



RISK-BASED VULNERABILITY MANAGEMENT

Automate your vulnerability management program with Balbix: Discover, prioritize, and fix your riskiest vulnerabilities at high velocity

ARE YOU LOSING THE WAR AGAINST SECURITY VULNERABILITIES?

As per a [2022 Ponemon Institute](#) report, 54% of organizations experienced a cybersecurity breach in the past 12 months. In addition, new regulatory frameworks rolled out by the SEC, DORA, TSAASOE, and others now require that companies maintain clearly defined processes for evaluating the material impact of cyber attacks. The foundation of your cybersecurity efforts, therefore, must be a robust vulnerability management program designed to keep you ahead of potential threats and maximally automate your delivery of appropriate reports and supporting evidence to meet compliance objectives in the event that a breach occurs.

Mean-time-to-patch CVEs across the Fortune 500: 154 days*


*observations from Balbix prospects in 2022 before they started working with us




How can we identify blind spots in our asset inventory and vulnerability scanning coverage?



How can we discover new vulnerabilities in minutes or hours rather than days or weeks?




How can we correlate & consolidate vulnerabilities from our multiple tools deployed?




There are too many vulnerabilities to fix. How can we prioritize based on business risk?




Researching fixes is time-consuming. How can we quickly get accurate info to our remediation teams?



How can we dramatically speed up the pace of remediation and drive major reductions to our backlog?



What metrics can we use to measure remediation efforts vs. our SLA policies?



How can we automate observability & benchmarking to measure VM program performance?

The good news is that there is a better way forward—and one that can save considerable time and costs by automating vulnerability processes and consolidating tools into a single platform, simplifying operations and reducing Total Cost of Ownership (TCO). In the next few pages, we explore how Balbix can help dramatically improve your cyber security posture while reducing your TCO.

Vulnerability Management is Hard

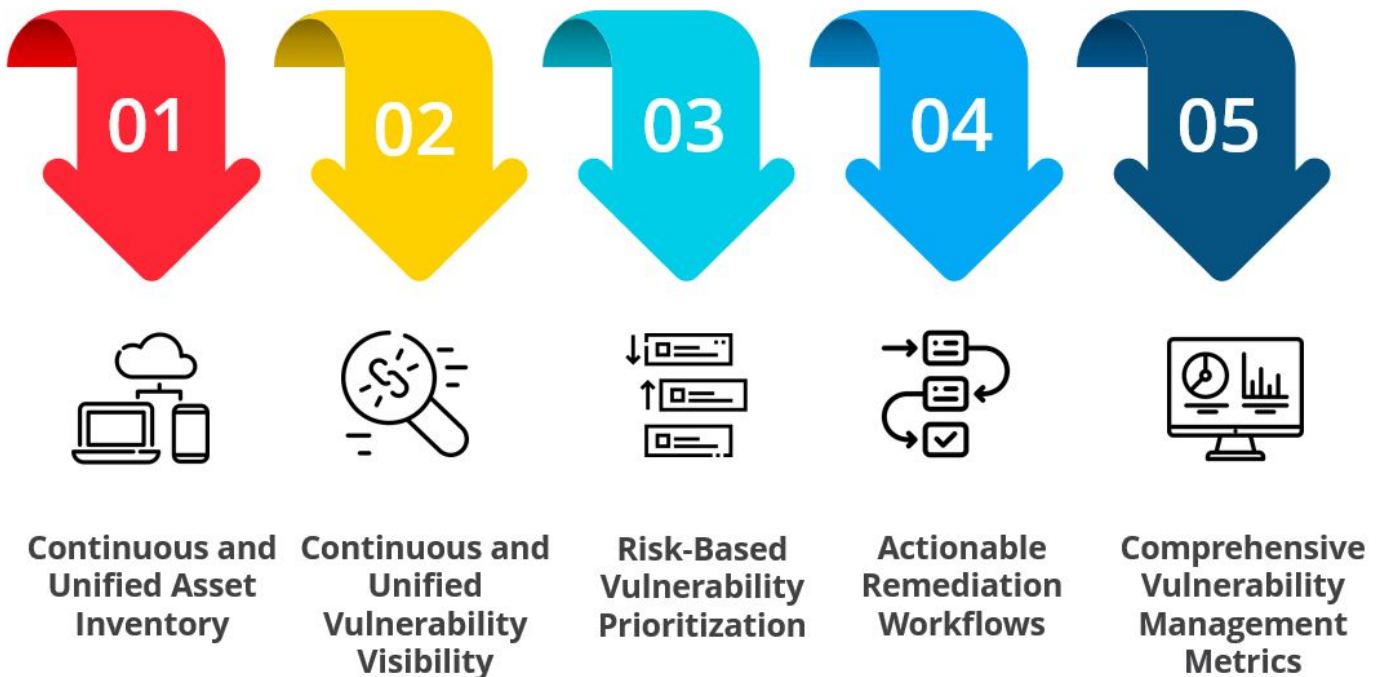
When Balbix starts working with large enterprises with 200K+ assets, we routinely observe over **50 million vulnerability instances** with about **200 open vulnerabilities per asset**. Mean open vulnerability age (MOVA) is typically 150 days or more.

These are 50 million wide open doors for attackers to get into the enterprise easily...

The Balbix RBVM Automation Playbook

Say goodbye to siloed tools, subjective decision-making, and tedious manual workflows. With Balbix, you can continuously assess your enterprise's cybersecurity posture and prioritize open vulnerabilities based on business risk. Balbix enables you to mitigate cyber risk quickly and effectively, giving you peace of mind and freeing up valuable time for your security team to focus on more strategic initiatives. You can maximally automate every phase of your vulnerability management process.

