

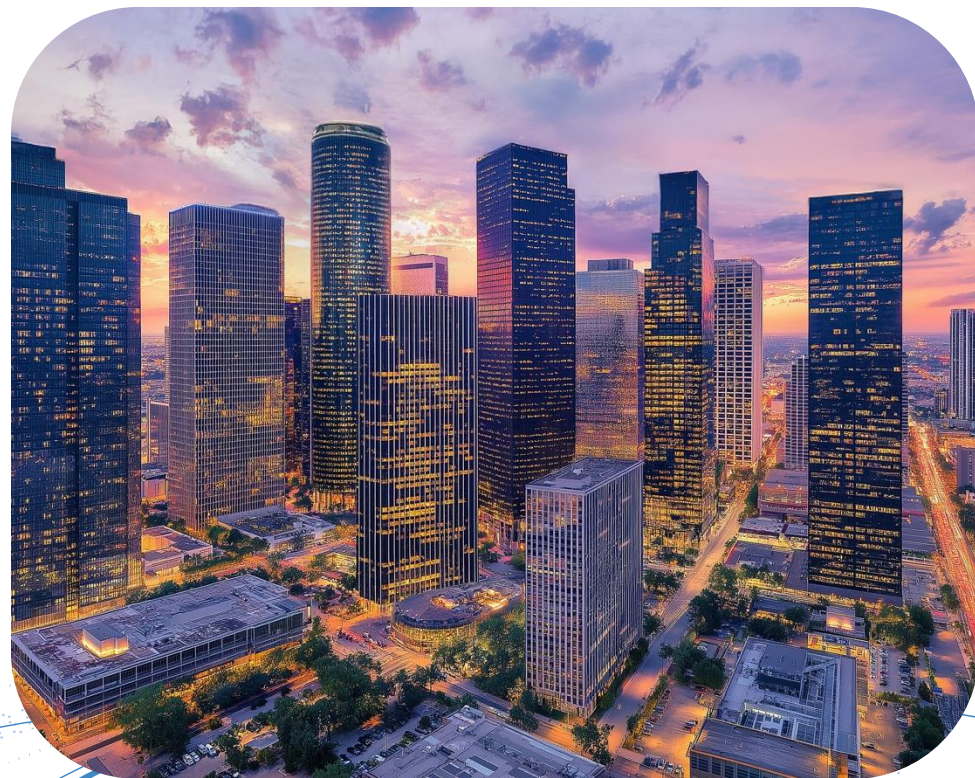
Perimeters are so 2015

Expanding Risk Operations
with **Identity Context**



Himanshu Kathpal

Vice President,
Product Management,
Platform and Technologies



Agenda

01

Identity is INDEED the new perimeter

02

Why identity exposures break risk operations

03

Introducing
Qualys ETM Identity

04

ETM Identity Use Cases and Outcomes

05

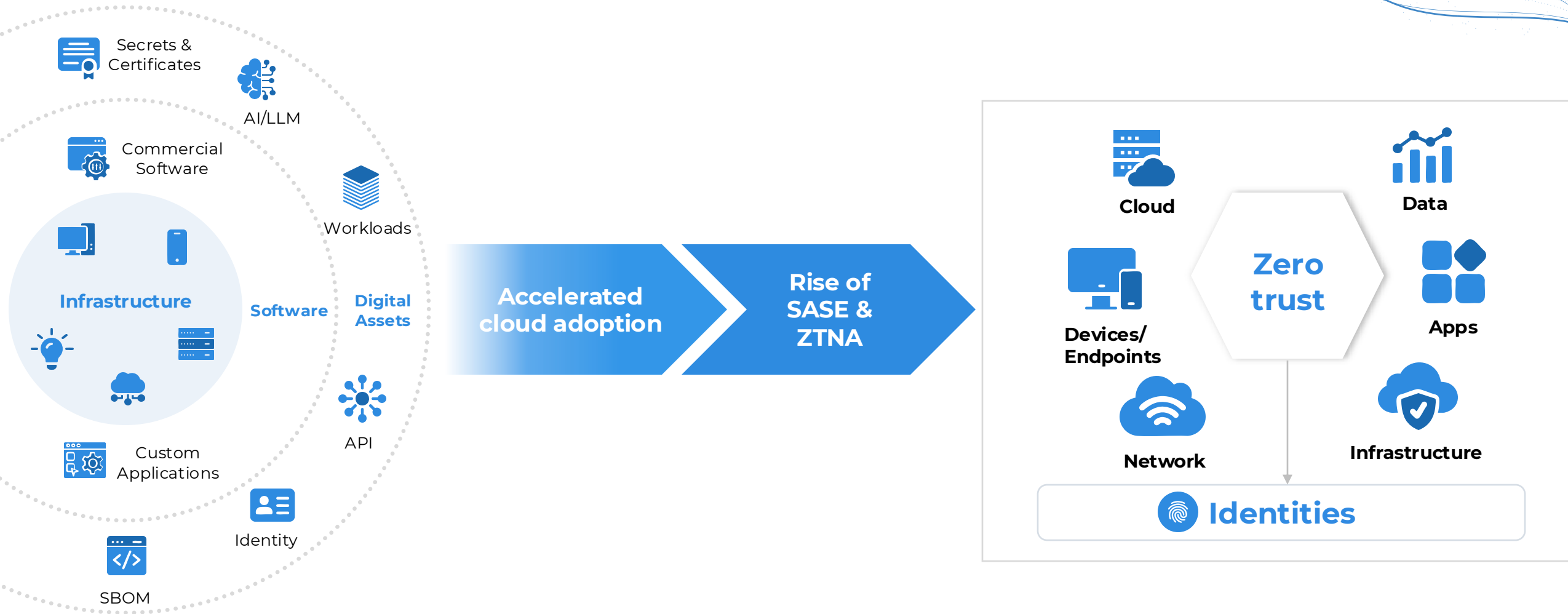
Demo

06

Industry leader, Corey Amsler's experience for ISPM Solutions

Rapidly Expanding Identity Attack Surface

From Cloud to SaaS to IoT: Each Login Adds to Risk



Identity is **INDEED** the new perimeter

It's 2025, cybercriminals
don't hack, they login



~80% of breaches involve credentials abuse

Threat actors now favour phishing, guessing, scraping, or buying credentials.

