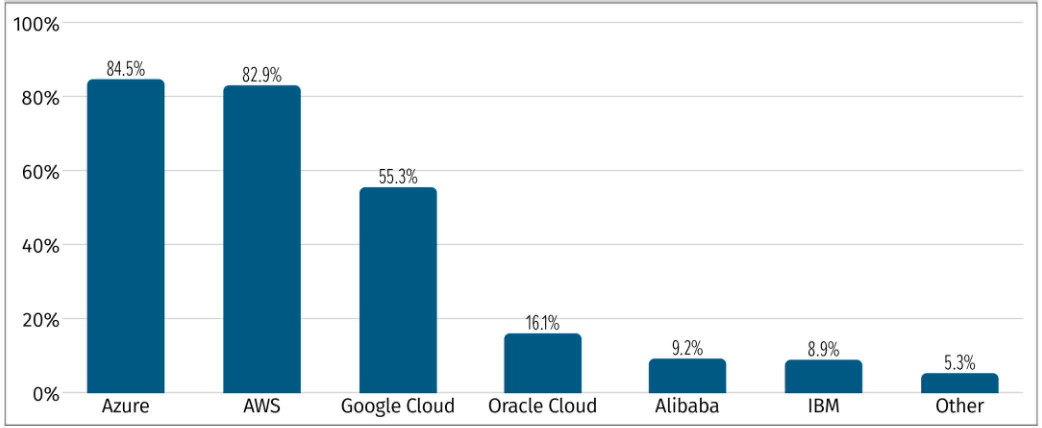
- Cloud services are evolving rapidly, increasing the complexity of multicloud environments.
- AWS and Azure dominate, while Google Cloud lags in growth.
- There are significant challenges in cloud security, with many organizations reporting gaps.
- Adoption of various cloud security tools is growing, but awareness and usability vary.

Dominance of AWS and Azure in Multicloud Environments

Analyst Program

- AWS and Azure hold more than 80% market share among survey respondents.
- Google Cloud has 55%, with other providers such as Oracle Cloud and IBM trailing behind.

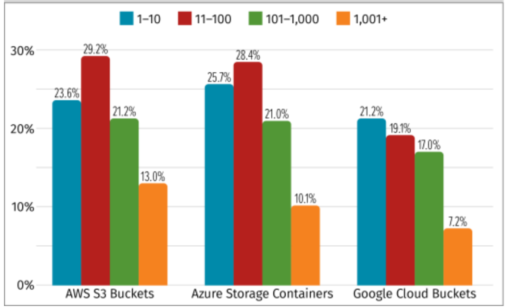
Which cloud service providers do you use? *Select all that apply.*



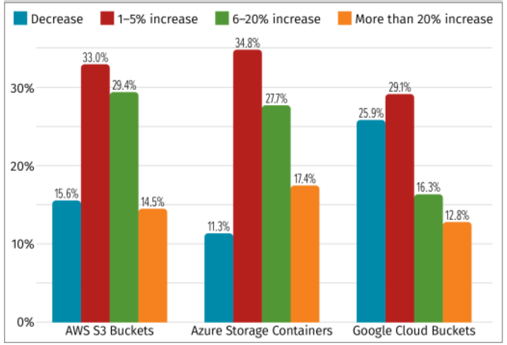
Security expertise is critical for all platforms used by the organization

Rapid Growth of Cloud Storage

How many buckets and storage containers does your organization use across all AWS S3 Buckets, Azure Storage Containers, and Google Cloud Buckets?



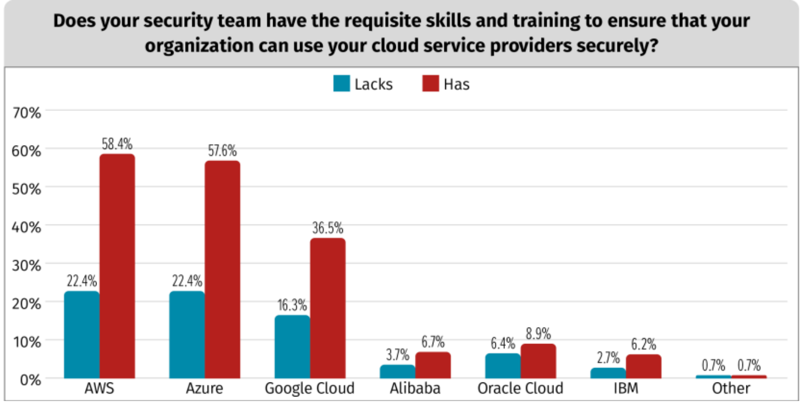
How many buckets and storage containers does your organization use across all AWS S3 Buckets, Azure Storage Containers, and Google Cloud Buckets (quantity change)?



- Cloud storage is widely adopted, with AWS and Azure leading the way.
- Diverse usage patterns indicate dynamic and evolving storage needs.
- Organizations need to adapt to fluctuating demands in cloud storage.

Gaps in Cloud Security Capabilities

- Confidence in cloud security teams is high, but significant gaps are reported.
- Gaps are particularly noted in skills and resources, especially with AWS and Azure.
- Continuous investment in training and leadership education is essential.



Does your security team have the requisite skills and training to ensure that your organization can use your cloud service providers securely?

Challenges in Managing User Identities

- Over 90% of respondents use Single Sign-On (SSO).
- 44% of those use multiple SSO providers due to different team preferences and mergers.

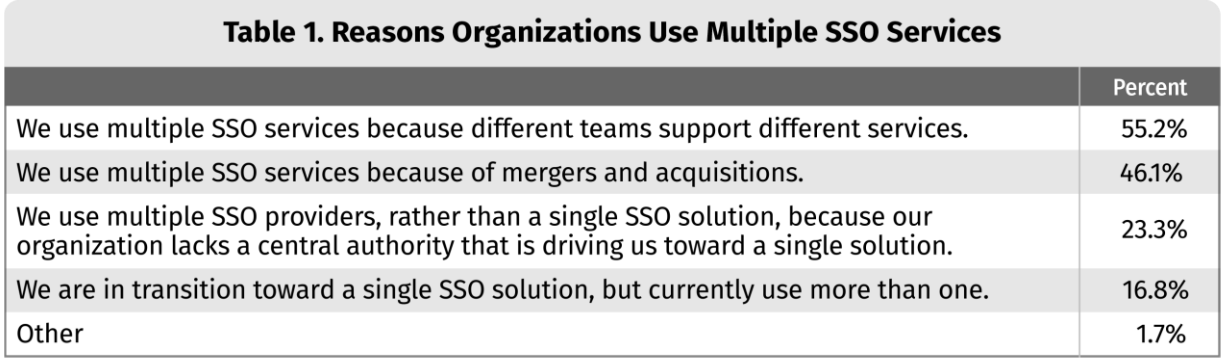
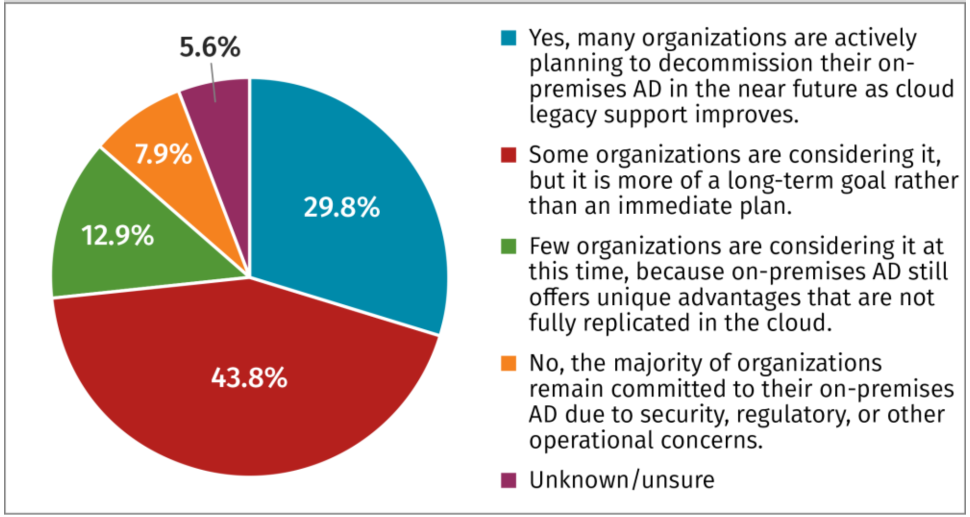


Table 1. Reasons Organizations Use Multiple SSO Services

	Percent
We use multiple SSO services because different teams support different services.	55.2%
We use multiple SSO services because of mergers and acquisitions.	46.1%
We use multiple SSO providers, rather than a single SSO solution, because our organization lacks a central authority that is driving us toward a single solution.	23.3%
We are in transition toward a single SSO solution, but currently use more than one.	16.8%
Other	1.7%

Cloud-Only Directory Services?

Do you believe that many organizations are considering the decommissioning of their on-premises Active Directory in favor of cloud-based directory services?

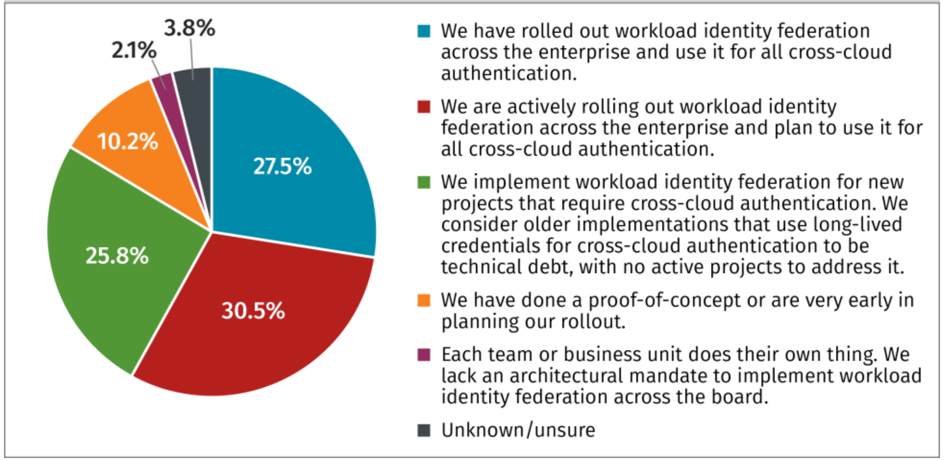


Increasing Adoption of Workload Identity Federation

Analyst Program

- 44% of organizations are using workload identity federation.
- A significant portion (29.9%) are unaware or unsure about its use.

What is the state of your organization's adoption of workload identity federation?

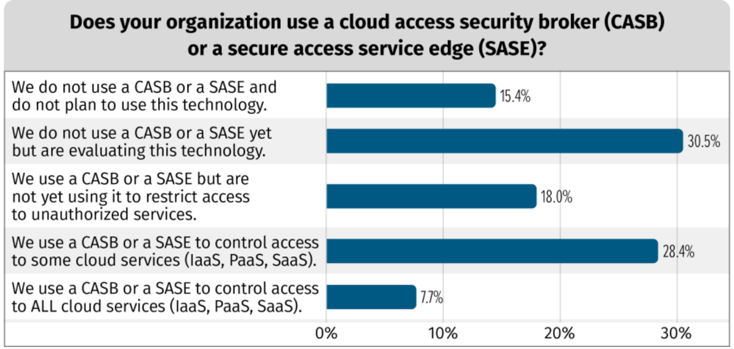


Opportunity for education and better awareness of its benefits.

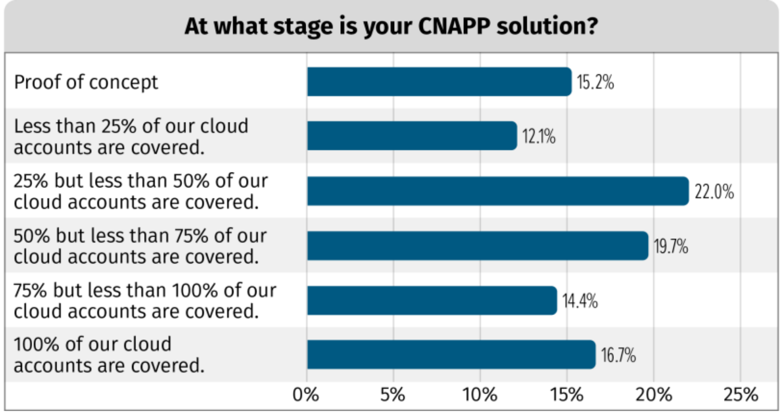
Adoption of Cloud Security Services

Analyst Program

- Various tools being adopted: CNAPP, CASB, SASE, CSPM, CIEM, and IaC scanning.
- Adoption rates vary, with opportunities for providers to enhance awareness.
- The need for improved usability and integration of these tools.


Does your organization use a cloud access security broker (CASB) or a secure access service edge (SASE)?

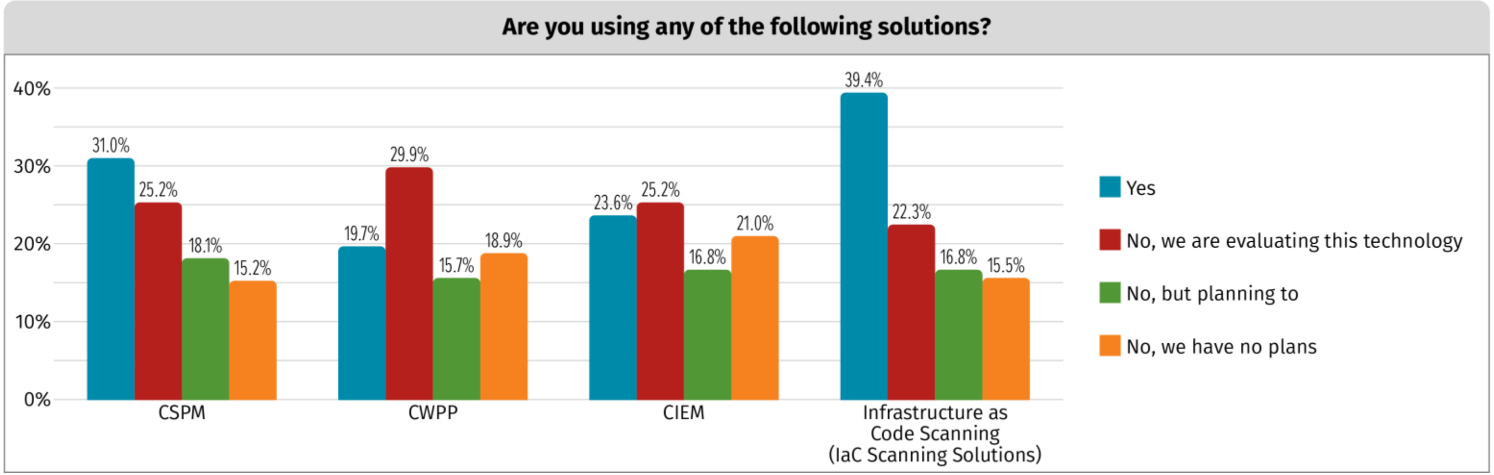
Cloud-Native Application Protection (CNAPP)



- 65.8% of organizations are using or considering CNAPP.
- Adoption is in the early stages, highlighting growth opportunities.

Confusion in the market due to overlapping features of CNAPP components.

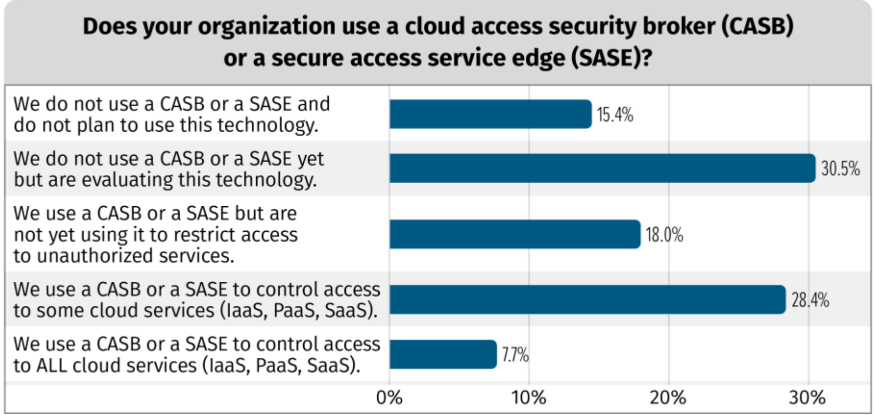
CNAPP Component Solutions



Analyst Program

The Rise of CASB and SASE

- There is growing interest in CASB and SASE technologies.
- Adoption is still in the early stages for many organizations.
- Barriers include lack of awareness, cost concerns, and technical challenges.

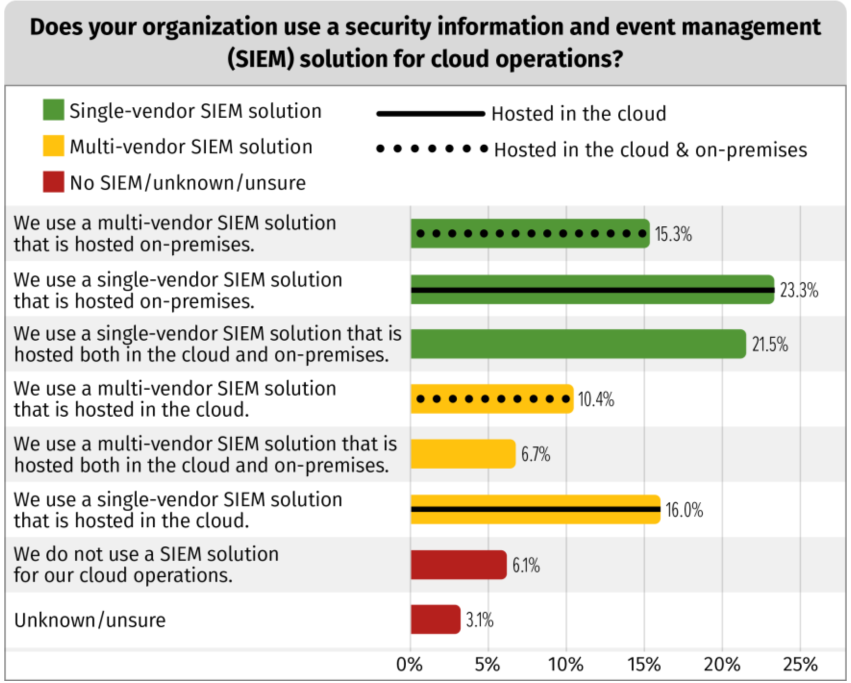


Security Information and Event Management (SIEM)

Analyst Program

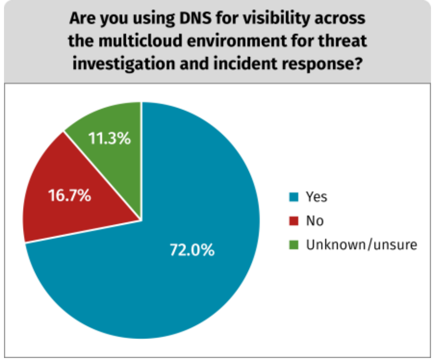
- Preference for cloud-hosted SIEM solutions is increasing.
- Hybrid deployments are also on the rise.