Let's take a closer look at these 5 phases* of the Balbix RBVM Automation playbook:



* These phases are aligned with Gartner's Top 5 Elements of Effective Vulnerability Management [Published: 23 Sept 2022, Author: Jonathan Nunez]



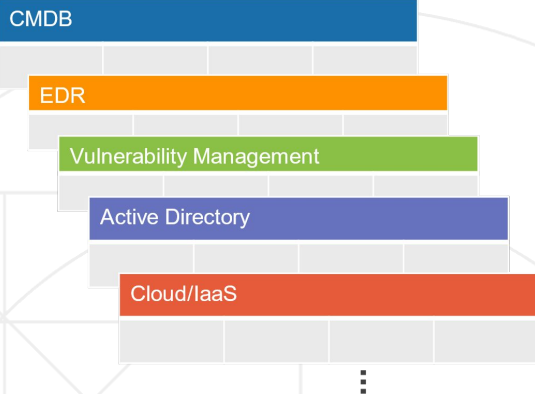
1 Continuous & Unified Asset Inventory

Comprehensive Asset Inventory

You can't secure what you can't see. Balbix's AI-Powered Risk-Based Vulnerability Management (RBVM) provides maximum visibility based on a deduplicated, correlated, and comprehensive asset inventory. In addition, Balbix inference capability provides an additional 35%-100% more coverage over existing vulnerability management tools, including increased asset coverage, timely awareness of new vulnerabilities, accurate actionability through version and patch supersedence knowledge, improved patch prioritization, and simplification of software management by avoiding the need to address numerous individual vulnerabilities and their instances.

By ingesting relevant data from your IT, cybersecurity, and home-grown tools, Balbix provides a continuous, unified view of all assets. Balbix tracks 450+ attributes for each asset, including information about network interfaces, storage, open ports and services, system details, users, software inventory, and any existing (or missing) security controls.

Ingest, cleanse, normalize,
deduplicate, correlate and infer



Searchable, unified view with >450 attributes
for assets across on-prem, cloud and mobile

Balbix

- System Details
- Users
- Software Versions (SBOM)
- App Context
- Business Tags
- Security Controls
- Discoverability
- IP/MAC Address
- Ports
-

The Balbix platform covers assets across your traditional data centers, cloud, mobile and SaaS. Assets are automatically deduplicated, correlated, categorized, grouped and enriched with business context. Applications are discovered, deduplicated, analyzed and an application-to-infrastructure mapping is created.

This inventory can be searched using natural language search as well as filtered search. Dynamic groups of assets that match specific attribute conditions can be defined, and then tracked in custom dashboards for the various jobs, projects and workflows in your daily operations.



Unified Asset Inventory, Vulnerability, and Risk Model

Do you struggle to consolidate findings from multiple assessment tools and establish an accurate RBVM process? Do you worry about big coverage gaps in your vulnerability management program?

Balbix has you covered!

In addition to providing a continuous, unified view of all assets, Balbix consolidates all vulnerabilities into a single, unified risk model. By continually ingesting findings from various vulnerability assessment tools, including IT infrastructure, IoT/OT, web apps, and cloud, Balbix ensures that all vulnerabilities are tracked and prioritized in one place.

As Balbix analyzes vulnerabilities and builds out the unified risk model, the system also surfaces coverage and confidence metrics based on the vulnerability data provided by all your tools. So, as an example, if you have good coverage for servers from Tool A and IOTs from Tool B, but don't have good coverage of your user endpoints, Balbix will be able to identify and highlight this.

Even if your enterprise lacks existing tools or has significant data or coverage gaps, Balbix offers asset and vulnerability discovery capabilities via native sensors for continuous, near-real-time vulnerability assessment.

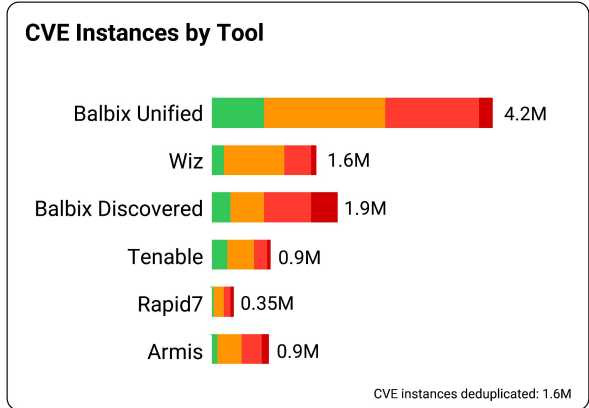
2 Continuous & Unified Vulnerability Visibility

Infer Vulnerabilities in Near Real-Time

When a critical zero-day vulnerability is announced, do you wait for days and weeks to complete your assessments and identify vulnerable assets?

