
tenable
Optimising Business Outcomes
From Your Existing Cybersecurity Strategy
Nathalie Dib - Territory Manager
Graham Harris - Security Engineer

AGENDA

Tenable, what we do and why –

- Threat Intelligence
- Real Attck paths
- Exposure Management

tenable

The world around us.... The Threat Intell context

Business
Digital
transformation.

Technology growth
A.I.

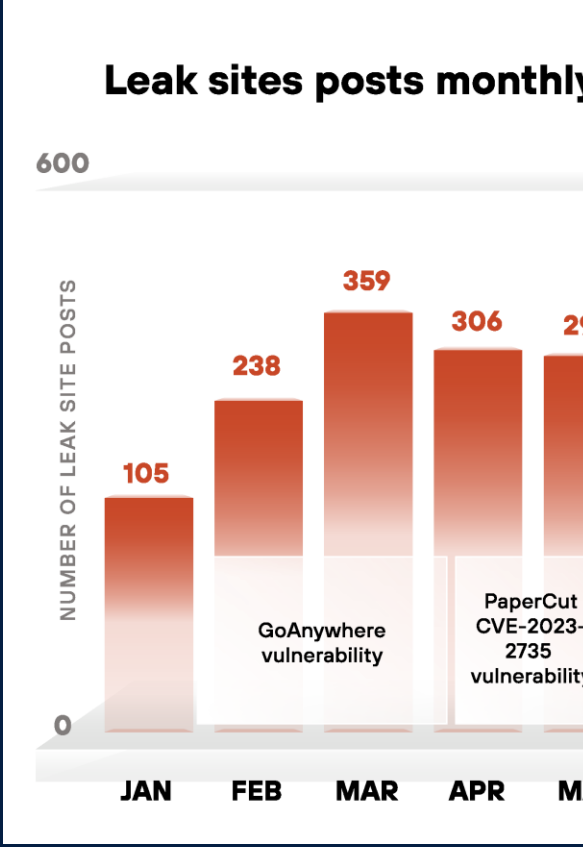
Multiple crises
Geo-political
context.

