

The background features a dark blue gradient with large, overlapping, semi-transparent shapes in shades of purple, pink, and orange, creating a modern, abstract design.

AWS re:Invent

NOV. 27 – DEC. 1, 2023 | LAS VEGAS, NV

SEC229-S

SPONSORED BY CENTER FOR INTERNET SECURITY

Securely configure your AWS environments with CIS & Qualys

Mia LaVada

Product Manager, CIS Benchmarks and Cloud Center for Internet Security (CIS)

Nayeem Islam

Vice President, Product Management Qualys

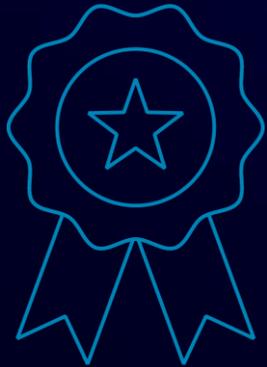


Agenda

- About CIS
- Why secure configurations are key
- CIS Benchmarks
- Key market trends in cloud security
- Challenges in cloud security
- Cloud misconfigurations
- Cloud security posture management

About the Center for Internet Security

Creating confidence in the connected world



Independent
and trusted



Proven and
effective



Collaborative



Operational
expertise



Sustainable

Secure configurations are key



74% of breaches include the human element

- Either via error, privilege misuse, use of stolen credentials, or social engineering

Source: 2023 Verizon DBIR

Breaches caused by cloud misconfigurations

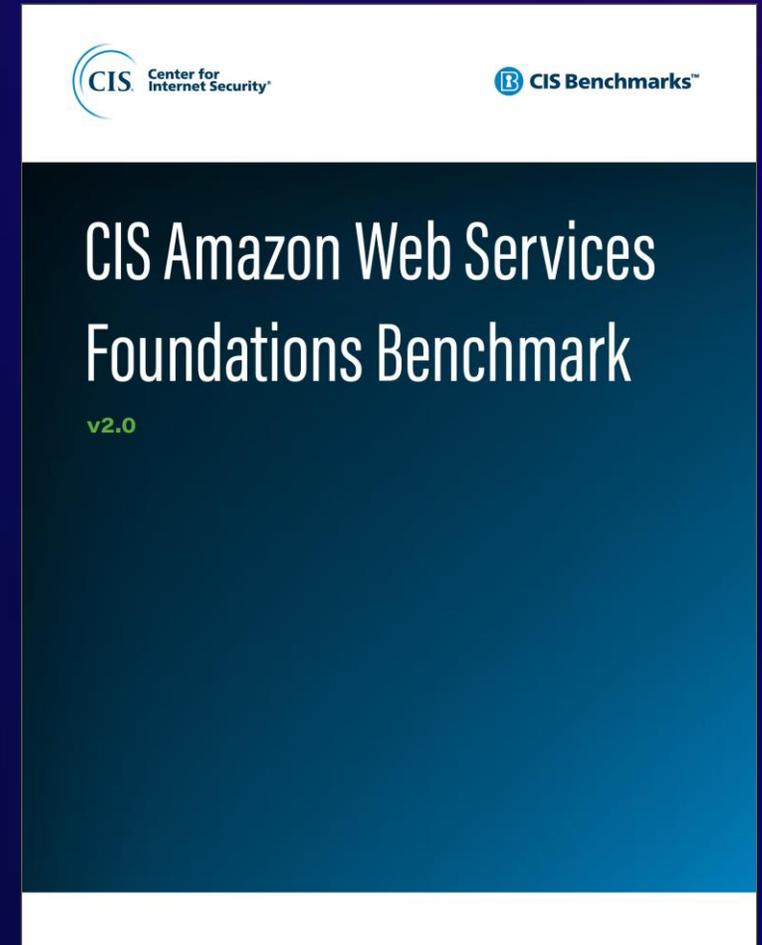
- Took 244 days to identify and contain
- Cost an average of \$4.14M

Source: 2022 IBM Security Cost of a Data Breach Report

CIS Benchmarks

Consensus-developed secure configuration guidelines

- 100+ CIS Benchmarks
- Covering 25+ vendor product families
 - Operating systems, server software, cloud providers, network devices, desktop software
- Recognized by industry frameworks
 - FISMA, FedRAMP, PCI DSS
- Community developed
 - CIS members, subject matter experts, security community experts, and technology vendors
- Provide audit and remediation procedures



How are CIS Benchmarks available?

