

CISO **New Zealand**

# Agentic AI in Action: Risk Reduction Through Automation



**Joanne McKenzie**

Senior Technical Account Manager  
Qualys

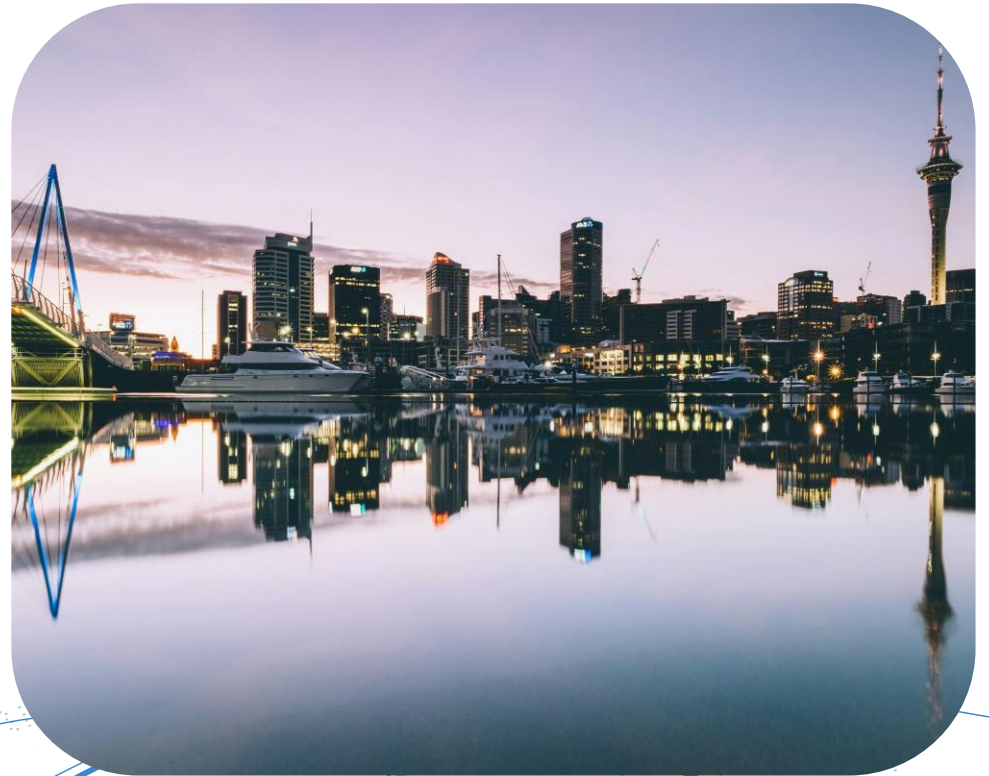


Photo by [Dan Freeman](#) on [Unsplash](#)