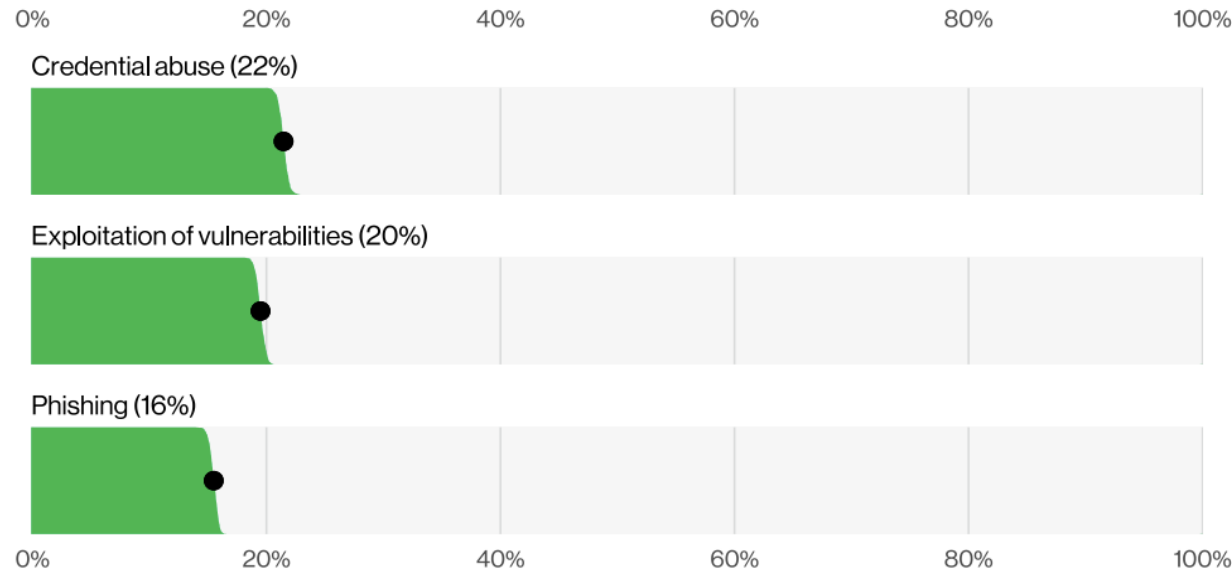
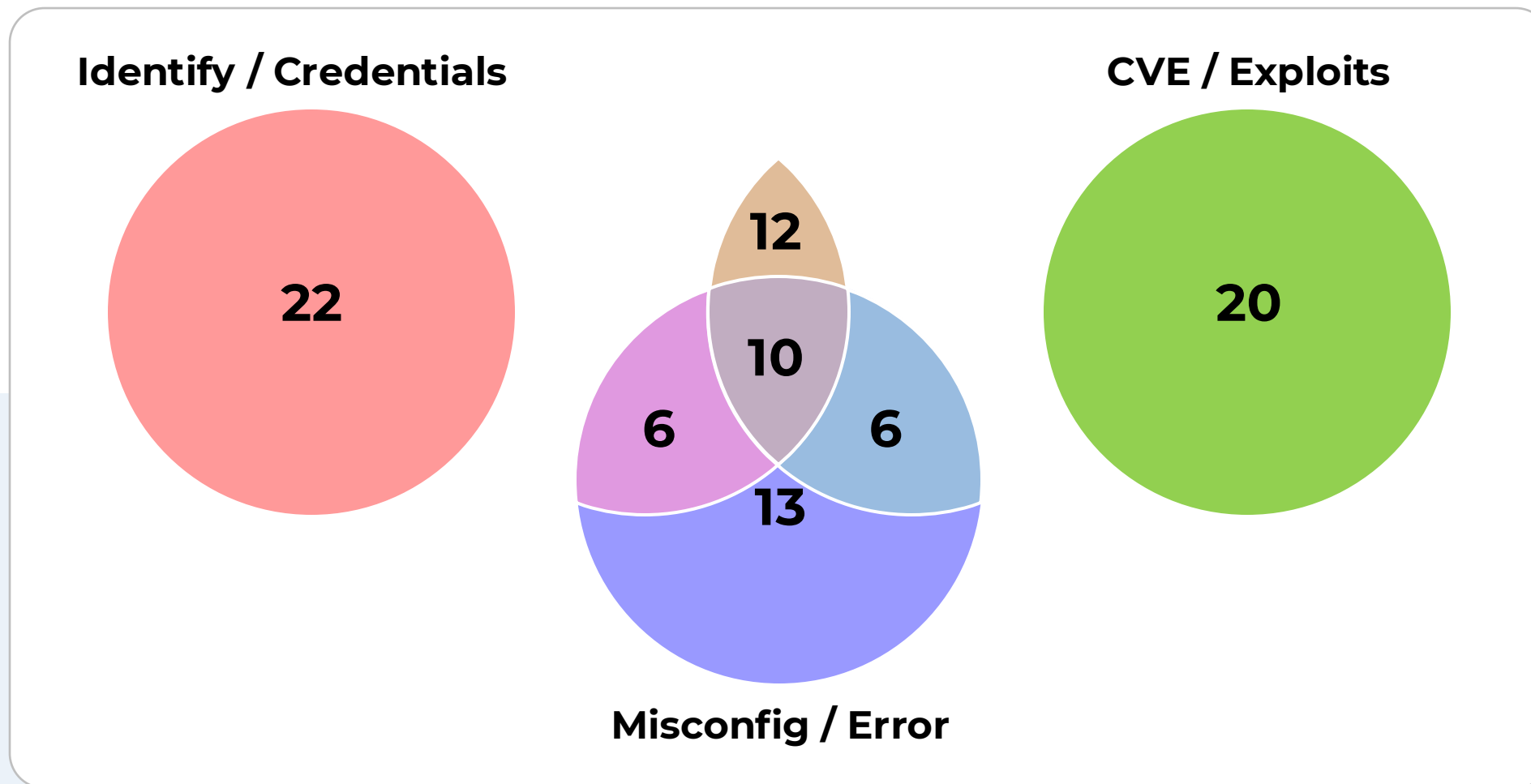


Figure 1. Known initial access vectors in non-Error, non-Misuse breaches (n=9,891)

Hybrid attack vectors rule the roost

34% of the breach vectors are combination of Identity weaknesses, CVEs, & Misconfigs.



