RISK-BASED VULNERABILITY MANAGEMENT:

A CISO Executive Guide

Using business context to prioritize risk issues

Balbix®

Align Your Vulnerability Management Program to the Business

The hard truth is that most security teams are failing at vulnerability management because it's completely disconnected from the business. They have no idea which vulnerabilities have the potential for doing the most damage to your business. As a security leader, this isn't easy to accept. Throwing more people at the problem won't solve it—not that you have more resources.

In this guide, we'll uncover the reasons why aligning vulnerability management with the business is difficult. We'll also discuss measures your team can take to overcome these challenges.

Challenge:

Why vulnerability management is out of step with business risks

Fundamentally flawed approach and outdated technology

The biggest reasons why your vulnerability management program is failing and disconnected from your business and its mission is because your security team is still operating in an old model and using outdated technologies.

Legacy vulnerability assessment (VA) scanners inundated your security team with streams of vulnerability data without any business context. As a result, the number of vulnerabilities is staggeringly high and stays stubbornly high. The data volume is an operational challenge. And your security team struggles to demonstrate progress—which kills morale and leads to burnout.

Your security team's primary strategy for remediation is fixing vulnerabilities with high CVSS scores regardless of the underlying assets because this is what their tools are telling them to do. The problem is that if an asset is critical to your business mission, then even a low or medium vulnerability can have a catastrophic impact. Instead, your team should be focused on risks to your critical business assets, as we'll explain shortly. Using asset impact and risk to prioritize vulnerabilities is necessary, however, clean asset and business impact data is difficult to get. Even when you have it, it can be a challenge to convince auditors to accept that new process.

Shifting to an asset-centric approach isn't easy

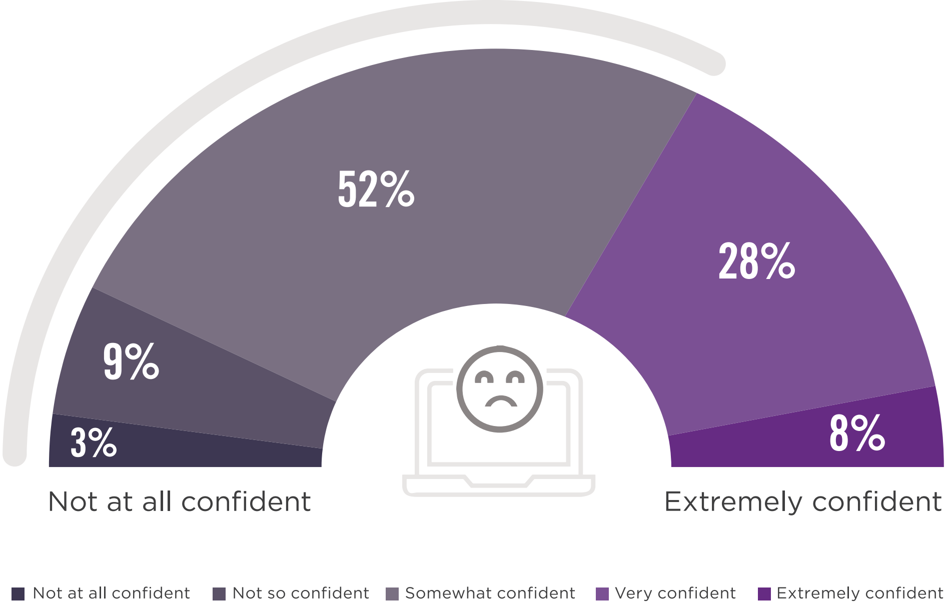
As we noted earlier, your team needs a major paradigm shift from being vulnerability-focused to asset- and risk-focused BUT this isn't an easy shift. To start, they need to have enterprise-wide visibility into the assets of your organization. Unfortunately, for most security organizations, a unified, accurate and continuously updated view of their company's assets is practically impossible.