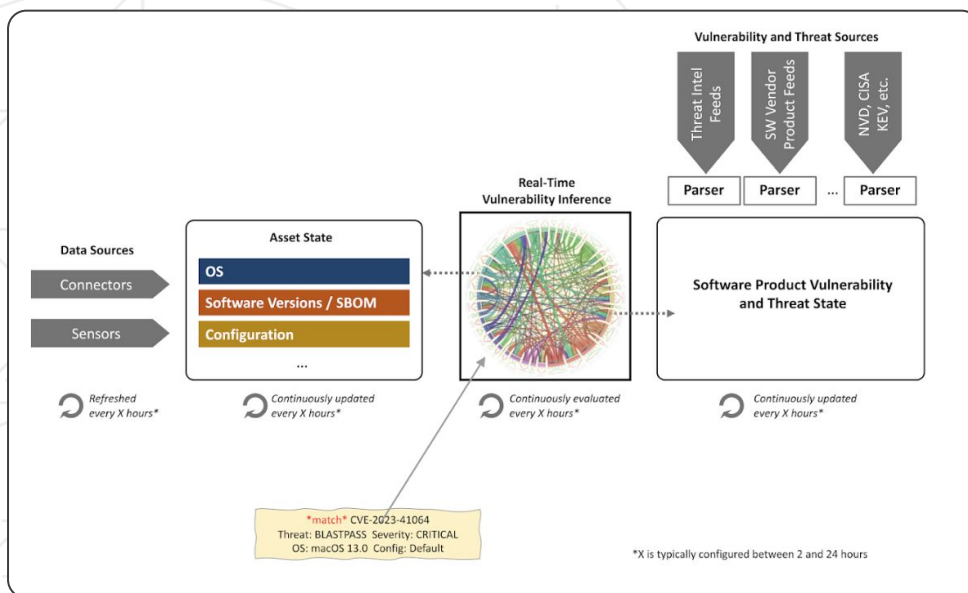
With Balbix, you can be done within hours. By leveraging up-to-date asset and software inventory, Balbix provides near-real-time discovery of vulnerabilities via direct inference, with no additional scans required.

Here is how this works: In the previous section we explained how Balbix always knows which software versions are deployed on your assets.



By analyzing and correlating this information continuously with vulnerability information from vendor, government, research and other data sources, Balbix can simply tag which assets are vulnerable. Additionally, Balbix's inferred vulnerabilities are deduplicated and corroborated with those generated from third-party tools, ensuring a comprehensive and up-to-date view of your enterprise's security posture.

Balbix's vulnerability inference significantly increases speed and coverage of detection, enabling high-accuracy vulnerability detection on assets not covered by your existing assessment tools.



Dynamically Track and Trend Asset Groups

How do you stay on top of potential threats to your critical business assets, such as new CISA Known Exploited Vulnerabilities? How do you track remediation and SLA performance by business segment without the usual manual headaches?

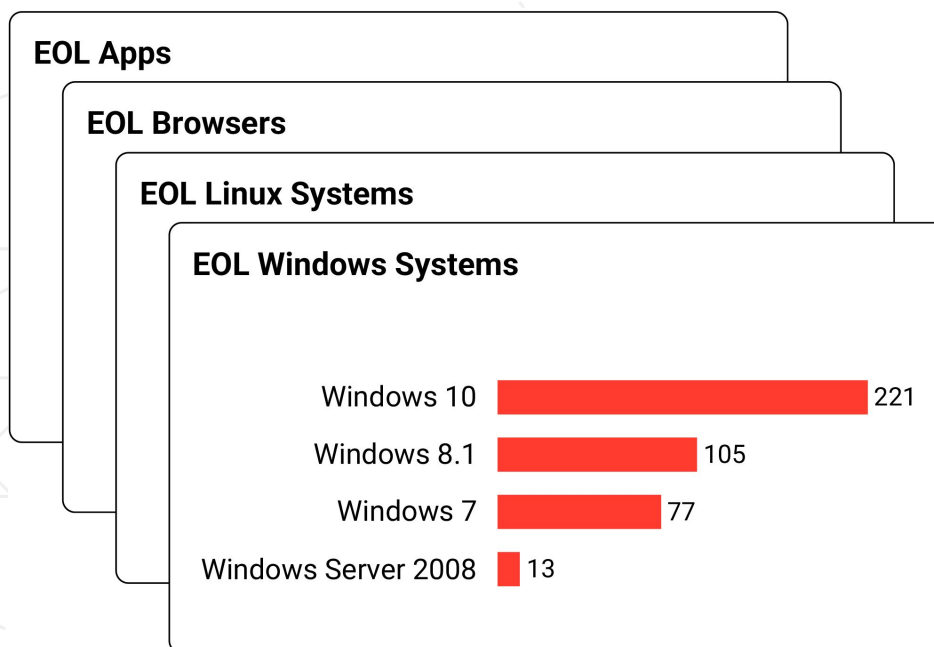
With Balbix, You can easily create custom asset groups based on a wide range of asset, vulnerability, business, and user attributes that update dynamically as assets and attributes evolve. This allows you to closely monitor your critical assets and assign owners to specific groups for clear responsibilities and accountability. If you are an asset group owner, you can view vulnerability trends in near real-time, and by filtering CVE lists based on custom groups, you can prioritize which vulnerabilities to address first.

With the automation powered by Balbix, manually monitoring critical assets is a thing of the past.

Detect End-of-Life Software

Identifying end-of-life (EOL) software in your environment is essential for effective vulnerability management. These instances are highly vulnerable to attack as the vendor offers no security updates or patches.

Balbix makes it easy to identify EOL instances of software across Windows and Linux systems. To do this, all you need is to search for “EOL systems”. Since Balbix maintains up to date software inventory and version information, a moment later you have the information you are looking for.