WEF Risk Report 2024

Cyber Insecurity in the TOP 5 for the next 2 years

https://www.weforum.org/publications/global-risks-report-2024/digest/

10 January 2024



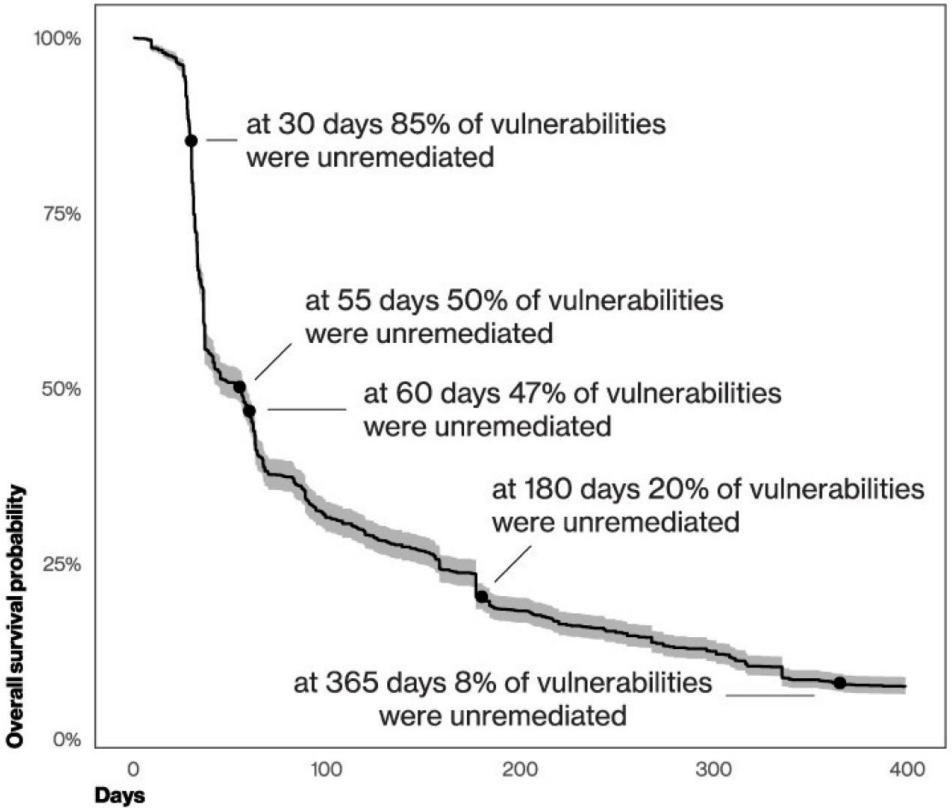


Figure 19. Survival analysis of CISA KEV vulnerabilities

Source : Ransomware Retrospective 2024: Unit 42 Leak Site Analysis
Source : Verizon Data Breach Incident Report 2024