- CIS Benchmarks PDFs are available for free, noncommercial use
 - <https://www.cisecurity.org/cis-benchmarks>
- CIS SecureSuite Membership
 - Machine-readable formats of CIS Benchmarks
 - CIS Configuration Assessment Tool, CIS-CAT Pro
 - Multiple tiers including End User and Commercial Tier (Product Vendor)
 - **Qualys** is one of the CIS SecureSuite Product Vendor Members

Qualys TotalCloud (CNAPP)

Reducing risk through unified vulnerability, threat, and posture management, from development to runtime

What we see as key market trends

Looking ahead

Posture (CSPM), workload protection (CWPP),
threat detection (CDR), container security (CS)
Can we extend cloud security with enterprise
security function?

Convergence of
cloud security



Get more
security



End-to-end security through integrated
"mesh" of use cases, intelligence, and
automation
How can I get integrated actionable view?

Many reports but CIO &
board need a view on
cyber risk status?

Board-level risk
communication



Too many
vulnerabilities,
misconfigurations,
patches, and alerts
What is my real risk?

Risk-based
prioritization



ROI-driven
consolidation



Too many agents and tools,
manual cost
How can I get better ROI
from current investments?

Key market trends



What we see as key market trends

Looking ahead

Posture (CSPM), workload protection (CWPP),
threat detection (CDR), container security (CS)
**Can we extend cloud security with enterprise
security function?**

**Convergence of
cloud security**



Key market trends

Qualys TotalCloud

A comprehensive
CNAPP solution

Reducing risk
through unified
vulnerability, threat,
and posture
management, from
development to
runtime



TotalCloud

Cloud-native
application
protection platform
(CNAPP)



Cloud security posture management (CSPM)

Inventory of public cloud resources; detection and remediation of misconfigurations and nonstandard deployments



Infrastructure as code (IaC) security

Protects infrastructure by scanning IaC code for misconfigurations and nonstandard deployments before it is deployed



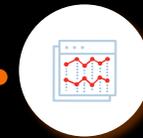
Cloud workload protection (CWP)

Scanning for vulnerabilities in the cloud environment
(VMDR with FlexScan)



Cloud detection and response (CDR)

Continuous real-time protection of the multicloud environment against active exploitation, malware, and unknown threats



