

CYBER ASSET ATTACK SURFACE MANAGEMENT

Build the foundation of your cyber program with Balbix: Unlock your existing data to see all assets, identify and fix control gaps

Navigating The Maze: Is Your Cyber Asset Landscape Under Control?

For cybersecurity leaders, a comprehensive understanding of cyber asset inventory and attack surface is vital for a good cybersecurity posture and acceptable levels of cyber risk. An accurate asset inventory is also foundational for compliance with regulatory requirements and well as with key frameworks such as NIST CSF.

However, asset inventory data is typically locked inside numerous siloed tools. Keeping up with sprawling and dynamic IT environments is very hard. Our experience with numerous customers reveals key challenges they face with respect to attack surface visibility:

After adopting Balbix, our customers **increased IT asset visibility by an average of 87%**



How can we harness existing tools to achieve a comprehensive view of our asset inventory?



How can we continuously track our inventory in an IT environment that changes so rapidly?



How can we streamline and automate the process of asset prioritization for compliance and risk analysis?



How can we establish a reliable asset-level foundation for an effective vulnerability management program?



How can we ascertain the consistent deployment of our security controls and compliance with policy?



How can we get full visibility to manage upgrades, software rollouts & EOL OS remediations?



How can we obtain a holistic view of our apps, including related infra, prioritized vulnerabilities, risk, and ownership?



Once we gain a full picture of our inventory, how can we implement an action plan to drive down risk?

Good news - there's a better way! By using Balbix's Cyber Asset Attack Surface Management (CAASM), you can comprehensively address these challenges and effectively boost visibility, control, and resilience.

Asset management poses significant challenges

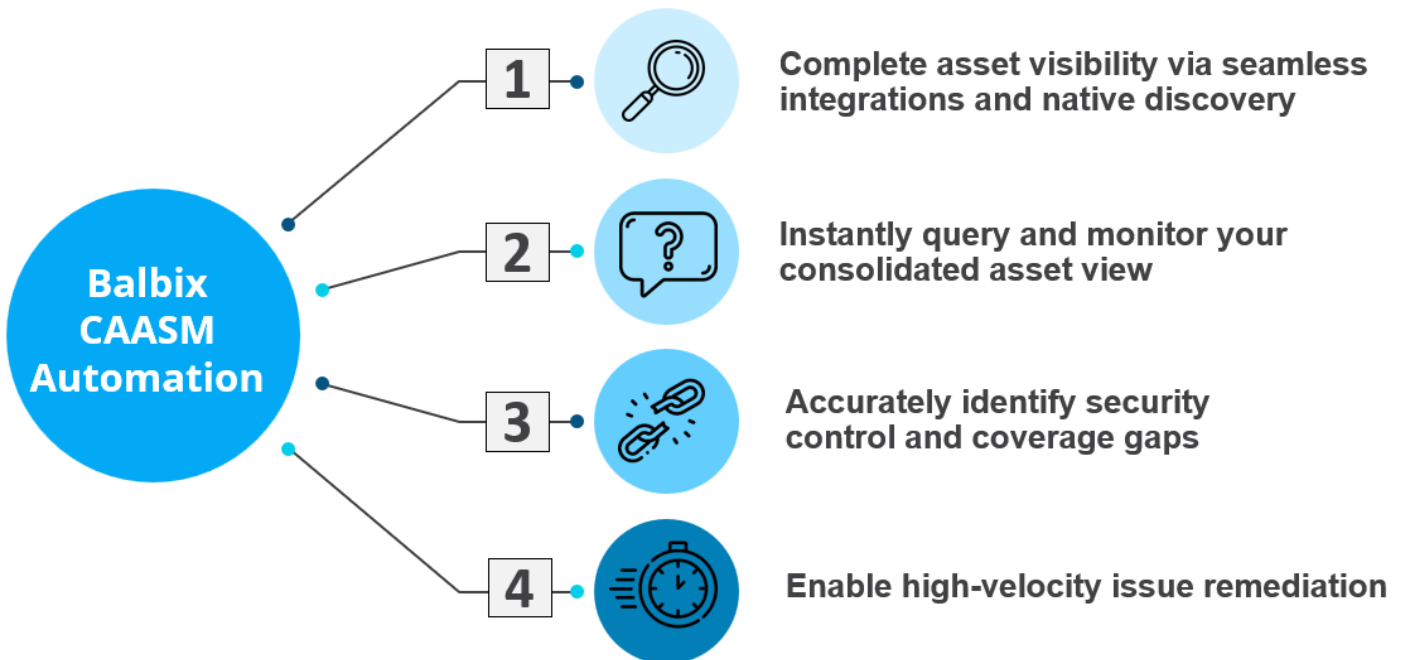
When Balbix engages with very large enterprises with 500K+ assets, we typically encounter over 75K+ unique software applications deployed.