tenable

Attack surface complexity

Risk of Exposure

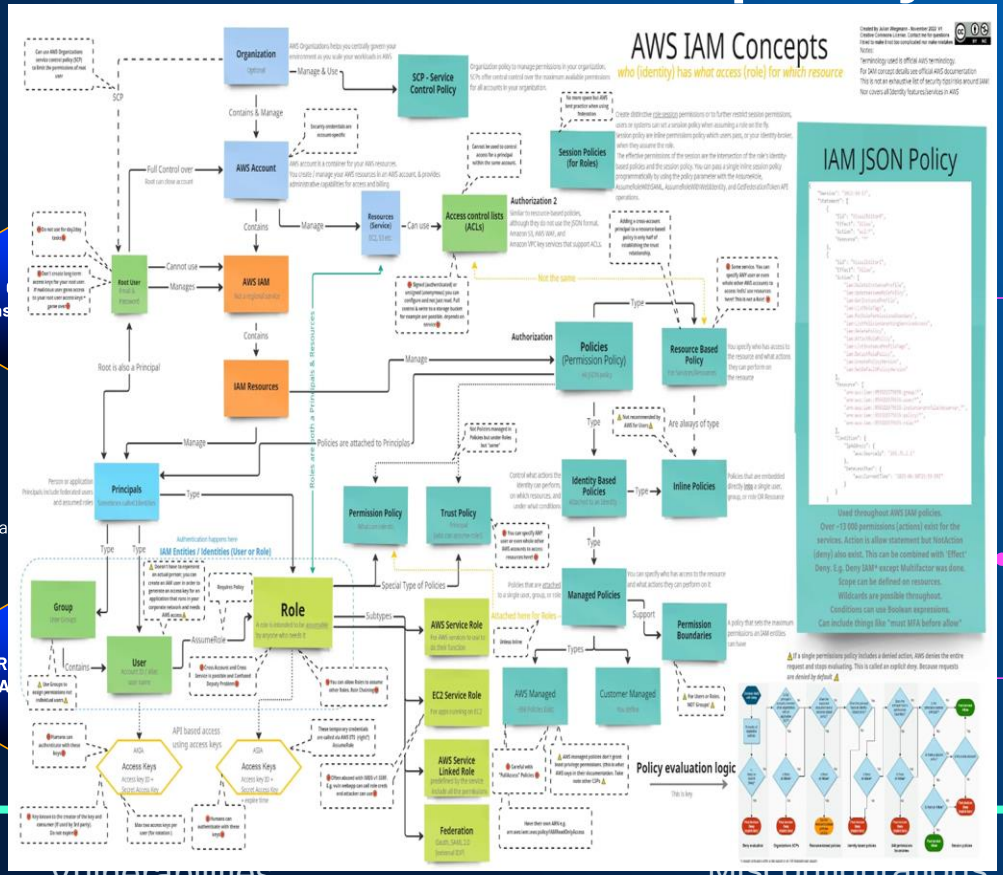
Container

Laptop

Mobile

ICS/SCADA

Applications



Vulnerabilities

Misconfigurations

Attack surface Complexity

tenable

AGENDA

- Real Attck paths

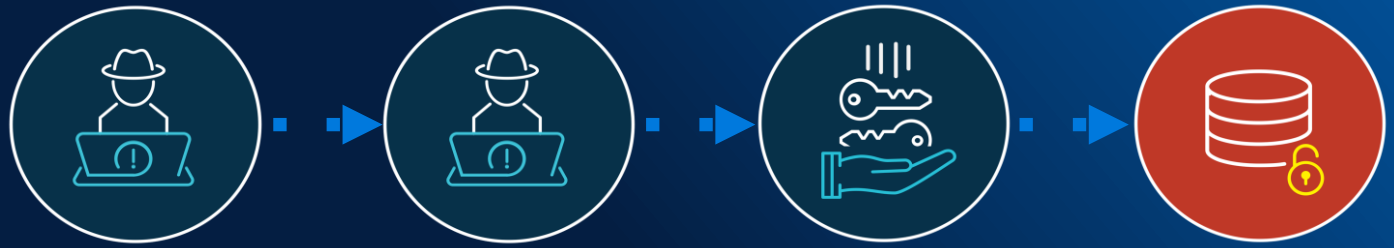
tenable

Toxic combination Cloud Access -> LastPass

Objective : exfiltrate & **delete**

Goal : monetize or publish the data obtained

Operating mode : Toxic combination combining an old (2 years) known vulnerability, identity compromission, wrong cloud access, from a home worker



Vulnerable App Exploited (CVE-2020-5741)

KeyLogger installed

DevOps Master Key Having access to the Cloud storage decryption key

Cloud Unencrypted Database/S3

Developer target selected after the first data breach (August 22) – Identity Compromised

tenable

Biggest 2023 data breach -> DarkBeam

Objective : exfiltrate

Goal : monetize (extorsion only) login credentials, specifically email and password combinations.

Operating mode : ElasticSearch / Kibana unprotected **Access, non-malicious human error.**

usernames and passwords

health	status	index	uuid	pri	rep	docs.count	docs.deleted	store.size	pri.store.size
green	open	[redacted]-2019.04	DjGMc7VoSJexpwM4CAalGQ	5	0	8419	0	51.7mb	51.7mb
green	open	[redacted]-2018.10	M18r6UUfTsCBfxikd5q3Mg	5	0	163721	13	1.1gb	1.1gb
green	open	[redacted]-2018.12	u6mvnOY6TnO6u2WzcfmJ_g	5	0	182113	104	1.4gb	1.4gb
green	open	[redacted]-2019.03	6jVuuDR4Tdi1Pd9npoU5kA	5	0	194468	695	1.2gb	1.2gb
green	open	[redacted]-2019.01	h7Ezp5gYSv6jG-Y40Wcf8g	5	0	215969	115	2gb	2gb
green	open	[redacted]-2019.02	TDt81AivRKukJzOsUFh04w	5	0	189657908	466383	218.8gb	218.8gb
green	open	email-2	yjCCtoCkSBCXeJfiSXthzg	5	0	239635510	84198975	81.9gb	81.9gb
green	open	email-6	1eFEqvcCR0GBADwVRfeaJw	5	0	239640444	81944720	81.4gb	81.4gb
green	open	email-9	9zN-OD2xTSWN20KRCoMOjQ	5	0	239651348	82721708	81.6gb	81.6gb
green	open	email-b	QqLBWD5bR2CcfwTmYwsblQ	5	0	239657545	83456018	81.8gb	81.8gb
green	open	email-c	u57X50HpRVyq0PISkrkLVg	5	0	239660329	82824611	81.6gb	81.6gb
green	open	email-8	JRG_kK0hTyutstmSvim5cg	5	0	239661288	81163247	81.3gb	81.3gb
green	open	email-a	8j9LYm_DS-qYGkKJ9giM7w	5	0	239661662	83290455	81.7gb	81.7gb
green	open	email-1	Wc-p1S2KSE--6m6SDiUh1w	5	0	239662511	82008061	81.4gb	81.4gb
green	open	email-0	_kV_63pvT1Oh3PZrhQ7a0g	5	0	239663361	79711849	80.9gb	80.9gb
green	open	email-f	JmhkVDtNTieS3J0bUB2x9A	5	0	239664424	80282082	81gb	81gb
green	open	email-4	gVpPnQxJQKGY47BA6mMK1w	5	0	239667855	79470476	80.8gb	80.8gb
green	open	email-3	X2k4TIm0ROK_2PmKqLW0LA	5	0	239670242	80255347	81gb	81gb
green	open	email-d	YwLOA4v0RWqBsvq9mz2xPQ	5	0	239672625	82880420	81.6gb	81.6gb
green	open	email-7	ZqG9UiLcSfy7TjD4FZhNmQ	5	0	239682351	80771765	81.1gb	81.1gb
green	open	email-5	jhwEDUa2T-K9ujbT496iZw	5	0	239686954	80562633	81.1gb	81.1gb
green	open	email-e	OJlvosJ8On2VHXVl0GOwCw	5	0	239688029	82317917	81.5gb	81.5gb
green	open	[redacted]-2018.11	6qz-OKkNTpiL06F_JoxCIQ	5	0	250586977	1248110	310.4gb	310.4gb
green	open	fdns-any-2021.10	2MQFcZ1fSeuoxuSn-RBSTQ	5	0	2989576945	0	523.1gb	523.1gb