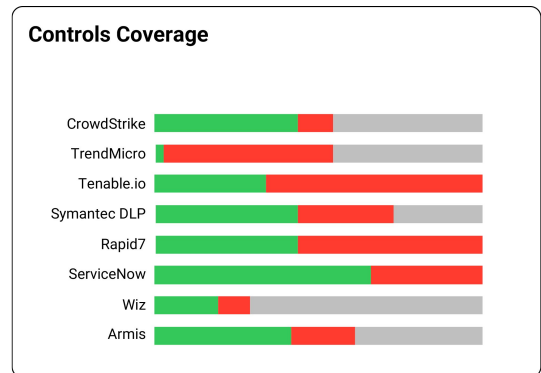
Software Component Vulnerability Detection via SBOM (e.g., Log4j)

Software component vulnerabilities pose a major concern to most enterprises because they are pervasive and difficult to detect. It is also not easy to remediate or mitigate software component vulnerabilities with speed and accuracy.

With runtime visibility into the Software Bill of Materials (SBOM), including the full dependency tree, Balbix enables you to automatically and accurately detect vulnerable components across all assets, without requiring access to application or 3rd party source code. With a simple search query, Balbix will identify module vulnerabilities, such as Log4j and Spring4Shell, that are difficult to detect.

Uncover Coverage Gaps

With so many different tools and assets to manage, it can be difficult to ensure that everything is properly monitored. The Balbix solution provides continuous monitoring of your IT and cybersecurity tools, allowing you to identify any gaps in coverage. With Balbix, you can analyze asset coverage, vulnerability coverage, and even individual vulnerability instances, pinpointing which tools are deployed or missing observations for specific groups of assets. With this information, you can confidently fix any deployment or coverage issues, ensuring that your environment is fully protected.



Ensure Data Fidelity & Coverage

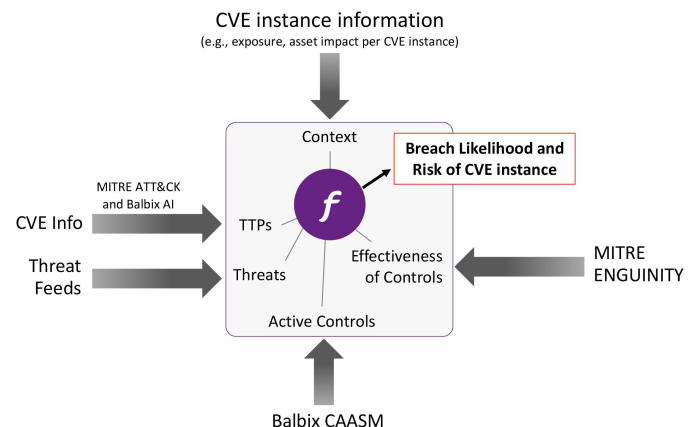
Are you facing limited data or deployment challenges when it comes to comprehensive vulnerability assessment and prioritization?

Don't worry, with Balbix's optional sensors you can gather detailed system information, software inventory, SBOM, configuration, user data, and more. This information enables high-fidelity vulnerability inference and remediation confirmation, allowing you to stay ahead of potential security threats. These lightweight software agents can be installed quickly and provide valuable data to enhance your vulnerability assessment and prioritization.

Don't let data limitations hold you back - let Balbix's sensors fill in the gaps and improve your security posture.

Detect Control Effectiveness

Balbix enables you to analyze controls for efficacy against the vulnerabilities present in your environment.



3 Risk-Based Vulnerability Prioritization

True Risk Based Scoring

Without an integrated approach to risk management, organizations have varied definitions of risk for different cybersecurity program areas such as Risk-Based Vulnerability Management (RBVM), Cyber Risk Quantification (CRQ), and Governance, Risk, and Compliance (GRC). This leads to inconsistencies between risk assessment and risk treatment, and bad risk management decisions.



$$\text{Risk} = \text{Likelihood} \times \text{Impact}$$

Balbix's unified risk model helps you solve this problem. Balbix's risk-based prioritization is based on a comprehensive five-pronged \$-based risk calculation that incorporates information about vulnerability severity, threat levels, exposure, compensating security controls and business impact. Balbix's approach results in highly accurate prioritization, which aligns with your business risk appetite and avoids unnecessary work by your teams on fixing low-risk issues.

Pre-Integrated and Automated Threat Intelligence

Effective risk-based prioritization of vulnerabilities requires up-to-date evaluation of the global threat level. This involved considering adversary activity, extent of exploit development and usage in malware.

Unlike other solutions that require you to identify and manually integrate threat intelligence into their vulnerability management process, Balbix natively incorporates pre-curated and pre-integrated threat intelligence, including near-real time proprietary, commercial and open-source feeds.

Balbix helped a Fortune 100 Telco to find and mitigate Log4j in days instead of months. Cyber risk mitigated: approximately \$125M. Cost savings: \$3.5M

