ivanti

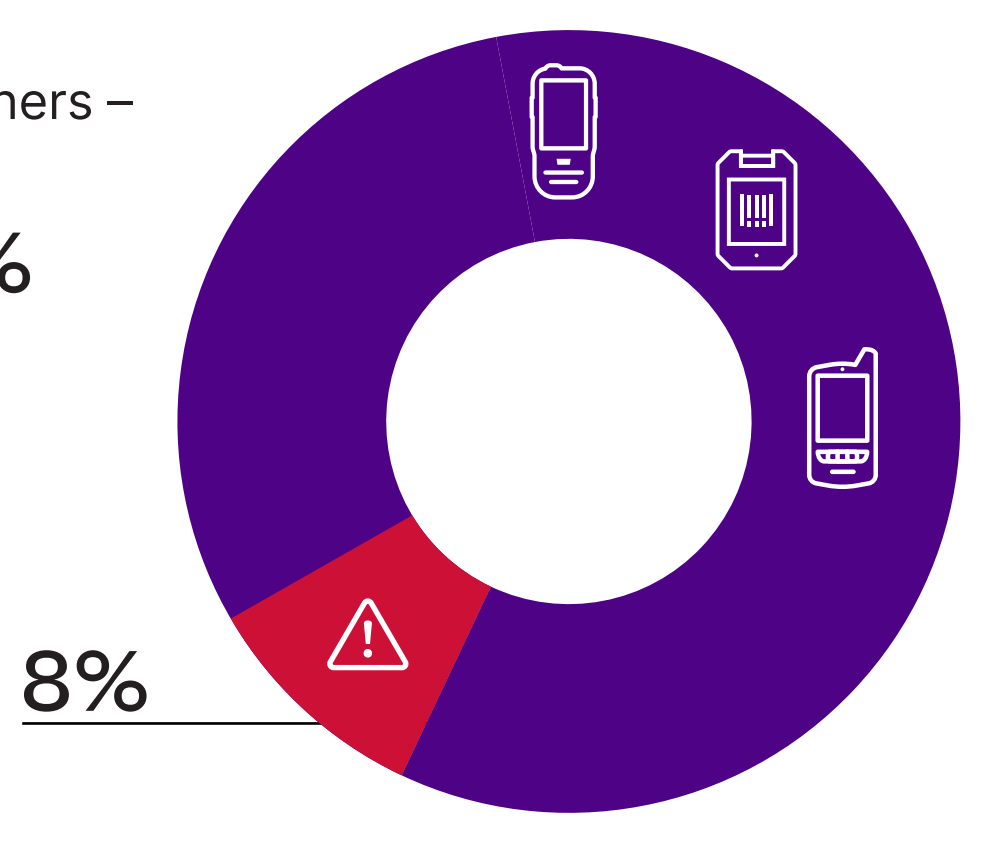
Five Things to Fix About Vulnerability Management

1 Your vulnerability blind spots

You can't protect and patch what you can't see – or know to look for.

1 of every 3 employees at Fortune 1000 companies use unapproved cloud-based SaaS apps.[i]

Three of the most popular scanners – Nessus, Qualys and Nexpose – **still miss almost 8%** of known ransomware vulnerabilities combined.[ii]



2 Lack of team bandwidth

Imagine trying to patch every vulnerability or risk that exists – or just manually reviewing vulnerabilities for those most relevant to your organization and environment.