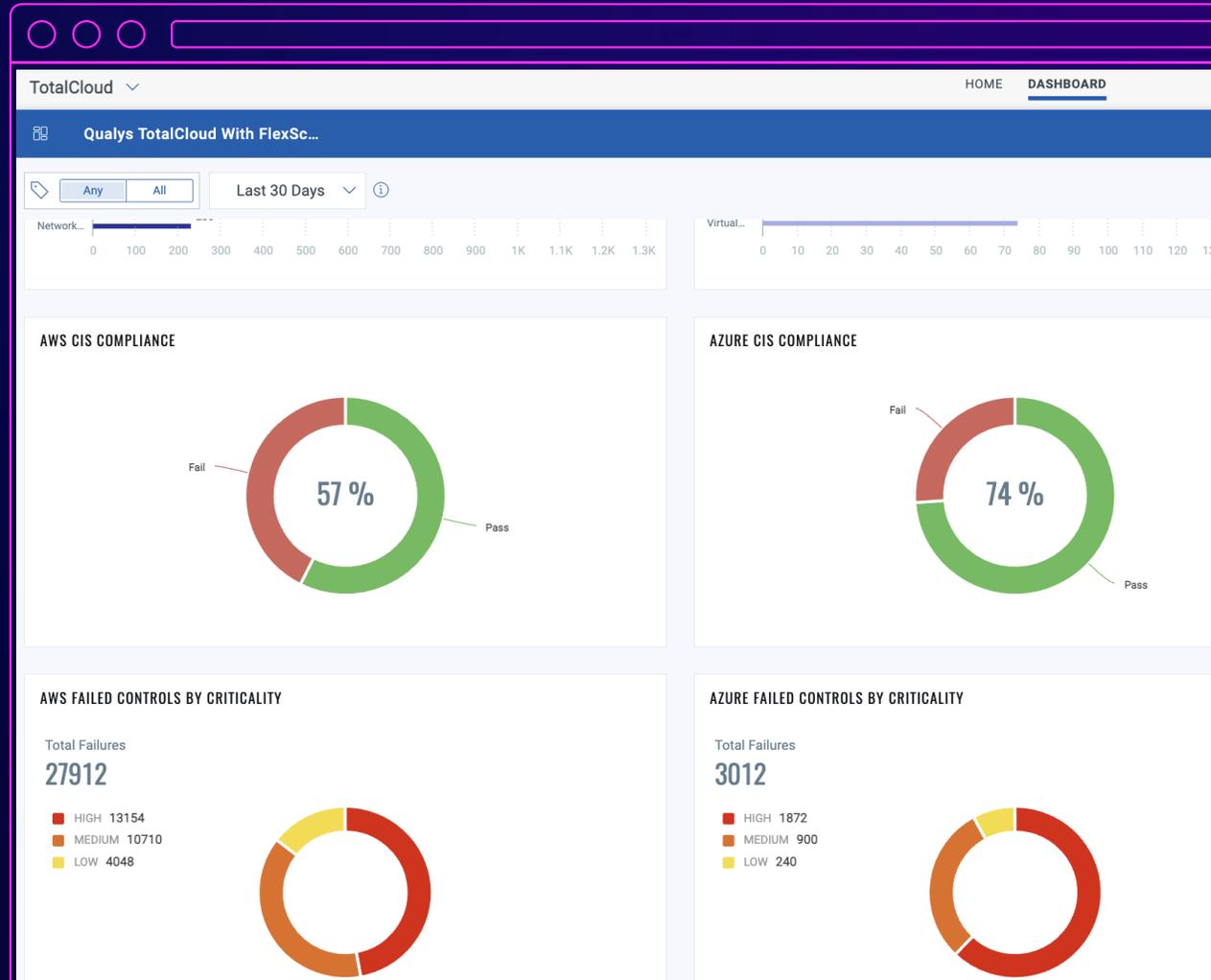
Kubernetes & container security (KCS)