Stolen creds + missing MFA = **terabytes & millions of \$\$\$** out the door

Snowflake: A watershed moment in cybersecurity industry

Failure mode

- Info-stealer creds
- Password reuse
- No MFA on **Snowflake customer accounts**

Business Impact

- At-least **165 orgs** targeted
- Extortion (\$0.3B-\$1B)
- Massive data exfiltration (Ticketmaster, Santander, others)

Snowflake Breach Exposes 165 Customers' Data in Ongoing Extortion Campaign

Jun 11, 2024 · Ravie Lakshmanan

Data Theft / Cloud Security



As many as 165 customers of Snowflake are said to have been impacted by an ongoing campaign designed to facilitate data theft and extortion, with implications than previously thought.

Google-owned Mandiant, which is assisting the cloud data security efforts, is tracking the as-yet-unclassified activity cluster up to a motivated threat actor.

More Than 2 Million People Impacted In Snowflake-Related Attack

BY KYLE ALSPACH

JULY 11, 2024, 1:44 PM EDT

Advance Auto Parts disclosed that data belonging to 2.3 million customers was exposed in an April attack targeting its Snowflake deployment.



Why identity exposures break risk operations

- AD/Entra is the **core of blast radius**.
- Compromise means **persistence**, not entry.
- Identity sprawl is messy and creates **toxic combinations**.
- **Weaponizing exposures** has never been easier.



No identity risk
visibility



Identity & asset risks
siloed



Ambiguity in
ownership



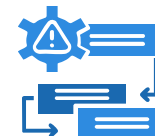
Lack of **audit trail**

Introducing **Qualys ETM Identity**

Consolidates identity posture across your attack surface to **measure**, **communicate**, and **eliminate** identity risks.

Operationalize Identity Risk Reduction

The loop every Risk Operations Center (ROC) needs for Identity Security



Unified Asset Inventory

- Active Directory (AD)
- Microsoft Entra ID
- Okta
- Ping Identity

Risk Factors Aggregation

- Qualys Agent (AD)
- Native IdP/IDaaS Connector (Entra ID, Okta, Ping)
- 3rd Party Tools (SailPoint, BloodHound, etc.)

Threat Intelligence

25+ threat intelligence feeds including Qualys Live TI, MITRE ATT&CK, Talos, McAfee, CISA KEV, EPSS

Business Context

- ServiceNow CMDB
- BMC Helix CMDB
- Qualys ETM Business Value / Risk Appetite / VAR

Risk Prioritization

- Identity TruRisk™
- Identity Insights
- Attack Path Analysis

Risk Response Orchestration

- TruRisk™ Eliminate
- AD Policy Controls
- ITSM Workflows
- Identity Actions
- Custom playbooks
- Integrity Monitoring

Compliance & Executive Reporting

Audit-ready executive reporting
DISA STIG, CIS M365 & more

How will you be
ROC Ready from Day 1
For Your Identity Infrastructure



Unified
Asset
Inventory

Risk Factors
Aggregation

Threat
Intelligence

Business
Context

Risk
Prioritization

Risk
Response
Orchestration

Compliance
& Executive
Reporting

500K
ALL IDENTITIES



10k (2%)
Risky Identities

98% Reduction

THREAT
INTELLIGENCE

Weak policies (credentials, MFA etc.), External exposure of credentials, Excessive privileges creating attack paths to crown jewels

ASSET
CONTEXT

1.2k (<1%)
Business context and
asset context

99% Reduction

Business criticality of Identities (privileged identities), Asset vulnerabilities and misconfigs connected to these Identities



Unified
Asset
Inventory

Risk Factors
Aggregation

Threat
Intelligence

Business
Context

Risk
Prioritization

Risk
Response
Orchestration

Compliance
& Executive
Reporting

Comprehensive visibility across AD, Entra ID, IdPs, IDaaS, PAM

- ✓ Collect human/machine identities with attributes, memberships, tokens, keys.
- ✓ Classify externally exposed identities, guest users, shadow admins and infra.
- ✓ Manage tech-debt from EOL/EOS, unauthorized packages, baselines.
- ✓ Map ownership & lineage with versioned inventory for audit and Zero Trust.

Qualys Enterprise TruRisk™ Platform

Inventory All Assets Compute Container Storage Software Application Resource Identity Network

Users Groups Permissions Roles

14.1K
Total Users

Search

Action (0) Group By

1 / 18 pages Total 8 items

USERNAME & ID	TYPE	IDENTITY TRURISK	STATUS	MFA	LAST LOGIN DATE	SOURCE	EXTERNALLY EXPOSED	GROUPS	ASSET COUNT
Sam Wilson ID: 142341	User Account	958	Active	No	July 9, 2025 06:16 PM	Okta First Found: Feb 26, 2025... 11:36 PM	Yes	24	24
John Doe ID: 22132	Service Account	859	Inactive	No	July 9, 2025 04:15 PM	First Found: Feb 23, 2025... 06:37 PM	No	24	48
Emily Johnson ID: 22141	Service Account	857	Locked	No	July 9, 2025 03:16 PM	Okta First Found: Feb 21, 2025... 06:16 PM	Yes	24	114
Clara Simmons ID: 22142	Admin Account	851	Active	No	July 8, 2025 02:55 AM	First Found: Feb 19, 2025... 02:45 PM	Yes	30	218
Michael Tran ID: 22143	User Account	847	Locked	No	July 8, 2025 01:38 PM	First Found: Feb 7, 2025... 01:38 PM	No	18	312
Sara Jenkins ID: 22144	Guest Account	845	Active	Yes	July 7, 2025 04:17 PM	Okta First Found: Jan 24, 2025... 09:05 AM	Yes	29	415
Liam Patel ID: 22145	Service Account	843	Inactive	No	July 6, 2025 08:19 PM	First Found: Jan 18, 2025... 05:30 PM	No	22	678
Emily Zhang ID: 22146	Admin Account	840	Locked	Yes	July 2, 2025 11:36 PM	First Found: Jan 13, 2025... 07:15 AM	Yes	27	114