Prioritize Risks and Patches

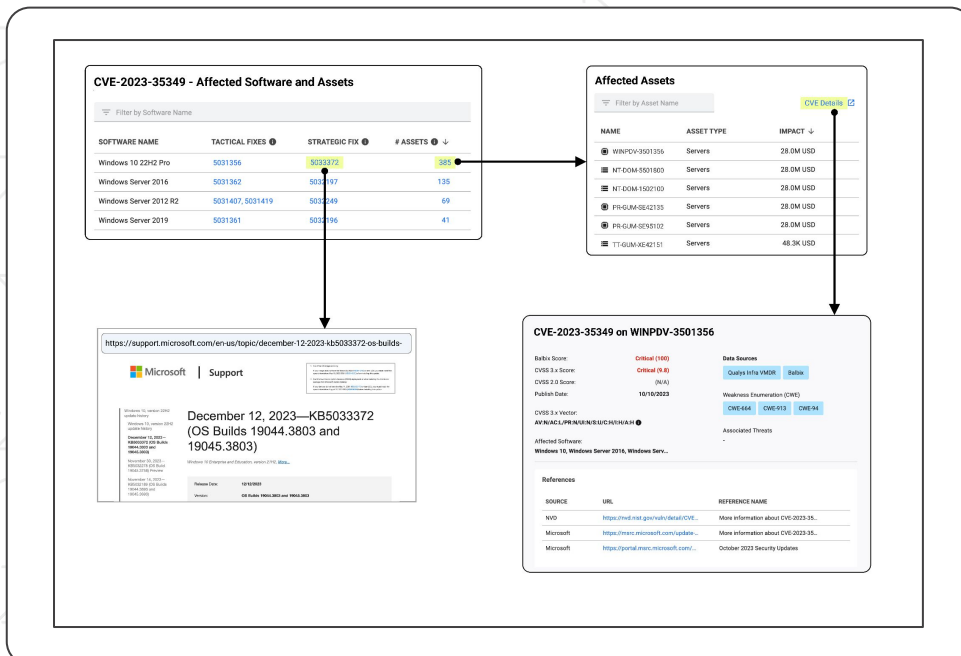
Unlike traditional solutions, Balbix takes a holistic approach to risk-based prioritization by employing distinct approaches for war-time and peace-time vulnerability management scenarios.

- **War-time** refers to an environment that is under attack or imminent threat, where critical vulnerabilities have suddenly been recognized, requiring significant time and effort to deploy emergency patches or mitigations, on specific assets.
- **Peace-time** vulnerability management, on the other hand, refers to the routine management of vulnerabilities in a non-crisis environment.

Given the different challenges, constraints, and goals of peace-time and war-time scenarios, unique approaches are required for each. Balbix's CVE and Patch Prioritization solutions address these requirements effectively.

For war-time scenarios, **Balbix's CVE Prioritization** provides real-time prioritization of critical CVE instances, considering factors like severity, threat level, software vendor, and category. Balbix identifies those assets where the open/unmitigated CVEs in question are adding cyber risk above the agreed upon risk appetite/tolerance thresholds. Other instances of these CVEs can be left alone until the regular patching cycle.

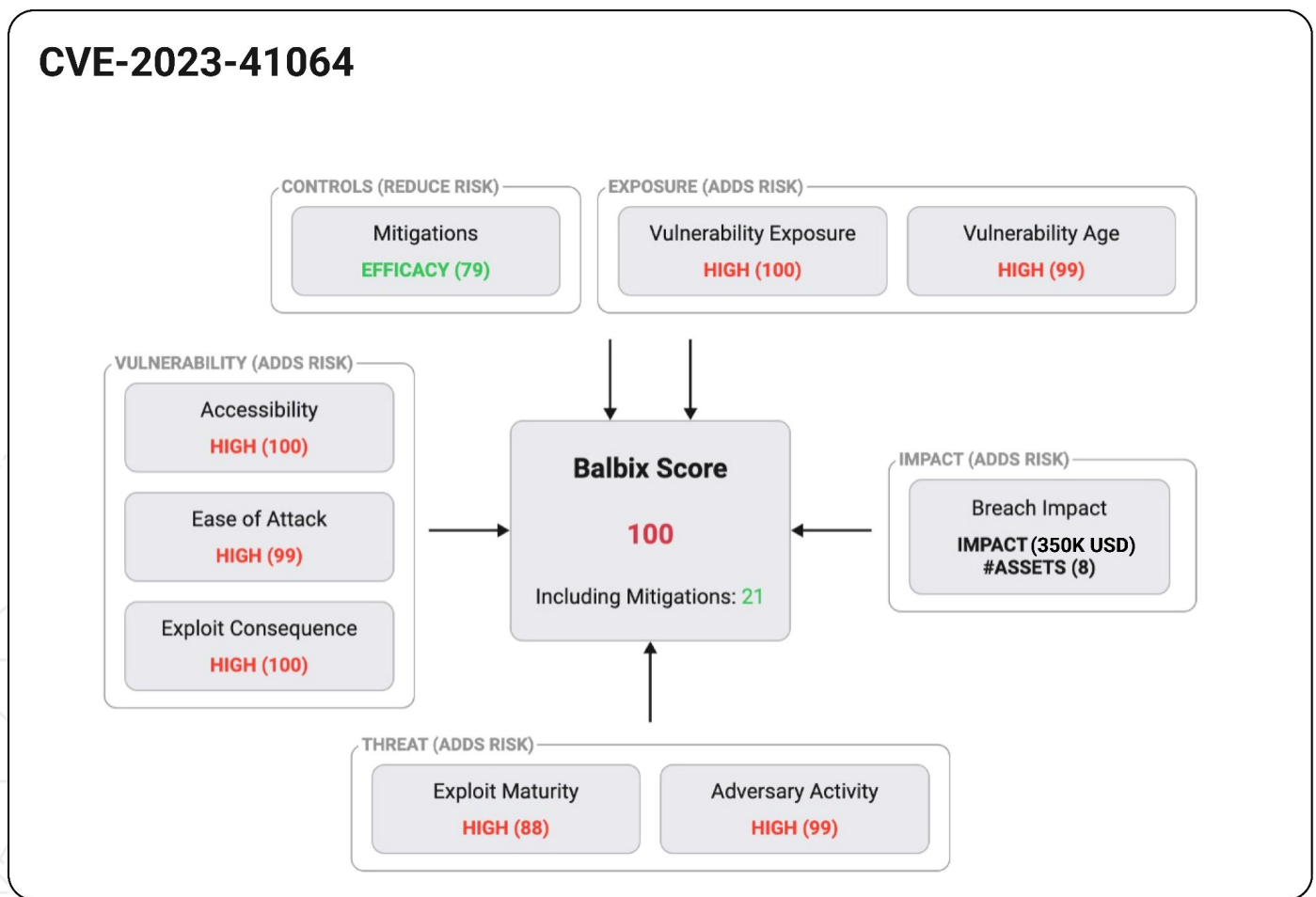
For peace-time scenarios, **Balbix's Patch Prioritization** automatically recommends optimized patches based on overall risk reduction while minimizing the number of patches to be applied. Balbix considers the number and severity of vulnerabilities, threat data, and business impact of assets when making these recommendations.