# Agenda

**01**

Importance of accurate Asset Inventory

**02**

Aggregation and Prioritisation of Risk

**03**

AI Powered Patch Reliability Scoring for Automated Patching

**04**

Agentic AI Risk Reduction

**05**

GRC Executive Reporting

**06**

Summary

# Unified Asset Discovery & Inventory

## Known Asset Sources

### Qualys Native Sensors



### Qualys 3rd Party Connectors



### CMDB Connectors



## Unknown Assets

## Known Assets

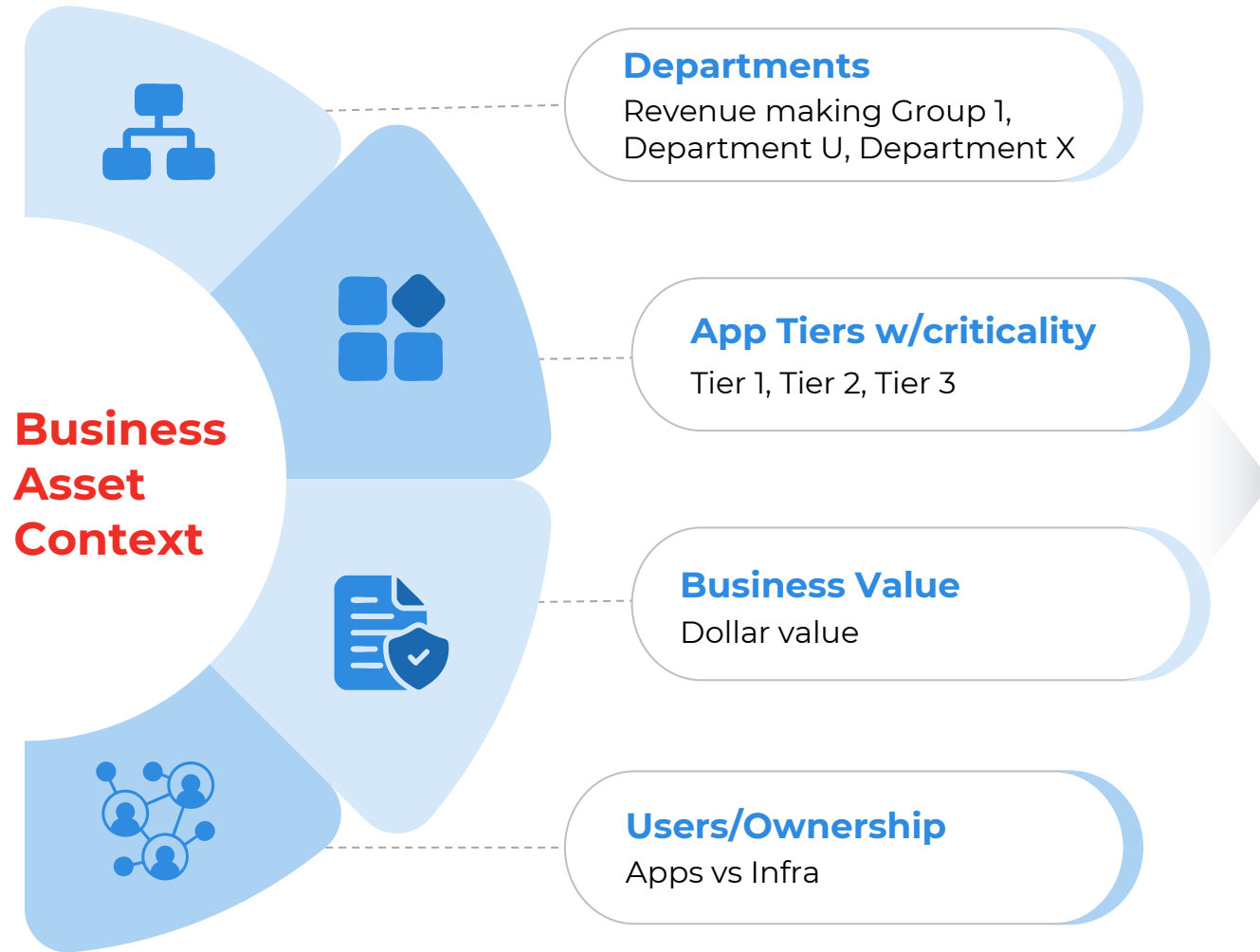


## Unknown External Assets

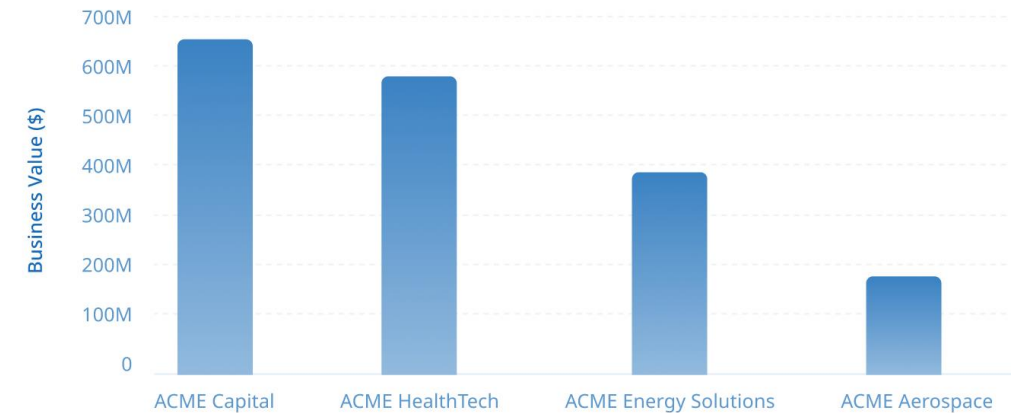


# Unified Asset Inventory: Business Context

## A Real-World Illustration



Organizations / Subsidiaries



# New & Constant **Cyber Risk** Challenges

Every tool is measuring risk differently, what are top 10 Risks?

## SaaS



## IOT



## Applications



## Data



## Code



## Vuln Management



## Public Cloud



### Qualitative

- ✗ Severe / Critical
- ✗ Category 1,2,3 etc..
- ✗ Urgent / Low
- ✗ Medium / High
- ✗ Pass / Fail

### Quantitative

- ✗ 10, 50, 100
- ✗ 1-5

### CVSS

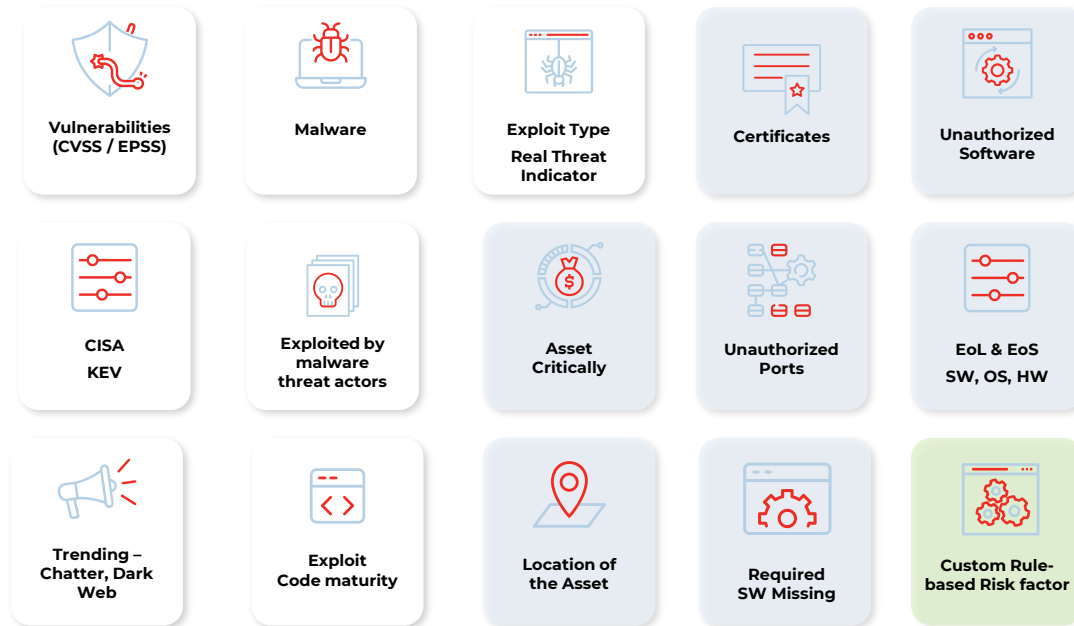
- ✗ 1-10

**40,003 CVEs discovered in 2024**

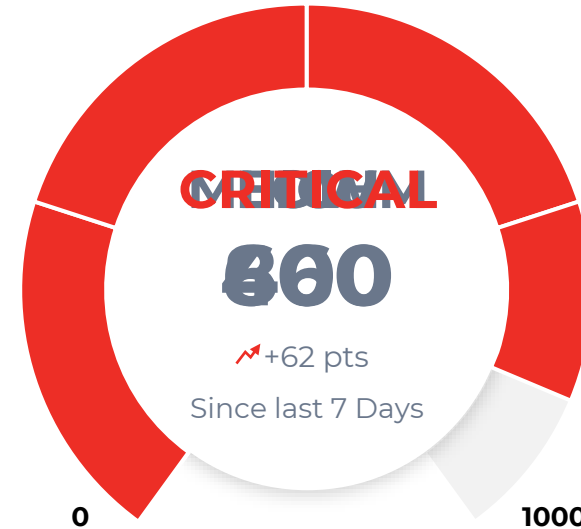
**39%**

**Increase in vulnerabilities** and exposures (CVEs) discovered worldwide.  
– Qualys Threat Research

# TruRisk™ Most Comprehensive Scoring...



## TruRisk™ Score



Total Assets

**110K**

Total Findings

**1.5M**

## Top Risk Factors

CISA/NCSC Vulnerabilities

**143.2K**

Internet Exposed Assets

**20.4K**

Misconfigurations

**92.4K**

Incidents

**19**



# Qualys Enterprise TruRisk Management (ETM)

First Risk Operations Center (ROC)

885 Critical  
TruRisk™ Score



# Prioritizing risky exposures which Matter, from millions of exposures

## Risk Operations Center (ROC)



**62.5M**  
ALL FINDINGS

**\$3.12 M**  
Cost of Remediation

THREAT  
INTELLIGENCE

**2.17 M (4%)**  
Risky Exposures  
(QDS/QVSS)

**96% Reduction**

Dark web trending  
**Weaponized by threat actors**  
Malware/Ransomware attacks  
in the industry