3.8 Billions records exposed

(Secure ?) file transfer 2023 -> MoveIT

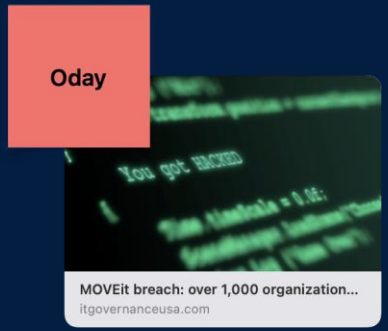
Objective : exfiltrate **& delete**

Goal : monetize and publish

Operating mode : 0_day and non-patched vulnerability (after several months)

Impact : **8000+organisations*, 1587 breach notifications, 60 Millions users**

Group : ClOp ransomware (RaaS)



Formed in 2019 encrypting sensitive data and extorting its victims.

MOVEit attack is noteworthy because they've **abandoned encryption** and are **simply extorting** their victims not to release the data they've stolen.

Other file transfer attacked by ClOp

- GoAnywhere (File transfer attack)
- Accellion (File transfer attack)

tenable

AGENDA

- Exposure Management

  a Pro-active apporach.

tenable

tenable one™

Comprehensive Visibility & Exposure Management
for a Hybrid Multi-Cloud World

Inventory Assets

- MULTI-CLOUD
- IDENTITY
- UNMANAGED
- WEB APPS
- OT/ICS
- PRIVATE & IT

Analyse Risk

- RESEARCH
- AGGREGATE
- NORMALIZE
- CONTEXTUALIZE

Communicate Priorities

- TECHNICAL EXPOSURE
- BUSINESS EXPOSURE
- COMPLIANCE
- REMEDIATIONS

Program ROI's	Business ROI's
PRODUCTIVITY GAIN REDUCED RISK BETTER COMMUNICATION	ENABLE BUSINESS
ROBUST DETECTION ENHANCED CONTEXT IMPROVED PRIORITIZATION	COMMUNICATE & PRIORITIZE RISK
AGGREGATION OF DATA CONSOLIDATION OF TOOLS REDUCED COST	CONSOLIDATE & OPTIMIZE EFFICIENCY

tenable®

To scale, we must approach security from an attacker's perspective...