Without comprehensive visibility, these hundreds of thousands of assets and tens of thousands of software applications create a virtual playground for attackers, offering hidden passages for them to breach and infiltrate the enterprise with ease.

The Balbix CAASM Automation Playbook

Balbix's CAASM capabilities enable security teams to overcome asset visibility and exposure challenges by providing organizations with a near real-time, up-to-date, comprehensive and unified view of their assets, clearly laying out the attack surface.

Let's take a closer look at these four key stages of the Balbix CAASM playbook:



1

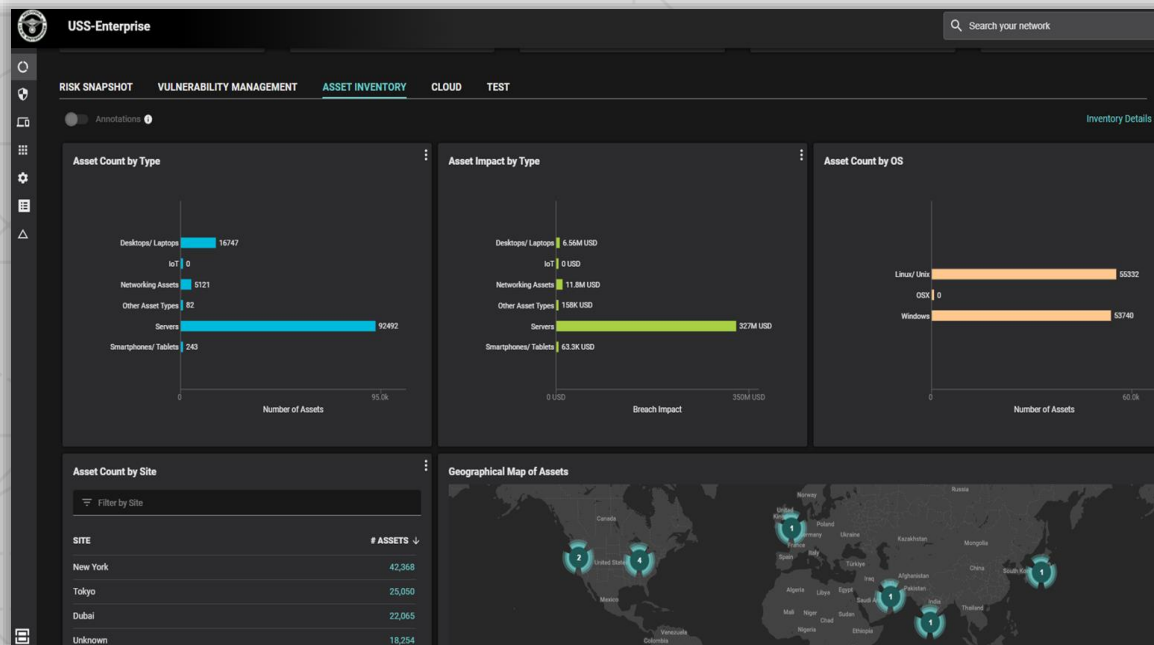
Complete Asset Visibility via Seamless Data Integrations and Native Discovery

Deduplicated, Correlated, Continuous Asset Inventory

A blind spot in understanding your organization's asset inventory is like driving at high speed with your eyes closed - you never know what dangers lie ahead. With the ceaseless evolution of cybersecurity threats, you need a clear and comprehensive understanding of your organization's asset inventory. Balbix's platform delivers precisely this, through its unified asset inventory and automation capabilities. Natively supporting a wide range of asset types, Balbix offers a comprehensive, unified view of your assets by ingesting relevant data from your IT, cybersecurity and relevant business tools. The Balbix platform tracks over 450 attributes for each asset, including software inventory, system config, network interfaces, storage, open ports and services, users and existing (or missing) security controls.

Trust is paramount when it comes to asset data, and Balbix provides a solid foundation for your vulnerability management program through a deduplicated, correlated, and comprehensive asset inventory. Balbix automatically cleans conflicting and duplicate data during the ingestion process, correlating information from multiple sources. This asset enumeration process ensures that the information you receive is accurate and up-to-date, enabling you to make informed decisions about your cybersecurity posture.