- Assets change constantly—devices are added, reconfigured, and retired.
- Information is siloed and fragmented. Different parts of the organization use their own tools to manage assets, tools such as CMDB, EDR, VM, Active Directory, native IaaS tools and other cloud infrastructure management applications.
- The collection and categorization of asset information across multiple tools is often performed manually. This reduces the time available to fix issues and leads to conflicting data.
- Asset data is not updated in real-time—which means the data is often stale. As a result, security teams have little confidence in the data from existing tools.

What legacy vulnerability management tools don't do is give your team the data they need. There are huge vulnerability detection gaps for networking, containers, clouds and firmware. For example, VA scanners do a poor job of finding vulnerabilities like Log4Shell and Spring4Shell that are lurking in the software components and services of your assets. Finding these types of vulnerabilities in your custom apps is especially challenging since your existing tools are optimized for popular commercial products.

Legacy tools are also not designed to address the needs of all the different teams involved in remediating vulnerabilities—including security, IT and devops, business and assets owners. The result is a lack of accountability and a culture of blaming others. We'll discuss coverage gaps and the lack of prioritization in more detail later.

64% of organizations say they are, at best, somewhat confident in their security posture



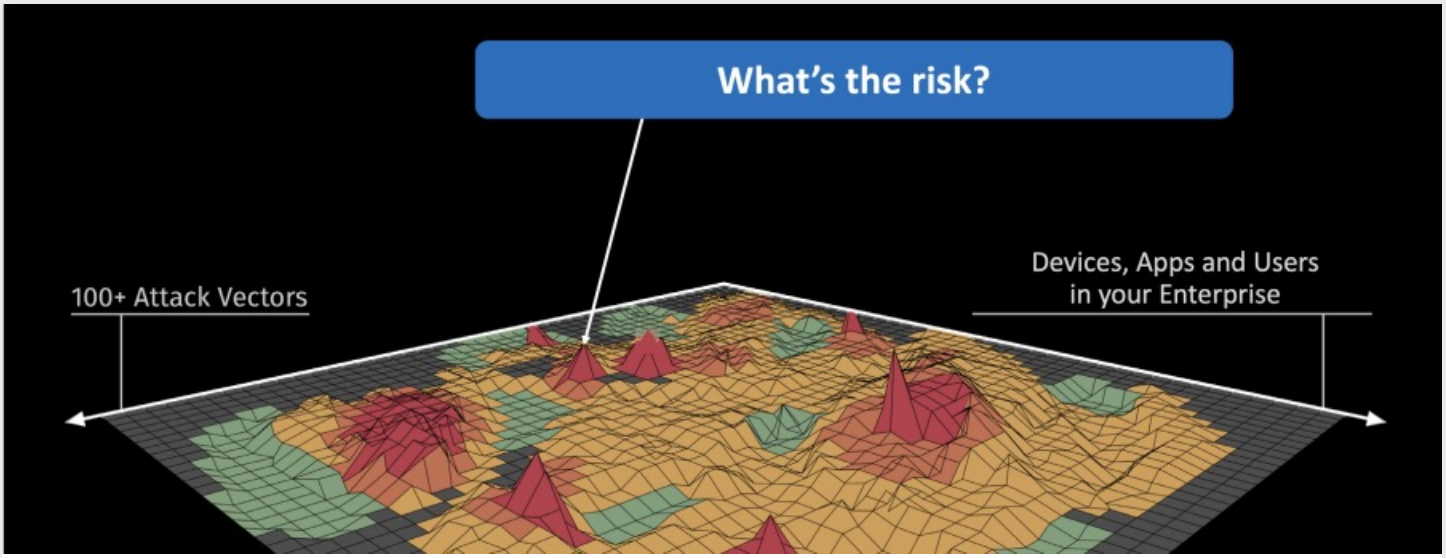
64% of organizations are not confident in their security posture. A lack of visibility into their asset inventory and their inability to prioritize vulnerabilities based on business risk contribute to this.