Discover the
ATTACK SURFACE

1

Identities

Assets

Identify external & internal facing assets & identities

Identify
PREVENTABLE RISK

2

Vuln I Misconfig I Excess Permissions

Detect 3 forms of risk used to gain access & move laterally

Align with
BUSINESS CONTEXT

3

Business Service A

Business Process B

Link assets, identities & risk to business to focus on what matters

Remediate
TRUE EXPOSURE

4

Excessive Machine Permissions

Enforce Least Privilege

Assess attack path viability & choke points for remediation

Continuously
OPTIMIZE INVESTMENTS

5

People

Process

Tech

$$$

Risk

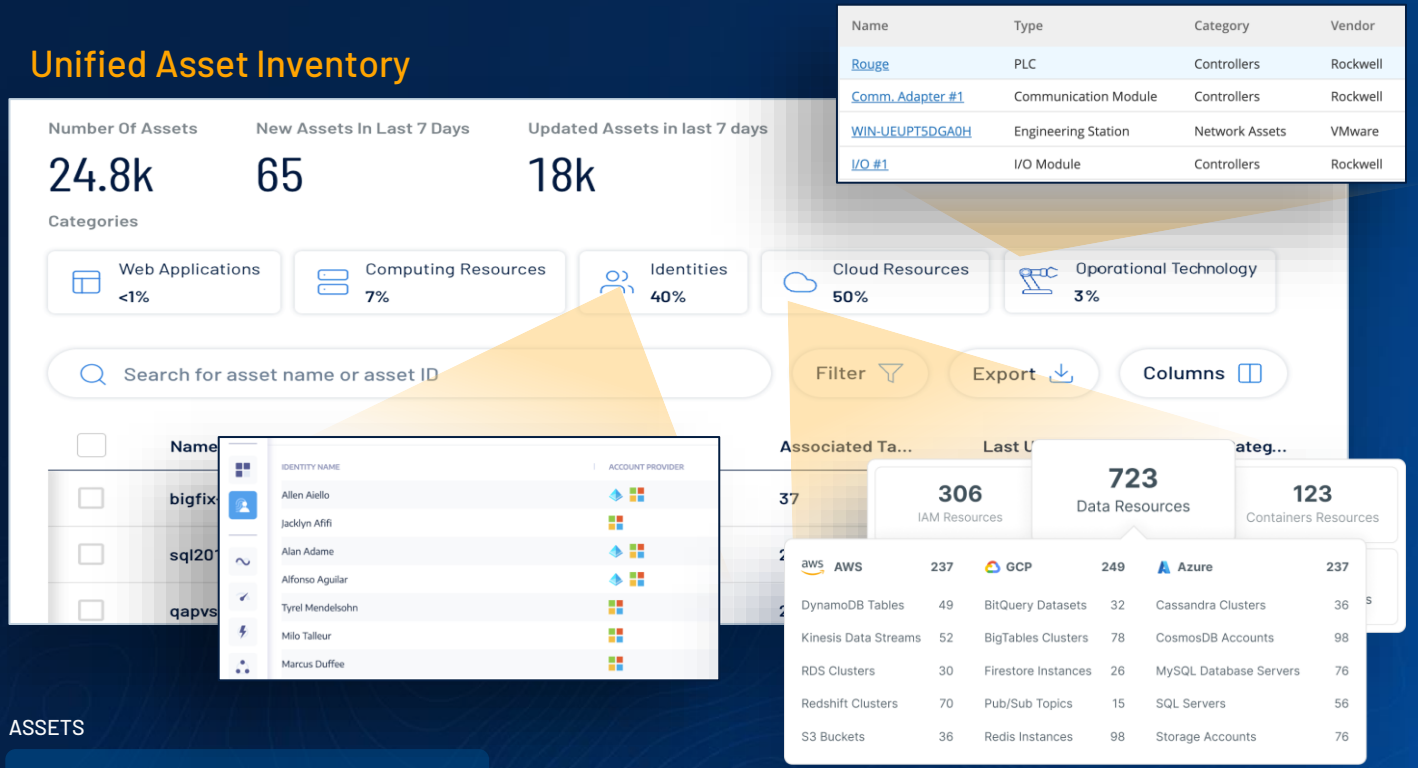
Compl.

Innov.