© 2024



Unified
Asset
Inventory

Risk Factors
Aggregation

Threat
Intelligence

Business
Context

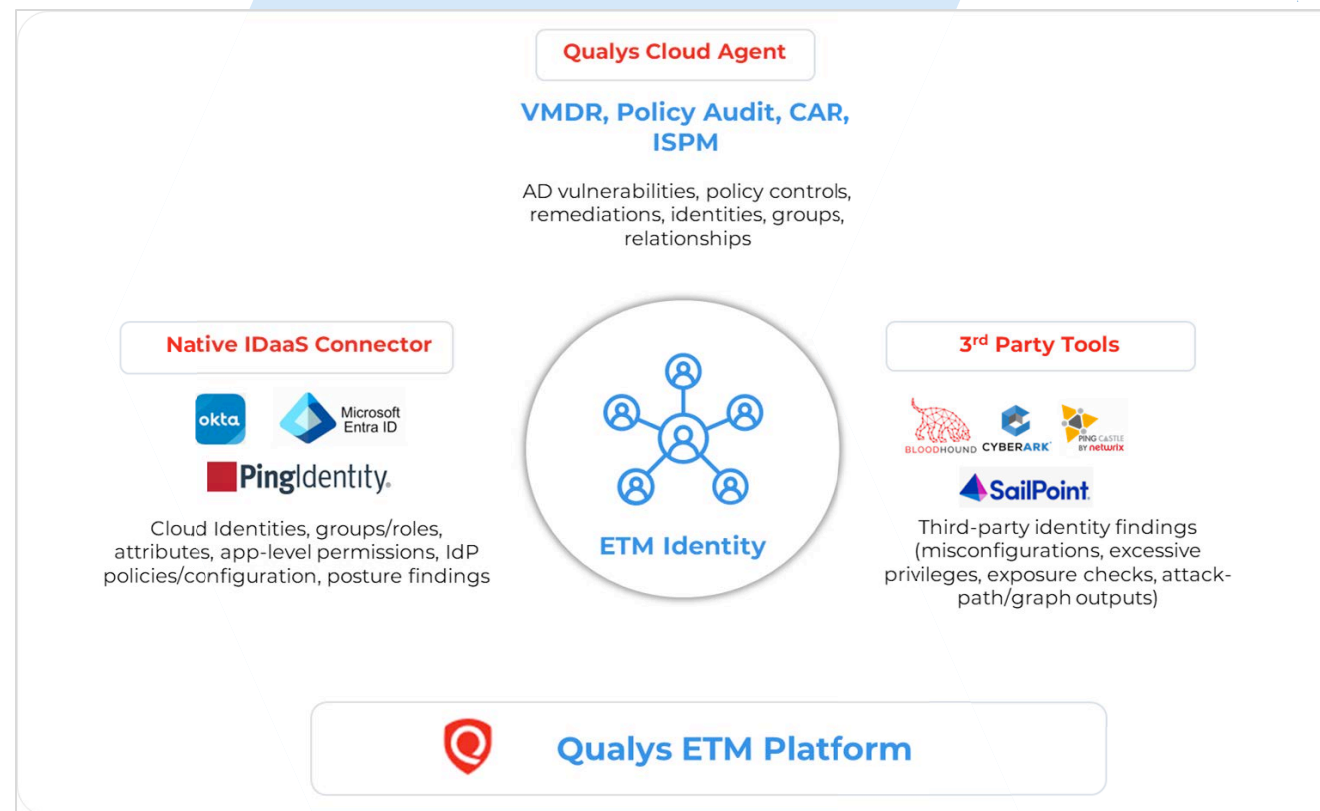
Risk
Prioritization

Risk
Response
Orchestration

Compliance
& Executive
Reporting

Unify identity posture into a single cyber-risk view with Agentic AI

- ✓ Detect CVEs, misconfigs, IORs via prebuilt scripts.
- ✓ Ingest 3rd-party findings (BloodHound, PingCastle, IdP/IDaaS exports).
- ✓ Dedupe, enrich signals with **25+ threat-intel and directory sources**.
- ✓ Assess against DISA STIG, CIS M365, and Zero-Trust controls.