Discover, track, and continuously secure containers – from build to runtime

Cloud security posture management

Comprehensive inventory of your public cloud workloads and infrastructure

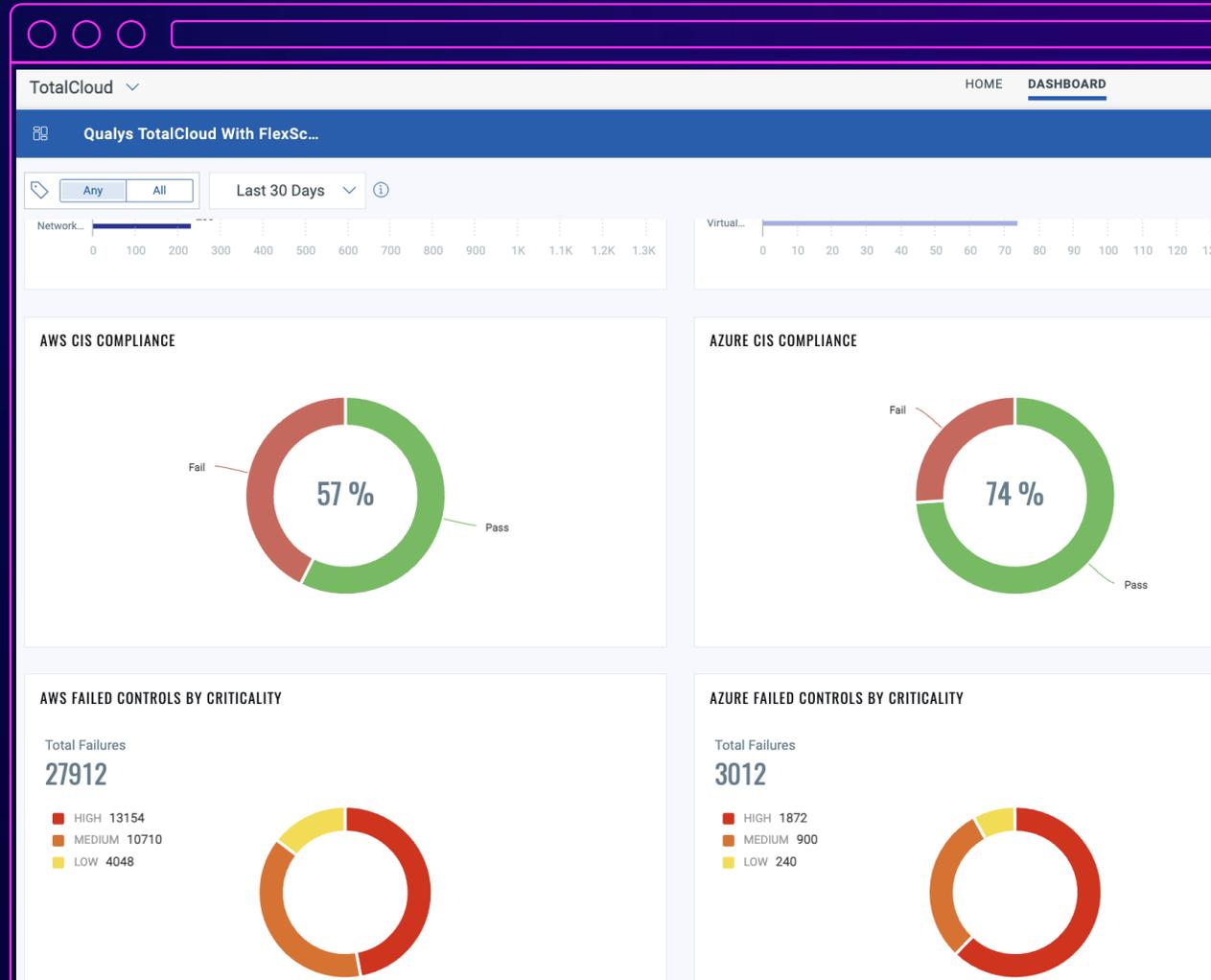
- Identify and remediate misconfiguration across 100% of your cloud assets
- 1000+ out-of-box controls, including Qualys best practices and CIS standards
- Supports 30+ compliance mandates such as PCI DSS and HIPAA and complete coverage of CIS benchmarks
- Automatically alert, ticket, or remediate misconfigurations
- One-click remediation for many high-visibility controls



CIS Benchmarks

<https://www.cisecurity.org/partner/qualys>

- CIS Amazon Web Services Foundations Benchmark v1.5.0, Level 1
- CIS Amazon Web Services Foundations Benchmark v1.5.0, Level 2
- AWS Identity and Access Management (IAM), Amazon S3, Amazon EC2



CIS Benchmarks

- Wide coverage of CIS policies and beyond

- Amazon Linux 2
- Amazon Linux 2023
- Amazon Linux AMI
- Amazon RDS

- RDS assessment via native data collection

The screenshot displays the Qualys Cloud Platform Policy Compliance dashboard. The main view shows four compliance metrics for 'PCD_Policy Compliance' over the last 30 days:

- OVERALL COMPLIANCE:** Total Count 606K, 60.01% Pass (363K), 232K Fail, 10.3K Error.
- OVERALL COMPLIANCE FOR DATABASE:** Total Count 4.04K, 73.97% Pass (2.99K), 1.02K Fail, 35 Error.
- OVERALL COMPLIANCE FOR OS:** Total Count 591K, 60.62% Pass (358K), 223K Fail, 10.3K Error.
- OVERALL COMPLIANCE FOR MIDDLEWARE:** Total Count 174, 67.82% Pass, Fail, Error counts not fully visible.

An inset window titled 'Create a New Policy' is open, showing a 'Policy from Library' section. It lists 21 policies, including:

- CIS Benchmark for Microsoft SQL Server 2019, v1.2.0 [Automated and Manual, Level 1 and Level 2] - AWS RDS]
- CIS Benchmark for Microsoft SQL Server 2019, v1.2.0 [Automated and Manual, Level 1 and Level 2] - Database Engine and Level 1 - AWS RDS]
- CIS Benchmark for Amazon Linux 2, v2.0.0 [Automated and Manual, Level 1 and Level 2]

The 'Technologies' list on the left includes Amazon Linux 2 AMI, Amazon Linux 2023, and Amazon Linux AMI, all of which are checked.

Thank you!

Mia LaVada

Mia.Lavada@cisecurity.org

Nayeem Islam

Nislam@qualys.com



Please complete the session survey in the mobile app