Balbix includes support for the world's top three cloud providers - Microsoft Azure, Amazon Web Services, and Google Cloud Platform - as well as traditional data center, IoT/OT and mobile employee devices. This unified coverage cuts through the confusion of multi-cloud and infrastructure assets, boosting productivity by negating the need to juggle multiple tools and dashboards.





Deep Visibility into Runtime SBOM to Uncover Software Component Attack Surface

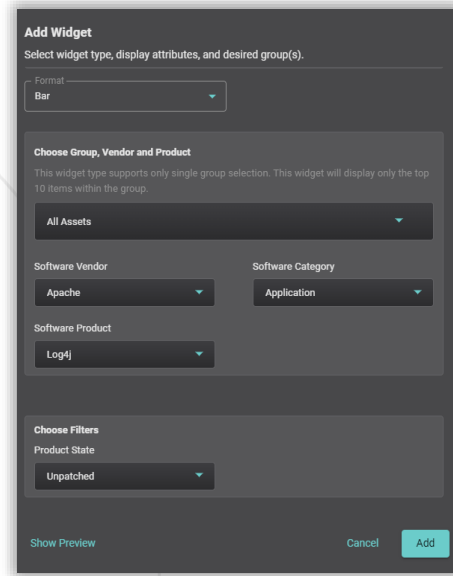
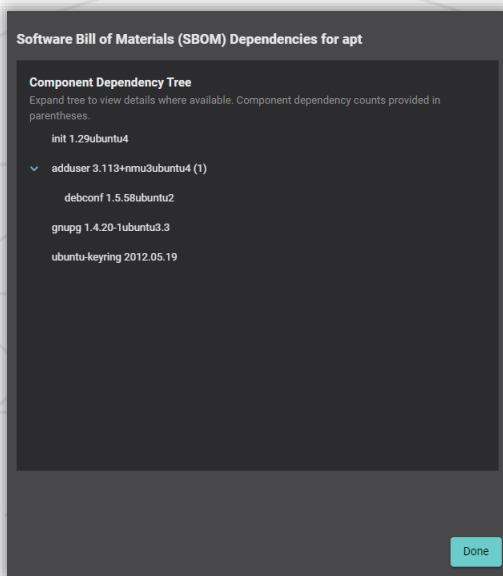
Identifying and securing all software components in your environment is incredibly challenging. Manually tracking each component is time-consuming and error-prone, increasing the risk of security breaches due to overlooked vulnerabilities.

Balbix offers a solution to these issues, providing near real-time monitoring of your Software Bill of Materials (SBOM), which can assist your security teams in identifying and responding to potential vulnerabilities more effectively. Balbix SBOM details include software versions, installation paths, and complete dependency trees, making it easier to comprehend the full range of software components in your environment.

Tracking third-party packages, including those from open-source projects, can be particularly arduous. Balbix provides visibility into these packages, irrespective of where your assets are located - whether they're on-premise, in the cloud, or in hybrid and multi-cloud environments.

Understanding multi-level software dependencies is another obstacle that Balbix helps overcome. It provides insights into these trees, including nested dependencies, which can aid in understanding the potential security implications of each component.

Balbix supports key industry-standard SBOM formats such as OWASP CycloneDX and SPDX. This allows for easy export of SBOM to other operational tools, reducing the need for manual tracking.



“Three times more assets have been identified and correlated by Balbix compared to the previous inventory process.”