Unified
Asset
Inventory

Risk Factors
Aggregation

Threat
Intelligence

Business
Context

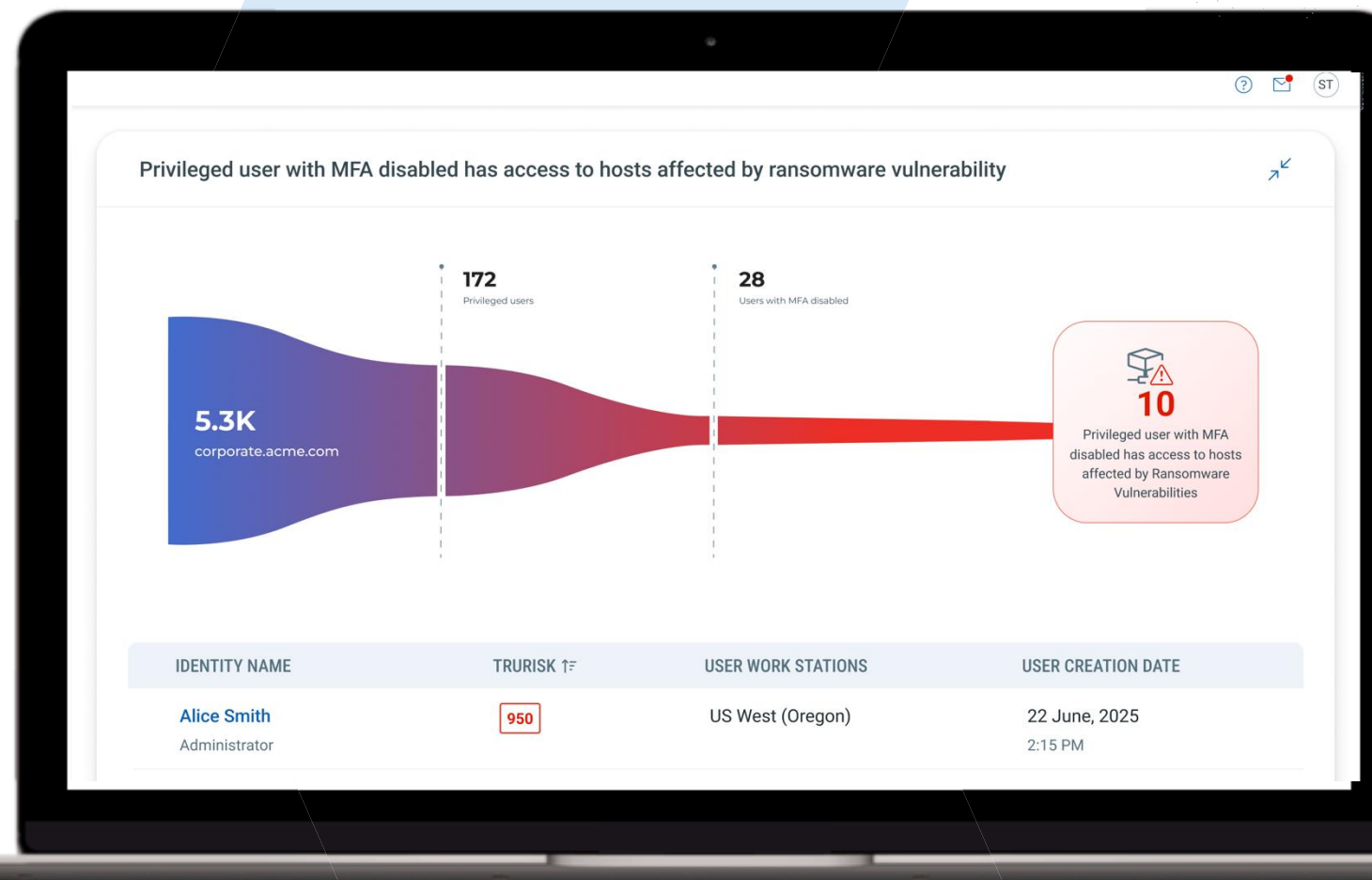
Risk
Prioritization

Risk
Response
Orchestration

Compliance
& Executive
Reporting

Convert identity risk signals into prioritized, business-impact actions.

- ✓ Correlate privileged users, MFA gaps, stale/service accounts with asset exposures.
- ✓ Surface toxic combinations linking identity and asset risks for next best action.
- ✓ Actionable insight cards
 - Privileged user without MFA on zero-day hosts
 - Admin with weak password on public web servers.





Unified
Asset
Inventory



Risk Factors
Aggregation



Threat
Intelligence



Business
Context



Risk
Prioritization



Risk
Response
Orchestration



Compliance
& Executive
Reporting

Expose hidden AD relationships and lateral routes to prioritize attack paths.

- ✓ Visualize privileges, GPO influence, cross-domain hops to find exploitable paths
- ✓ Protect Crown Jewels by focusing on highest-impact routes.
- ✓ One-click fixes (remove rights, enforce MFA, disable/quarantine) with verification.
- ✓ Rank paths by Identity TruRisk™, asset criticality, and tech debt.

← Insight Details: User with GenericAll rights on GPO can control Domain Controllers OU