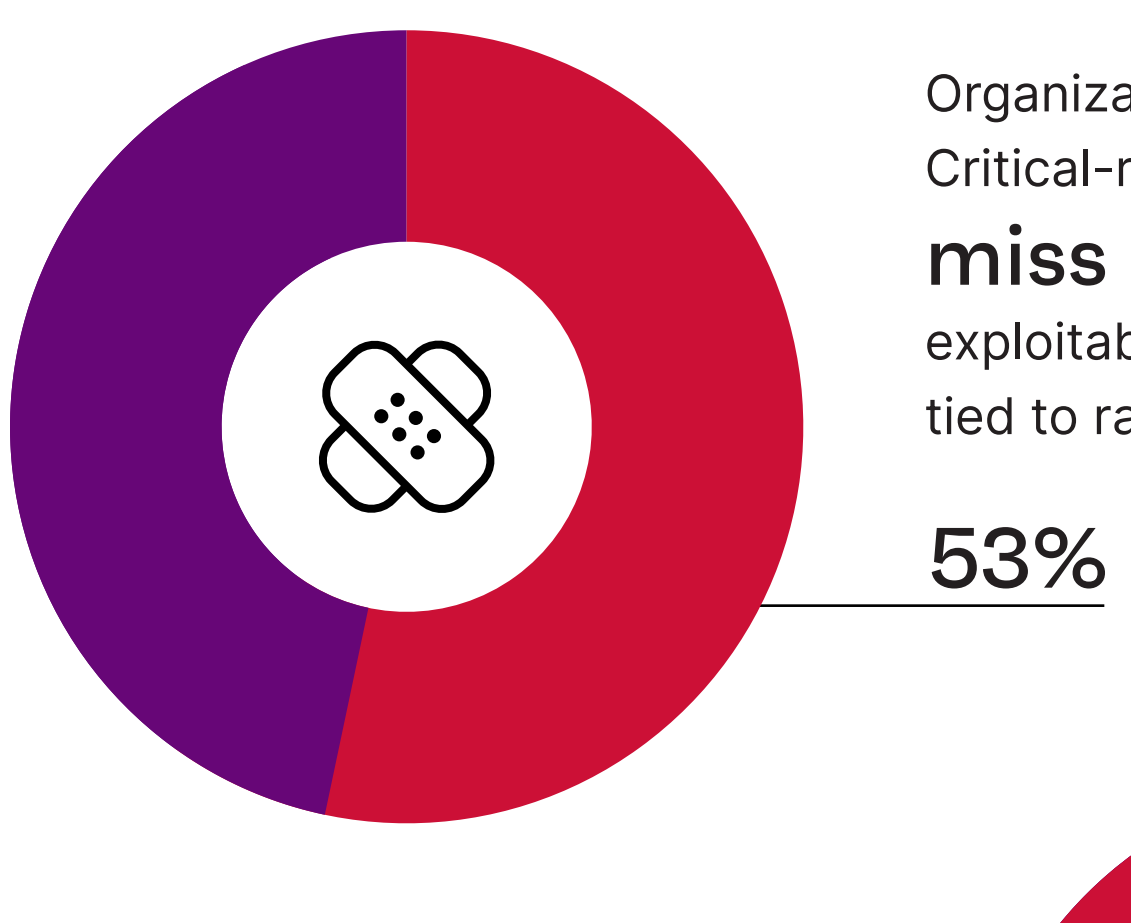
236,000+ Total number of Critical Vulnerabilities and Exposures (CVEs)

29,000+ Weaponized CVEs

9,600+ CVEs with Remote Code Execution (RCE) and/or Privilege Escalation (PE) capabilities

