Business Aligned & Threat Based Prioritization

Focusing the security program and its partners on what matters most.

Let’s Start With Some Numbers

The stats speak volumes. **It’s become increasingly impossible to address all operational exposures.** Focus is critical.

40,187

Vulns

in 2024.
13,610 were either critical or high

3X

Exploits

increase in exploitation of vulnerabilities as an initial point of entry

137

MTTR

Days Average # of days it took for critical vulns to be addressed

60%

Backlog

Average number of vulns left unaddressed in an average org

Growing Pressure

The complexity of our business landscapes have evolved exponentially. We didn't move to the cloud, we added the cloud and many non-traditional assets to an already complex environment at an unparalleled and accelerated rate.

41.2B

The number of connected assets (IT/OT/IoT/IoMT) is expected to grow from 23.8 to **41.2 billion by 2025.**

Attack surface expansion means organizations are **unable to keep up with regulatory security and compliance.**

80%

Of assets will be **unseen, unmanaged and not secured by 2025.**

Unmanaged and specialized IoT/OT assets create **blind spots and security risks.**

90%

IT professionals say **rapidly-changing environments** make asset management difficult.

Shift from air-gapped environments and the convergence of IT/OT due to the **prioritization of efficiency.**

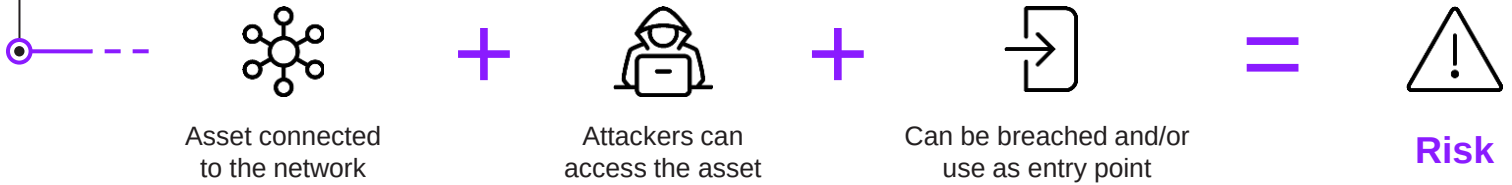
60%

of data breaches involved **unpatched OT asset vulnerabilities.**

OT and IoT environments are now the primary target of ransomware attacks because **OT/ICS environments host the enterprise's most critical assets.**

Every Connected Asset expands the **Attack Surface**

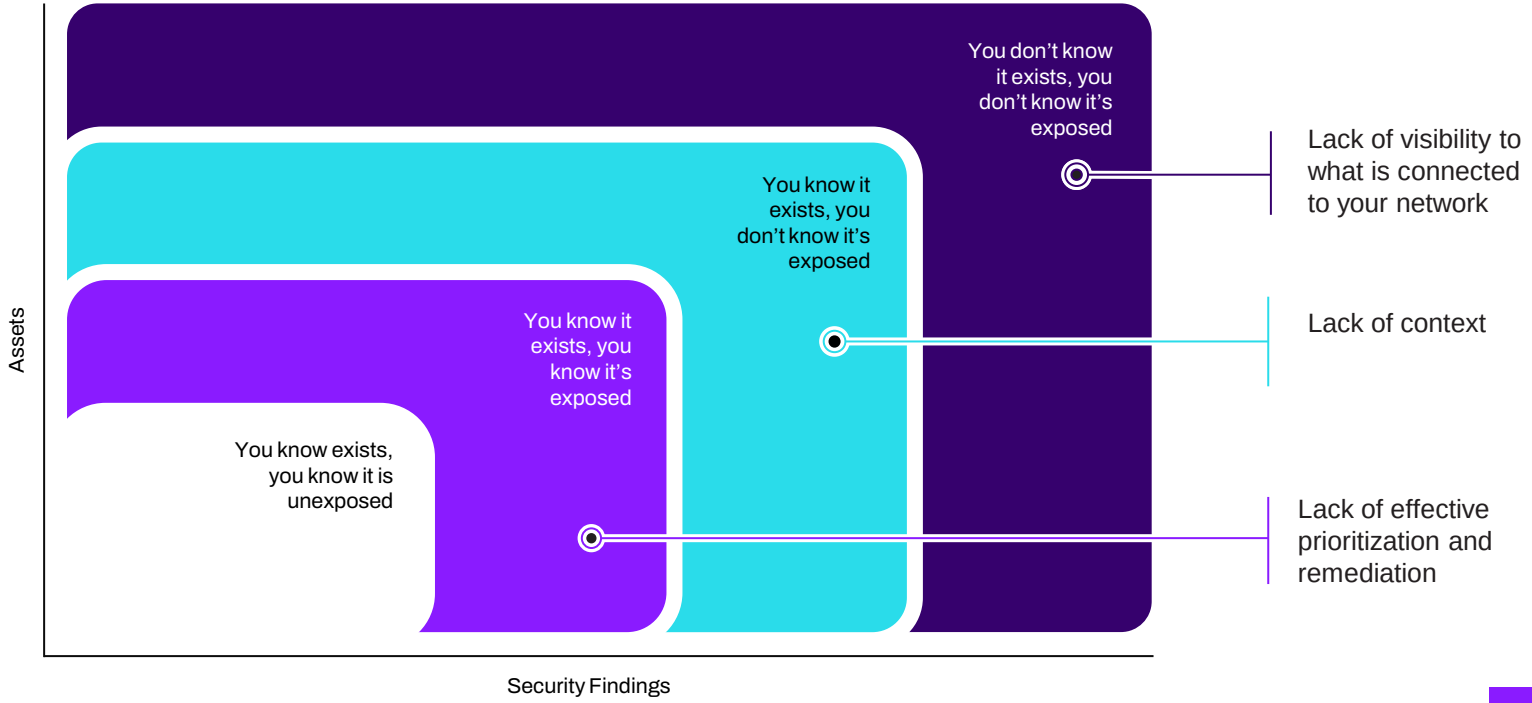
Assets



Security Findings

- EOL/EOS OS or App
- CVEs
- Default Credentials
- Missing Agents
- Insecure Protocols
- Security Control Coverage Gaps
- Bad Segmentation
- External Facing