Unified
Asset
Inventory

Risk Factors
Aggregation

Threat
Intelligence

Business
Context

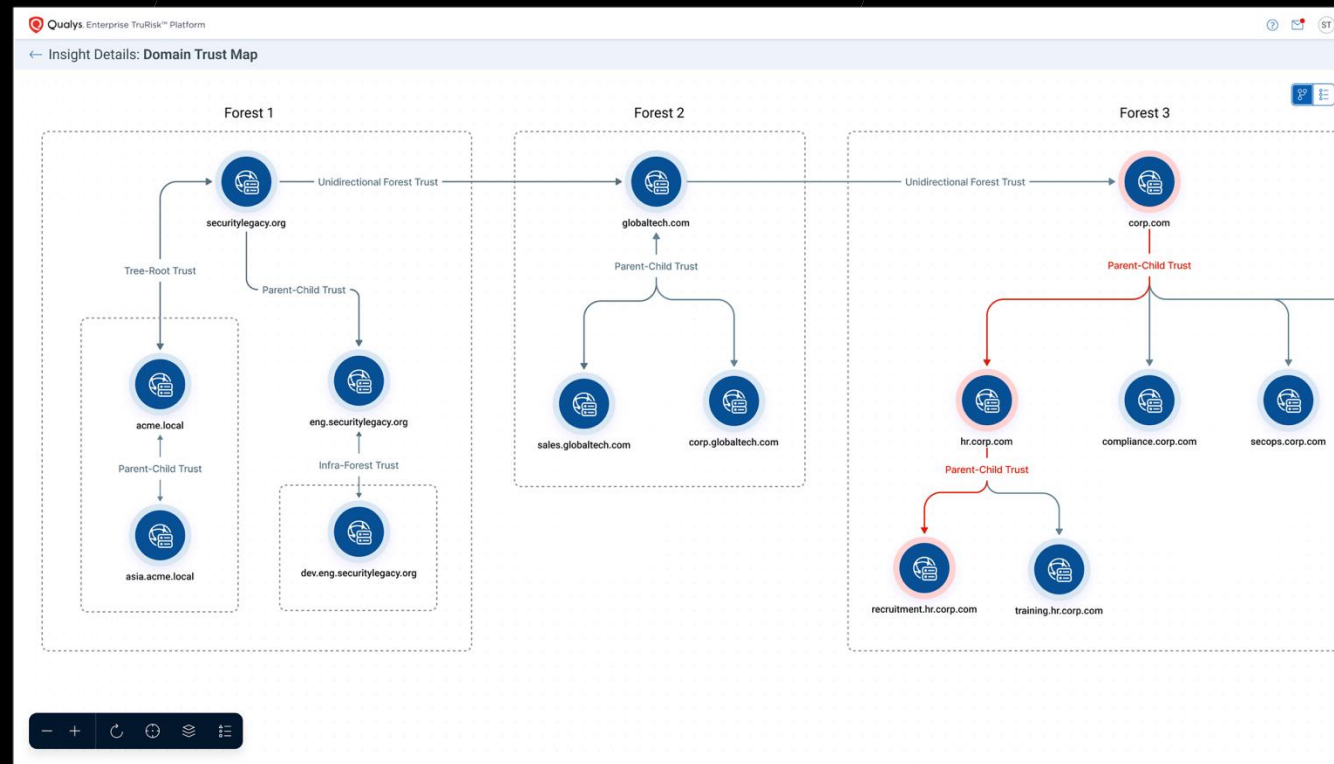
Risk
Prioritization

Risk
Response
Orchestration

Compliance
& Executive
Reporting

Detect hidden AD lateral paths and harden inter-domain/forest trusts to block easy traversal

- ✓ Map forests, domains, and trust types to spot risky trusts.
- ✓ Expose Tier-0/DC routes by correlating trusts with privilege paths.
- ✓ Rank weak trusts to collapse blast radius fast with one-click fixes.





Unified
Asset
Inventory

Risk Factors
Aggregation

Threat
Intelligence

Business
Context

Risk
Prioritization

Risk
Response
Orchestration

Compliance
& Executive
Reporting

+100



Identity
misconfiguration

+100



Over Privileges

+100



Cross Path
and Attack
path

+200



Externally
Exposed



Sam
Wilson

5 ICS

IMMUNITY

REVERSING
LABS

GREYNOISE
INTELLIGENCE

CYBERSECURITY
& INFRASTRUCTURE
SECURITY AGENCY

McAfee

VDE

MITRE
ATT&CK

GitHub

MISP
Threat Sharing

PZ
PROJECT ZERO

CANADIAN CENTRE FOR
CYBER SECURITY



Square
Security

metasploit

Kaspersky
Industrial
CyberSecurity

Google

EPSS
Exploit Prediction Scoring System

TALOS

packet storm

FIRE EYE

Qualys.
ROCon 25
The Risk Operations Conference
AMERICAS

950

Critical



Unified
Asset
Inventory

Risk Factors
Aggregation

Threat
Intelligence

Business
Context

Risk
Prioritization

Risk
Response
Orchestration

Compliance
& Executive
Reporting

345

Low

TruRisk™ Score

+220



Vulnerabilities



Misconfigurations



Identities

+110



Internet
Facing

+210



Business
critical/PCI or
sensitive data



No EDR Present

885

Critical

TruRisk™
Score



Unified
Asset
Inventory

Risk Factors
Aggregation

Threat
Intelligence

Business
Context

Risk
Prioritization

Risk
Response
Orchestration

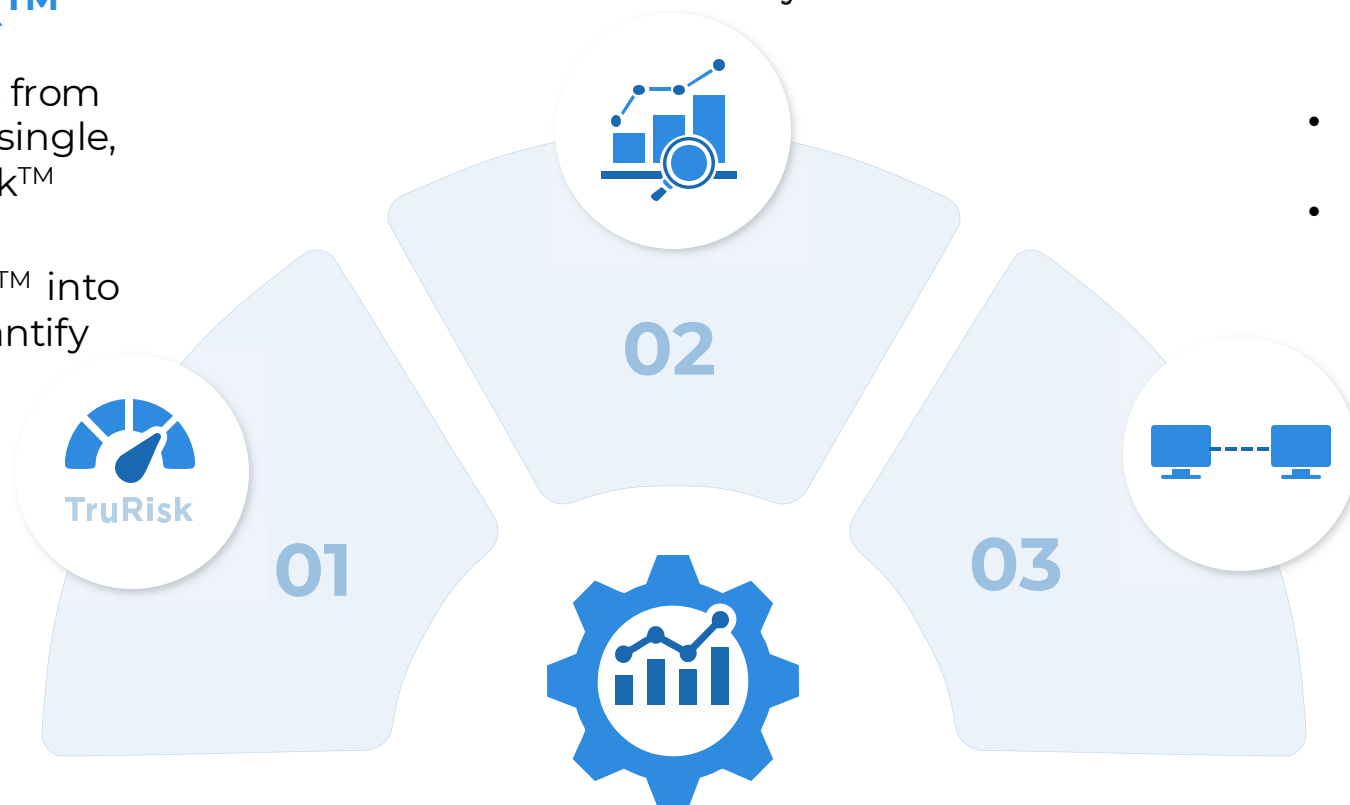
Compliance
& Executive
Reporting

Identity Insights

- Correlate signals from tech-debt
- Calculate toxic combinations of asset risks and identity risks