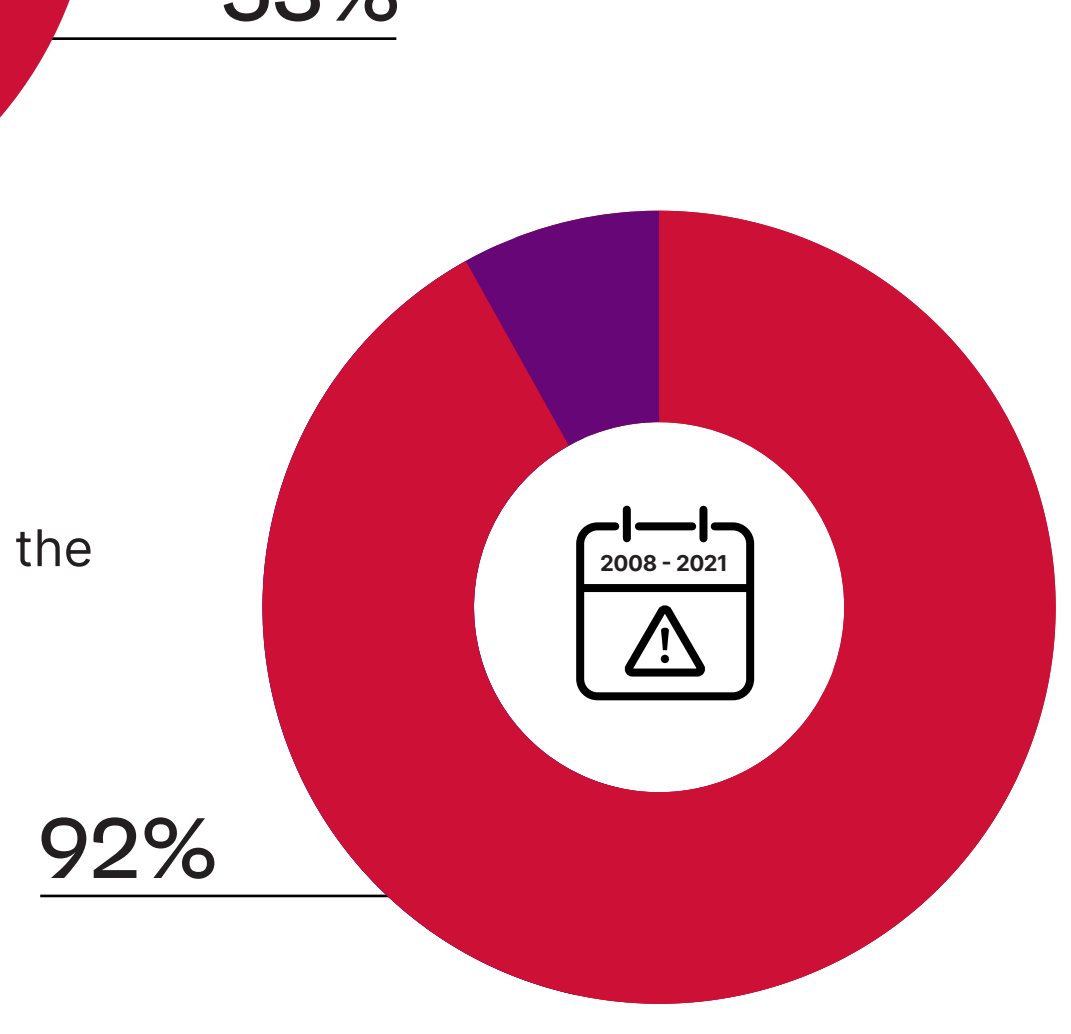
3 Exposure to less "critical" and older CVEs

Not all vulnerabilities pose the same risk – and you can't tell what's relevant for your organization just by looking at age or criticality.



Organizations only patching Critical-rated CVEs would **miss 53% of all** exploitable vulnerabilities tied to ransomware.[iii]

92% of all actively trending vulnerabilities are older than the past year – with some first published in 2008![iv]



4 Few program resources and internal buy-in

Basic RBVM

Prioritization through CVSS scores & scanner scores

Weaknesses
Is heavily dependent on data quality and frequency of scanner updates

Misses lower-scored vulnerabilities relevant to organization-specific risks

Strengths
Vulnerabilitymanagement exists

Intermediate RBVM

Prioritization through exploitation probability of past year's CVEs

Weaknesses
Needs constant manual tuning & verification

Misses still-relevant older vulnerabilities (+1 year)

Strengths
Prioritizes remediation beyond CVSS score

Emphasizes new vulnerability patches

Advanced RBVM

Prioritization through multi-sourced threat intelligence & contextualized organization risks