Source: Cybersecurity Insiders 2022 State of Security Posture Report

Vulnerability data silos and coverage gaps

Another challenge is the abundance of vulnerability assessment tools used across the enterprise. It's not uncommon for an enterprise to have 30-40 tools (for endpoints, web, networks, applications, databases, cloud infrastructure, etc.) as a result of acquisitions, mergers or simply because there's no enterprise-wide standard. Having numerous scanning tools is painful for your team to operationally manage. Manually collecting, correlating and analyzing the information from these data silos takes time and introduces errors—time your security team needs to fix vulnerabilities before they're exploited. Scans take time to cover the environment and it can take days/weeks to understand status via new scans, even when hot vulnerabilities are made public. Your team is under intense pressure to handle these "wartime" scenarios efficiently and struggle to respond quickly and accurately to ensure confidence.

There's also the issue of attack surface coverage. The attack surface for most enterprises was already large and is now exploding. However, traditional vulnerability assessment tools monitor less than 5% of the enterprise attack surface. They primarily focus on CVEs (unpatched software vulnerabilities) and some simple security configuration issues, mostly across traditional assets.



Representation of an enterprise attack surface.

Missing contextual business information

The lack of business context about vulnerabilities and assets is one of the biggest reasons your team isn't aligned to the business. Security teams should know the role of an asset, its criticality to the business, whether it is exposed to outside threats and whether security controls are in place. For example, vulnerabilities (with known exploits) discovered in source code repositories for customer-facing applications should be considered more important than vulnerabilities found in the guest sign-in kiosks in a building lobby. Unfortunately, most tools lack the automatic data classification and contextualization that is critical for focusing a limited budget and resources on mitigating risks that impact your company's mission.

It is extremely difficult to manually collect, correlate and analyze contextual information since contextual data typically resides in different tools and data repositories. Cyber risk context tends to reside mostly in specialized cybersecurity tools (and also, one of the reasons why a traditional CMDB doesn't meet the needs of your team). IT context is spread across multiple tools such as AD, CMDB and ticketing systems, while business context tends to be spread across a third set of databases and spreadsheets. Unifying and correlating contextual data across these different tools into a common risk schema is a difficult task. For example, tools may use different formats and semantics for the same attributes of assets or users—surfacing contradictory information which then require manual inspection and correction. Different tools also have their own scoring mechanisms, which makes it difficult to normalize vulnerability scoring.

Risk scoring is an additional issue. Risk scores from legacy tools aren't tailored to your business because custom scoring requires AI that can apply specific risk algorithms for your business, and a complex data export chain—from VM tools to risk-based vulnerability tools to a data warehouse.

Unactionable remediation instructions

Most security and IT ops teams are still set up to handle CVE-by-CVE remediation operations. They want to move to patch-focused operations—but inertia is difficult and legacy tools don't provide the ability to easily focus at a vendor, product or patch level.

Scanning tools typically provide a long list of potential fixes to evaluate. Alarmingly, they also provide the wrong fixes. For example, a tool can instruct your team to use a patch for a Windows platform when the assets are on Linux. Not only does this mean your team is wasting their time and increasing risk, it also makes your security team look like they don't know what they're doing when they provide wrong instructions to the patching teams. Some tools have remediation and mitigation instructions that go beyond a patch, but if these instructions aren't manually communicated to the IT and patching teams then vulnerabilities won't be properly addressed.

Inefficiency also happens when a scanning tool doesn't identify the easy wins such as the latest and best superseding patch. For example, your tools should recommend a patch that will address a large percentage of open CVE instances in order to burn the open instance number down on an asset. Or they could recommend a series of patches that will reduce the risk score of an asset by the greatest amount.

Without the right remediation instructions, your IT teams end up touching the same asset multiple times on instructions from your security team. Again, your team looks like they don't know what they're doing. IT ops and patching teams don't have the ability nor time to sort through information or make decisions. The security team needs to provide them with precise, simple instructions with sequencing. Fix instructions need to be dummy-proof.