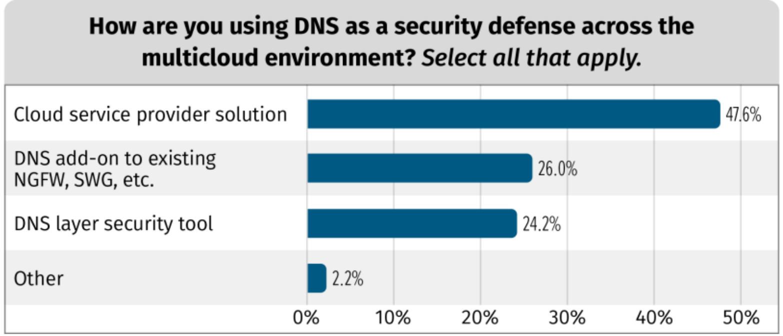
Integrated and cloud-centric security strategies are needed!



DNS Security in Multicloud Environments

- DNS security adoption is growing but remains inconsistent.
- A significant portion of organizations are unprotected or unsure of their DNS security measures.
- The need for increased awareness and tailored solutions.


Are you using DNS for visibility across the multicloud environment for threat investigation and incident response?


How are you using DNS as a security defense across the multicloud environment? *Select all that apply.*

The Growing Role of AI in Cloud Security

Analyst Program

- Strong interest in AI for multicloud security, but implementation varies.
- AI is used for threat detection, security automation, and compliance.
- Challenges include lack of expertise and concerns about AI’s effectiveness.

Conclusion

- Multicloud environments present both challenges and opportunities.
- Security requires continuous investment in skills, tools, and leadership education.
- A combination of cloud-native and third-party solutions is key to a robust security posture.

You cannot secure what you don’t know.

corelight

Questions or Comments?

Connect with Ashish Malpani,
Head of Product Marketing

For General Event Discussion:
#discussion

corelight

Gain control of multi-cloud complexity

Ashish Malpani

Cloud Security Challenges

Shallow threat detection
Detections using flow log analysis are limited, e.g. flow logs can only detect C2 communication with known command and control server.

Attackers evade EDR
APTs find ways to bypass EDR and CNAPP solutions by using LOTL techniques, such as PowerShell scripts or WMI tools, that mimic legitimate system activities.

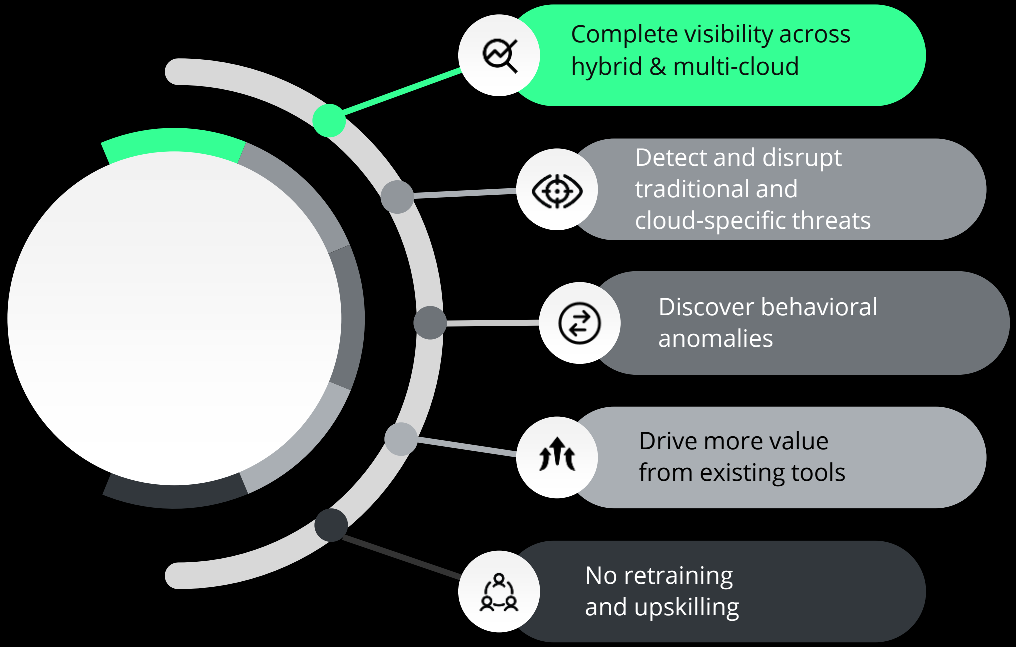
Inconsistent telemetry
Cloud logs are not exhaustive, often have inconsistent schemas, and sometimes are not designed for security use cases, multiplying the cost of downstream analytics and automation.

More tools means more learning
From AWS GuardDuty to GCP Security Command Center, adopting multi-cloud strategy results in tool sprawl and training needs for the security team which impacts automation and incident response.

Security teams waste precious cycles plumbing incompatible tools for visibility and correlating shallow datasets — both impossible tasks.

How can we solve it?

Identify and mitigate risks faster from across your *entire* network


Complete visibility across hybrid & multi-cloud
Detect and disrupt traditional and cloud-specific threats
Discover behavioral anomalies
Drive more value from existing tools
No retraining and upskilling

Identify all services across cloud environments along with consistent network telemetry

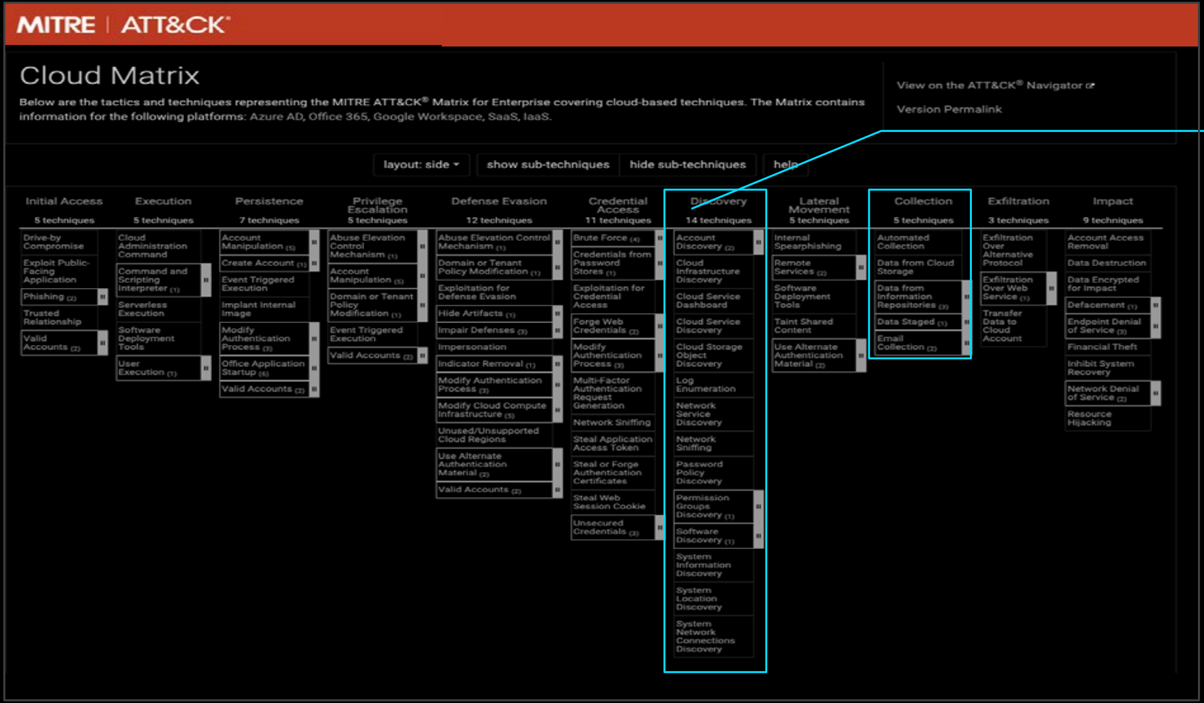
Empower security teams with traditional and cloud-specific detections to disrupt attacks by detecting lateral movement and data exfiltration behaviors specific to the cloud.

Detect when a host is reaching out to multiple services in an attempt to see which ones it has access to, a common indicator of a compromised host.

Fill the coverage gaps and transform cloud traffic to deliver detailed logs, files, and insights for faster triage in SIEM/ XDR architectures.

Extend security teams’ capabilities to cloud without new resources with insights from cloud traffic already integrated into your SIEM/XDR solutions.

TTPs that Map to MITRE ATT&CK Matrix for Cloud Based Techniques



Cloud Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise covering cloud-based techniques. The Matrix contains information for the following platforms: Azure AD, Office 365, Google Workspace, SaaS, IaaS.

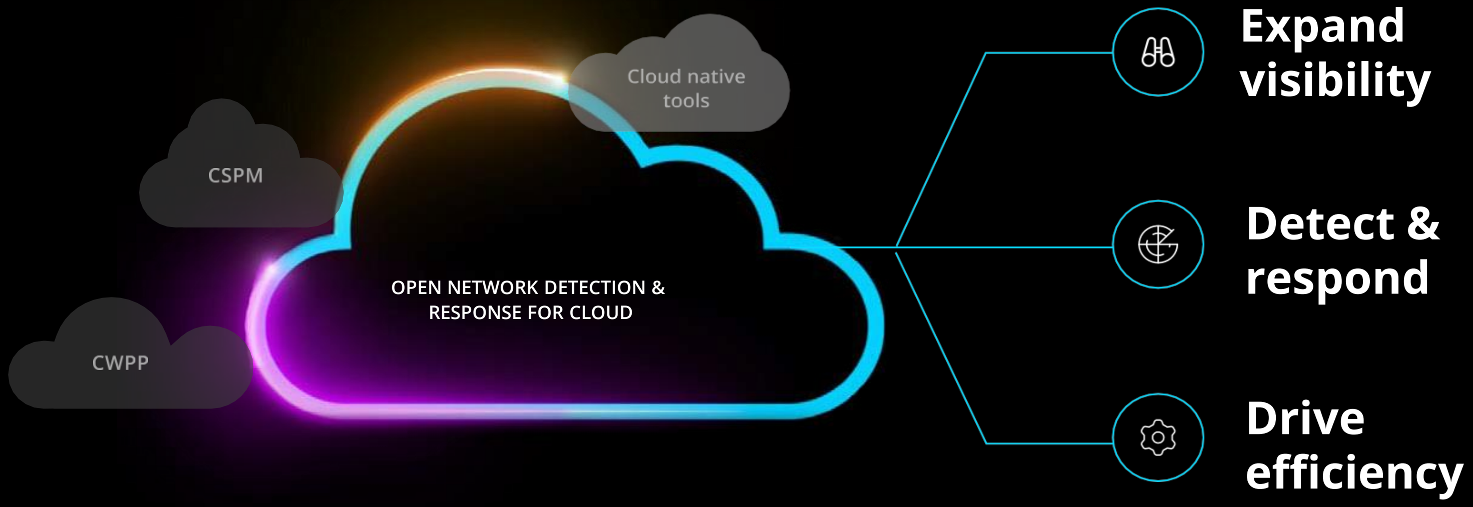
Initial Access 5 techniques	Execution 5 techniques	Persistence 7 techniques	Privilege Escalation 5 techniques	Defense Evasion 12 techniques	Credential Access 11 techniques	Discovery 14 techniques	Lateral Movement 5 techniques	Collection 5 techniques	Exfiltration 3 techniques	Impact 9 techniques
Drive-by Compromise	Cloud Administration Command	Account Manipulation (5)	Abuse Elevation Control Mechanism (1)	Abuse Elevation Control Mechanism (1)	Brute Force (4)	Account Discovery (2)	Internal Spearphishing	Automated Collection	Exfiltration Over Alternative Protocol	Account Access Removal
Exploit Public-Facing Application	Command and Scripting Interpreter (1)	Create Account (1)	Account Manipulation (5)	Domain or Tenant Policy Modification (1)	Credentials from Password Stores (1)	Cloud Infrastructure Discovery	Remote Services (2)	Data from Cloud Storage	Exfiltration Over Web Service (1)	Data Destruction
Phishing (2)	Serverless Execution	Event Triggered Execution	Domain or Tenant Policy Modification (1)	Exploitation for Defense Evasion	Exploitation for Credential Access	Cloud Service Dashboard	Software Deployment Tools	Data from Information Repositories (3)	Transfer Data to Cloud Account	Data Encrypted for Impact
Trusted Relationship	Software Deployment Tools	Implant Internal Image	Event Triggered Execution	Hide Artifacts (1)	Forge Web Credentials (2)	Cloud Service Discovery	Taint Shared Content	Data Staged (1)		Defacement (1)
Valid Accounts (2)	User Execution (1)	Modify Authentication Process (3)	Valid Accounts (2)	Impair Defenses (3)	Modify Authentication Process (3)	Cloud Storage Object Discovery	Use Alternate Authentication Material (2)	Email Collection (2)		Endpoint Denial of Service (3)
		Office Application Startup (6)		Impersonation	Multi-Factor Authentication Request Generation	Log Enumeration				Financial Theft
		Valid Accounts (2)		Indicator Removal (1)	Network Sniffing	Network Service Discovery				Inhibit System Recovery
				Modify Authentication Process (3)	Steal Application Access Token	Network Sniffing				Network Denial of Service (2)
				Modify Cloud Compute Infrastructure (5)	Steal or Forge Authentication Certificates	Password Policy Discovery				Resource Hijacking
				Unused/Unsupported Cloud Regions	Steal Web Session Cookie	Permission Groups Discovery (1)				
				Use Alternate Authentication Material (2)	Unsecured Credentials (3)	Software Discovery (1)				
				Valid Accounts (2)		System Information Discovery				
						System Location Discovery				
						System Network Connections Discovery				

Detecting a host during discovery of a role permissions through service enumeration is immutable and a powerful way to **detect and remediate a compromised host.**

- Network service discovery
- T1046, used widely
- Cloud service discovery
- T1580, used in Pacu and Scattered spider
- System network connections discovery
- T1049 used widely

Detection of network-level collection techniques is immutable and a powerful way to **stop data exfiltration before it occurs.**

- Data collection
- T1530, many examples including scattered spider
- Data staging
- T1074, many examples including Shark, QUIETCANARY
- Data exfiltration techniques



CLOSE CLOUD VISIBILITY GAPS **WITH NDR**

In multi-cloud environments, achieving comprehensive visibility and rapid threat detection is essential. NDR is a key solution for effective threat detection in these environments.

With NDR, you gain the ability to identify all services and activities within your environments, marrying network telemetry with host data enrichment for a **complete view.**

Thank you!

Scan the QR code to learn more about
Corelight Cloud Security Solutions

https://corelight.com/solutions/cloud-solutions

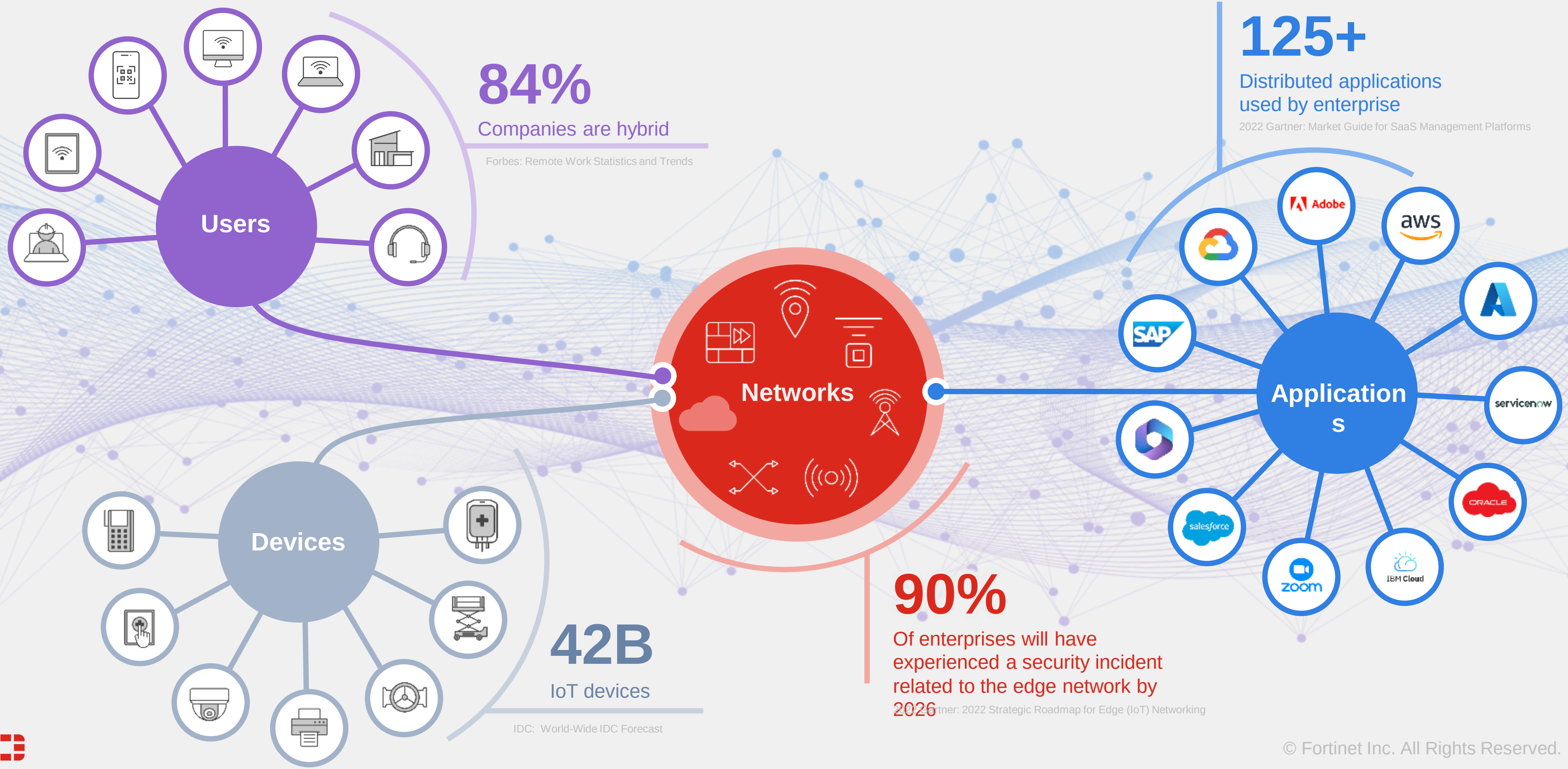
Questions or Comments?