**\$612K**  
Cost of Remediation

ASSET  
CONTEXT

**304K (<1%)**  
Prioritized exposures  
for Business (with ACS context)

**99% Reduction**

**Business Critical Assets** (PCI, Internet  
Facing, DB, Revenue making App)

**\$311K**  
Cost of Remediation

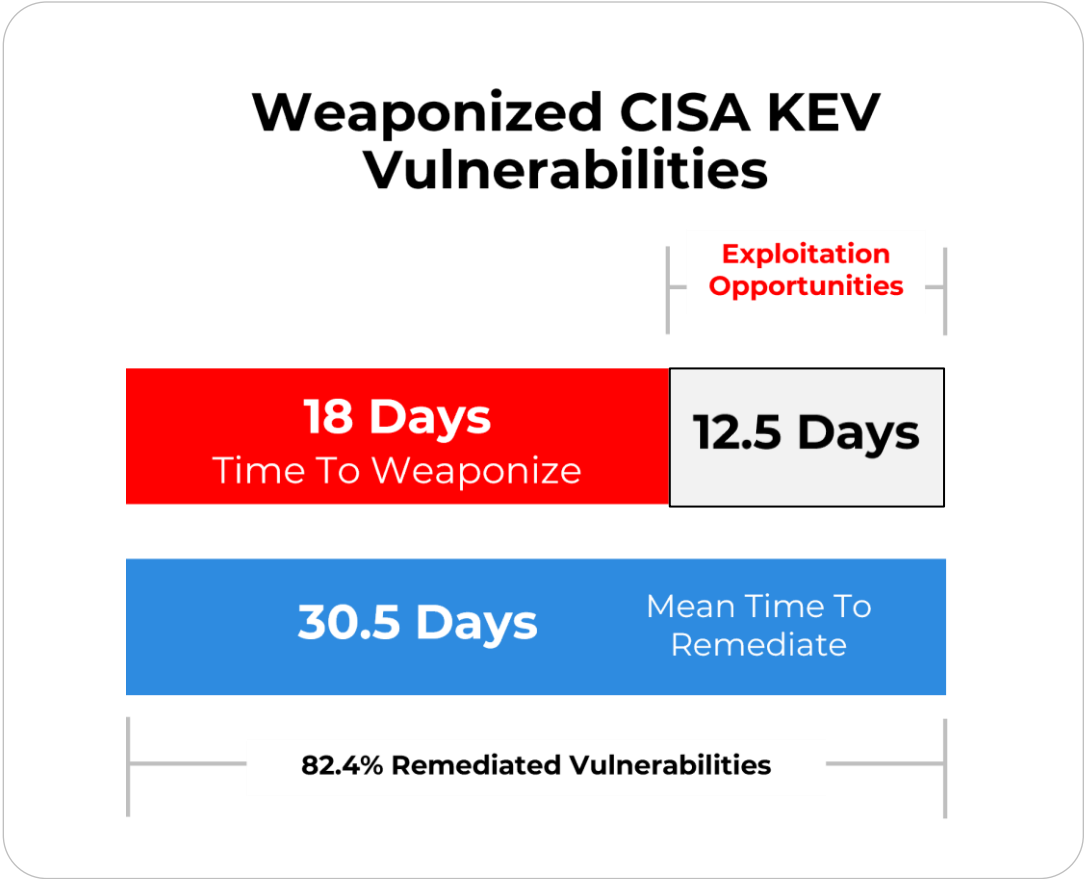
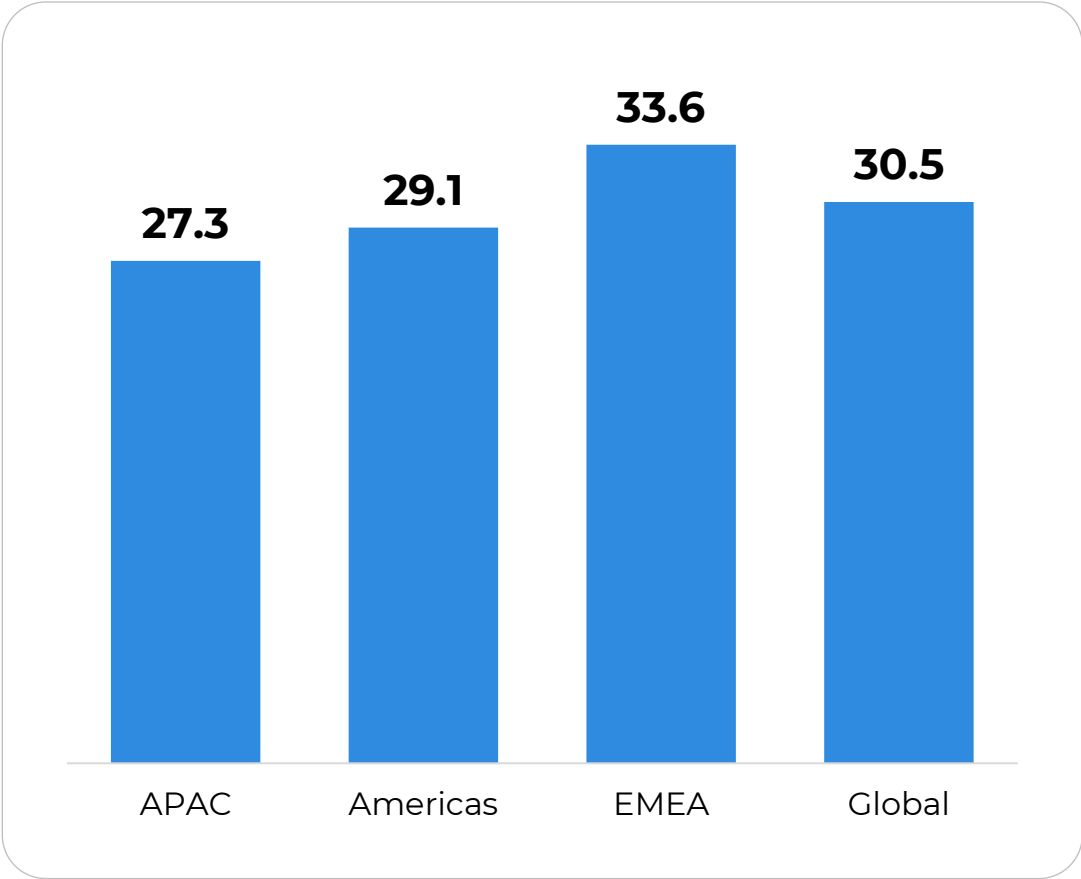
# Prioritize the exposure with threat-context



# Deprioritize the exposure, if no threat-context



# Problem in Risk Reduction is 2-Fold



# Impact of Qualys TruRisk Eliminate

140M

Patches + Mitigations  
Deployed in last 12 months

Exchange

Smart Chaining

Microsoft No VPN

Rollback

RBAC

Patch via SCCM

Linux Intune

ServiceNow

Zoom

Junos

PowerShell

ivanti

solarwinds

Cisco

Microsoft SQL Server

VMware ESXi

5% Windows

Customers in 0-5 days MTTR

Android

9% iOS

Customers in 6-10 days

Red Hat Enterprise Linux

32%

Customers in 11 to 17 days

Jet Brains

Python

Apache HTTP Server Project

Google

Jenkins

Progress MOVEit

mongoDB

Java

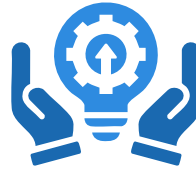
40%  
Faster MTTR  
than traditional patch

# Remediate Smart, Break Less with AI-powered Patch Reliability Score



## Automate the safe majority

- Classify each patch (High, Medium or Low)
- Risky vulns with **high-reliability** recommended for automated patching.
- Cutting **MTTR by 50–75%**



## Fewer outages, smarter testing

- Focus human effort on **Medium** with smart patch ring jobs.
- Result: **change-failure rate ≤5–10%** and fewer SEV incidents tied to patching.



## Risk-aware when patching is risky

- When reliability is **low**, recommends mitigate / isolate until safe to patch.
- Keeping MTTR for risky vulns in single digits while protecting crown-jewel assets.