Measure and prioritize resources for better outcomes

Document the attack surface

- **Discover all identities:**
  - Continuous discovery of Human & Machine IDs
  - Multi-Cloud & Active Directory
- **Discover all assets:**
  - Cloud, Hybrid Apps, Unseen assets, OT, IoT, IT
  - Details: Config, change history, connections...



IDENTITIES

Human Machine

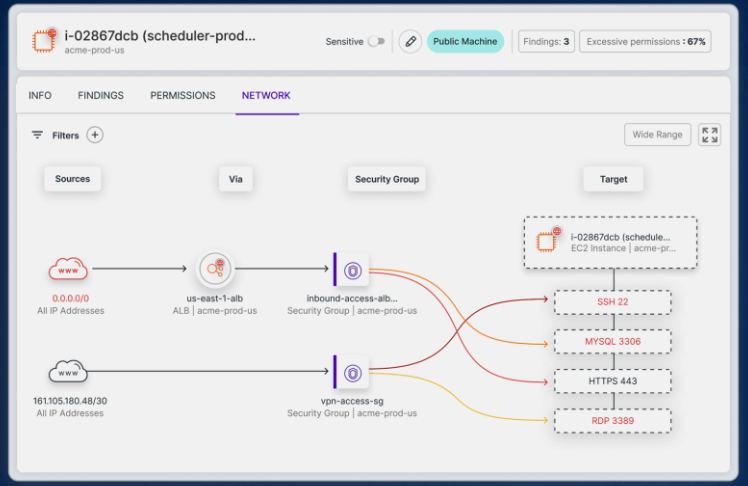
ASSETS

Cloud Hybrid Apps Unseen OT I IoT IT