Connect with Aidan Walden,
Global Director, Cloud DevOps, Architecture & Engineering

For General Event Discussion:
#discussion

Securing Access to the Hybrid Cloud

Traditional Networking is Built on Trusting Everyone and Connecting Everything



84%

Companies are hybrid

Forbes: Remote Work Statistics and Trends

125+

Distributed applications used by enterprise

2022 Gartner: Market Guide for SaaS Management Platforms

90%

Of enterprises will have experienced a security incident related to the edge network by 2026

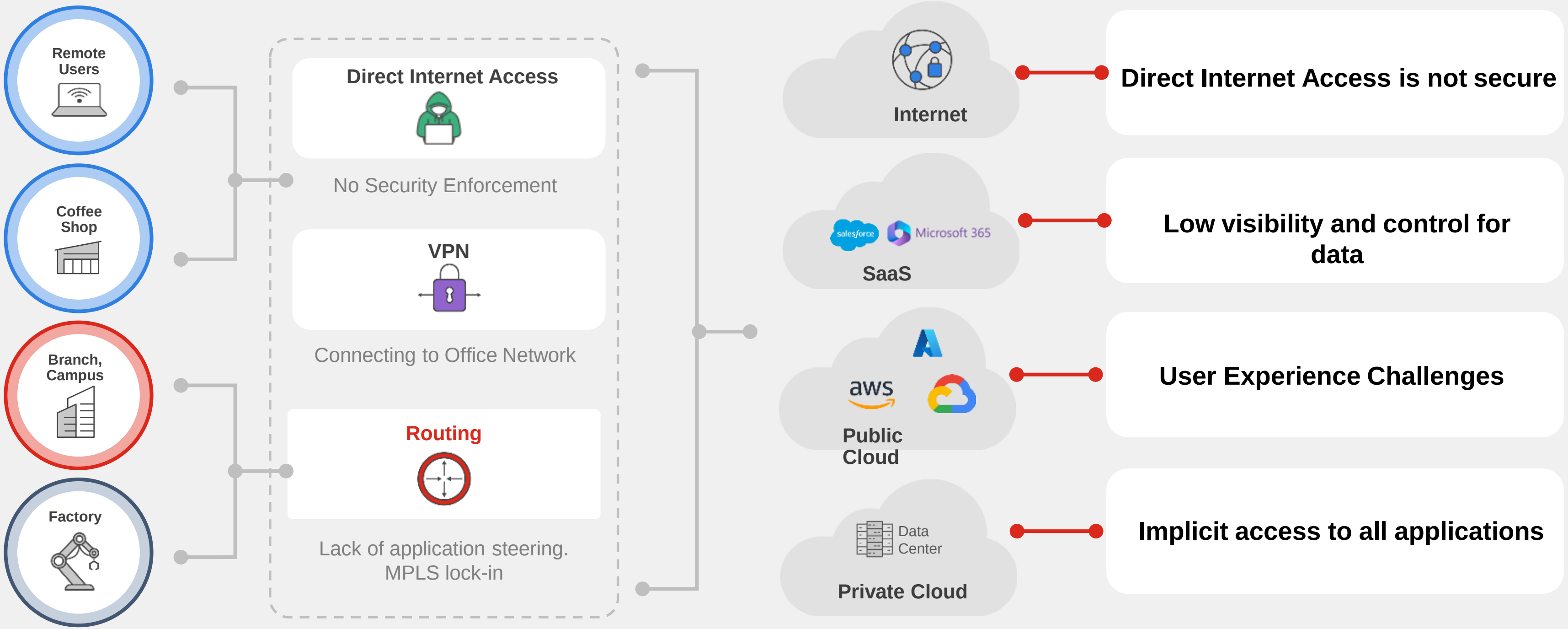
2022 Gartner: 2022 Strategic Roadmap for Edge (IoT) Networking

42B

IoT devices

IDC: World-Wide IDC Forecast

Current Technology Requires Transformation



Remote Users

Coffee Shop

Branch, Campus

Factory

Direct Internet Access

No Security Enforcement

VPN

Connecting to Office Network

Routing

Lack of application steering. MPLS lock-in

Internet

salesforce

Microsoft 365

SaaS

aws

Public Cloud

Data Center

Private Cloud

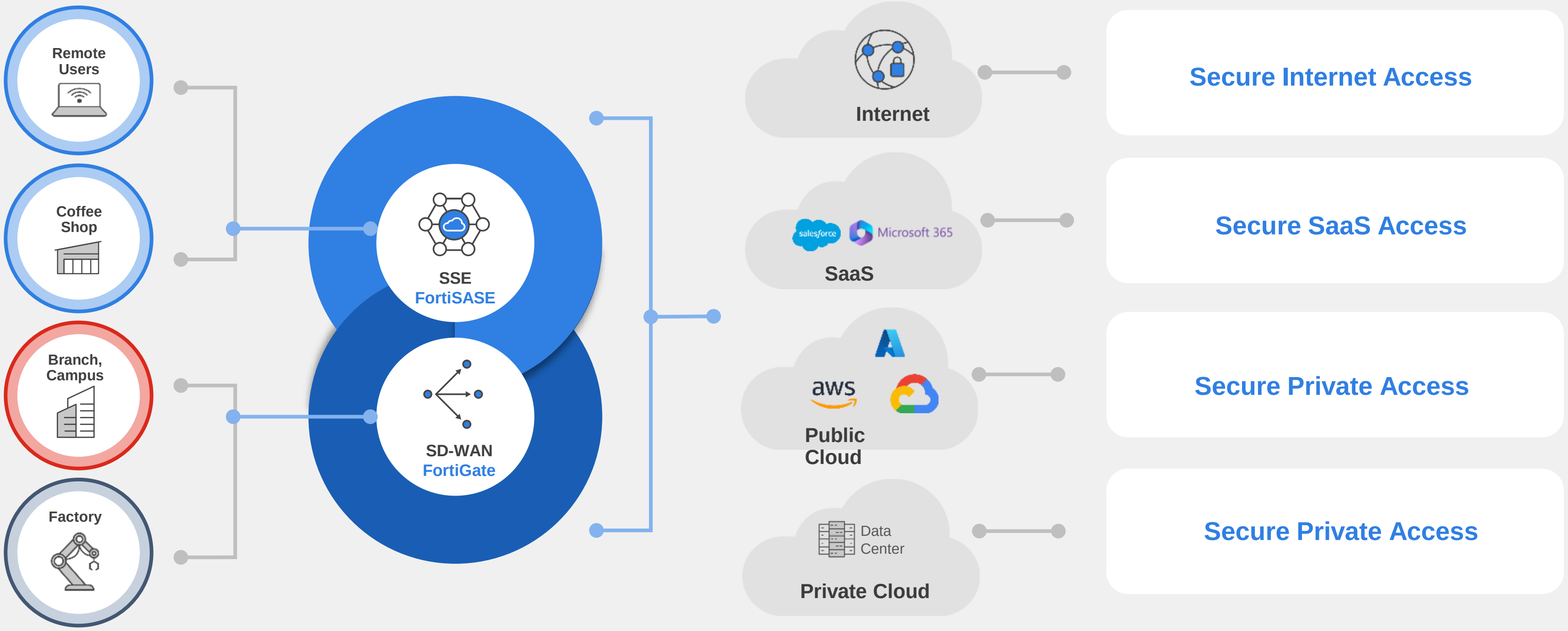
Direct Internet Access is not secure

Low visibility and control for data

User Experience Challenges

Implicit access to all applications

Unified SASE delivers Single Vendor Approach



Unified (Policies, Agent)

Simple (Intuitive UI, Simplified Pricing)

Flexible (One OS across SSE,SD-WAN)

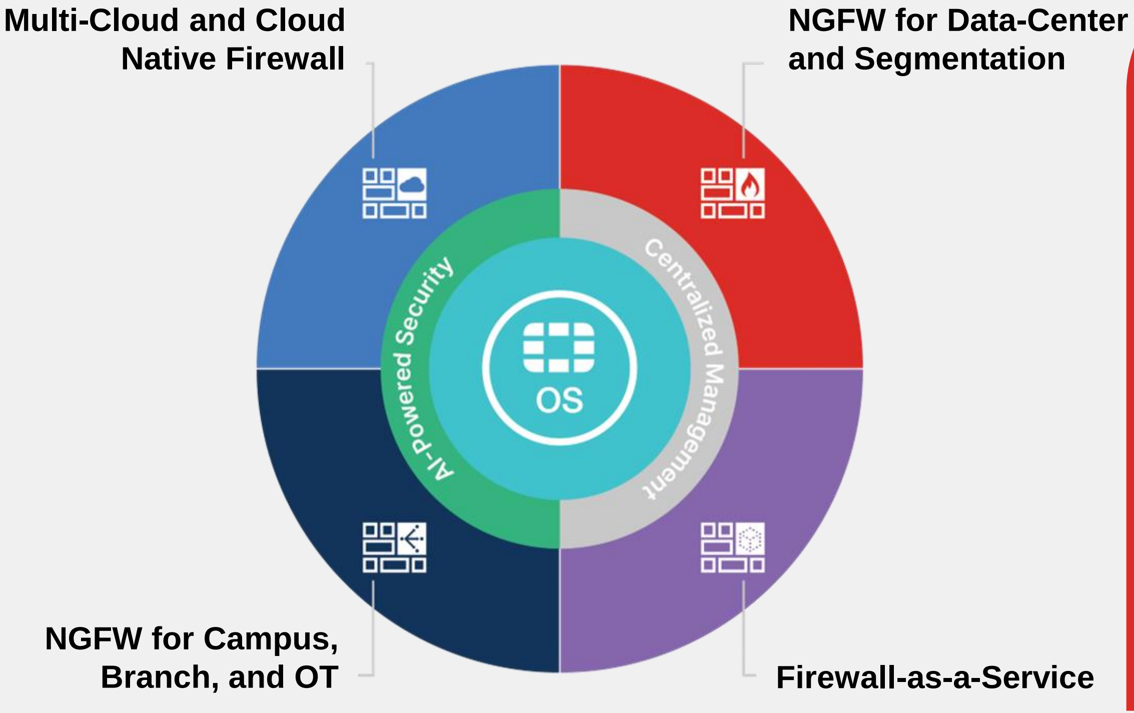
Zero Trust Mindset

Never Trust, Always Verify for resource protection

- Grants network access only after identity is authenticated and authorized
- Limits network access only to necessary resources/applications
- Continuously adjusts network access in near real time, based on device/user context

Hybrid Mesh Firewall

Centralized and unified management simplifying cybersecurity operations


Multi-Cloud and Cloud Native Firewall
NGFW for Data-Center and Segmentation
AI-Powered Security
Centralized Management
OS
NGFW for Campus, Branch, and OT
Firewall-as-a-Service

"By 2026, more than 60% of organizations will have more than one type of firewall deployment, which will prompt adoption of hybrid mesh firewalls."

Source: Gartner Network Firewall MQ 2022

Extend Protection Across the Entire Network with Unified Security

Secure Networking

Hybrid Mesh Firewall

Evolution of NGFW to Hybrid Mesh Firewall for unified management that simplifies operations, reduces risk, and ensures compliance at scale

Accelerated ASIC | Branch | Campus | Data Center | Cloud Native | Virtual | FWaaS

Secure Connectivity

FortiLink converges networking and security for secure WLAN/LAN equipment to provide security and automation, improve visibility and control, and reduce TCO.

FortiLink | FortiAP | FortiSwitch | FortiExtender | FortiNAC

AI-Driven Technologies

FortiOS

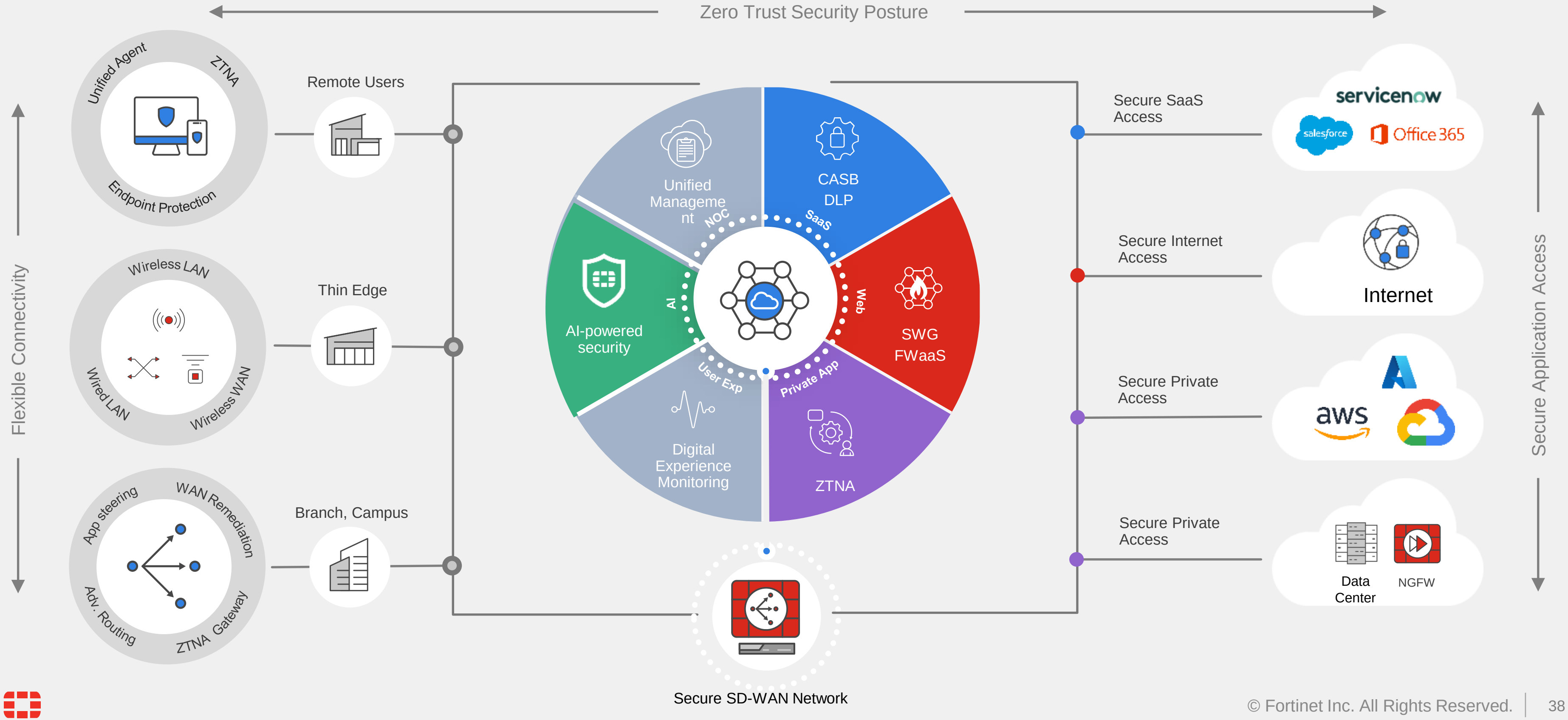
FortiGuard Labs

AI for Networking (AIOPS)

Unified Management

FortiSASE – Cloud Delivered Security Service Edge

Secure access for the hybrid workforce



Unified SASE Use Cases

Secure SD-WAN for Branch and Campus

Transitioning from MPLS to Broadband via SD-WAN reduces cost and enhance application performance. This shift optimizes user experience along with providing security for direct internet access

Clear ROI, Controller-less, Convergence

Secure Remote Users for Internet Access

Enable secure web browsing for remote users to protect from known and unknown threats along with providing seamless user experience

AI-Powered Security, Unified Agent, Unified Management

Upgrade Remote Access for Private Applications

Transition to explicit application access under a zero-trust mindset to ensure secure application access avoiding lateral movement of threats

Real-time, Universal Enforcement, Clear ROI

SaaS Control and Data Protection

Address Shadow IT visibility challenges by deploying SaaS application control. Safeguard sensitive information using data loss prevention for hybrid workforce

Single SASE License, Unified Management, Data Protection

Thin Edge for Secure Access

Deploy and manage Access point as a hardware agent to connect with SASE and enable secure access for users and unmanaged devices

Industry's Only, Secure Access, Flexible Connectivity

Protect Web Applications and APIs

Secure applications and APIs from web attacks, zero-days, and sophisticated bots.

AI/ML and Automation, Minimum False Positives, Flexible Deployment

Fortinet Security Fabric

Broad

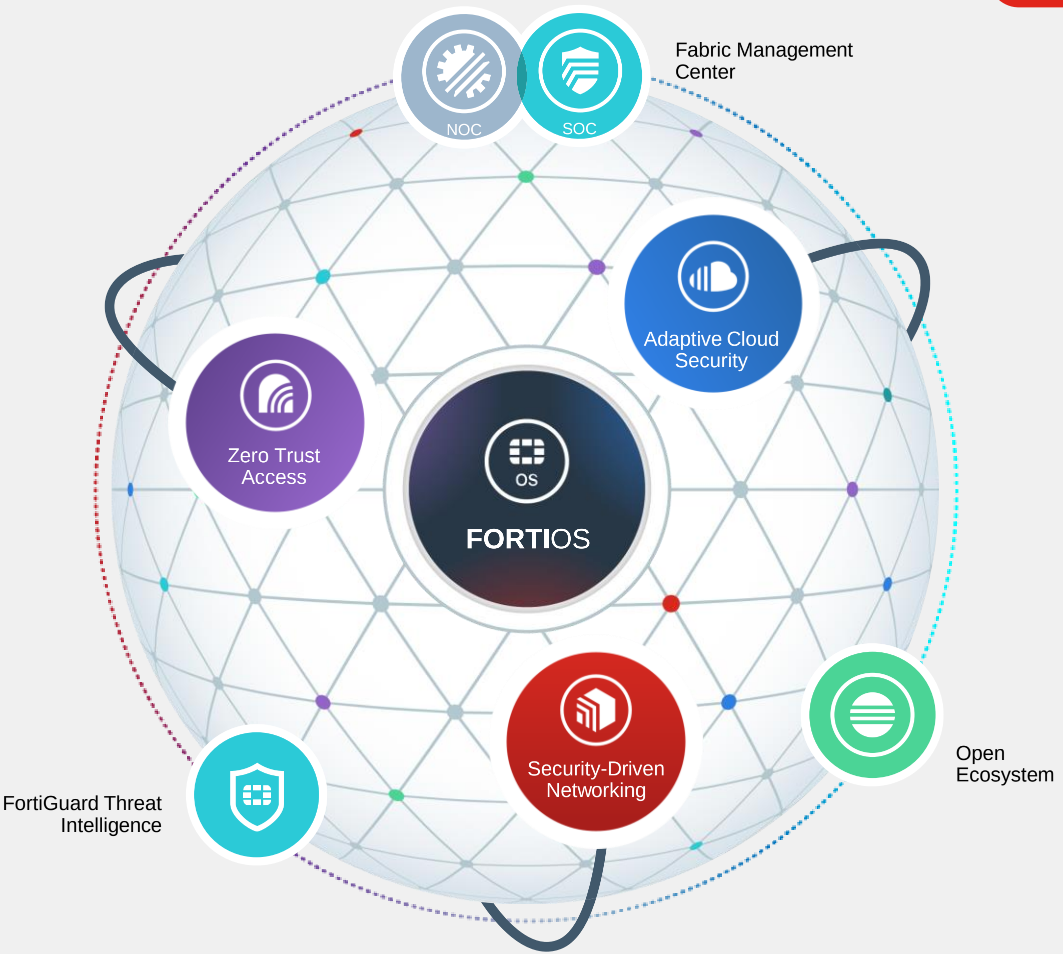
visibility and protection of the entire digital attack surface to better manage risk

Integrated

solution that reduces management complexity and shares threat intelligence

Automated

self-healing networks with AI-driven security for fast and efficient operations



FORTINET®

infoblox®

Questions or Comments?

Connect with Bob Hansmann,
Sr. Product Marketing Manager - Security

For General Event Discussion:
#discussion

SANS 2024 MULTICLOUD SURVEY: Navigating the Complexities of Multiple Clouds

AN INFOBLOX PERSPECTIVE

Bob Hansmann
Security Products Team
Infoblox, Inc

infoblox.