# TruRisk Eliminate

## Mitigate

- Leverage Qualys TRU's provides mitigations to address vulns that cannot be patched/ fixed due to operational risk.
- Mitigated vulns are flagged in VM reports

## Customize to your Needs

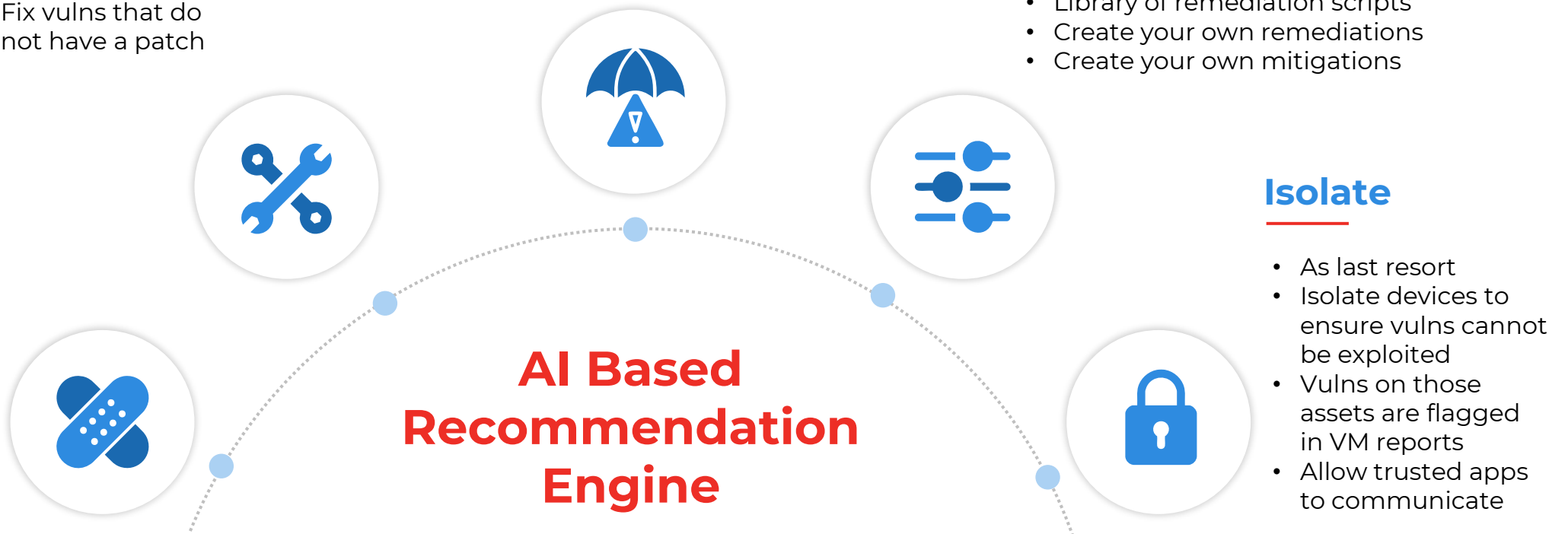
- Library of remediation scripts
- Create your own remediations
- Create your own mitigations

## Fix

- Fix vulns that do not have a patch

## Patch

- Patch Windows, Mac, Linux OS and 3rd party apps
- Automation with Zero-Touch



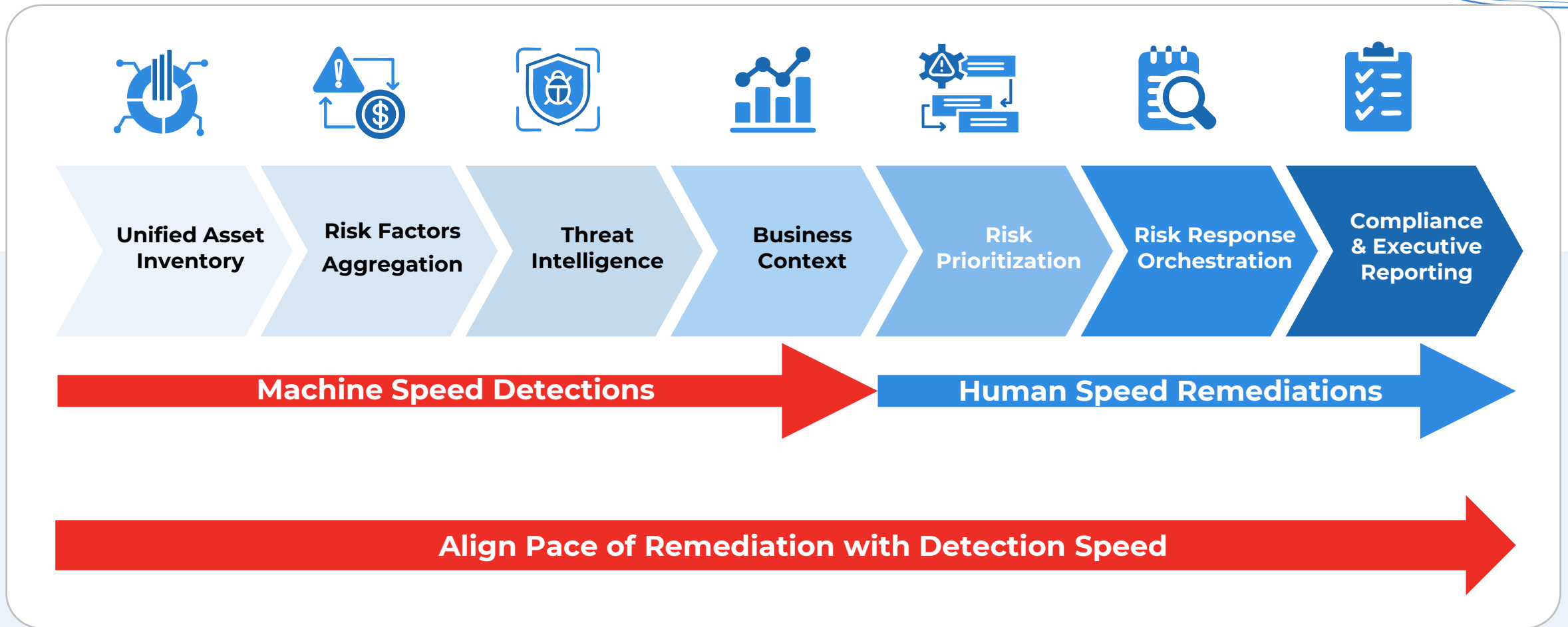
## Isolate

- As last resort
- Isolate devices to ensure vulns cannot be exploited
- Vulns on those assets are flagged in VM reports
- Allow trusted apps to communicate

Map vulns to remediation & mitigation actions

# Risk Operations Center (ROC)


Measure, Communicate and Eliminate Cyber Risk



# A Marketplace of Cyber Risk Agents

Your skilled, digital workforce for autonomous risk management

Reliable



Agent Nyra ★ 4.8

**Threat-Informed Risk Prioritization**  
Continuously monitors trending high-profile threats in your industry, for prioritizing their risk to your environment, by correlating them to attacker's tactics and techniques.

Core Skills  
Threat Intelligence Threat Prioritization MITRE Attack


Projected Agent Impact  

85%  
Monitoring of Trending Threats

22%  
Reduction in Cyber Risk

Employ

Popular



Agent Sara ★ 4.7

**Autonomous Patch Tuesday Lifecycle**  
Automates Patch Tuesday from CVE mining to mapping patches, assets, and apps, enabling adaptive remediation to reduce risk and exposure windows, freeing teams to focus on higher-value security priorities with less business impact.

Core Skills  
Patch Tuesday Vulnerability Management Vulnerability Remediation


Projected Agent Impact  

15%  
TruRisk Score Reduction

75%  
Faster Patch Closure (MTTR)

Employ

Trending



Agent Nova ★ 4.9

**Discover and Prioritize the Risk of External Attack Surface**  
Get hacker's eye view of your internet facing assets revealing the toxic combinations of open ports, listening service, risky vulnerabilities and business context of the asset to continuously prioritize and reduce your external attack risk.