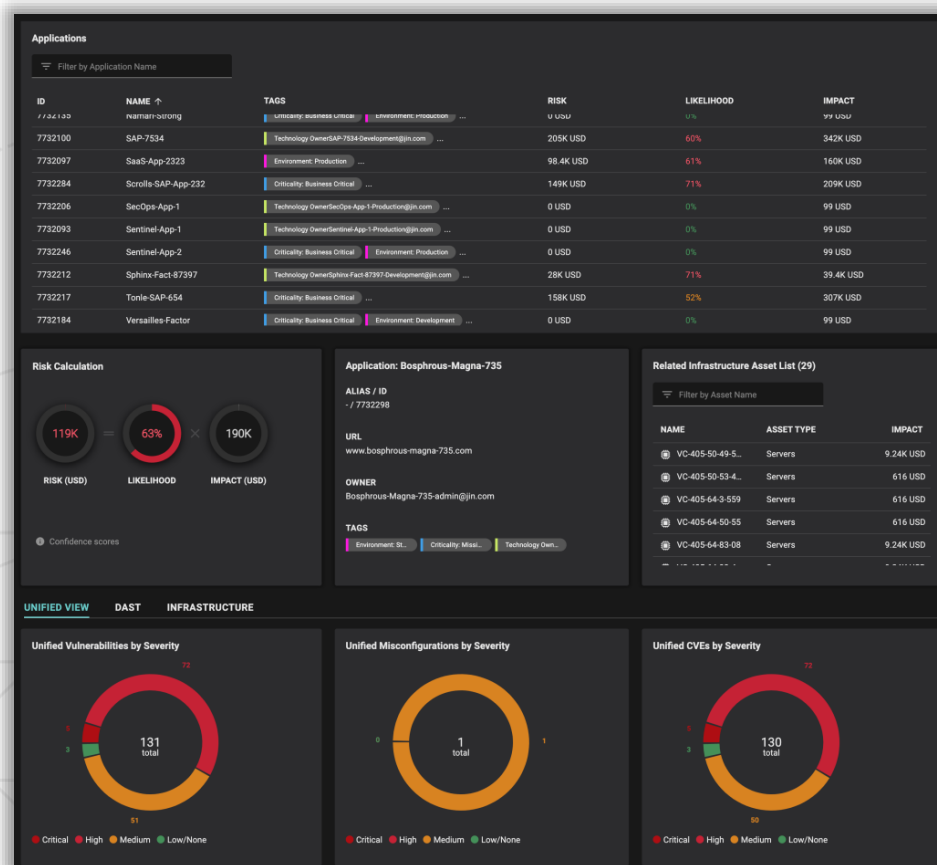


Extend Visibility to Your Full Application Inventory

Do you find it challenging to maintain a comprehensive view of all your custom or web-based applications? Does gaining an in-depth understanding of the full-stack view of each application, along with its supporting infrastructure and associated risks, appear like an insurmountable task?

Balbix offers a simplified and reliable solution, providing a unified view of your complex application landscape. Whether your applications are on-premises, hybrid, or in a multi-cloud environment, Balbix enables you to assess the security posture and identify risks across your entire application ecosystem.

Balbix not only enumerates your full application inventory but also presents a full-stack view of each application and its associated infrastructure. This actionable insight provides the foundation for your security team to effectively prioritize high-risk applications, streamline remediation across a unified view of app-related vulnerabilities, and make data-driven decisions on application risk management. Balbix is here to turn what once seemed like an overwhelming application security challenge into a controlled, secured, and empowering experience.

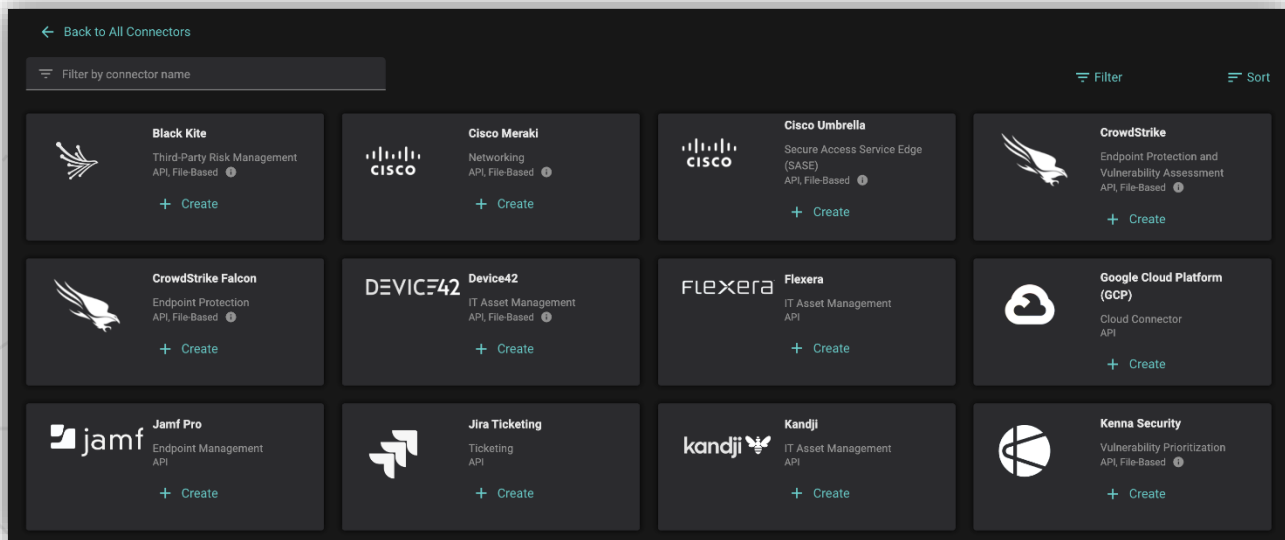


Seamless, Near Real-Time Data Ingestion via Scalable Connector Framework

Handling the massive volumes of data available from key security, IT and business tools is a monumental challenge for organizations. Extracting useful insights from this massive data ocean is not an easy task, and gaps in analysis can leave potential vulnerabilities in your cybersecurity strategy.