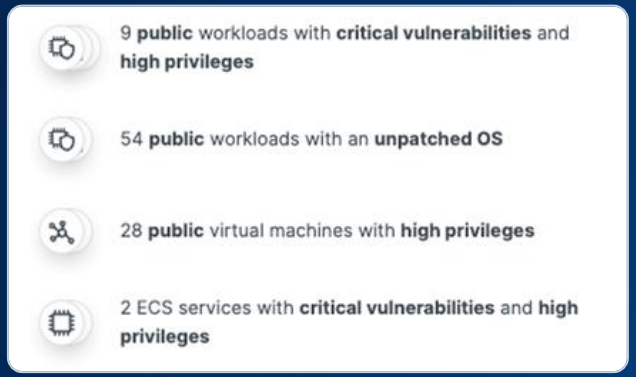
tenable

Contextual Intelligence: Prioritize Technical Exposure

Network Exposure

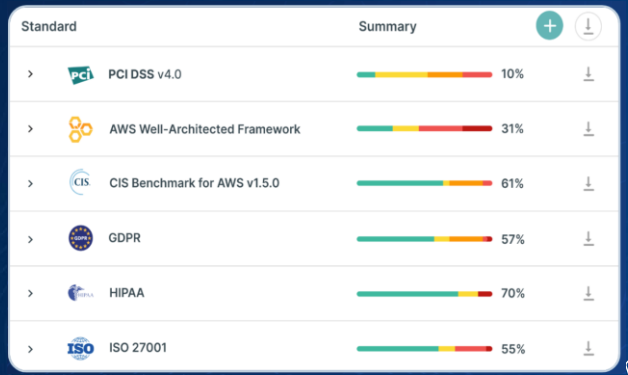


Toxic Combinations



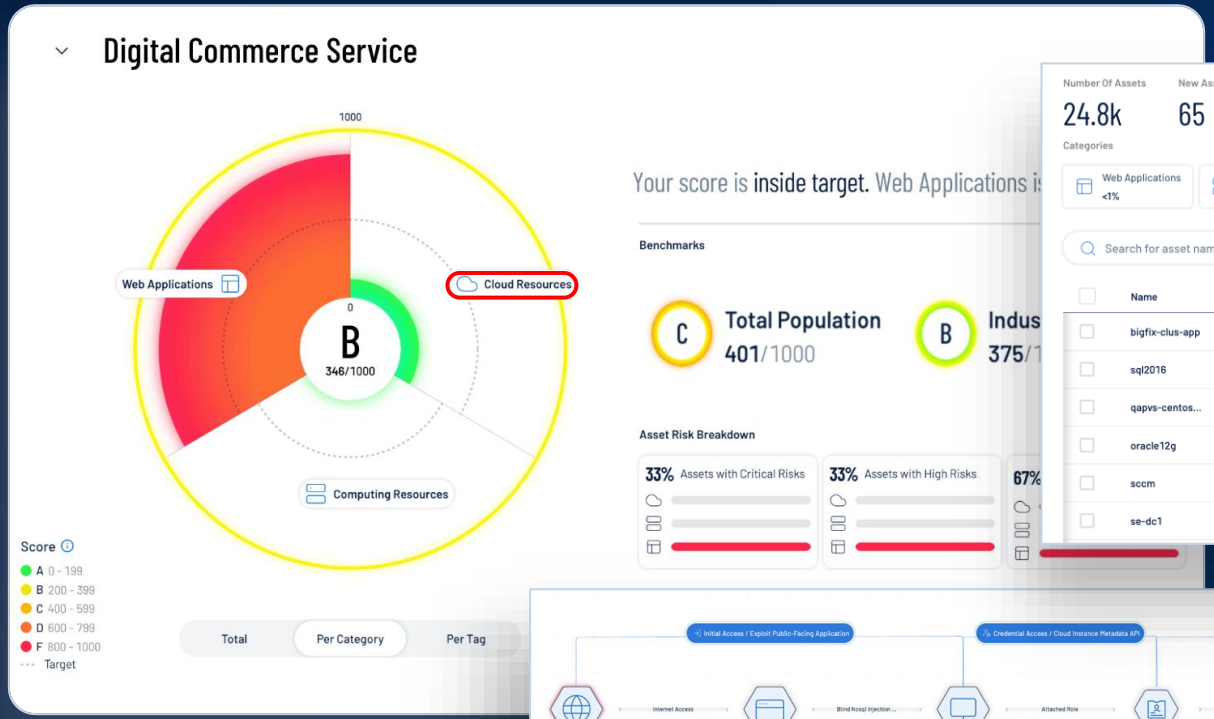
Permissions & Usage

Compliance



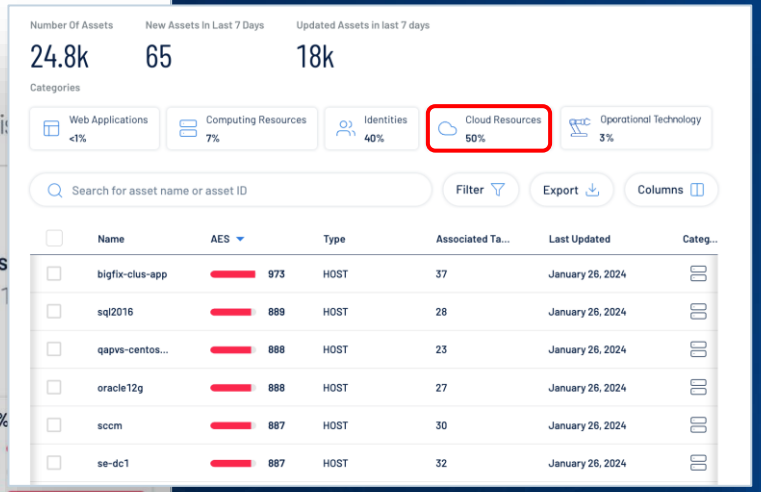
tenable

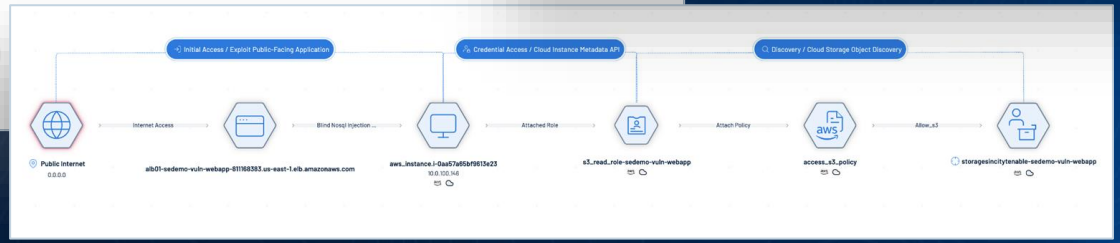
Optimize Communication: Across Teams & with Execs