Identity TruRisk™

- Integrates identity risks from multiple sources into a single, intuitive Identity TruRisk™ score for each user
- Roll up Identity TruRisk™ into overall TruRisk™ to quantify risk in business terms



Attack Paths

- Visualize attack paths and prioritize based on TruRisk™.
- Understand blast radius impact of key accounts



Unified
Asset
Inventory

Risk Factors
Aggregation

Threat
Intelligence

Business
Context

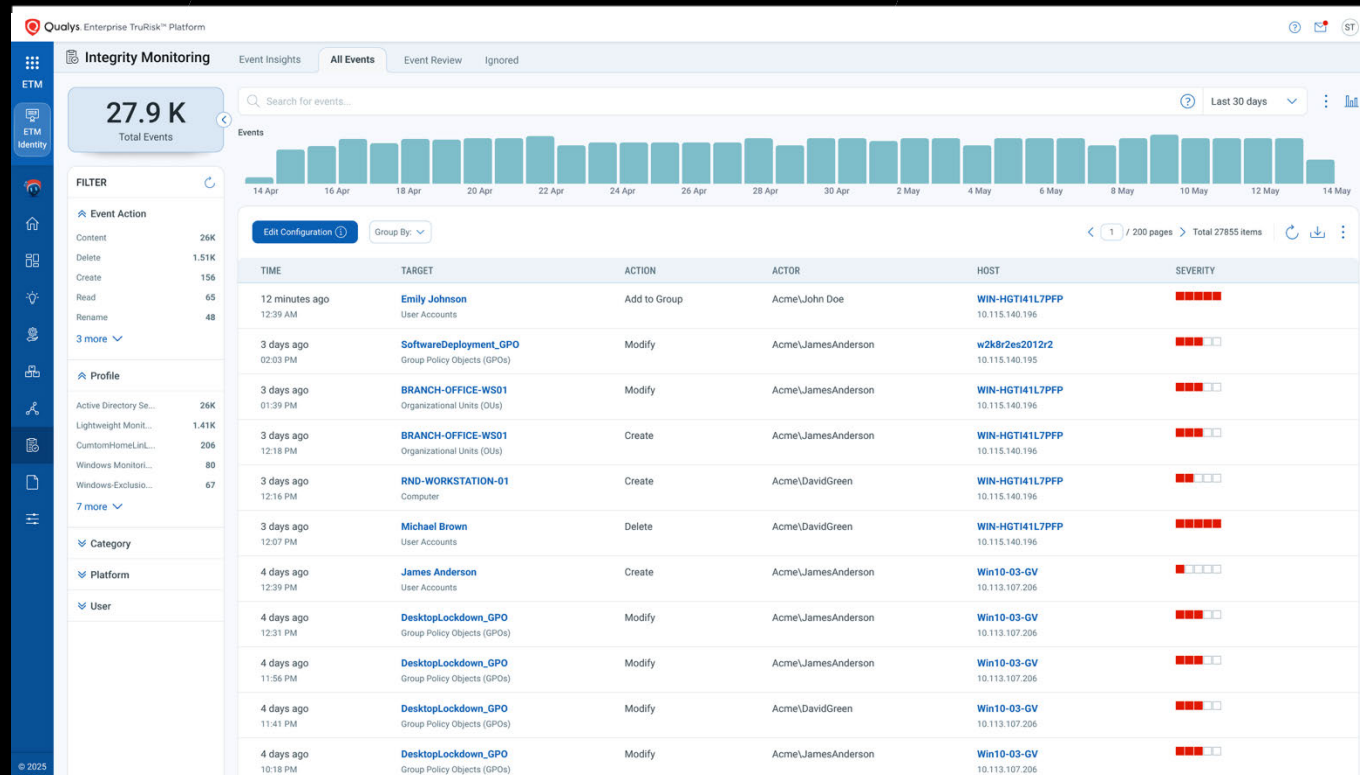
Risk
Prioritization

Risk
Response
Orchestration

Compliance
& Executive
Reporting

Real-time identity change detection with attribution, forensics, and audit trail.

- ✓ Monitor AD objects for privilege escalations, MFA disablement, policy tampering.
- ✓ Record who changed what, when, where across AD objects/registry/schema.
- ✓ Event-driven alerts reduce dwell time and speedy response.
- ✓ Audit trail of changes and remediation actions for compliance.





Unified
Asset
Inventory

Risk Factors
Aggregation

Threat
Intelligence

Business
Context

Risk
Prioritization

Risk
Response
Orchestration

Compliance
& Executive
Reporting

Identity Actions

One-click actions:
disable/quarantine, enforce
MFA, reduce privileges,
remove toxic rights.

01

02

Patch + Fix

Remediate identity
vulnerabilities &
misconfigurations with 200+
AD controls & scripts.

03

Mitigate

Use policy hardening &
compensating controls when
patching isn't feasible.

04

Customize for your needs

Build custom controls &
playbooks with CAR,
aligned to approvals.

05

ITSM Workflows

Scale via SNOW/Jira
(auto-open/advance/close)
with evidence.

Isolate

Quarantine
devices/accounts; allow
only trusted apps until
risk is removed.

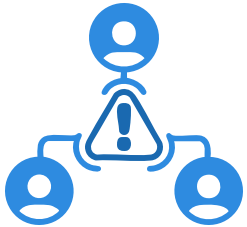
06

Validate & Re-score

Confirm fixes, update
Identity TruRisk™, roll into
org TruRisk™.

07

One solution for unified identity risk management



De-risk human and machine identities for reduced identity-driven attack surface



Cut tool sprawl with unified risk telemetry into a single view for frictionless risk orchestration



Make faster decisions with one risk language for board-ready prioritization.



Eliminate the most exploitable attack paths first using closed-loop remediation.