Team dynamics between your team and other teams and stakeholders is hard since each team has its own set of objectives and requirements and the tools aren't addressing all of their needs sufficiently. Internal threat teams scream to have their set of high-priority CVE's made a priority. Asset and app owners and patching teams push back on frequent patching—given concerns around app downtime and disrupting end user productivity.

Poor reporting compounds the problem. When systems can't be touched or patched, exceptions need to be baked into the patching SLA reports so that teams don't get penalized for poor performance. Reporting is also inaccurate when it can't consider patching SLAs that may be defined in a matrix of severity, threat level, internet exposure, asset type, and even dynamic risk-based SLAs. It can also be difficult for your security team to ensure accountability and validate that the patching has been completed if your tools are unable to provide them with real-time visibility on actual progress.

Solution:

Use automation and advanced analytics to align vulnerability management with your business

To align their vulnerability management program with the business, CISOs at Fortune 500 companies and other leading organizations are turning to automation and advanced analytics are the tools your team needs to shift from the old CVE model to an asset and risk focused approach instead. Automation and analytics unify and enrich vulnerability and asset data with the business contextualization security teams need to prioritize their work based on business impact. They also address the fact that, for most organizations, management of their expanding attack surface is no longer a human-scale problem.

Here's how you can add automation and AI to each phase of your vulnerability management process—discovery, prioritization and response:

Discovery

A unified, accurate and real-time view of your assets and vulnerabilities

Automation solves the problem of collecting asset and vulnerability information across your entire enterprise at scale. Automation allows your team to collect, correlate and analyze asset data from multiple repositories in real-time—reducing the time to inventory down from days, weeks or months to hours—and giving you the enterprise-wide visibility you need. The right analytics-based enabled asset inventory solution can also identify the components of an application, even custom apps and provide a real-time SBOM, which is essential to identifying component-based vulnerabilities such as Log4Shell.

AI is also used to resolve conflicting or duplicate information. And, it can infer additional details about an asset, for example, how an asset is used, by whom, how often, and in what context. Analytics can also enable intelligent tagging that makes it easier for business users to search for assets and vulnerabilities in everyday language such as "iOS devices in Mountain View susceptible to Spectre" or "unpatched DNS servers in Texas," and get the answers quickly.

Using automation, data can be continuously ingested from your various security tools to provide a more accurate, real-time view of your vulnerabilities. AI also reduces false positives by interpreting and translating the different formats and semantics from each of your tools into a common risk language and schema.

Prioritization

Added business context

Rather than prioritize cyber risks based on a simple CVSS score that has no business context, machine learning models and other data science models can be used to produce a risk model that predicts the likelihood of a data breach and the impact of a breach to your business on a per asset and per vulnerability basis. For example, AI can be used to help you understand whether an internet facing asset that has a high likelihood of being exploited is an application used by your finance team.

$$\overset{(\$)}{\text{Breach Risk}} = \overset{(\%)}{\text{Breach Likelihood}} \times \overset{(\$)}{\text{Breach Impact}}$$

An analytics powered risk model allows stakeholders to ask questions like "where will attacks start" or "what is the risk to our customer data", and get an answer within milliseconds, from which you can then drill-down into the details. Advanced analytics will also produce more precise insights as it learns more about your network's behavior over time. It also allows you to provide real-time risk dashboards to risk owners including business managers who are able to understand in financial terms, the potential impact of vulnerabilities—further connecting your team's effort to the overall mission of your company. A prioritized list of risks based on business impact drowns out all the other noise your team had to previously deal with under the old CVE-based model. AI also automatically detects changes and deviations in your environment which means your vulnerability management program can easily scale along with the growth of the business.