Business Exposure

Asset Inventory

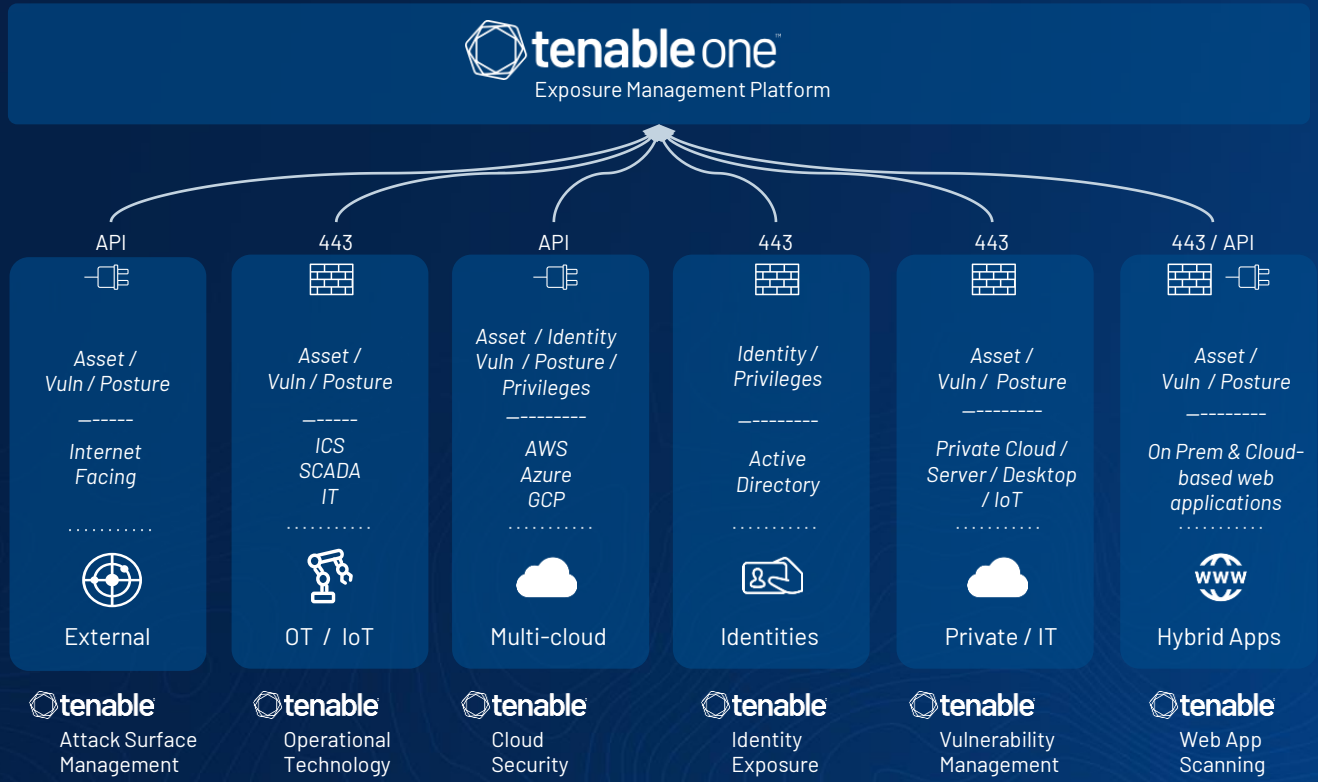




Attack Paths

tenable

Tenable One Sensor Data Collection



tenable


tenable
Thank You