This is where Balbix's connector framework comes into play. Designed for efficient and near real-time data ingestion, Balbix manages F100 enterprise-scale volumes of data and reliably supports environments housing millions of assets. In contrast to traditional methods that require significant manual involvement, Balbix simplifies the process through automation. With robust and flexible connector scheduling, data ingestion is automatic, reducing the need for constant supervision and manual control.

The versatility of Balbix's connector framework lies in its ability to support both cloud-based and on-premise data sources, including API and snapshot integrations. This functionality integrates data from various sources into a unified view. Moreover, Balbix employs comprehensive data models across a broad scope. These include device and application inventory, software inventory, vulnerability assessment, misconfigurations, dynamic application security, threat models, exposure, security controls, and business criticality. Balbix effectively correlates and deduplicates, turning raw data into information and ensuring no valuable insights are left unexplored.



Span your Key Data Sources with Extensive Integration Library

Having a comprehensive connector framework is essential, but it's only half of the equation. The other crucial part is leveraging that framework to its maximum potential. That's where Balbix's extensive integration library comes into picture. It supports a vast array of categories—from CMDB and Asset Management to EDR/XDR, Vulnerability Management, Cloud, IoT/OT, Network, Breach & Attack Simulation, Digital Footprint, Ticketing, GRC and more—allowing you to efficiently span a wide range of data sources.

Yet, the real magic of Balbix isn't only the breadth of its integration library. It lies in the speed and simplicity of configuration, enabled by our user-friendly, no-code interface. The days of struggling with complicated and fragile scripts and laborious data integration processes are over. With Balbix, you can swiftly set up your integrations, bringing clarity and control to your cyber asset landscape in mere minutes.



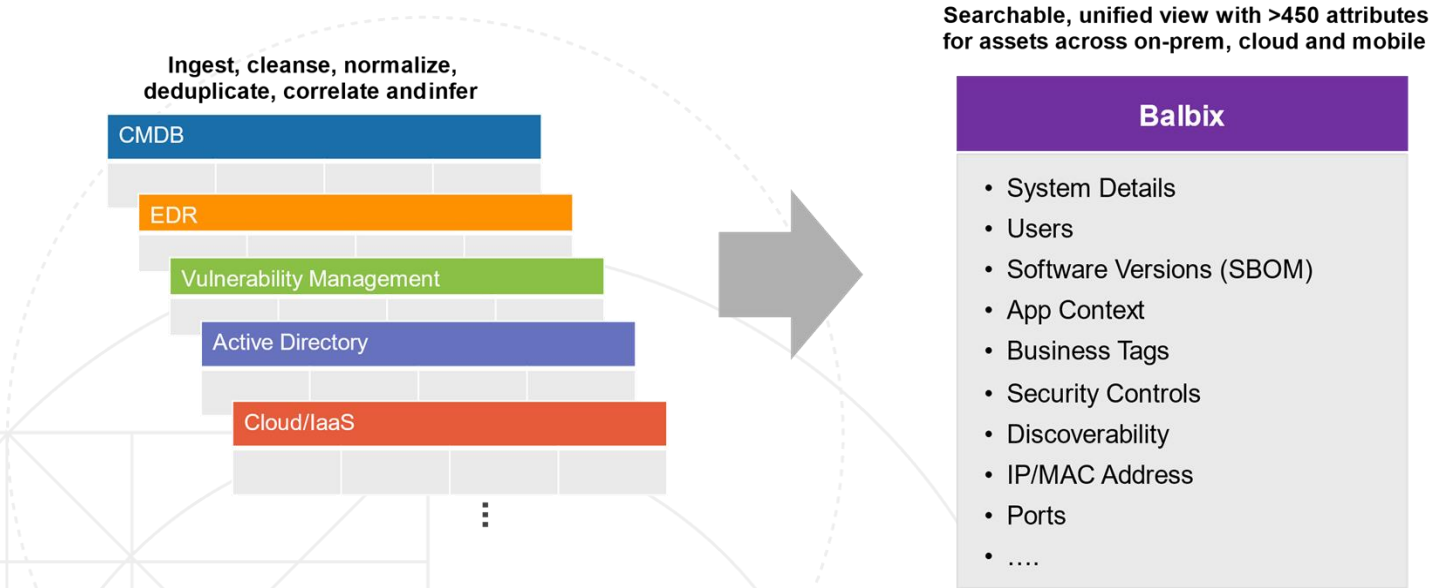
Tame your Data Complexity with AI/ML-Driven Automation

Are you facing impediments with data complexity when understanding your cybersecurity landscape? The issue isn't just about the sheer volume; it's also about conflicting and duplicate data, outdated classifications, and gaps that could render you and your team ineffective in handling threats.