Prioritize Vulnerabilities Based On Risk

To build cyber resilience, your cybersecurity teams need to understand the various tactics, techniques and procedures (TTPs) that adversaries use to design their attacks. However, with so many TTPs to assess and evaluate, it is not humanly possible for your security teams to do so manually.

This is where Balbix comes in to help. Balbix automatically maps all vulnerabilities instances to TTPs using the MITRE ATT&CK framework. Using MITRE ENGENUITY, Balbix also maps your deployed endpoint security controls to effectiveness against these TTPs. This dramatically enhances prioritization accuracy, while providing your teams with crucial insights for developing effective remediation and mitigation plans.



4 Actionable Remediation Workflows

Accurate Fix Information

Effective vulnerability remediation requires a deep understanding of the risks posed by each vulnerability and accurate instructions for fixing them quickly. But with so many possible fixes available, remediation teams can spend countless hours researching the best course of action.

Balbix eliminates this challenge by leveraging its detailed asset model and software inventory, including SBOM, to provide specific fixes tailored to each individual asset. In addition, Balbix provides detailed background information, such as CWE info and MITRE ATT&CK mapping, to provide necessary context for effective remediation.

Furthermore, Balbix recommends cumulative and superseding patches when available, maximizing the return on investment of patch operations.

The average Balbix customer was able to **reduce mean time to remediate (MTTR) by 40%** during the last six months of 2022.

Automate Dispatch and Ticketing

Are you looking for an efficient way to streamline your remediation process?

Through Balbix's integrations with ticketing platforms such as ServiceNow ITSM or Jira Service Management, creating remediation tickets is a breeze. By pushing detailed fix information to remediation tickets, your teams can quickly address prioritized vulnerabilities with minimal manual effort. Plus, these integrations enable your security and IT teams to work more efficiently by utilizing your established systems for remediation workflows.

Dispatch for Remediation

Vulnerability Remediation Summary

Vulnerabilities Selected	Fixes / Patches
CVE-2023-36025, CVE-2023-35349, CVE-20...	5032189, 5031356, 5031356, 5032189, 503...
Assets to Remediate	Vulnerability Instances to be Resolved
14518	26249
User	Group Context
Chris Griffith chris@balbix.com	All Assets

Configured Ticketing Integration* Connector Instance Name*

ServiceNow Ticketing Balbix-Instance

Ticket Prioritization

Impact* Urgency* Priority*

1 - High 1 - High 1 - Critical

location

North America

[Download Attachment \(CSV\)](#) [Cancel](#) [Submit Ticket](#)

Automatic Remediation Detection

Addressing security vulnerabilities requires a collaborative approach, which is often hard to track and coordinate. With Balbix, you can quickly confirm when vulnerabilities have been fully addressed, ensuring effective team coordination, faster overall remediation execution, and more accurate status reporting. No time-consuming “confirmation scans” are required to validate that issues are fixed.

Additionally, with optional Balbix sensors deployed you can easily detect any assets that still have a reboot pending and complete the remediation action within hours.

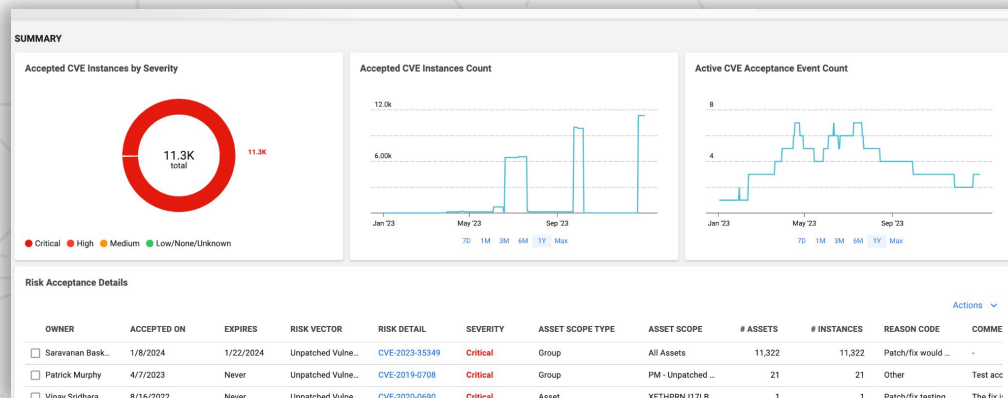
Microsoft Patch Status Reporting

On Patch Tuesday, you typically perform specific scans to identify which assets require critical Microsoft security patches. This can be a time-consuming and error-prone process. Balbix automates the entire process for you. With the power of Balbix analytics and flexible dashboard widgets, you can easily report on the effectiveness of your Microsoft remediation program, identify specific assets with missing (pending) patches by OS, and track installed patches. Rather than spending valuable time analyzing individual Microsoft vulnerabilities, Balbix enables teams to identify and deploy the necessary superseding fixes, efficiently and quickly addressing large numbers of CVEs in bulk.