Core Skills  
External Attack Surface Management (EASM) Threat Prioritization

Projected Agent Impact  


~25%  
Unknown Assets Discovery

~15%  
Hidden Risk Reveal

90%  
Faster detection of risk

Employ

Popular



Agent Chang ★ 4.6

**Audit-readiness Assessment & Reporting**  
Keeps you audit-ready continuously with autonomous evidence collection for in-scope assets, mapping to compliance requirements, delivering audit-readiness reports that highlight gaps and prioritize fixes, improving success while reducing manu...

Core Skills  
Compliance Management Audit Management +1


Projected Agent Impact  

85%  
Less Time

22%  
Less Audit Gaps

Employ

Reliable



Agent Sophia ★ 4.6

**Self-Healing Autonomous VM**  
Self-heals autonomous VMs by identifying security vulnerabilities and managing remediation under human supervision, reducing risk in real time. Ensures systems stay efficiently updated and resilient, minimizing the operational risk of threats.

Core Skills  
Continuous Discovery Risk Based Detection +1

Projected Agent Impact  


99%  
Visibility of Internet-Facing Assets

60%  
Reduction in Noise

4x  
Faster Detection for Critical CVEs

Employ

Reliable



Agent Vikram ★ 5

**Adaptive Cloud Risk Assessment**  
Discovers unknown and unmanaged (for cyber risk) cloud workloads and resources and assesses their risk with FlexScan strategies of agent & agentless scanning in cloud, making sure you never have a cloud asset without visibility into its risk

Core Skills  
CWPP CNAPP Cloud Security

Projected Agent Impact  

100%  
Visibility into Cloud Assets

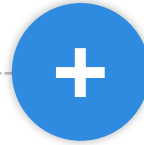
6 Mins  
To Define Flexible Scan Strategies in Cloud

22%  
Less Cyber Risk in Cloud

Employ



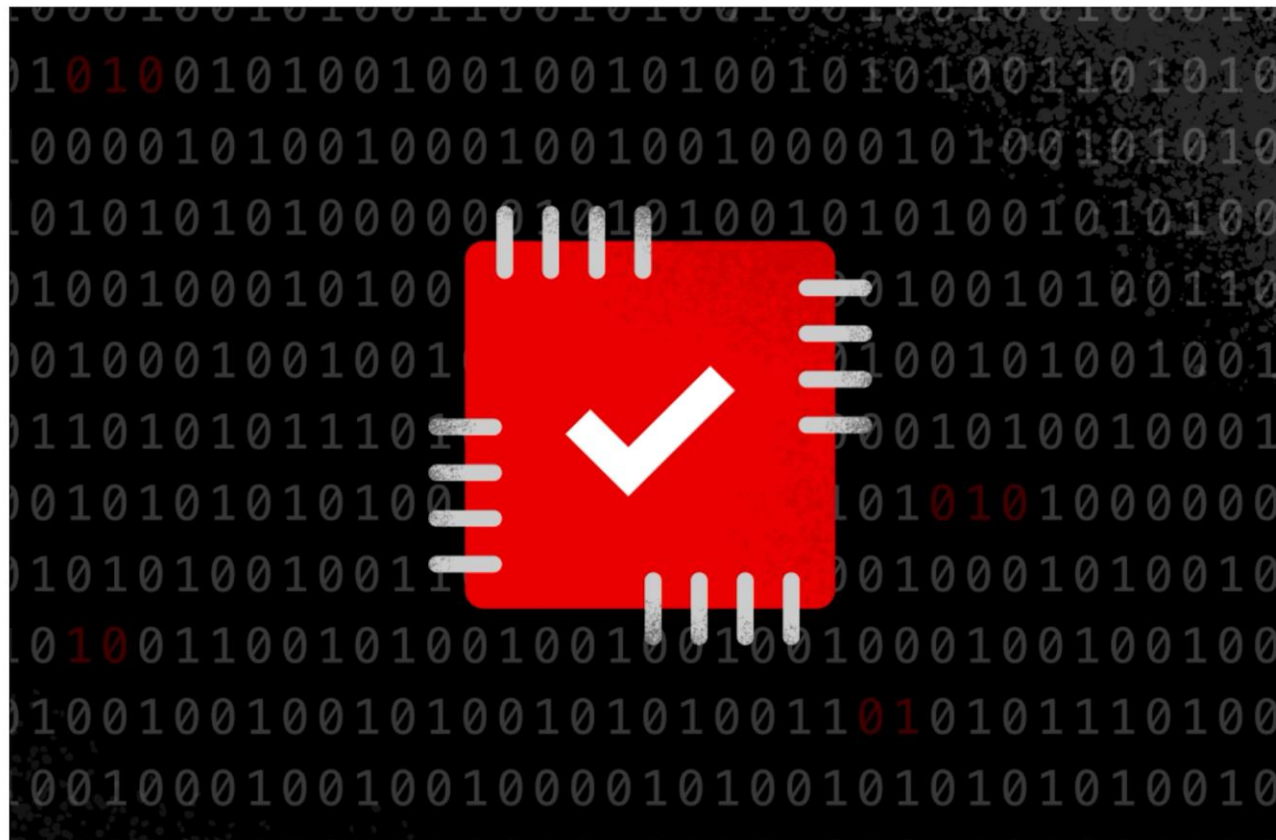
**Specialized Built-In Cyber  
Risk Agents**



**Build your Own  
Agents**














# July 2025 Patch Tuesday: One Publicly Disclosed Zero-Day and 14 Critical Vulnerabilities Among 137 CVEs

July 08, 2025 | Falcon Exposure Management Team | Exposure Management



Microsoft has addressed 137 vulnerabilities in its July 2025 security update release, more than