Balbix offers a solution to these problems with AI/ML-based automation. It cleanses your data thoroughly during the ingestion process, giving you a pristine, up-to-date asset inventory. The outcome? A reliable source of truth, cleansing inconsistencies and redundancies. That's what Balbix Host Enumeration logic helps achieve.

Additionally, Balbix automatically categorizes your assets and software, providing you with a comprehensive view of your network, whether it's the entire enterprise or individual business units. This means you have access to precise data in real-time, instead of depending on out-of-date manual classifications.

Balbix also incorporates business context into asset management. Balbix prioritizes your assets based on factors such as business-criticality, inherent risk, and user privileges. This empowers your security and IT teams with a clear roadmap for prioritizing actions and strengthening your cybersecurity posture.



Data Fidelity & Coverage Assurance via Sensors

For organizations struggling with asset coverage gaps from existing tools, Balbix's sensors help you gather best-in-class detail regarding system information, software inventory, SBOM, configuration, user data, and more with high accuracy. 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 on your host assets, networking assets, and unknown/rogue assets 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 with the highest fidelity.

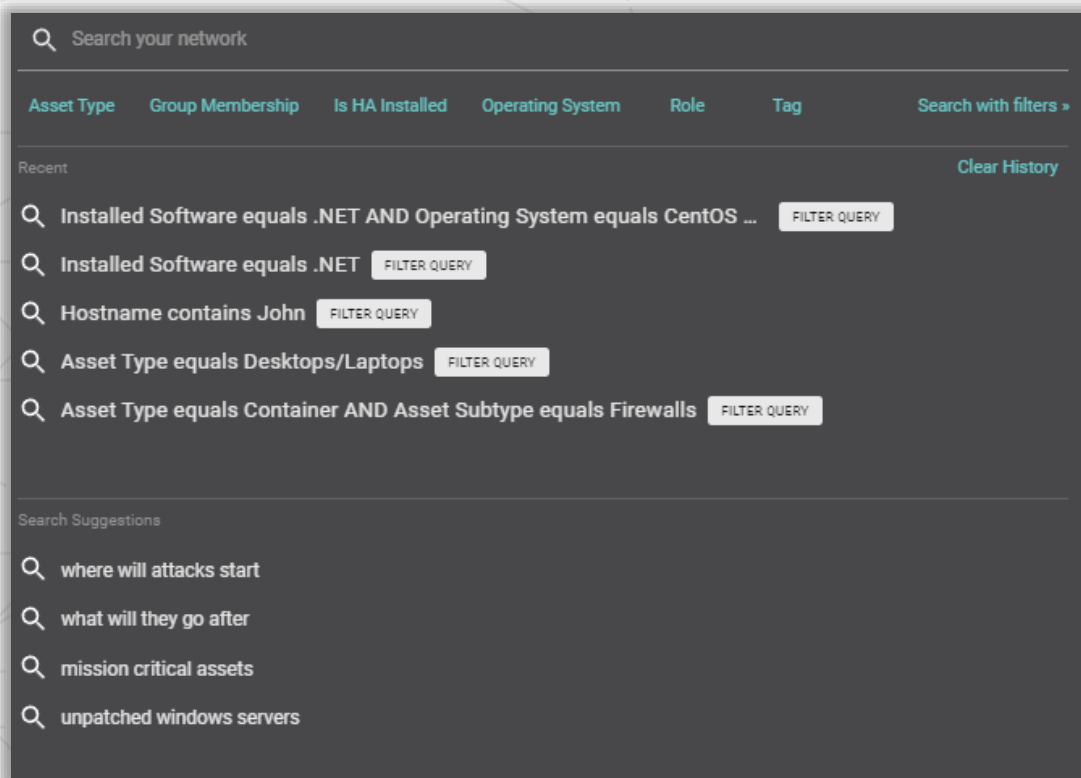
2

Instantly Query and Monitor your Consolidated Asset View

Natural Language and Advanced Filtered Search for Intuitive Queries

Picture this: You're in charge of cyber asset security at your organization. Each day, numerous queries related to assets, systems, software, and various data sources flow your way. These inquiries require an intricate understanding of key attributes such as asset type, hostname, site, subnet, software inventory, OS, business org alignment, location, and more. You might even need to include specific software inventory details like installed software or operating system status. Decisions need to be made, but you're stymied by manual processes and an overflow of information.