Vulnerability Risk Acceptance Management Framework

A successful RBVM program must provide a way for risk owners to accept and manage related risks in line with the organization’s policies. This is exactly what Balbix helps you enable.

Balbix makes it easy for risk owners to select the vulnerabilities (CVEs) they want to address, assign responsibility, document the reason for risk acceptance, and set an expiry target date. All risk acceptance events are automatically tracked and summarized in a comprehensive dashboard that includes vulnerability instances, trends, severity analytics, and associated details. Balbix’s vulnerability risk acceptance management framework also helps key stakeholders such as GRC leaders and auditors understand the level of risk the organization is taking on.



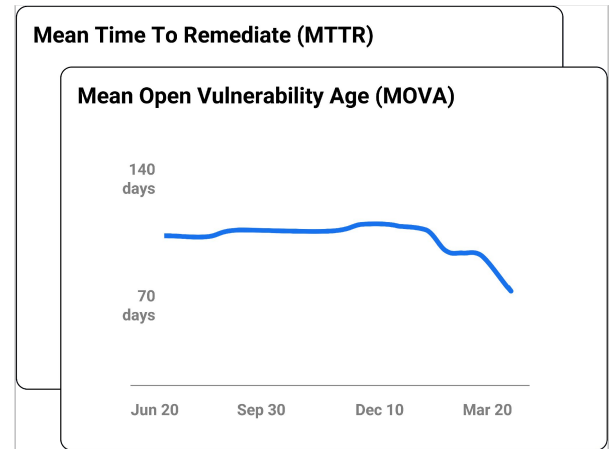
5

Comprehensive Vulnerability Management Metrics

Benchmark Vulnerability Management Performance

As a security leader, one of your top-of-the-mind priorities is to accurately measure the effectiveness of your vulnerability management program and ensure consistent risk reduction over time. Many organizations struggle to quantify their program's impact, leaving them under-resourced and vulnerable to ongoing threats.

With Balbix, you can automatically generate reports on key metrics like mean-time-to-patch (MTTP), mean-time-to-remediate (MTTR), and mean-open-vulnerability age (MOVA). Additionally, Balbix provides percentile benchmarking against a range of enterprise peers, enabling you to gauge your performance and fine-tune your SLA policies for optimal results.



“Our patching efficiency has also improved dramatically. Our mean time to patch (MTTP) has gone from 100 days to 38 days, a 62% increase in speed to patch.” – The Master Group

Targeted Compliance Reporting

How can you ensure your team is meeting critical compliance requirements beyond just reducing the number of vulnerabilities?

While vulnerability trends are important, they don't paint the full picture of your team's performance. Balbix provides an easy way to report compliance to your organization's patch SLA (service level agreement) policy, which specifies the number of days to patch vulnerabilities based on their severity and threat level on certain asset types.

With Balbix, you can also demonstrate compliance across other critical dimensions such as patch status, EOL status, and vulnerability assessment tool deployment coverage. This level of granular visibility empowers your team to quickly identify and address any compliance failures.



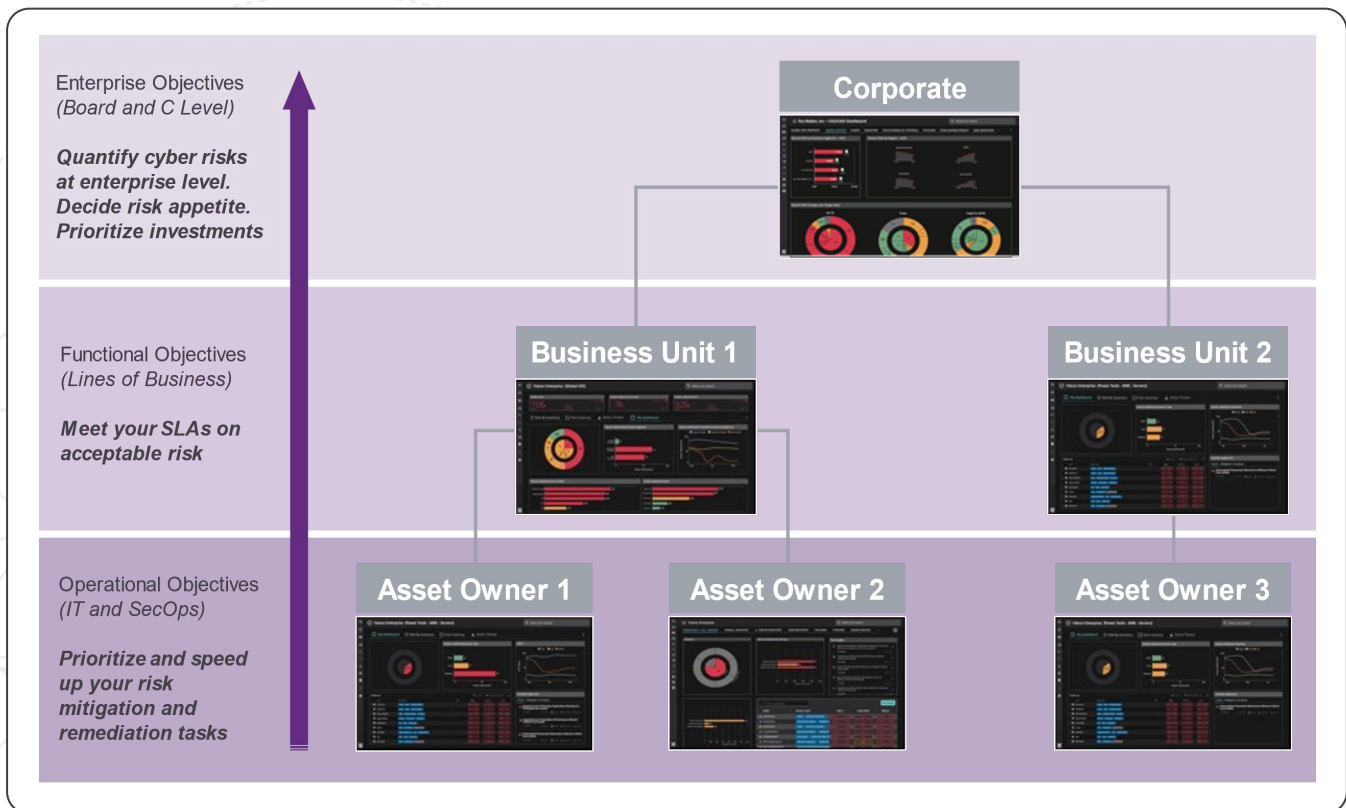
Powerful Analytics, Dashboards and Gamification