Response

Granular remediation instructions

AI can also be used to facilitate your team's remediation efforts significantly improving their MTTP and MTTR. It provides the granular remediation instructions required. AI analyzes different remediation scenarios and the related risk reduction results to recommend the best remediation option for your security team. For example, AI can provide highly tuned patch instructions. Rather than having your team remediate vulnerabilities one-by-one, AI enables patch prioritization that can be used to assess all the vulnerabilities on an asset and recommend the fewest number of patches required to remediate them all, including recommendations to remediate multiple vulnerabilities all at once using a single patch. Automation provides your team with closed-loop vulnerability remediation information including auto validation that systems have been re-booted with updates in place. Automated workflows connect remediation instructions with patch management, ticketing, orchestration and software distribution systems. Real-time automated dashboards can track mitigation and remediation against defined SLAs.

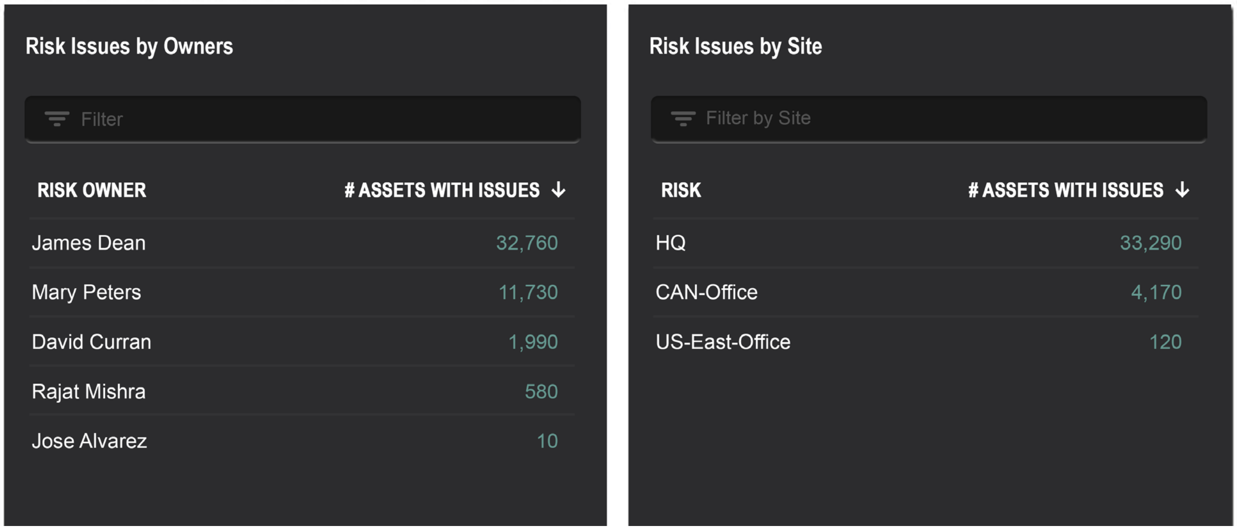
Assigned ownership for key stakeholders

Automation can also help to align remediation efforts to business priorities by identifying the owners of risk issues and assigning them remediation tasks. AI-powered dashboards for each stakeholder also invokes joint ownership for risk issues between business risk owners and your security team, and allows for collaborative approaches that minimize disruption to business services and user productivity.

How Balbix Can Help

Balbix is the leading cybersecurity posture automation company. Balbix Risk-based Vulnerability Management (Balbix RBVM) uses automation and AI to help you align your vulnerability management programs with business priorities and reduce business risk faster.

To identify and prioritize vulnerabilities, Balbix RBVM automatically ingests vulnerability and asset data from your existing tools, fills in data gaps, adds business context and uses sophisticated AI algorithms to calculate your overall risk based on breach likelihood. You can then view risk issues by site, business unit, risk owner, asset class, attack vector and CVEs to further align security and business leaders.