MULTICLOUD CHALLENGES

Inconsistent and Complex Network Management

Manual DNS management

Human error

Unsustainable processes

Fragmented deployments

Lack of Centralized Visibility

Ineffective resource tracking

Fragmented automations,

Unmonitored resource

Over-reliance on trouble tickets

Inefficient DNS Deployments

Legacy systems

Complex maintenance

On-site hardware burden

Complex upgrades

infoblox

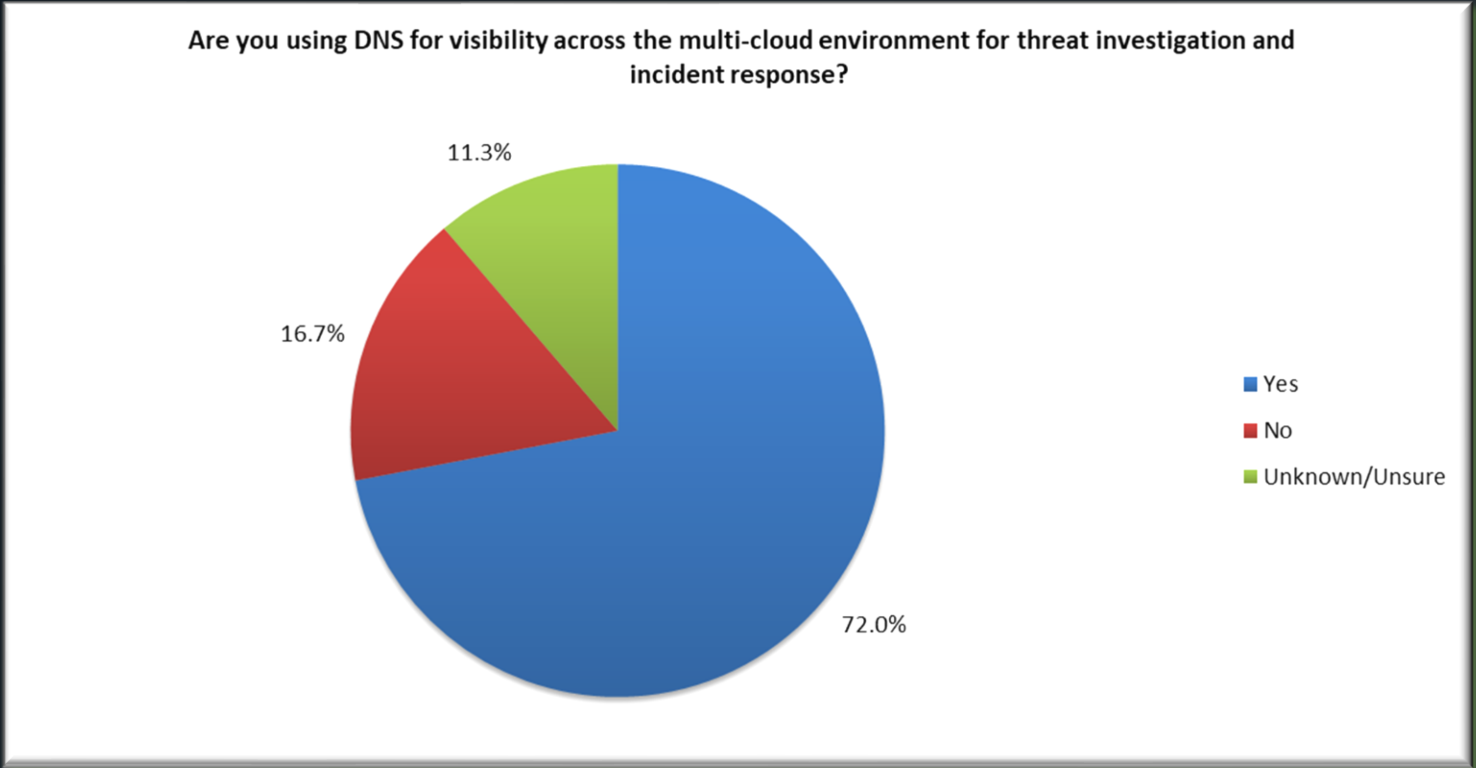
Why DNS Security for Multi-Cloud Environments?

DNS is not just a component-

IT'S THE BACKBONE

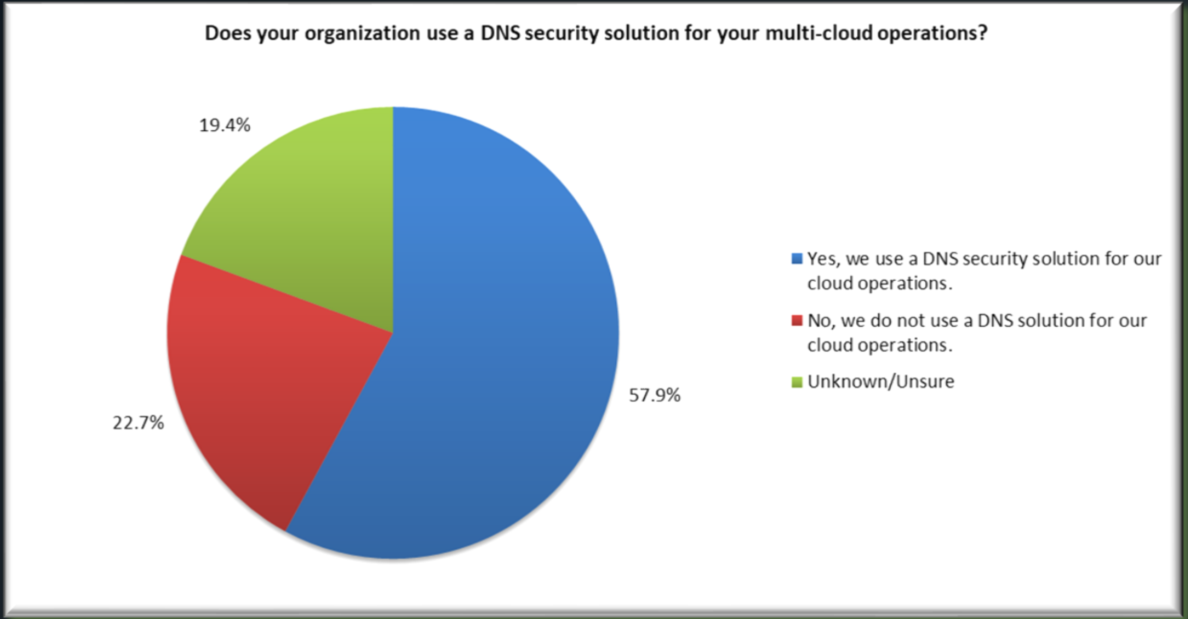
of your network, the linchpin that holds your operations together, can be the source of critical intelligence, and not only sees enterprise networks but also adversary infrastructure.

Are You Using DNS for Visibility in Your Multi-Cloud Environment?

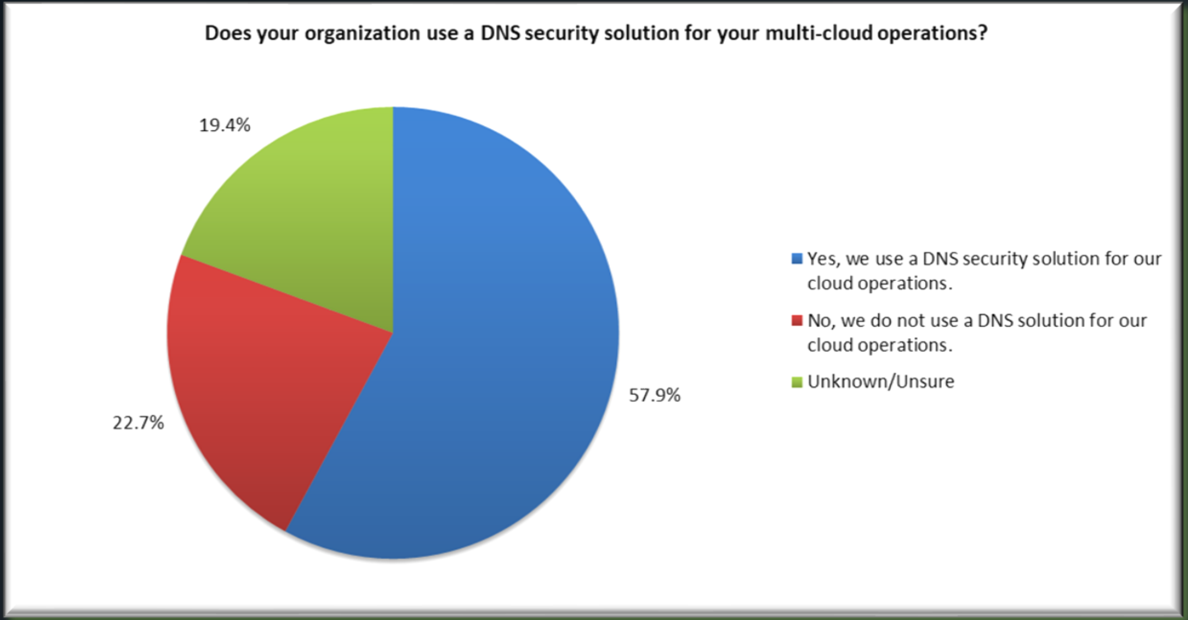


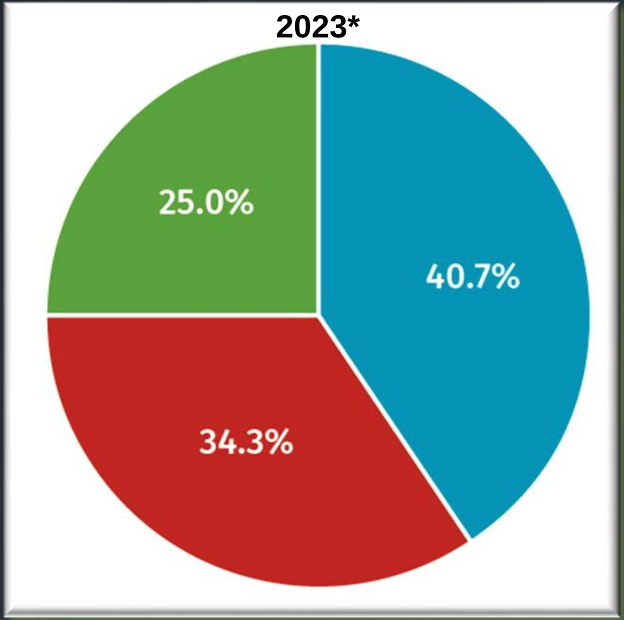
Are you using DNS for visibility across the multi-cloud environment for threat investigation and incident response?

Are You Using DNS for Security in Your Multi-Cloud Environment?



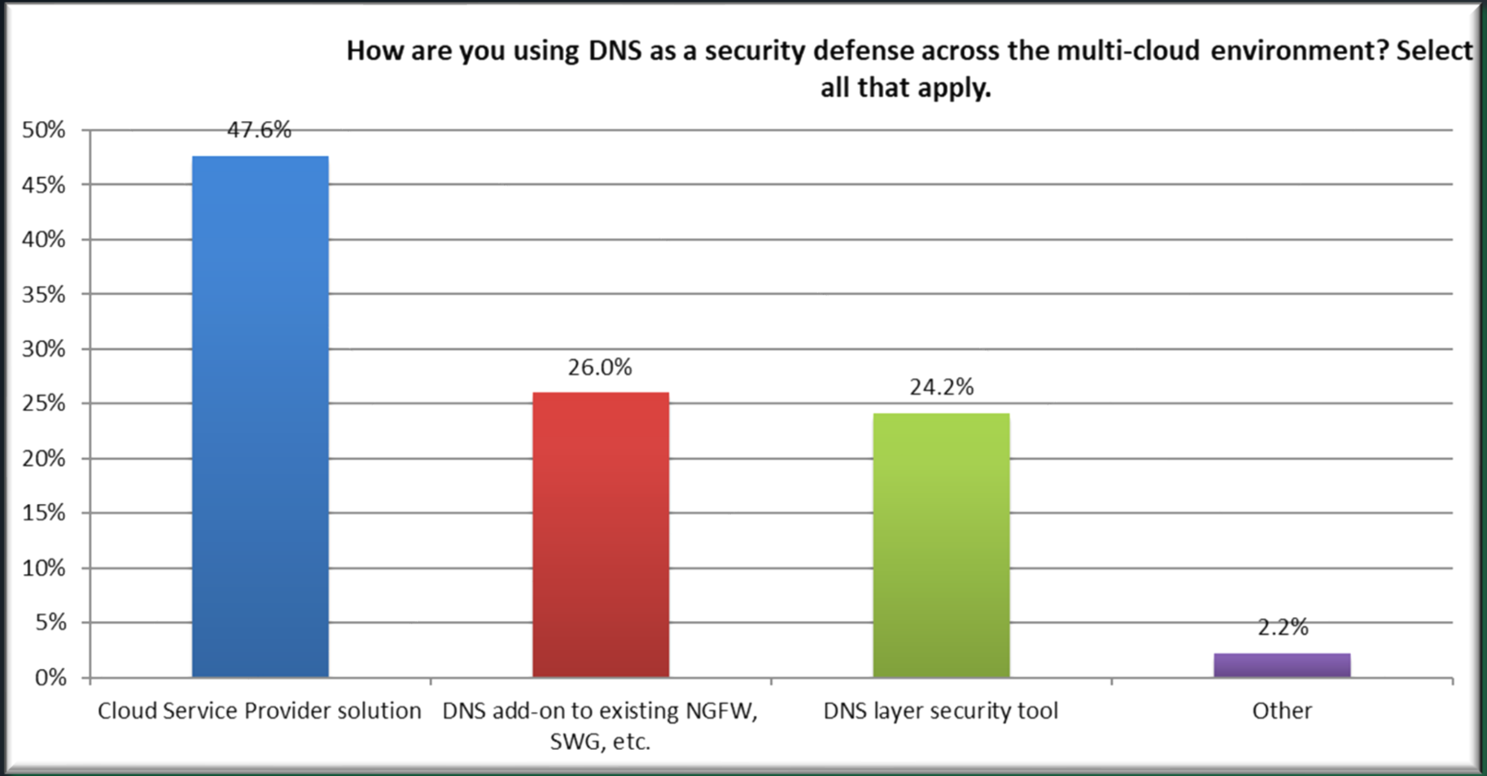
Are You Using DNS for Security in Your Multi-Cloud Environment?





* Source: SANS 2023 Multi-cloud Security Survey

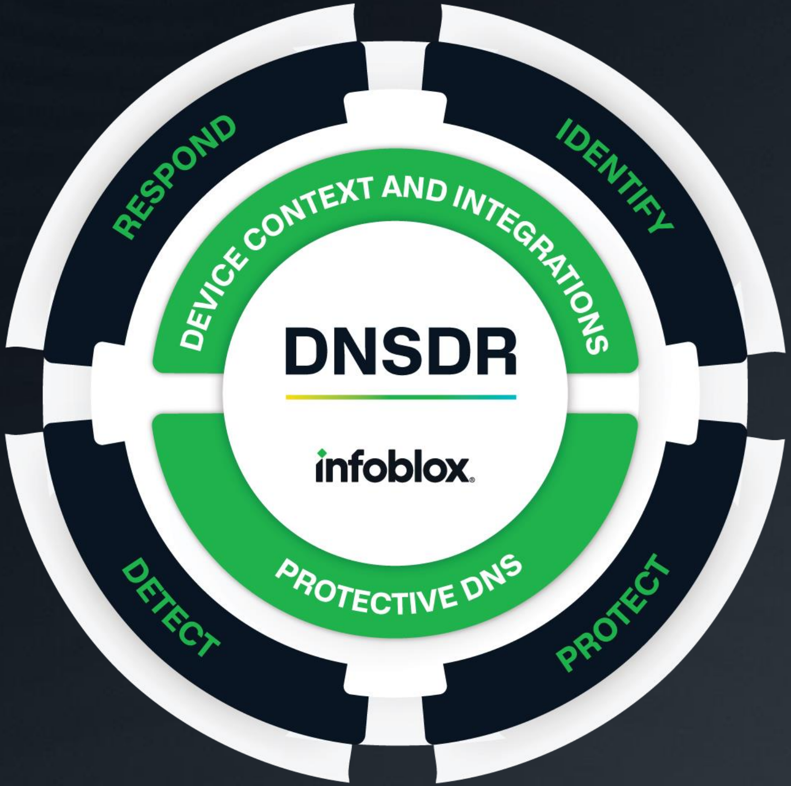
How Are You Using DNS as a Security Defense?



Securing DNS vs PDNS vs DNS DETECTION AND RESPONSE

infoblox.

Securing DNS vs PDNS vs DNS DETECTION AND RESPONSE



PROTECTIVE DNS - The first line of defense

PROTECT

Blocks known Phishing, DGA, C2, Malware, Ransomware, Exfiltration and Suspicious Domains

DETECT

Detects and Blocks unknown malicious DNS with Threat Intelligence and Algorithms, and Application Discovery

DEVICE CONTEXT AND INTEGRATIONS - Automate for better protection

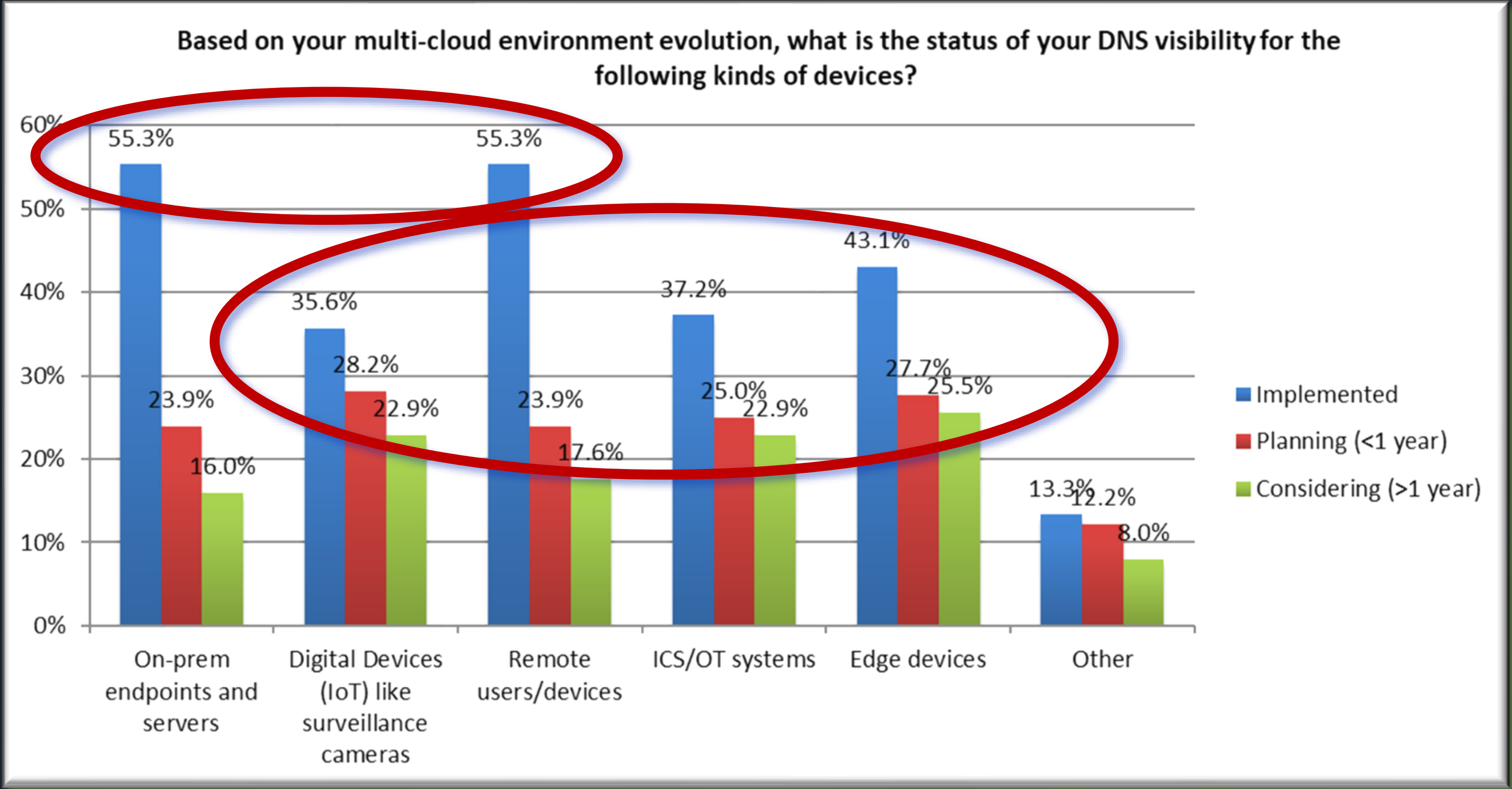
IDENTIFY

Maps DNS queries to user/device activity using IPAM (what device connected to what domain)