Weaknesses
Requires a comprehensive tool suite to cover multiple data sources

Strengths
Contains all possible sources of vulnerability data

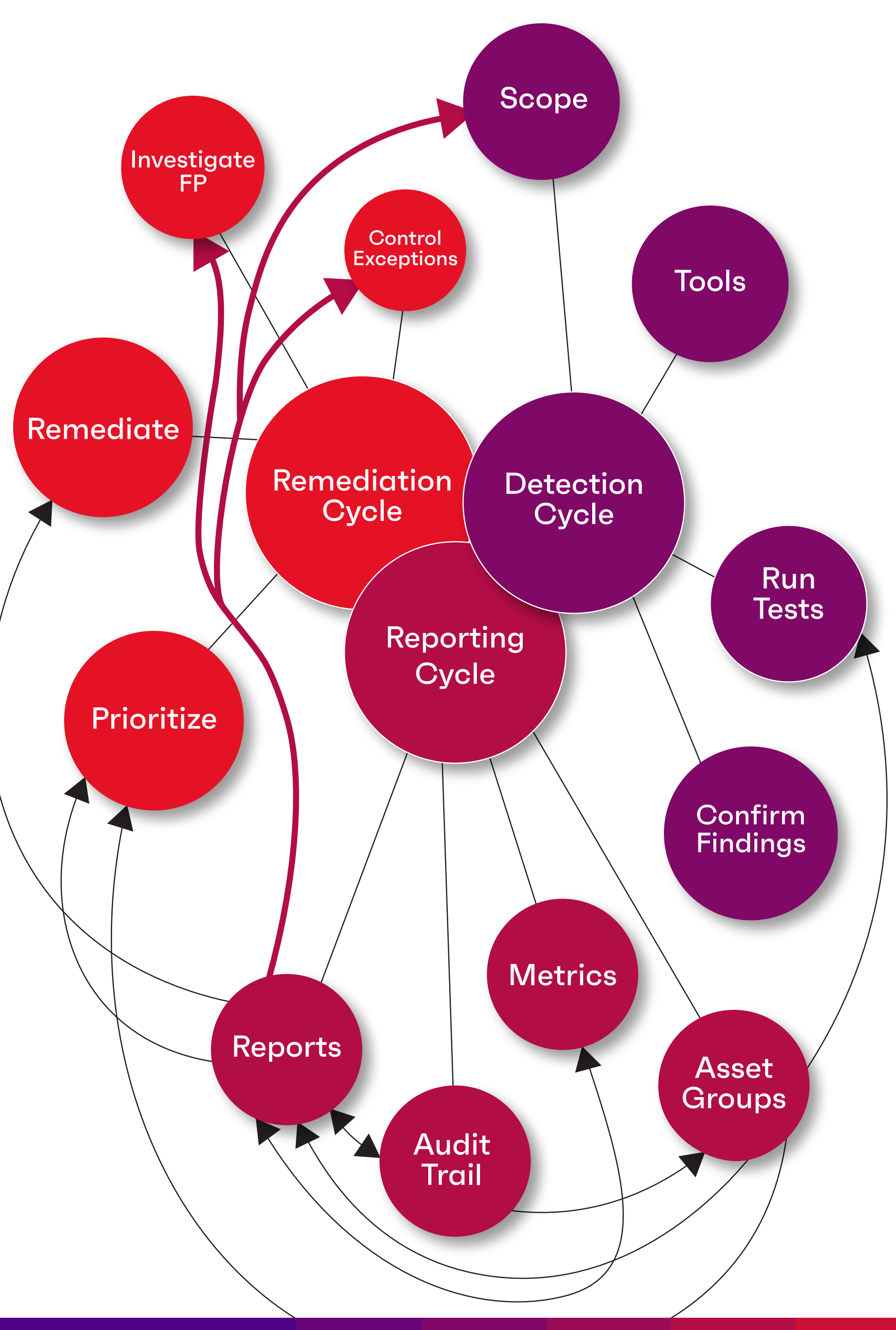
Prioritizes based on unique organization-specific risks

Pivots quickly to incorporate new contexts and refine prioritization

5 Reporting

Effective vulnerability management programs can quickly create a tangled web of required cross-departmental detection, remediation and reporting to execute properly.

Without some sort of automation tool to aggregate, prioritize and display vulnerability information and activities, your cybersecurity program could be killed by reporting requirements before it ever begins.[v]



It doesn't have to be this way.
Read the 2022 Spotlight Ransomware Report for the latest trending vulnerabilities.

Download the Report

i "Why shadow IT is the next looming cybersecurity threat" (The Next Web)
ii Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management
iii Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management
iv Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management
v OWASP Vulnerability Management Guide (OVMG) - June 1, 2020