## CATEGORIES

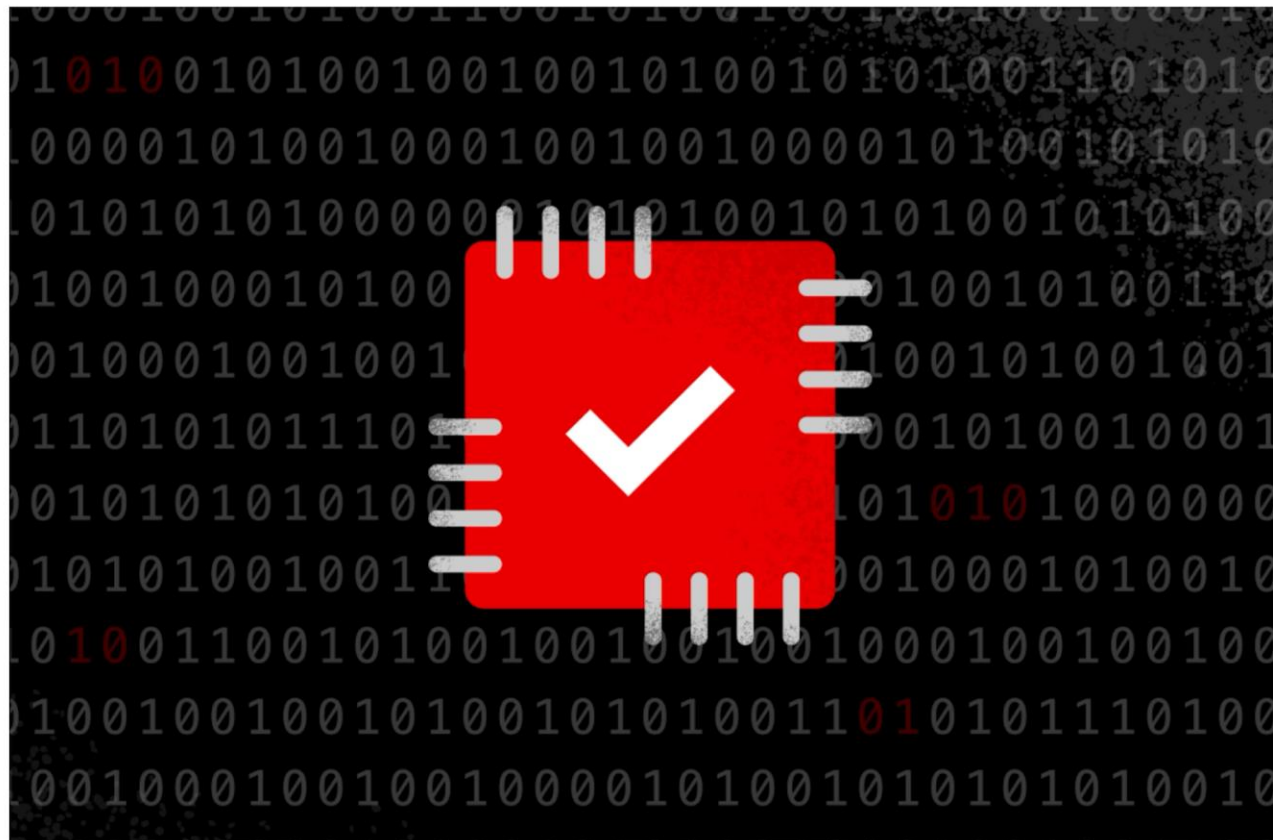
	AI & Machine Learning	30
	Cloud & Application Security	132
	Data Protection	16
	Endpoint Security & XDR	319
	Engineering & Tech	81
	Executive Viewpoint	170
	Exposure Management	100
	From The Front Lines	194
	Identity Protection	54
	Next-Gen SIEM & Log Management	101
	Public Sector	40
	Small Business	11
	Threat Hunting & Intel	196

## CONNECT WITH US
















# July 2025 Patch Tuesday: One Publicly Disclosed Zero-Day and 14 Critical Vulnerabilities Among 137 CVEs

July 08, 2025 | Falcon Exposure Management Team | Exposure Management



Microsoft has addressed 137 vulnerabilities in its July 2025 security update release, more than

## CATEGORIES

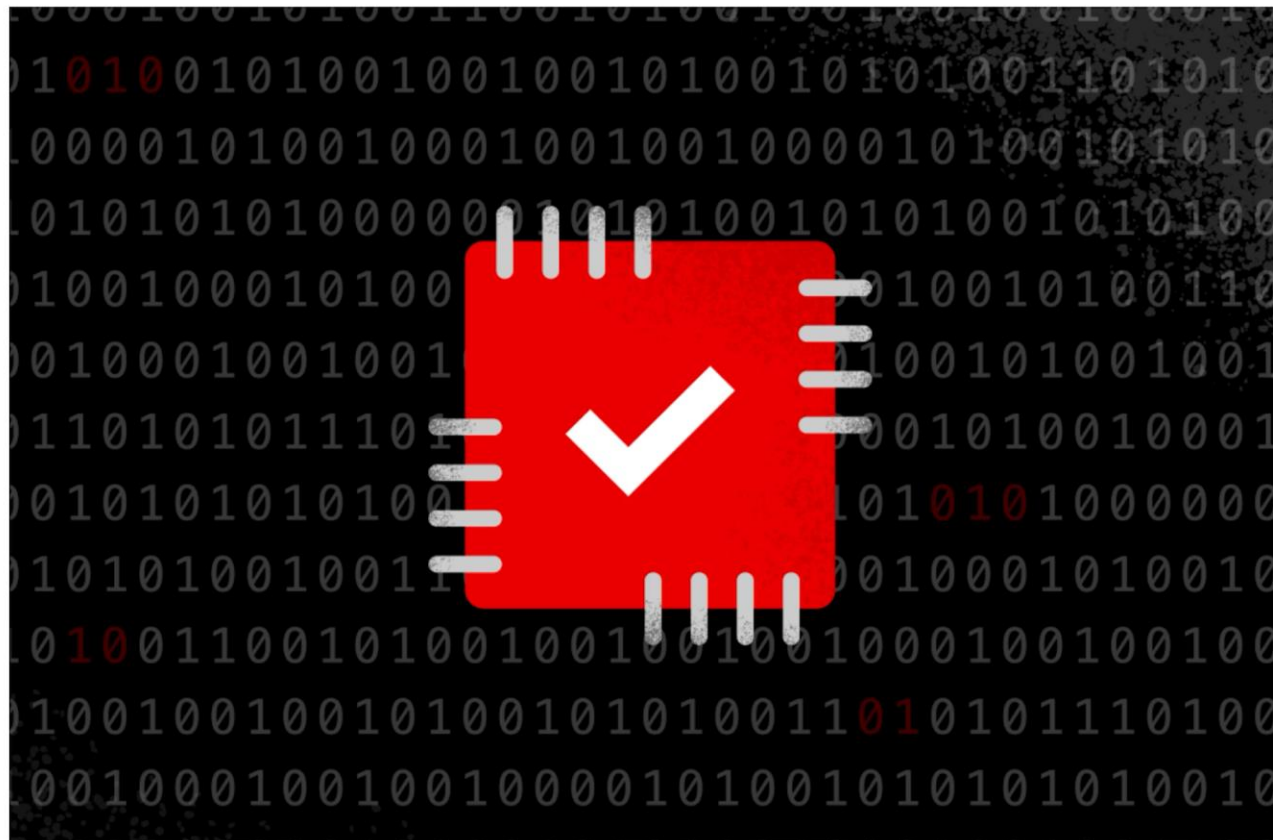
	AI & Machine Learning	30
	Cloud & Application Security	132
	Data Protection	16
	Endpoint Security & XDR	319
	Engineering & Tech	81
	Executive Viewpoint	170
	Exposure Management	100
	From The Front Lines	194
	Identity Protection	54
	Next-Gen SIEM & Log Management	101
	Public Sector	40
	Small Business	11
	Threat Hunting & Intel	196

## CONNECT WITH US
















# July 2025 Patch Tuesday: One Publicly Disclosed Zero-Day and 14 Critical Vulnerabilities Among 137 CVEs

July 08, 2025 | Falcon Exposure Management Team | Exposure Management



Microsoft has addressed 137 vulnerabilities in its July 2025 security update release, more than