RESPOND

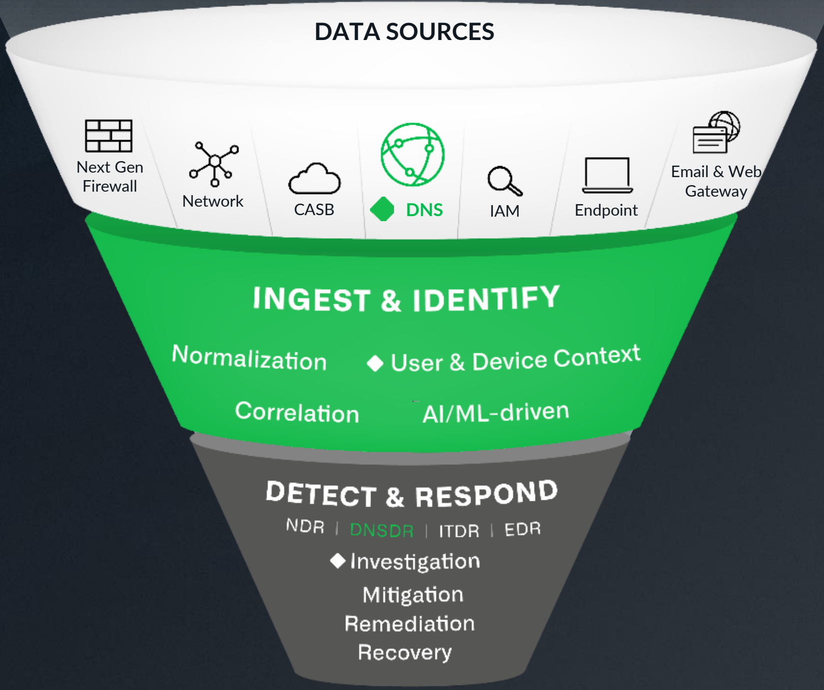
Automates remediation actions via ecosystem integrations and shares of DDI data to SOC (NIOS)

What is the DNS Visibility Status for Different Devices?



infoblox.

DNS Within the XDR ARCHITECTURE



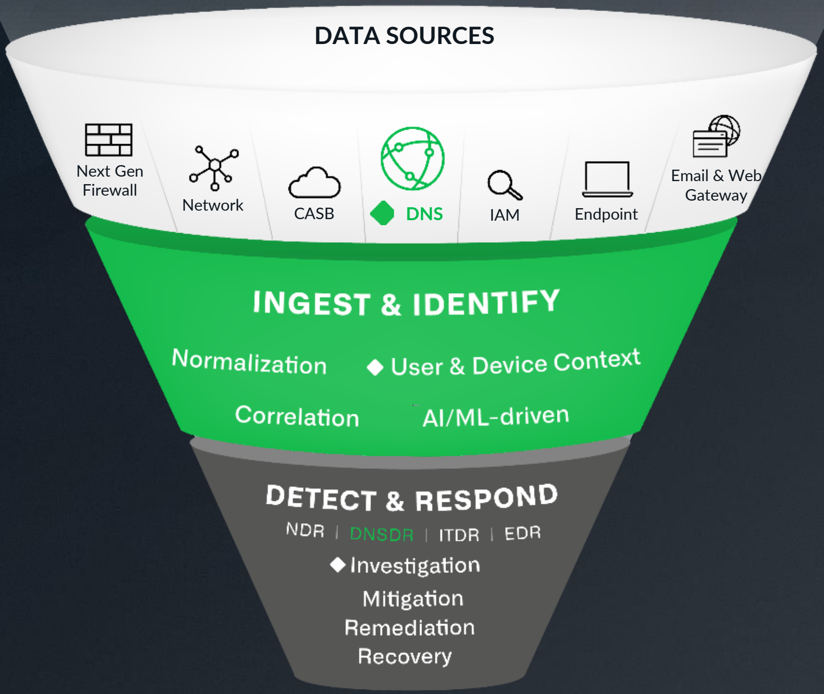
KEY TAKEAWAYS:

2023:

Although most organizations have implemented DNS security solutions, a significant portion remains unprotected or uncertain, highlighting **the need for increased awareness and education.**

infoblox

DNS Within the XDR ARCHITECTURE



DATA SOURCES

Next Gen Firewall | Network | CASB | DNS | IAM | Endpoint | Email & Web Gateway

INGEST & IDENTIFY

Normalization ◆ User & Device Context

Correlation AI/ML-driven

DETECT & RESPOND

NDR | DNSDR | ITDR | EDR

◆ Investigation

Mitigation

Remediation

Recovery

KEY TAKEAWAYS:

2023:

Although most organizations have implemented DNS security solutions, a significant portion remains unprotected or uncertain, highlighting **the need for increased awareness and education.**

2024:

Consider adding DNS security as part of your strategy.

Q&A

ありがとう köszönjük

Cảm ơn धन्यवाद

terima kasih gracias

고마워요 teşekkür ederim

Σας ευχαριστ

Спасибо obrigado

grazie

merci **THANK YOU!** 谢谢

takk

شكرا tack

ขอบคุณ

danke

bedankt kiitos

Panel Discussion 1

Questions or Comments?

Connect with Tamer Salman,
Principal Research Manager

Connect with Oz Wilder
Partner Director of PM

Microsoft

For General Event Discussion:
#discussion

Microsoft Security

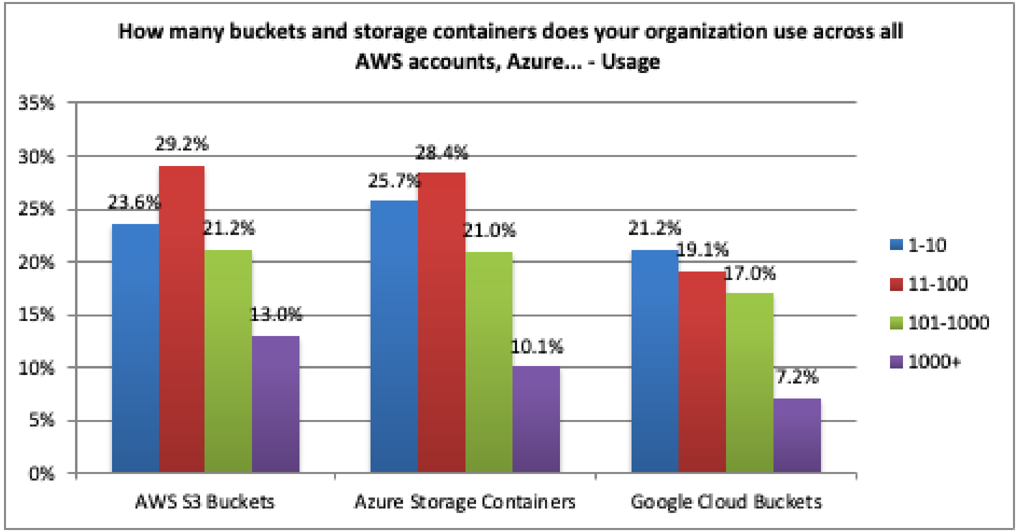
SANS Multicloud Security Defender for Cloud

Tamer Salman, Director of Research

Oz Wilder, Director of Product Defender

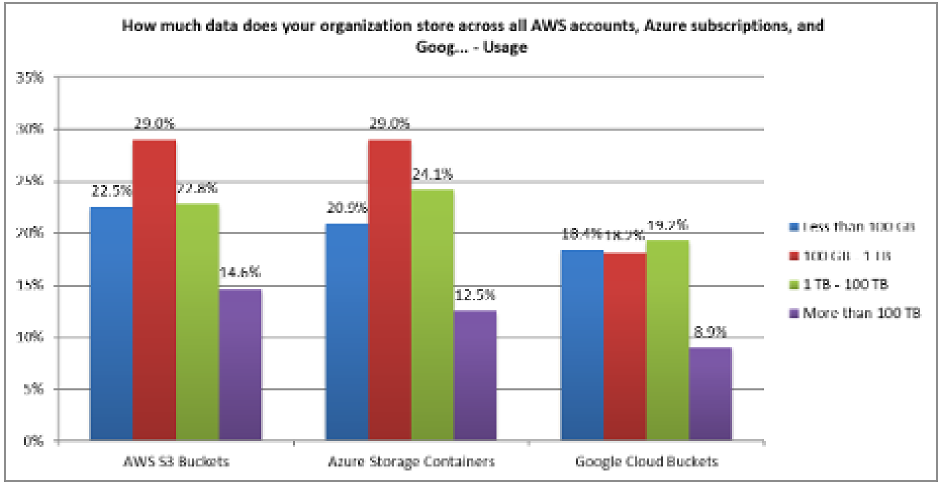
Agenda

1. The rise of storage
2. The challenges with securing AI application
3. Security tools proliferation and lack of skills

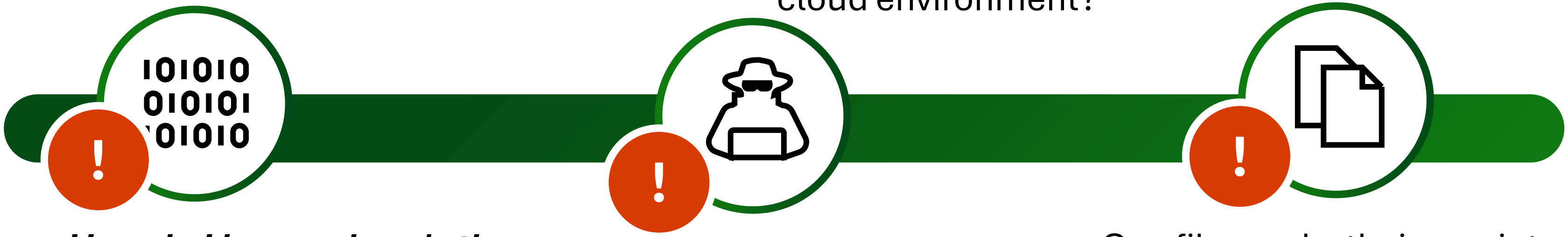


Cloud storage container usage is widespread and growing across all major providers, with AWS and Azure leading the market.

Cloud storage volume is experiencing significant growth across the major providers



Top Challenges



How do I know where's the sensitive data?

Would you know if sensitive data were stolen from your cloud environment?

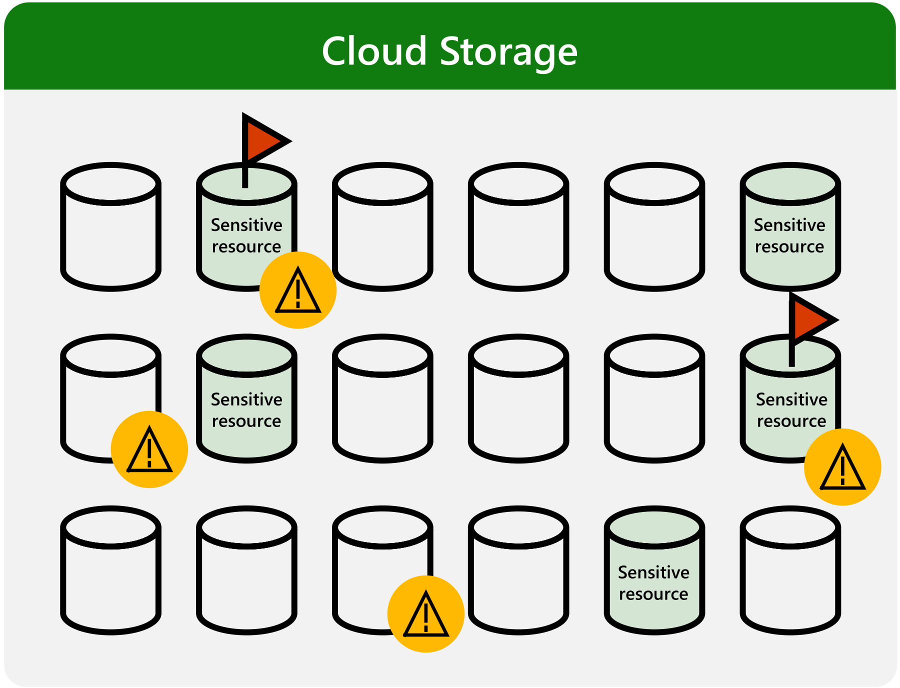
Can files make their way into your organization ***without*** being scanned for malware?

Sensitive data detection

How do I know where's the sensitive data?

Sensitive data detection

- A cloud-native scanning architecture guarantees low-friction onboarding, light scan in economic costs
- Ability to detection sensitive data by different classifications standards (e.g. PII, HIPPA, Financial records)



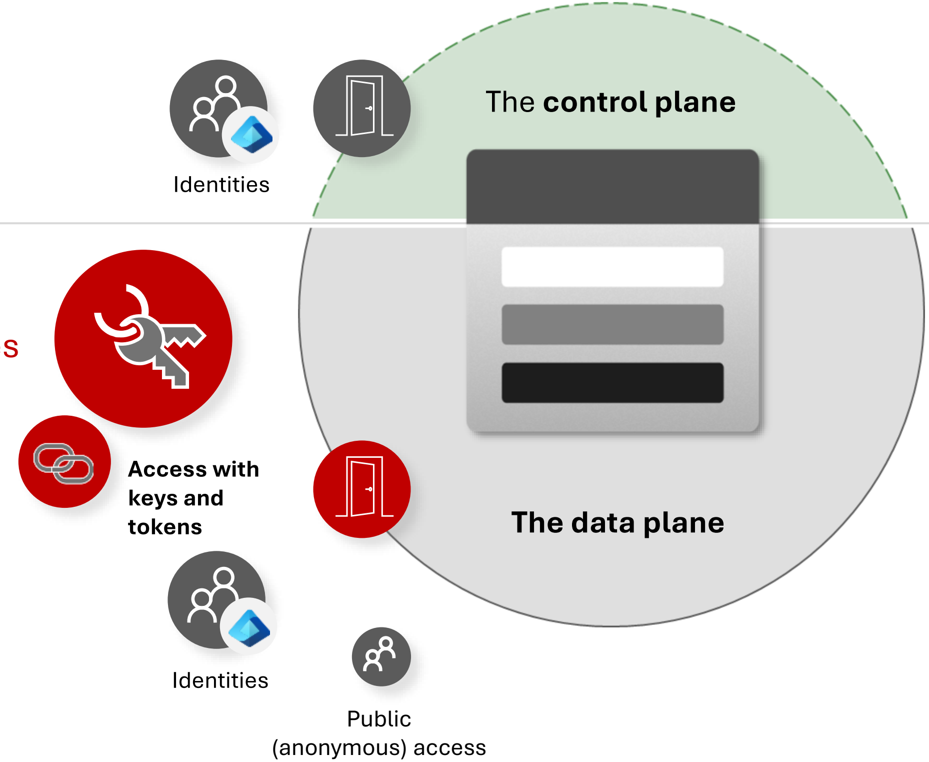
Multiple access options

Would you know if sensitive data were stolen from your cloud environment?

The **control plane**
is the hallway of the cloud where
everyone has an identity

65% Entities without identities
enter the data plane

32% Use authorization to
enter the data plane



Identities

The **control plane**

Access with keys and tokens

The data plane

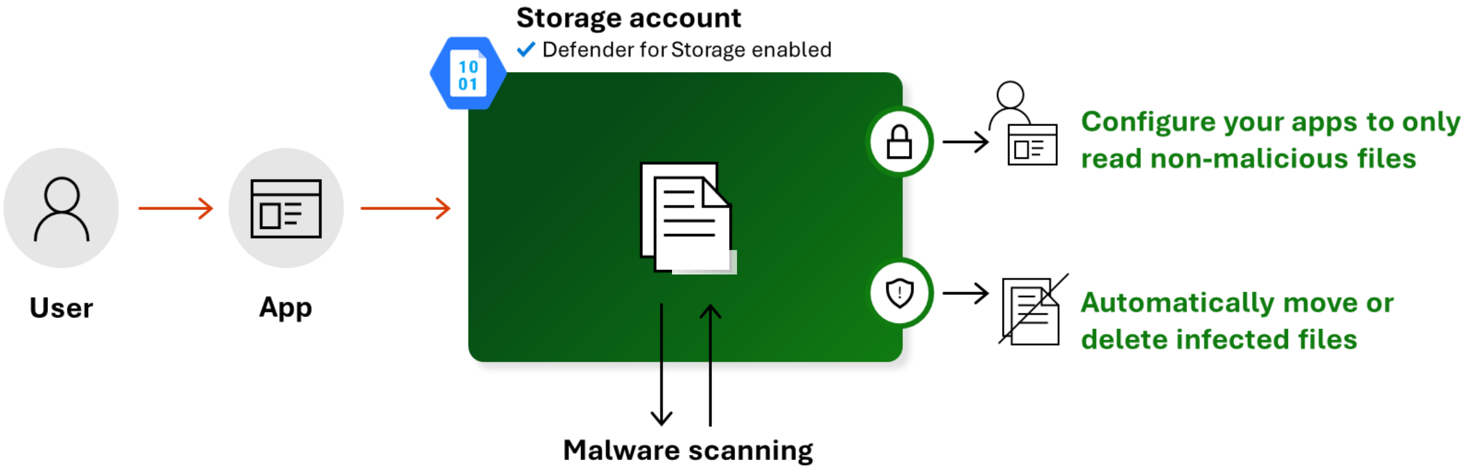
Identities

Public
(anonymous) access

Malware scanning

Can files make their way into your organization ***without*** being scanned for malware?