Now, imagine having a 'Google for cybersecurity' at your disposal, capable of processing natural language and advanced filtered searches for intuitive queries. That's what Balbix does for you. You can easily navigate previously challenging queries such as "Identify all Linux servers hosting databases within our South America eCommerce business unit and running EOL software", with remarkable speed and precision. Let's say a new vulnerability like Log4j or Spring4Shell pops up. With Balbix, identifying affected assets - even the ones with end-of-life software or operating systems - becomes a matter of seconds, not days or months. This immediate, data-driven decision-making eclipses traditional, often gut-based approaches, pivoting your security strategy from reactive to proactive.



Dynamic Groups Enable Precise Environment Views

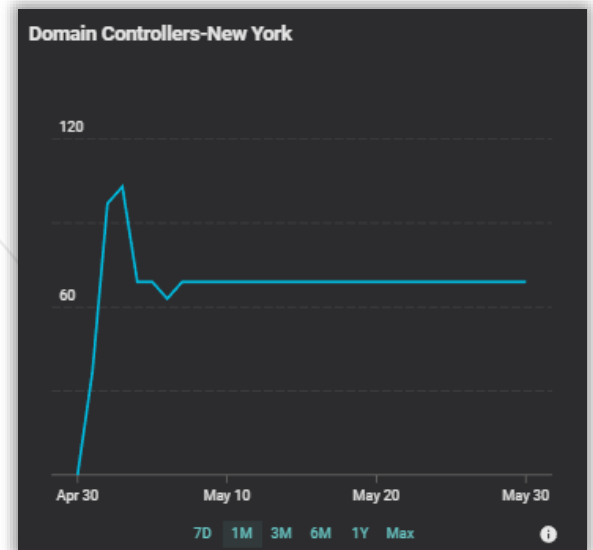
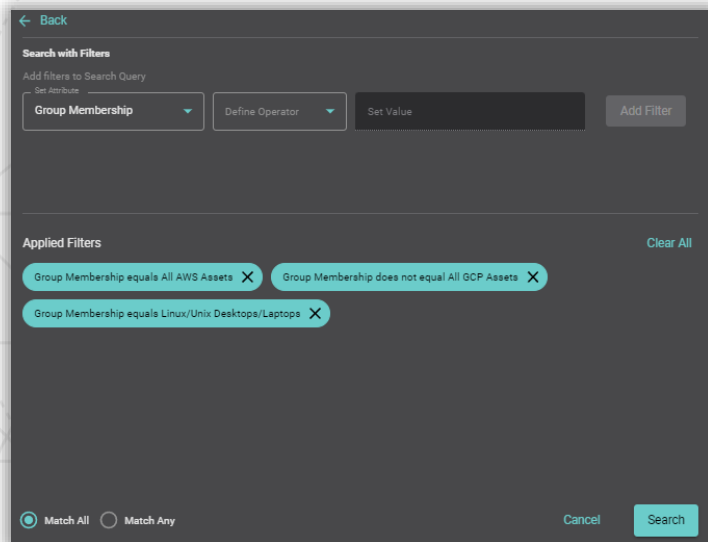
Are you seeking a flexible way to organize and report on your IT infrastructure and prioritize based on custom criteria for effective remediation?

Balbix has you covered with Dynamic Groups, coupled with real-time search. Dynamic groups allow you to form custom groups of assets based on a wide range of attributes, such as asset type, vulnerability status, business impact, and user characteristics. Additionally, you can assign specific owners to these groups, ensuring clear responsibilities and accountability.

With Balbix, you can swiftly create dynamic groups using user-friendly search. This is beneficial whether you're trying to identify all unpatched domain controllers in Paris running Windows Server 2019 without Tanium coverage or need to target all Linux servers or systems with CrowdStrike installed. Gone are the days of manual sorting or wading through large amounts of extraneous data to find exactly what you're looking for.

Furthermore, Balbix's dynamic groups are designed to automatically update with any changes to your assets or attributes, providing you with the most current information without the need for manual updates. This reduces the risk of missing any important details.

Balbix's dynamic groups also power comprehensive dashboards that facilitate visualization and analysis of your environment. They serve as a basis for workflow scoping and the implementation of role-based access control (RBAC). Assigning owners to specific asset groups ensures defined responsibilities and accountability, promoting proactive threat management.



“Pieces of critical cyber security data are typically scattered all over the place. Until correlated, coalesced and understood contextually, it is just another piece of data—there is no actionability. I get the whole picture from Balbix.”