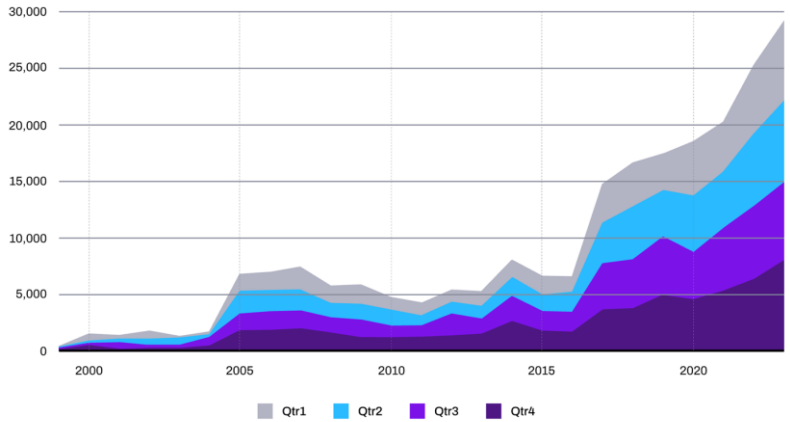
Visualizing Today's Attack Surface



Legacy Vulnerability Prioritization Is Failing

Relying on CVSS scores alone is not preventing material attacks from materializing. Threat actors are exploiting known industry-wide service practices and service levels.

Total CVEs Over Time



Unable to prioritize the **vulnerabilities that actually matter most.**

- It's become nearly impossible to keep up with even just the critical and high risk CVEs.
- Prioritizing actions that can reduce the highest number of vulns doesn't necessarily equate to reducing business risk.
- Threat actors are increasing targeting the vulnerabilities that they know we're not getting to, stringing multiple vuln exploits together to materially impact our operations.

Programs Should Focus On 3 Key Questions

- What do I **have**?
- What is **important**?
- How do I **fix “it”**?

The Path Forward

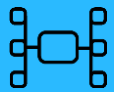
Discover, Identify, Contextualize

Find, identify, and contextualize all connected assets, map their connections and dependencies, relate assets to key business systems and services.

Assess and Prioritize

Assess, consolidate and dedupe all security findings.

Prioritize most urgent findings based on the likelihood to be exploited, early warnings and business impact.



Remediate

Orchestrate remediation and enforcement actions

Automate consolidation and remediation ownership assignment. Streamline operational management based on actual remediations.

Monitor and Report

Monitor for anomalous and exploitative actions with the potential to impact assets of importance and facilitate contextual responses.

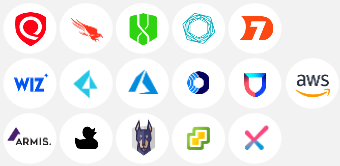
Report on executive level business risks of importance and risk reduction progress.

Proactive Risk Prioritization

Consolidate visibility of priorities (asset plus security findings)

Automation & Contextualization

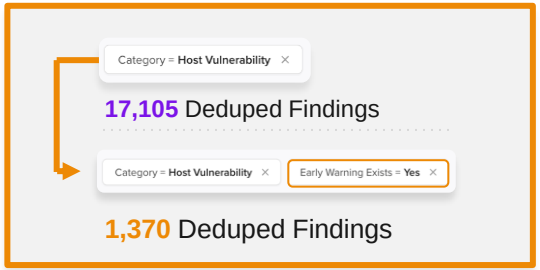
- Consolidate findings & automate assessment
- Inventory and enrich asset profiles
- Adapt risk scoring for technical, environment and business context



Tighten scope on vulnerabilities being exploited, weaponized on exposed, critical assets

Early Warning Vulnerability Intelligence

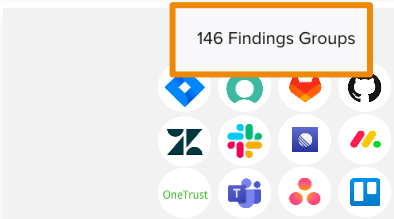
- Early warning intel on vulnerabilities being exploited
- Early identification of weaponized vulnerabilities
- Actual Risk: asset + finding +threat



Minimize the window of exposure with remediation operationalization

Remediation Lifecycle

- Assign owners for remediation tasks
- Group findings by fix for bulk ticketing
- Enable security team and fixer collaboration
- Monitor and report



Key Business Outcomes

Business-Based Priorities

Prioritize proactive and reactive efforts based on what matters to the business, how it's exposed, and how it's being targeted.

Business-Aligned Protection

Contextually justify, fund, and focus resources on implementing safeguards that positively affect the business in ways that matter.

Business-Focused Messaging

Deliver improved messaging about what's placing the business at risk, how that risk is being addressed / has been reduced, and how the security program is materially benefiting the business. Leave the legacy "cost center" mentality behind.

Thank you!