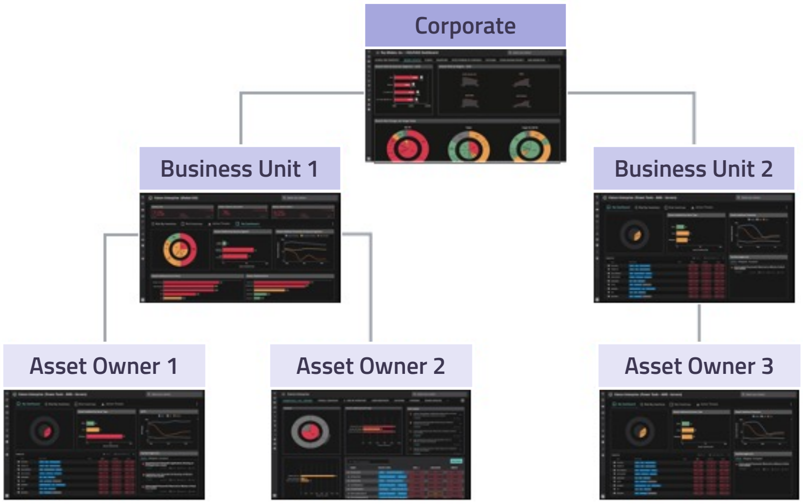
Risk Issues by Owners

RISK OWNER	# ASSETS WITH ISSUES ↓
James Dean	32,760
Mary Peters	11,730
David Curran	1,990
Rajat Mishra	580
Jose Alvarez	10

Risk Issues by Site

RISK	# ASSETS WITH ISSUES ↓
HQ	33,290
CAN-Office	4,170
US-East-Office	120

View risk issues by owner, business unit, asset class, etc.



Role-based risk dashboards align security and business owners.

Balbix RBVM then assigns risk issues and provides granular remediation instructions such as recommendations for the best patches to use. Working in collaboration, your team and risk owners can create remediation projects based on a patch cadence that won't disrupt business activities. Real-time dashboards enable project owners to track progress and clearly see if SLAs are being met.

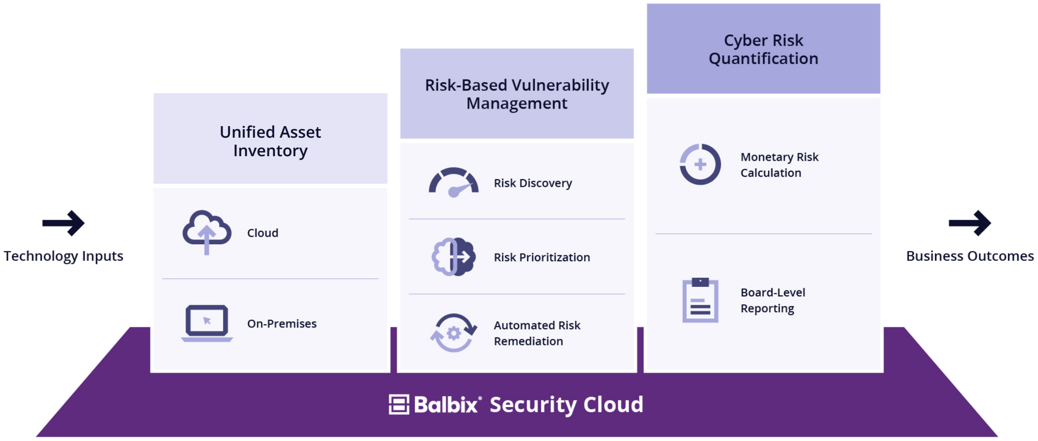
More details about Balbix's cyber risk quantification capabilities can be found here.

'Previously, responding to a new vulnerability like Sambacry required manual work, scriptwriting and communication between multiple teams to identify assets at risk and perform mitigation tasks. This process would take weeks. With Balbix, we can query for assets at risk and track remediation in real-time, shrinking the response time from weeks to hours.'

—Senior security leader, Fortune 50 telecommunications provider

Balbix Security Cloud

The Balbix Security Cloud uses AI and automation to reinvent how the world's leading organizations reduce breach risk. With Balbix, security teams can now accurately inventory their cloud and on-premise assets, conduct risk-based vulnerability management and quantify their cyber risk in monetary terms.



Cloud native and highly scalable. Integrates with existing tools.

Balbix®