## CATEGORIES

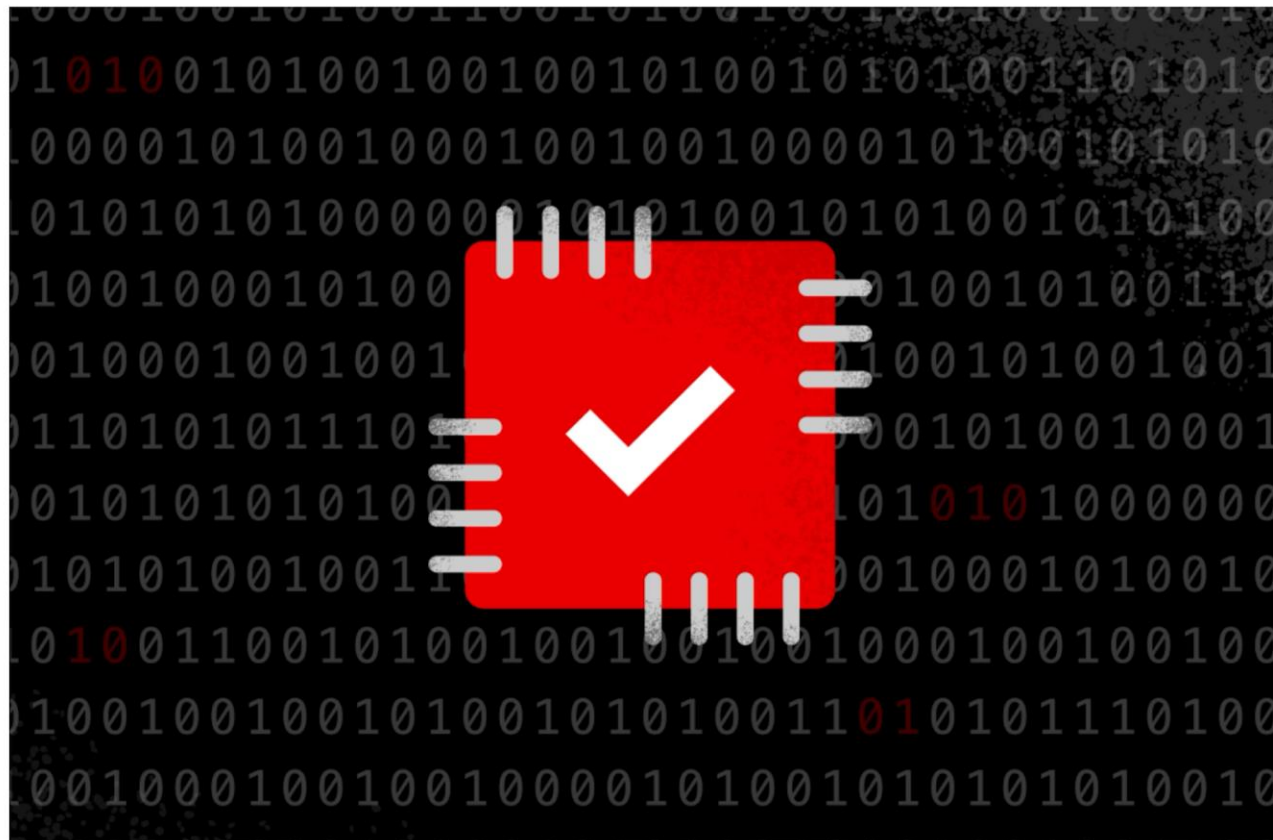
	AI & Machine Learning	30
	Cloud & Application Security	132
	Data Protection	16
	Endpoint Security & XDR	319
	Engineering & Tech	81
	Executive Viewpoint	170
	Exposure Management	100
	From The Front Lines	194
	Identity Protection	54
	Next-Gen SIEM & Log Management	101
	Public Sector	40
	Small Business	11
	Threat Hunting & Intel	196

## CONNECT WITH US
















# July 2025 Patch Tuesday: One Publicly Disclosed Zero-Day and 14 Critical Vulnerabilities Among 137 CVEs

July 08, 2025 | Falcon Exposure Management Team | Exposure Management



Microsoft has addressed 137 vulnerabilities in its July 2025 security update release, more than

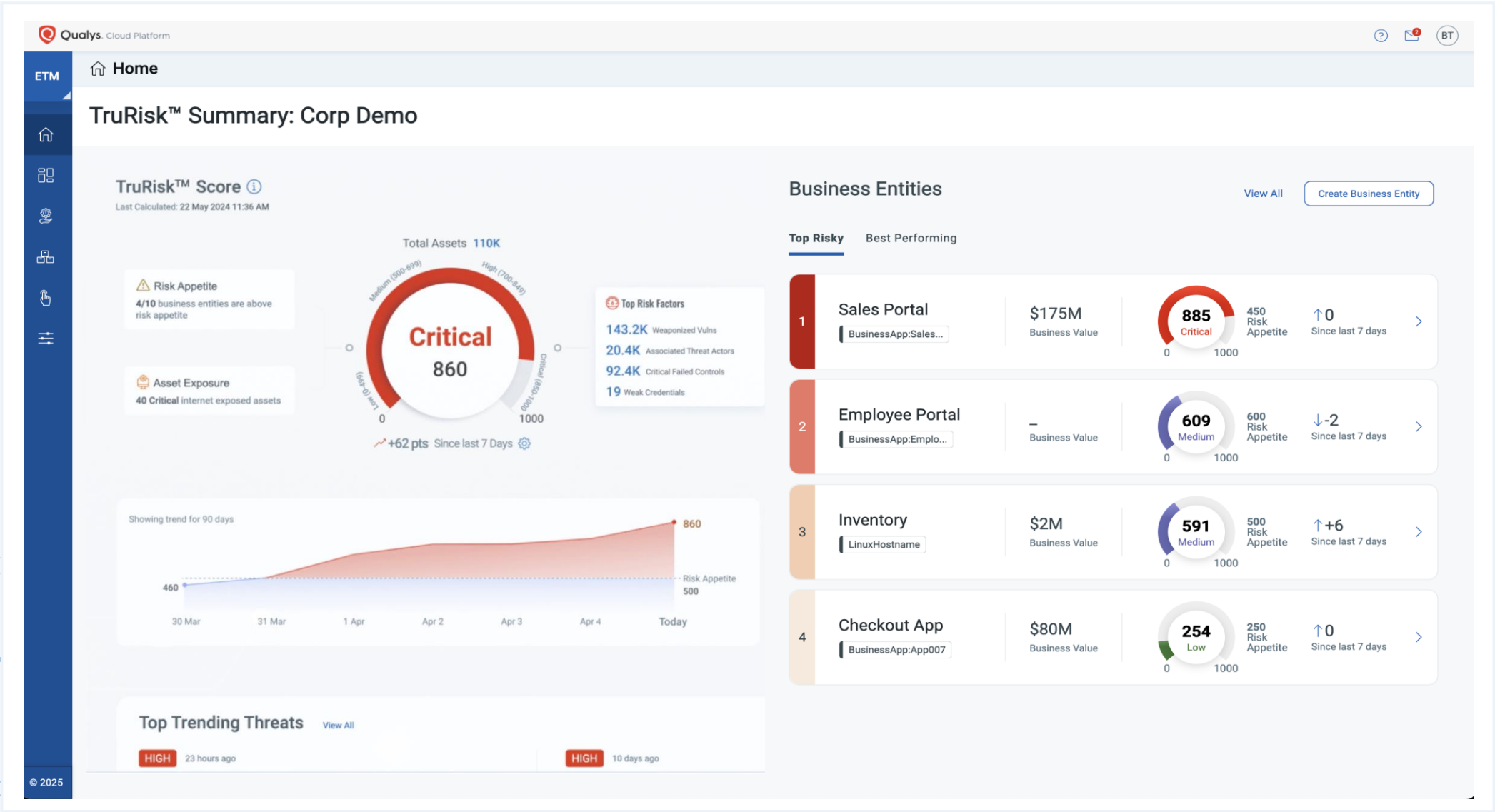
## CATEGORIES

	AI & Machine Learning	30
	Cloud & Application Security	132
	Data Protection	16
	Endpoint Security & XDR	319
	Engineering & Tech	81
	Executive Viewpoint	170
	Exposure Management	100
	From The Front Lines	194
	Identity Protection	54
	Next-Gen SIEM & Log Management	101
	Public Sector	40
	Small Business	11
	Threat Hunting & Intel	196