With Balbix, you can answer a nearly unlimited number of questions that come up as your vulnerability management teams go about their daily work. Balbix search allows you to query using the vocabulary of cybersecurity, IT, business context and cyber risk, e.g., “Which domain controllers in EMEA supporting our Retail BU are non-compliant to patch SLAs?”

You can create dynamic groups out of these search queries, enabling stakeholders to precisely monitor and dashboard critical assets in scope, making it easier to stay ahead of potential threats. By assigning owners to specific asset groups, you can ensure that each owner has a clear understanding of their responsibilities and hold them accountable.

Think of Balbix's dashboards as a distributed workbench for your team or organization that enables real-time monitoring, analysis, and collaboration. Executive and operational dashboards and reports can be shared with the key stakeholders involved, effectively gamifying the process of overall cyber risk reduction.

Using Balbix’s dashboards, you can provide each risk owner in your organization with the right information, the right support tools and the right incentives to do their part of risk management.

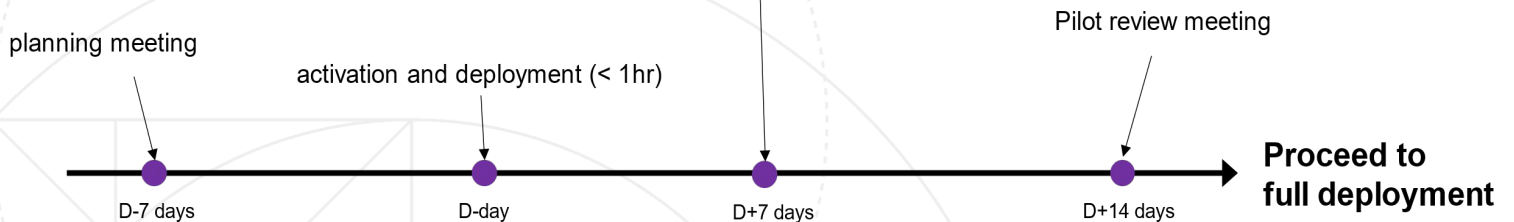
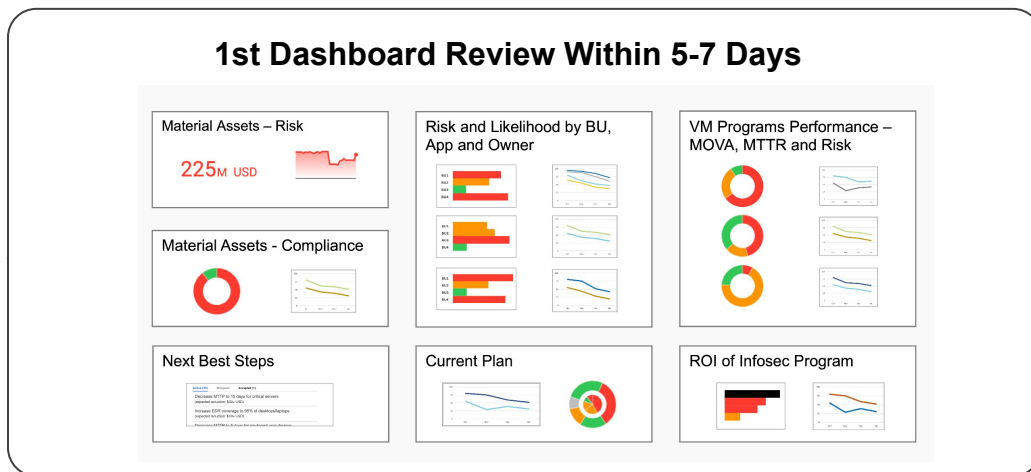


55% of Balbix customers deploy cybersecurity gamification for their organizations within three months of starting with Balbix

It is easy to get started...

The Balbix Security Cloud is a modern, SaaS-based platform that enables rapid enterprise deployment. It uses AI and automation to reinvent how the world's leading organizations reduce cyber risk. With Balbix, security teams can accurately inventory their cloud and on-premise assets, conduct risk-based vulnerability management and quantify their cyber risk in monetary terms.

A typical Balbix pilot deployment covers enterprise-wide scope with a prioritized set of data sources and takes a matter of hours to plan and configure. If you wish, you can sample all the capabilities described in this document running in your environment next week. Our pilots roll forward naturally into full production with rapid time-to-value.



Please visit www.balbix.com to schedule a call with us.