Near-real-time malware scanning across file types upon content upload

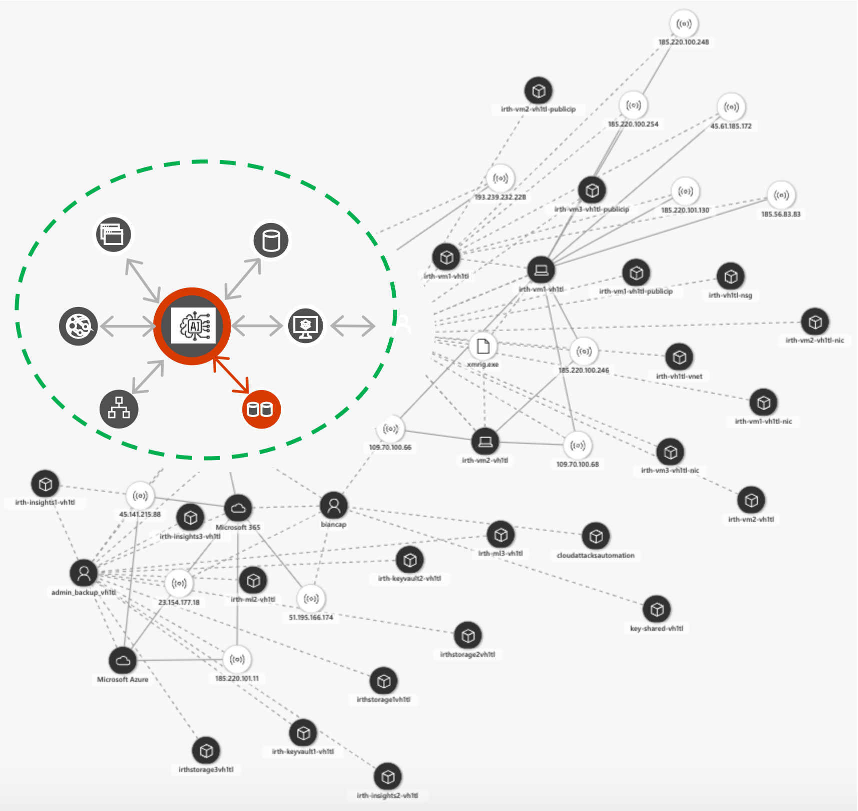

Storage account
✓ Defender for Storage enabled
10
01
User
App
Malware scanning
Configure your apps to only read non-malicious files
Automatically move or delete infected files

__AI adoption__ for multicloud security is __on the rise__, with diverse use cases emerging. Although interest is high, implementation levels vary, and organizations face challenges such as __lack of expertise__ and concerns about effectiveness.

AI based application

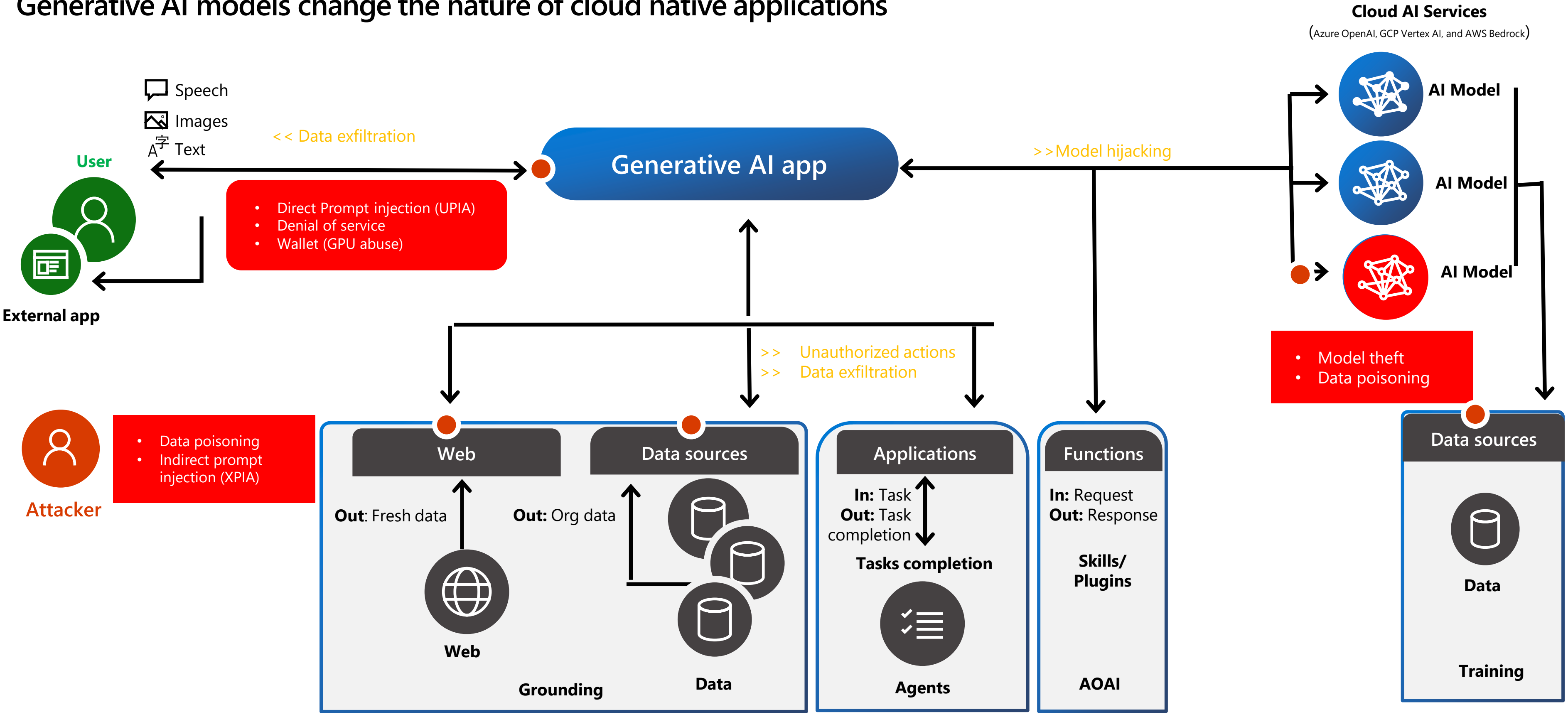
Modern Application / New Challenges

Predictability, Permissions and Scale



Generative-AI threat landscape

Generative AI models change the nature of cloud native applications



Cloud AI Services

(Azure OpenAI, GCP Vertex AI, and AWS Bedrock)

AI Model

AI Model

AI Model

Speech

Images

Text

<< Data exfiltration

User

External app

Generative AI app

>>Model hijacking

- Direct Prompt injection (UPIA)
- Denial of service
- Wallet (GPU abuse)

- Model theft
- Data poisoning

>> Unauthorized actions

>> Data exfiltration

Attacker

- Data poisoning
- Indirect prompt injection (XPIA)

Web

Out: Fresh data

Web

Data sources

Out: Org data

Data

Grounding

Applications

In: Task

Out: Task completion

Tasks completion

Agents

Functions

In: Request

Out: Response

Skills/ Plugins

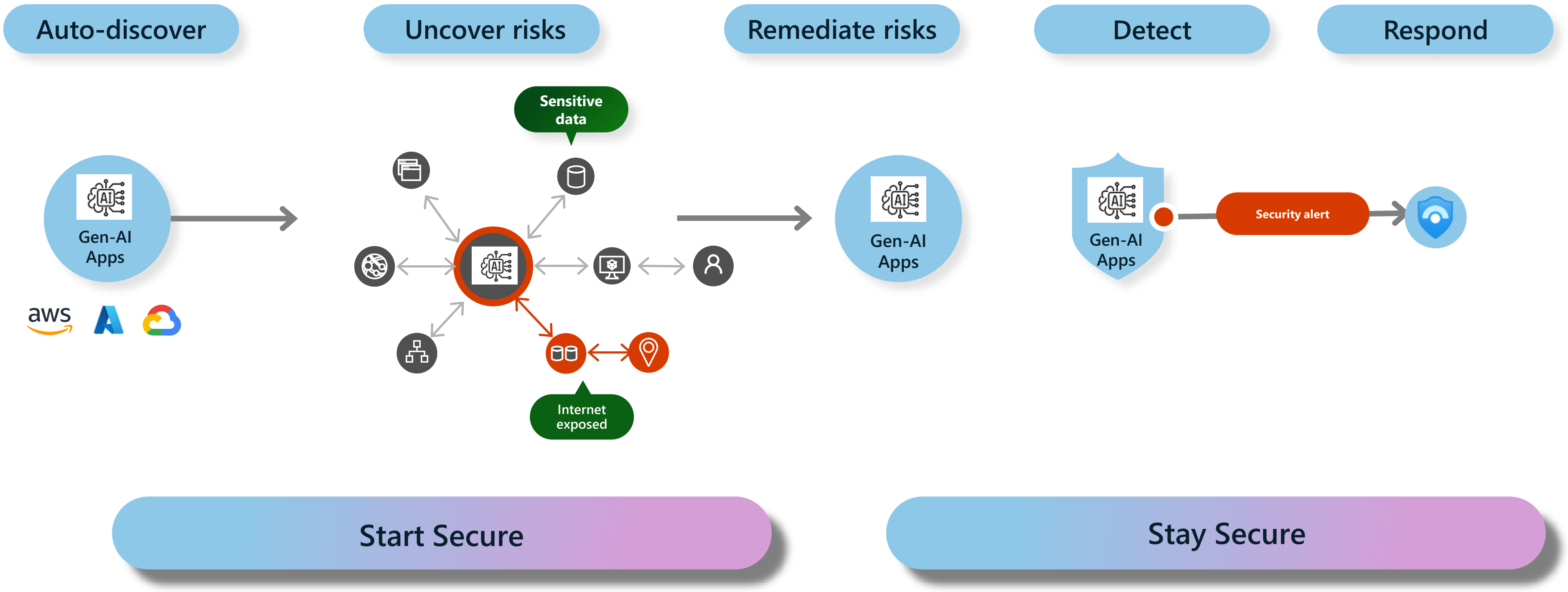
AOAI

Data sources

Data

Training

Secure Gen AI Apps



Auto-discover

Uncover risks

Remediate risks

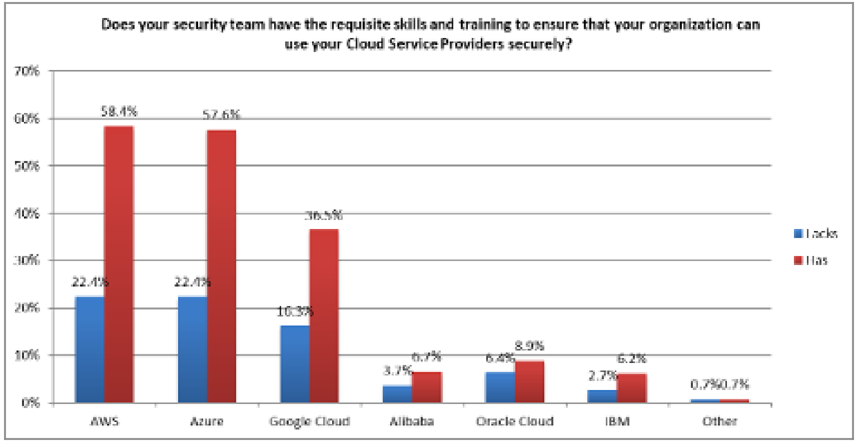
Detect

Respond

Start Secure

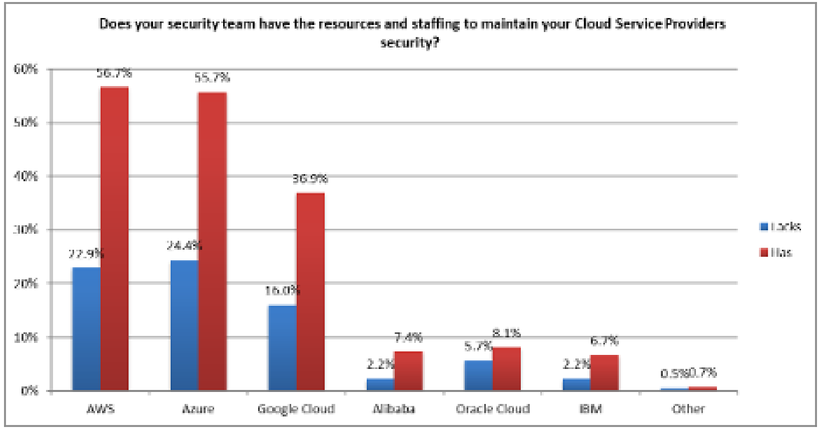
Stay Secure

Disconnected tools -> Disconnected view



Does your security team have the requisite skills and training to ensure that your organization can use your Cloud Service Providers securely?

The survey reveals a mixed perspective on cloud security resources and staffing. (See Figure 17.) Although the majority of organizations believe their teams are adequately equipped, a notable portion report lacking the necessary resources and personnel to maintain robust security measures in their cloud environments.

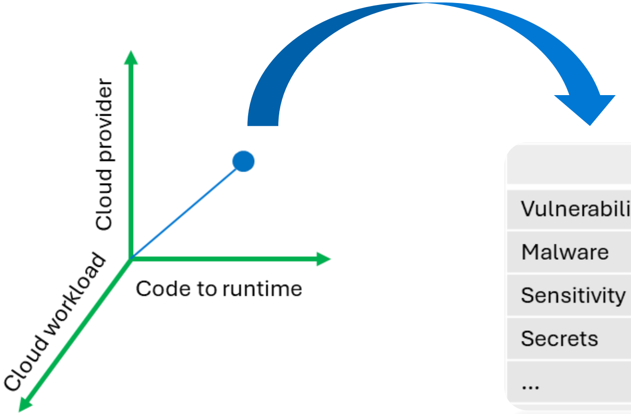


Does your security team have the resources and staffing to maintain your Cloud Service Providers security?

The Versatility of the Cloud; Breaking the Silos

- Virtual machines
- Containers
- Databases
- Cloud Storage
- Websites

...

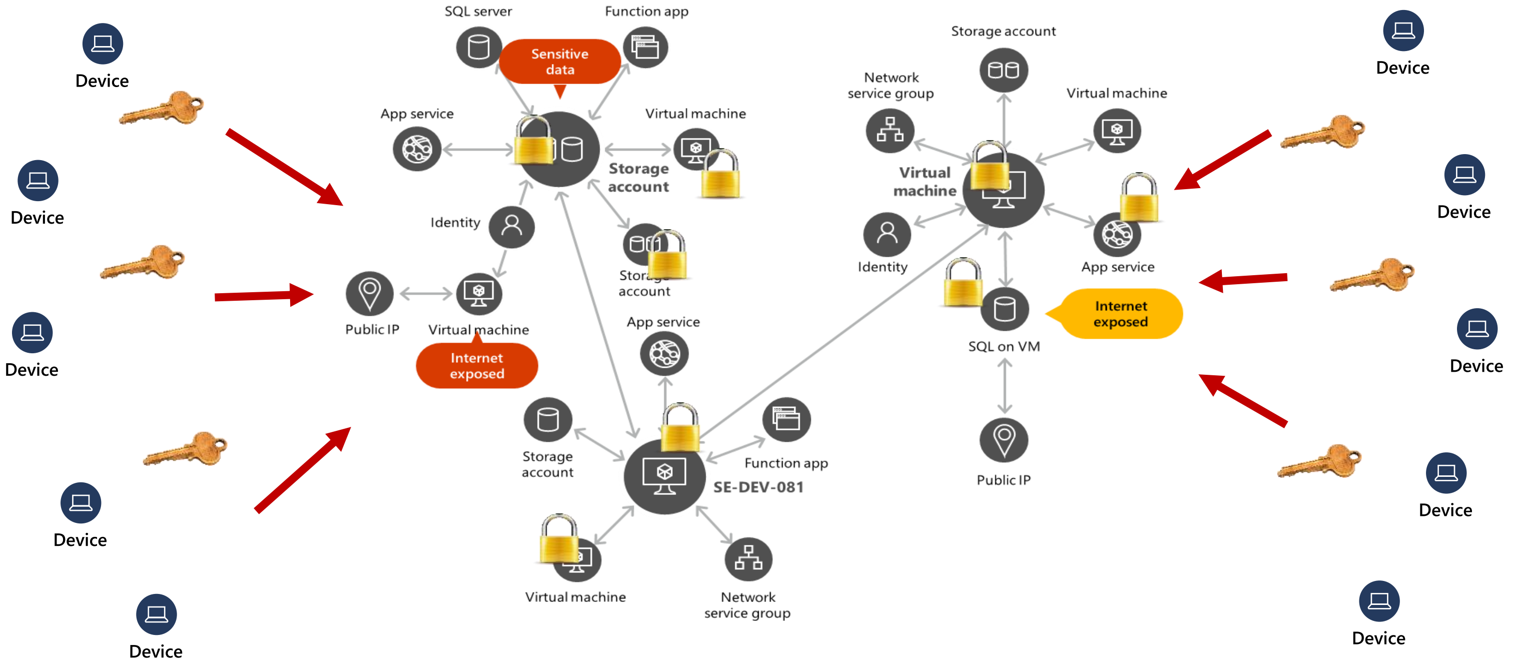


	Virtual machines	Containers	Databases	Cloud Storage	Websites	...
Vulnerability						
Malware						
Sensitivity						
Secrets						
...						

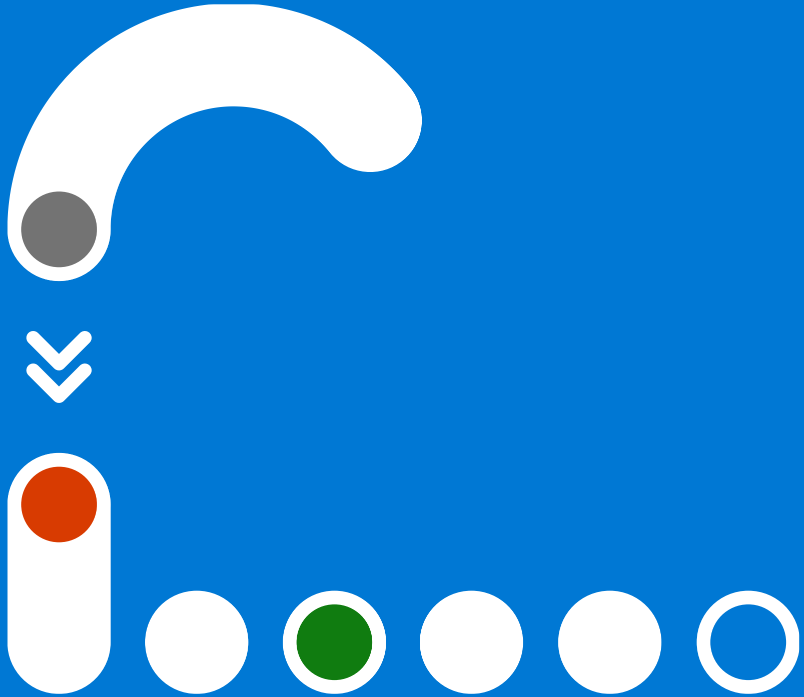
It takes a suite to secure you cloud estate

Vulnerability	Vulnerabilities in code / image repositories	Vulnerabilities in compute resources	
Sensitivity	Sensitive data in code	Sensitive data on disks	Sensitive data in storage/databases
Malware	Malware in code	Malware on machines / models	Malware in storage
Secrets	Secrets in code	Secrets on disks	Secrets in storage/databases

Going full suite; an enterprise look on cloud security



Thank You!



tenable

Questions or Comments?