**Let's take a closer
look with a demo**

Qualys ETM Identity

Scan QR Code for a no-cost
30-day trial.



Learn more
qualys.com
/identity



Scan QR code
and get early
access



Talk to our experts
for **personalized**
consultation.





GE VERNOVA

ENTERPRISE IDENTITY CONCERNS

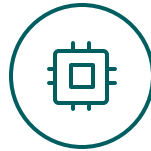
Corey Amsler, GE Vernova



Corey Amsler
Director
Risk Management - EVM



16 years at GE/GE Vernova



Extensive experience across spectrum of IT

- ✓ 6 Years Vulnerability Remediation/Patching
- ✓ 5 Years Vulnerability Detection and Response



GE VERNOVA



April 2, 2024
Spun off from GE



**Cambridge,
Massachusetts**
Headquarters



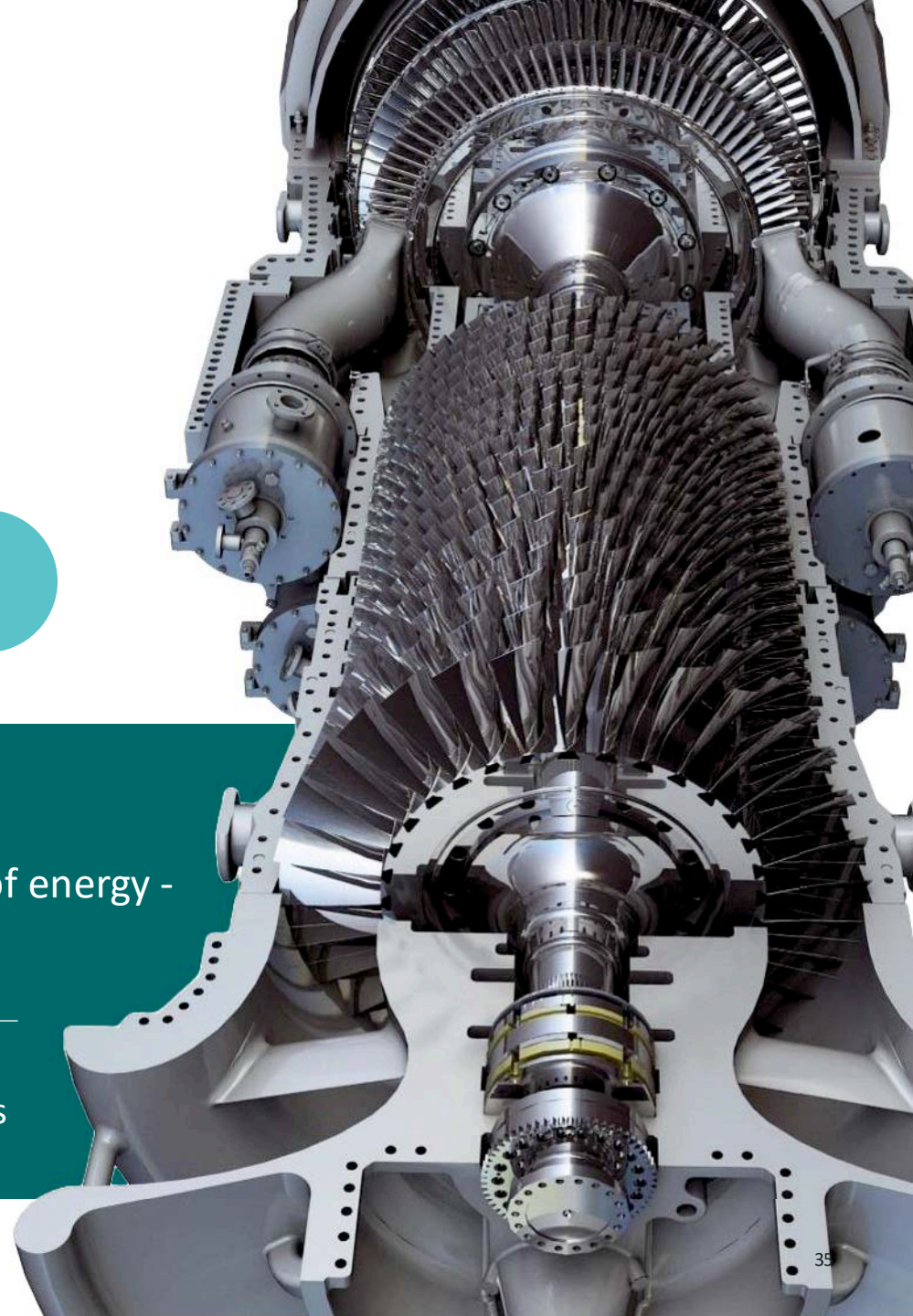
75,000
Employees



Our purpose:

Building on 130+ years of experience, we are leading a new era of energy - electrifying to thrive and decarbonize the world.

Generate ~25% of worlds electricity with 55,000 wind turbines and 7,000 gas turbines



Active Directory Security

AD Concerns



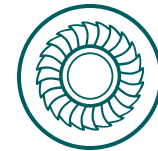
Passwords remain a weak link



Active directory service accounts



Excessive Permissions



Active Directory Certificate Security

Clouds Everywhere

Multi-Cloud Hybrid Environments



Multiple Identity Stores



Independent On-Prem and Cloud IDP



Lack of a holistic offering

Cyber Security Compliance

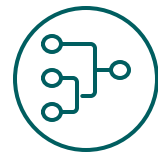
Name your regulation or favorite acronym



Constantly changing and new regulations



While necessary it does add a lot of burden



Similar controls across key regulations (HIPPA, SOC 2, Etc.)



Strong authentication



Password management



Access controls



Least privilege

What Do We Need



Coverage against
misconfigurations
in cloud IDS
solutions



Monitor active
directory in real
time for
suspicious
configuration
changes



Establish
comprehensive
KRI measures



Clearly and
transparently
prioritize
identity-related
security
weaknesses



Holistic
approach to
identity security
as part of an
interactive
dimension of
overall risk



Corey Amsler

Director

Risk Management - – EVM @ GE Vernova



www.linkedin.com/in/coreyamsler/



www.gevernova.com

Scan Here