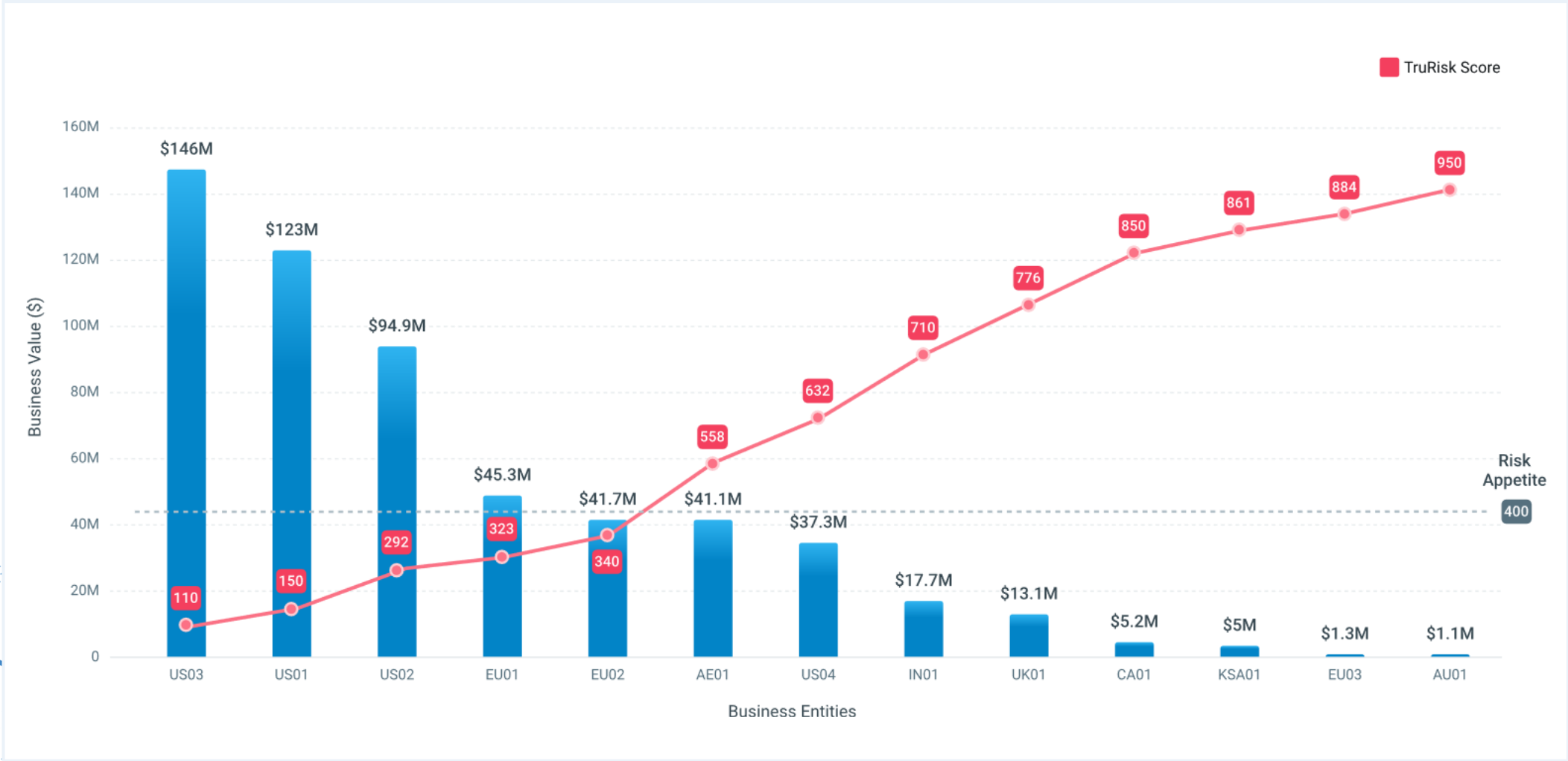
## CONNECT WITH US



# ETM - Executive Dashboards

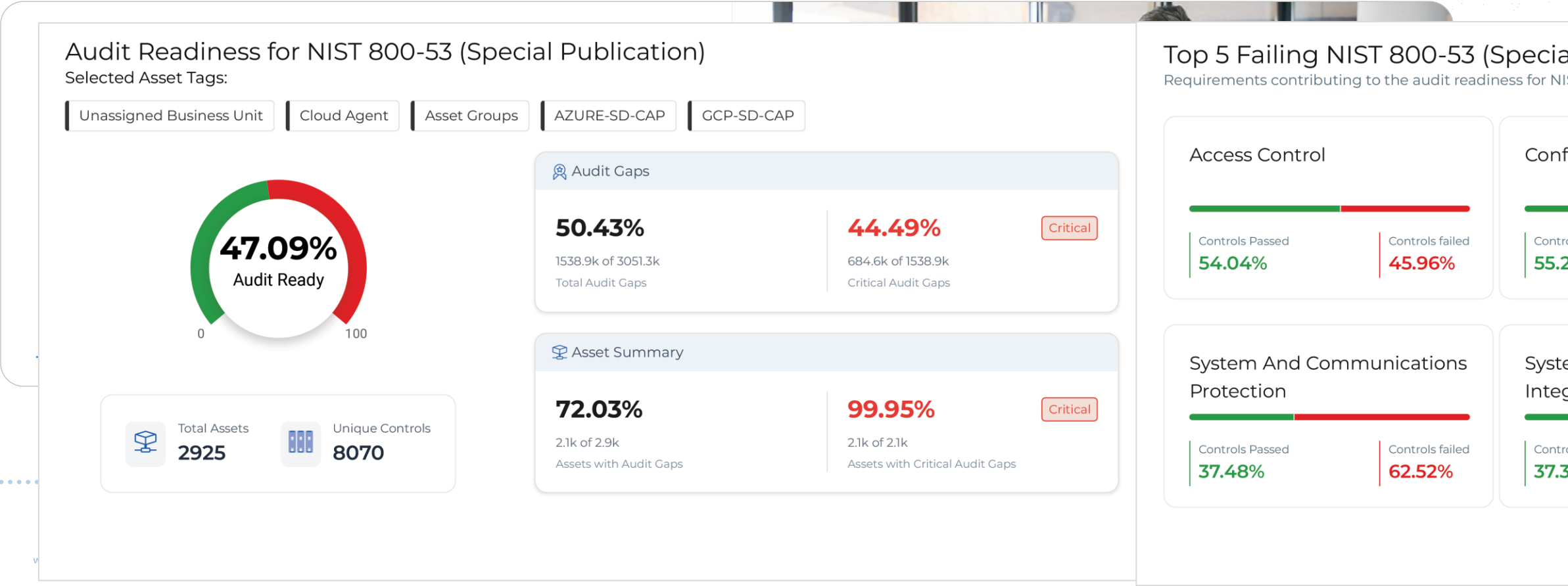


# ETM - Executive Dashboards



# Compliance Assessment and Reporting

Audit-Ready, Continuously Compliant to 100+ mandates from assessment to fixing



# Thank You