Connect with,
Product Marketing Manager

For General Event Discussion:
#discussion

SANS 2024 Multi-Cloud Survey Forum

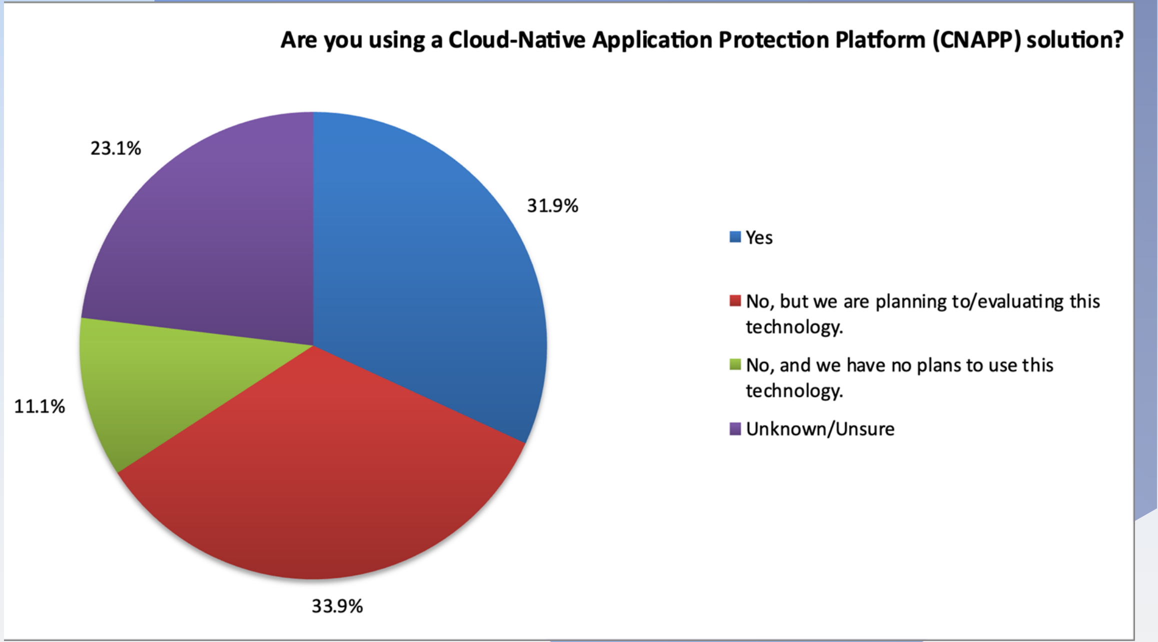
Becoming a cloud security expert with CNAPP

Christina DePinto, Tenable

Survey says …

> “CNAPP is gaining traction in the cloud security landscape, with a combined 65.8% of organizations either using it or actively considering it.”

- SANS 2024 Multi-Cloud Survey

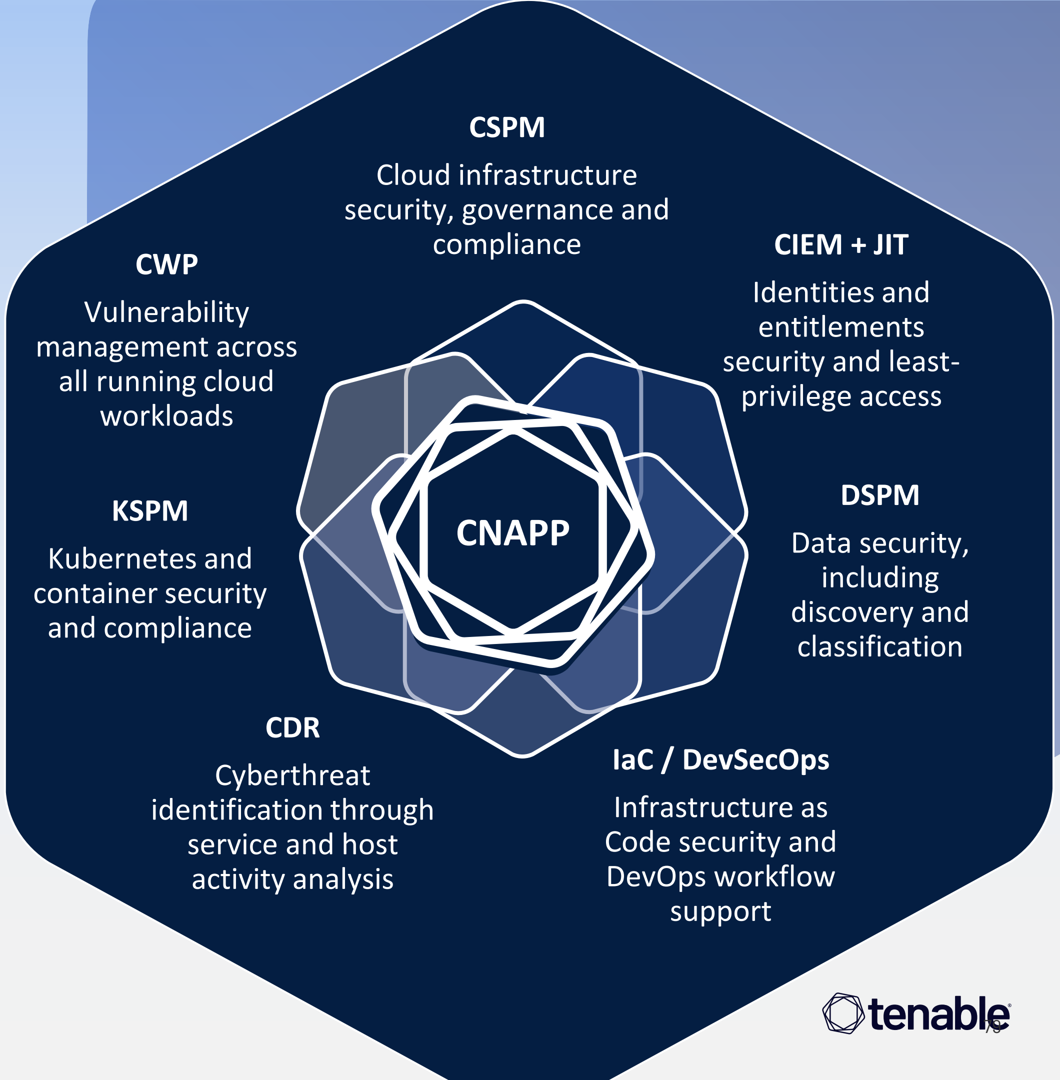


tenable

What is a CNAPP?

A **Cloud Native Application Protection Platform (CNAPP)**consolidates point security tools to assess cloud risks in context.

A CNAPP should analyze all your cloud resources — infrastructure, workloads, data, and identities — to prioritize the most consequential risks across hybrid and multi-cloud environments.



CSPM

Cloud infrastructure security, governance and compliance

CIEM + JIT

Identities and entitlements security and least-privilege access

CWP

Vulnerability management across all running cloud workloads

KSPM

Kubernetes and container security and compliance

CNAPP

DSPM

Data security, including discovery and classification

CDR

Cyberthreat identification through service and host activity analysis

IaC / DevSecOps

Infrastructure as Code security and DevOps workflow support

tenable Cloud Security

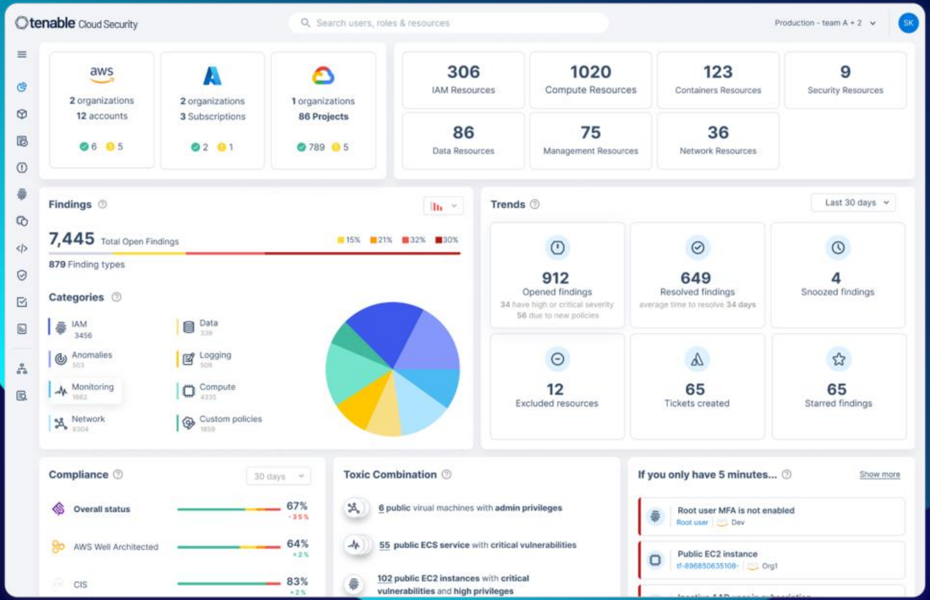
tenable

A CNAPP should help you answer…

#1) What is running in my cloud environment?

#2) How are my cloud resources being accessed?

#3) Where am I at risk? Why is it risky?



tenable Cloud Security

Search users, roles & resources

Production - team A + 2

SK

aws: 2 organizations, 12 accounts — 6, 5

2 organizations, 3 Subscriptions — 2, 1

1 organizations, 86 Projects — 789, 5

306 IAM Resources	1020 Compute Resources	123 Containers Resources	9 Security Resources
86 Data Resources	75 Management Resources	36 Network Resources	

Findings

7,445 Total Open Findings — 15% 21% 32% 30%

879 Finding types

Categories

IAM 3456	Data 339
Anomalies 503	Logging 509
Monitoring 1662	Compute 4335
Network 8304	Custom policies 1859

Trends — Last 30 days

912 Opened findings 34 have high or critical severity 56 due to new policies	649 Resolved findings average time to resolve 34 days	4 Snoozed findings
12 Excluded resources	65 Tickets created	65 Starred findings

Compliance — 30 days

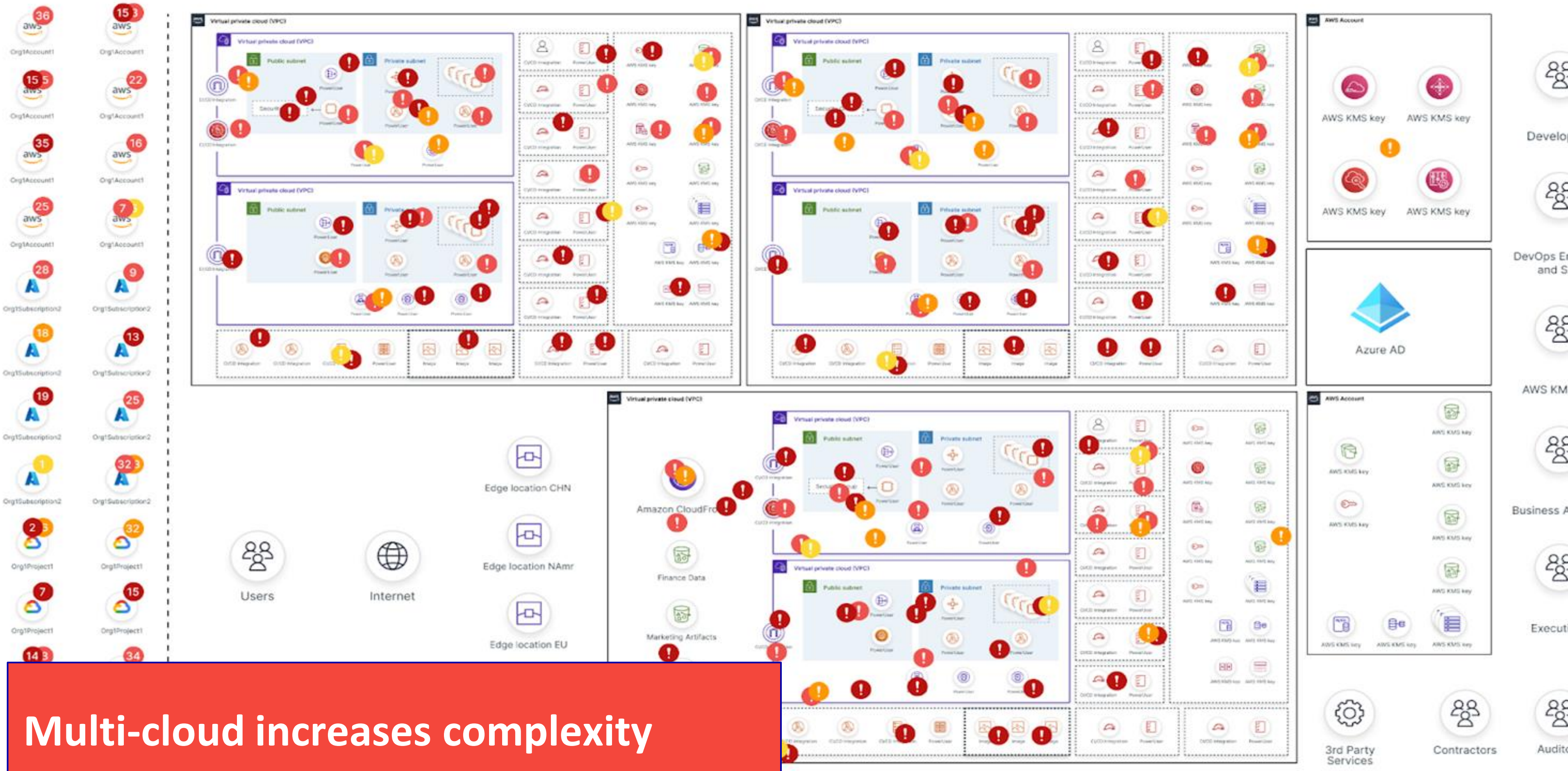
Overall status	67%	-35%
AWS Well Architected	64%	+2%
CIS	83%	+2%

Toxic Combination

- 6 public virual machines with admin privileges
- 55 public ECS service with critical vulnerabilities
- 102 public EC2 instances with critical vulnerabilities and high privileges

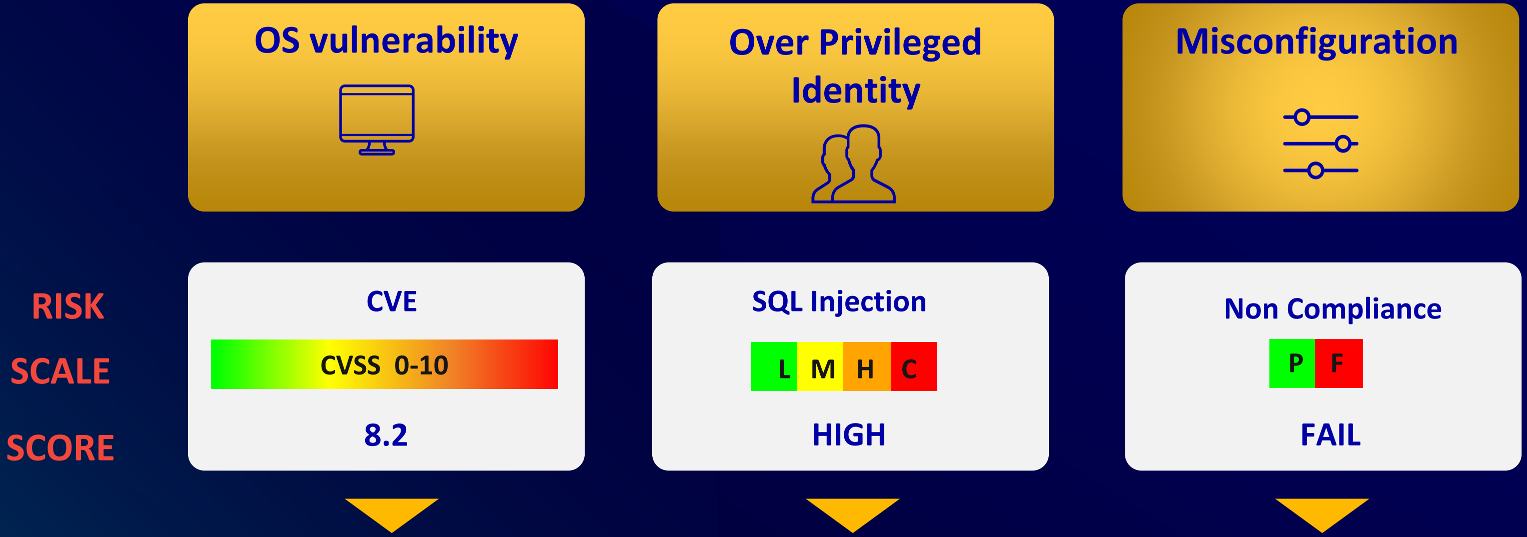
If you only have 5 minutes… — Show more

- Root user MFA is not enabled — Root user | Dev
- Public EC2 instance — tf-896850635108- | Org1



Multi-cloud increases complexity

How do you know what to fix first?



RISK

SCALE

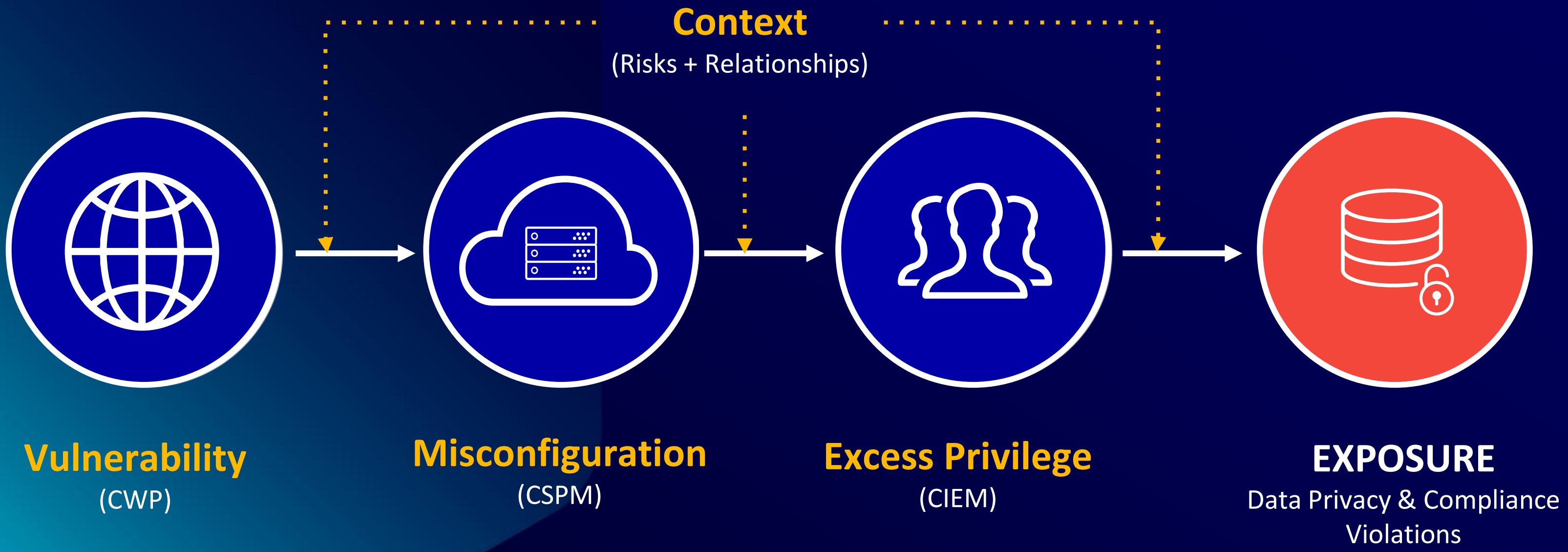
SCORE

OS vulnerability	Over Privileged Identity	Misconfiguration
CVE	SQL Injection	Non Compliance
CVSS 0-10	L M H C	P F
8.2	HIGH	FAIL

What represents a greater risk?

…or who should fix it?

Security starts with business focused visibility



Context

(Risks + Relationships)

Vulnerability

(CWP)

Misconfiguration

(CSPM)

Excess Privilege

(CIEM)

EXPOSURE

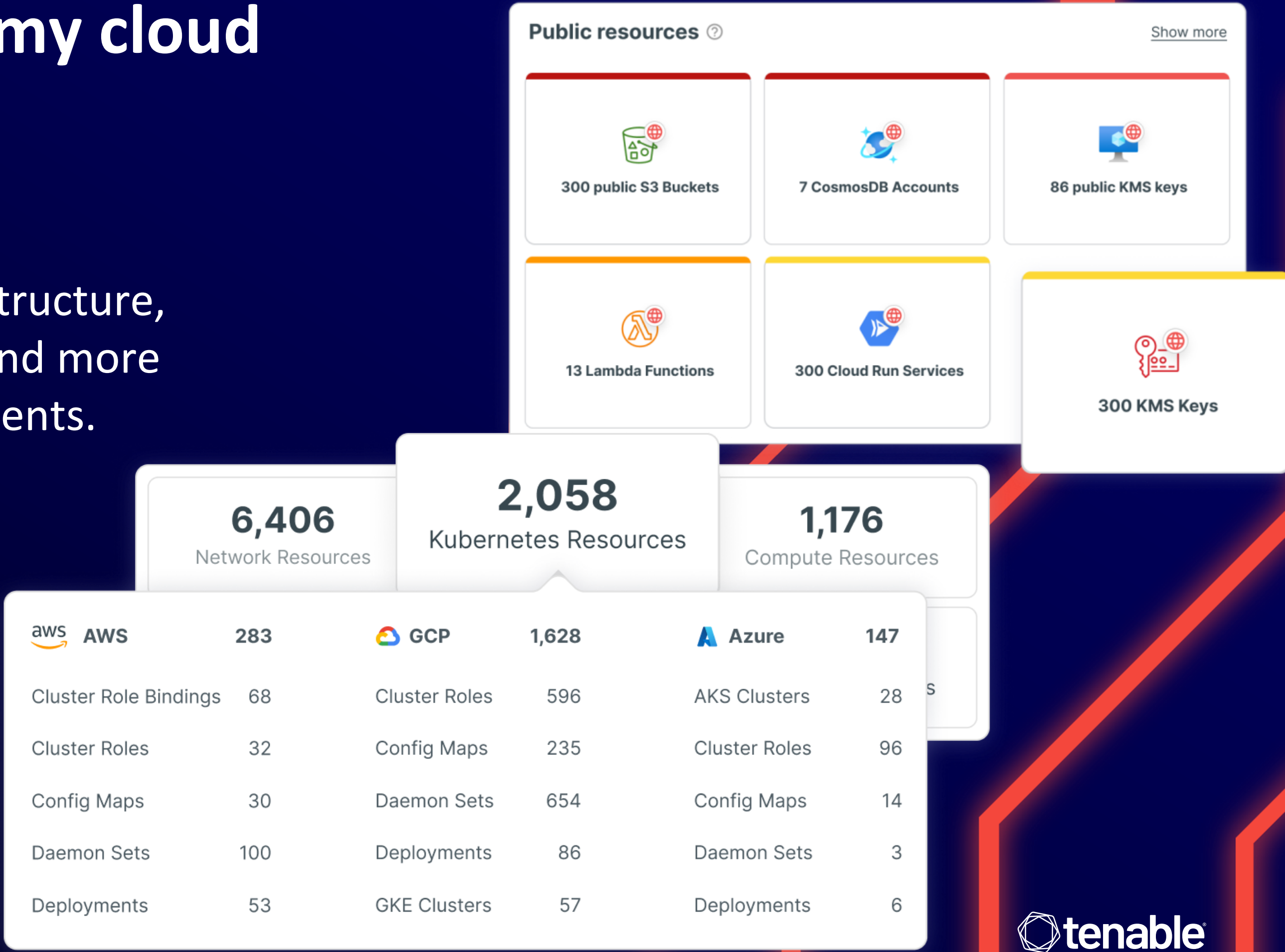
Data Privacy & Compliance Violations

…that breaks down silos and reduces exposure

tenable

What is running in my cloud environment?

Continuously discover infrastructure, workloads, identities, data and more across multi-cloud environments.



Public resources ⓘ Show more

- 300 public S3 Buckets
- 7 CosmosDB Accounts
- 86 public KMS keys
- 13 Lambda Functions
- 300 Cloud Run Services
- 300 KMS Keys

6,406	Network Resources
2,058	Kubernetes Resources
1,176	Compute Resources

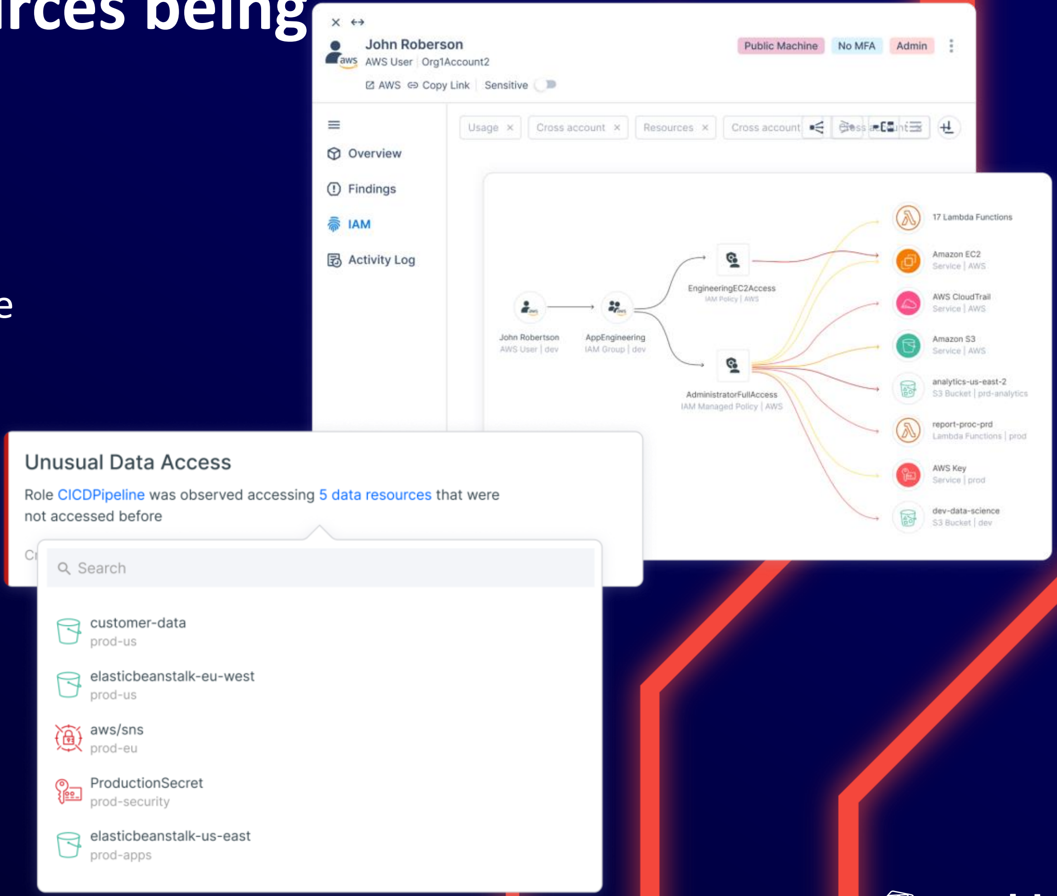
AWS	283	GCP	1,628	Azure	147
Cluster Role Bindings	68	Cluster Roles	596	AKS Clusters	28
Cluster Roles	32	Config Maps	235	Cluster Roles	96
Config Maps	30	Daemon Sets	654	Config Maps	14
Daemon Sets	100	Deployments	86	Daemon Sets	3
Deployments	53	GKE Clusters	57	Deployments	6

tenable

How are my cloud resources being accessed?

Discover who can access what, when, for how long - for all human and service identities.

Gain critical context, such as the relationships between resources and identities.



John Roberson
AWS User | Org1Account2
Public Machine | No MFA | Admin

Unusual Data Access

Role CICDPipeline was observed accessing 5 data resources that were not accessed before

customer-data
prod-us

elasticbeanstalk-eu-west
prod-us

aws/sns
prod-eu

ProductionSecret
prod-security

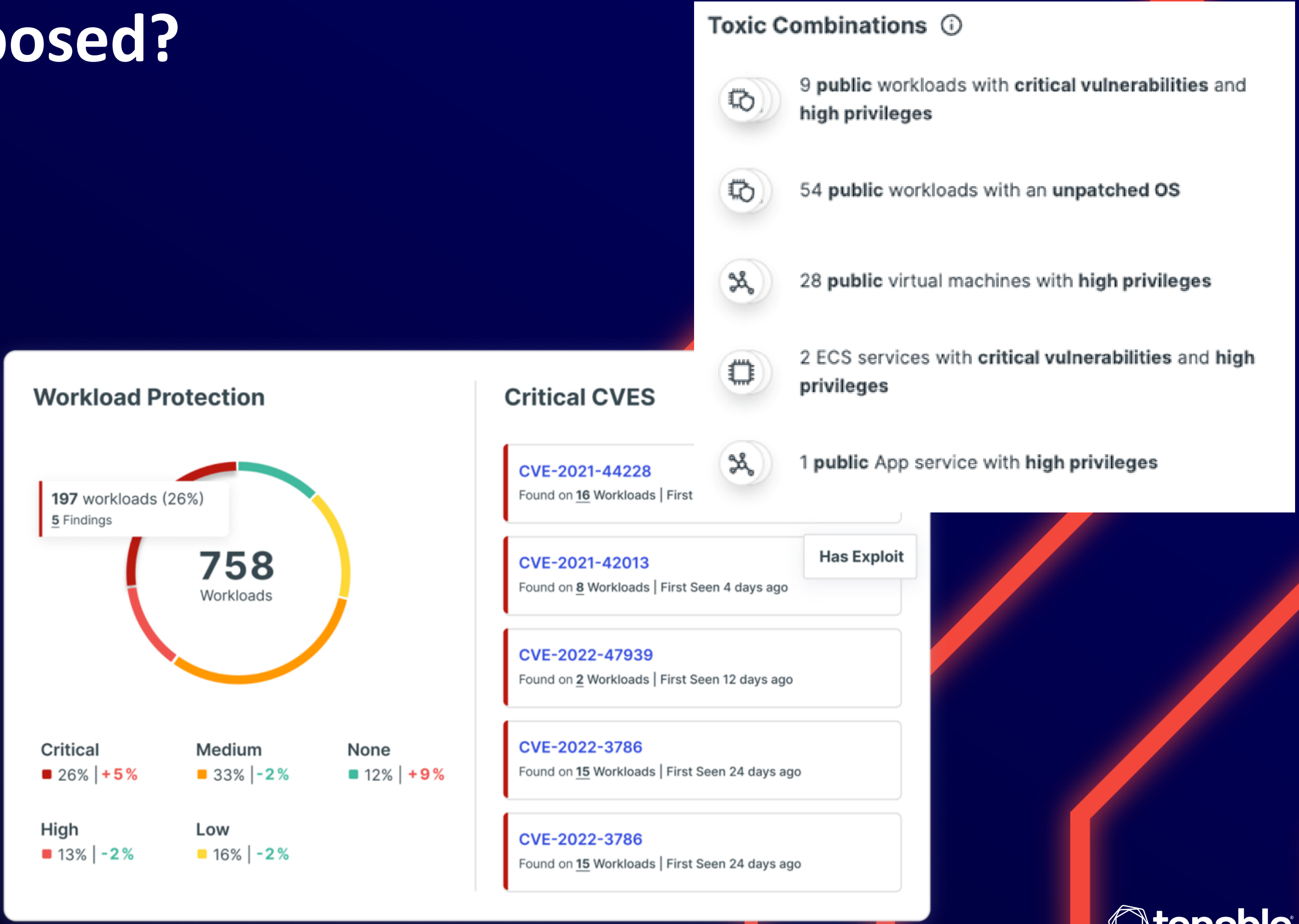
elasticbeanstalk-us-east
prod-apps

tenable

Where am I exposed?
Why?

Prioritize ‘toxic combinations’ of highest risk to your organization.

Get a list of all risks and violations, and detailed data about each.



Toxic Combinations ⓘ

9 **public** workloads with **critical vulnerabilities** and **high privileges**

54 **public** workloads with an **unpatched OS**

28 **public** virtual machines with **high privileges**

2 ECS services with **critical vulnerabilities** and **high privileges**

1 **public** App service with **high privileges**

Workload Protection

197 workloads (26%)
5 Findings

758
Workloads

Critical	Medium	None
🟥 26% | +5%	🟧 33% | -2%	🟩 12% | +9%
High	**Low**	
🟥 13% | -2%	🟨 16% | -2%	

Critical CVES

CVE-2021-44228
Found on 16 Workloads | First

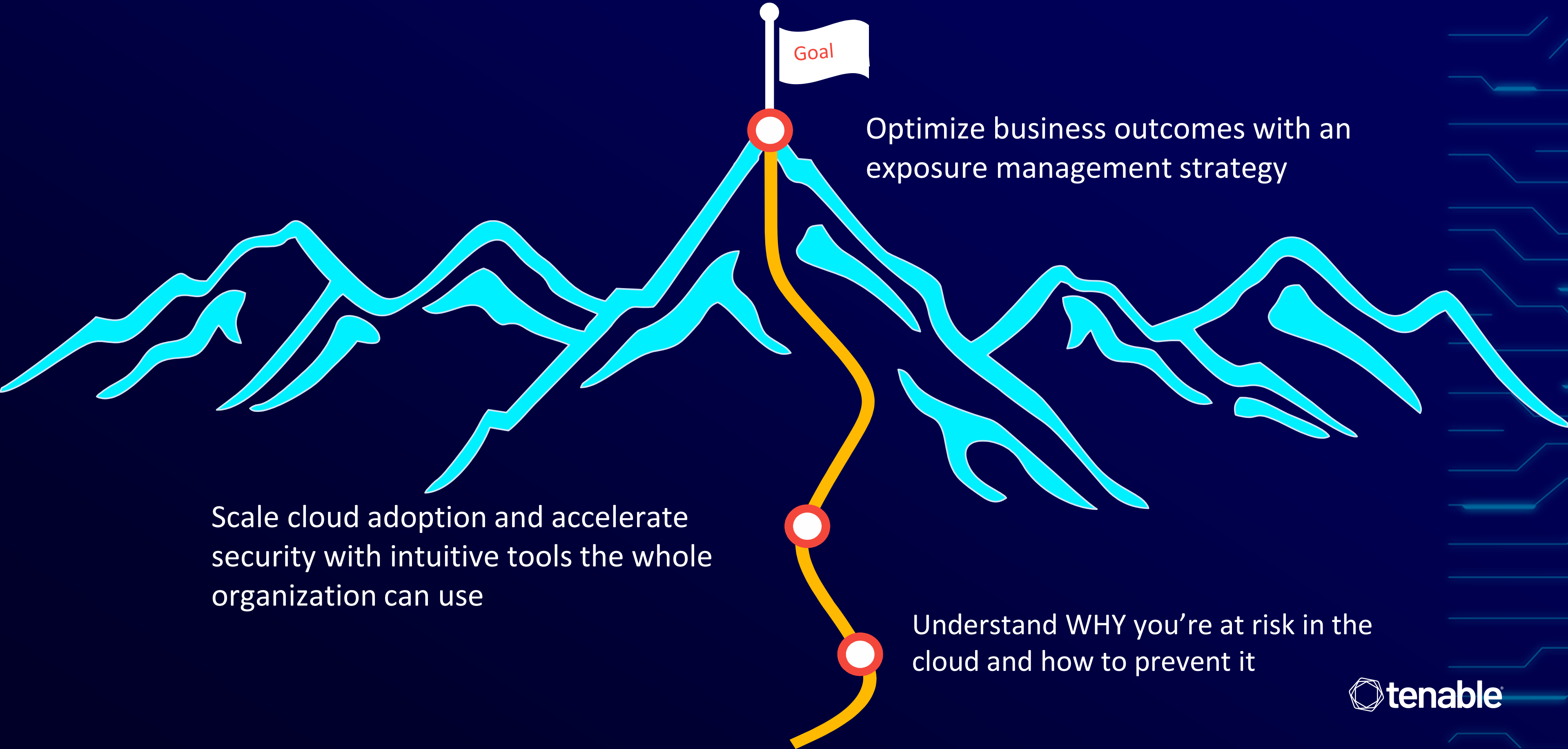
CVE-2021-42013 — Has Exploit
Found on 8 Workloads | First Seen 4 days ago

CVE-2022-47939
Found on 2 Workloads | First Seen 12 days ago

CVE-2022-3786
Found on 15 Workloads | First Seen 24 days ago

CVE-2022-3786
Found on 15 Workloads | First Seen 24 days ago

Scaling cloud adoption and security with CNAPP



Optimize business outcomes with an exposure management strategy

Scale cloud adoption and accelerate security with intuitive tools the whole organization can use

Understand WHY you're at risk in the cloud and how to prevent it

tenable

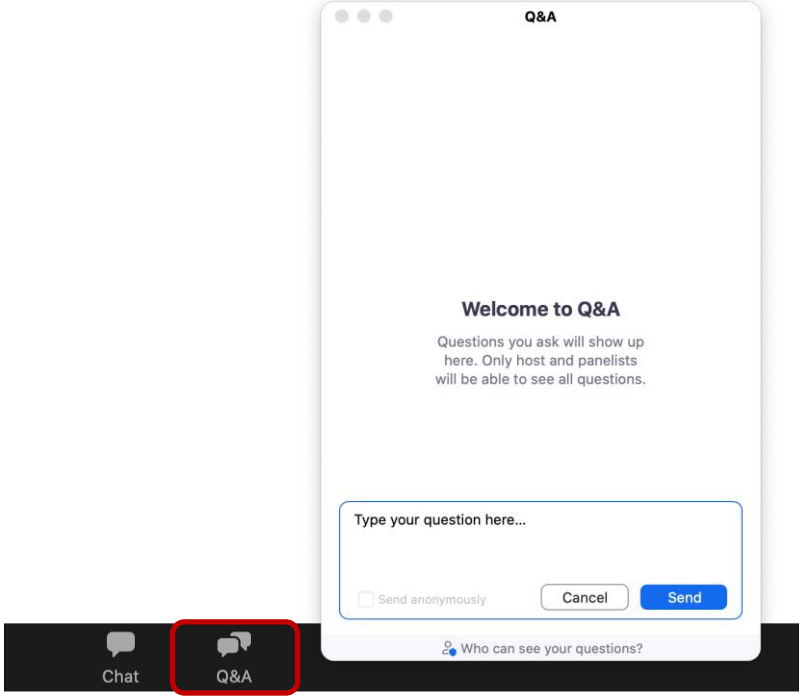
tenable®

Panel Discussion 2

Q&A

Please use **Zoom’s** Q&A window to submit questions to our presenters.

Type your question, tell us if it’s for a specific presenter, and then click Send.



Q&A

Welcome to Q&A

Questions you ask will show up here. Only host and panelists will be able to see all questions.

Type your question here...

Acknowledgments

Thanks to our sponsors:

corelight FORTINET infoblox
Microsoft tenable

To our special guests: Christina DePinto, Bob Hansmann, Ashish Malpani,
Tamer Salman, Aidan Walden, Oz Wilder

And to our attendees, thank you for joining us today!