– John Shaffer, CIO, **Greenhill**

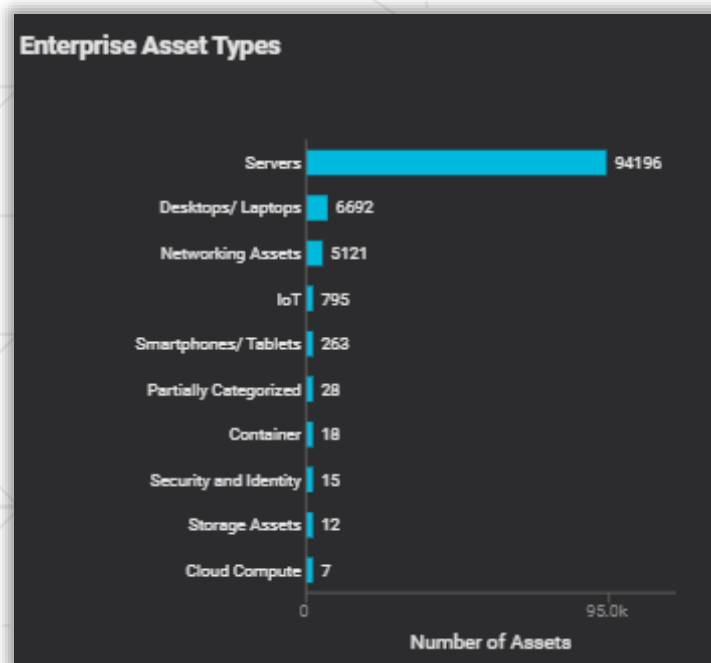
Effortless Custom Dashboarding for Comprehensive CAASM Insights

In the intricate landscape of cybersecurity, maintaining an accurate and timely understanding of all your assets is crucial yet complex. With Balbix's CAASM widget library, the difficulty of this task is significantly reduced, offering a panoramic view of your organization's cybersecurity landscape.

It helps you create tailored dashboards for different stakeholders and enables asset tracking by site, owner, impact, and type. It provides a comprehensive overview of your cyber infrastructure and exposes potential security coverage gaps. Whether you need a quick insight into your asset inventory, understanding risk factors across cloud assets, or both high-level data for broad presentations and detailed analysis of individual assets, Balbix can assist. In a practical sense, our platform enables you to answer key questions such as:

- What assets are in my environment?
- What is the complete inventory of my software products, including versions and components?
- How many assets exist in each category (e.g., servers, workstations, IoT devices)?
- Which software is installed on each asset, and what are the potential licensing violations or end-of-life risks?
- Do my security tools provide complete coverage for all assets? If not, what gaps are there?
- More...

By providing answers to these critical questions, Balbix enables you to monitor and track your assets, their attributes, and vulnerabilities in real-time. This facilitates informed decisions about your security investments and risk management strategies, propelling your cybersecurity strategy with a comprehensive view of your organization's landscape.



3

Accurately Identify Security Control and Coverage Gaps

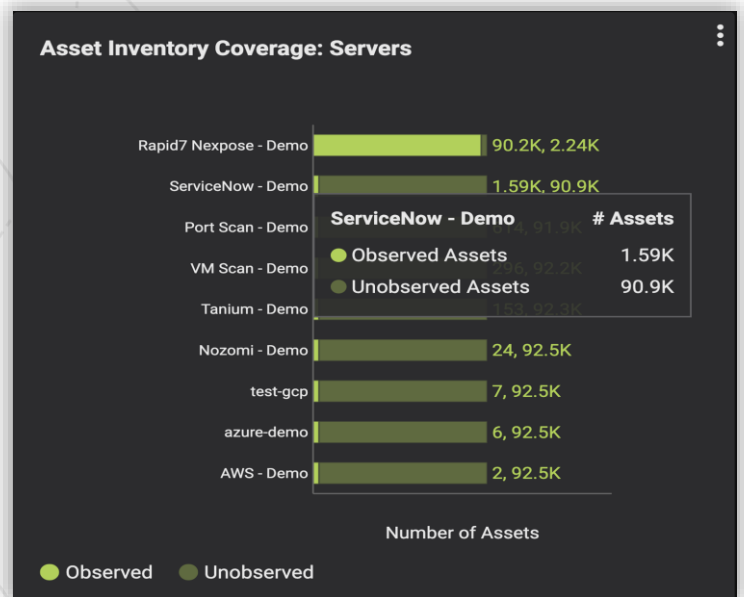
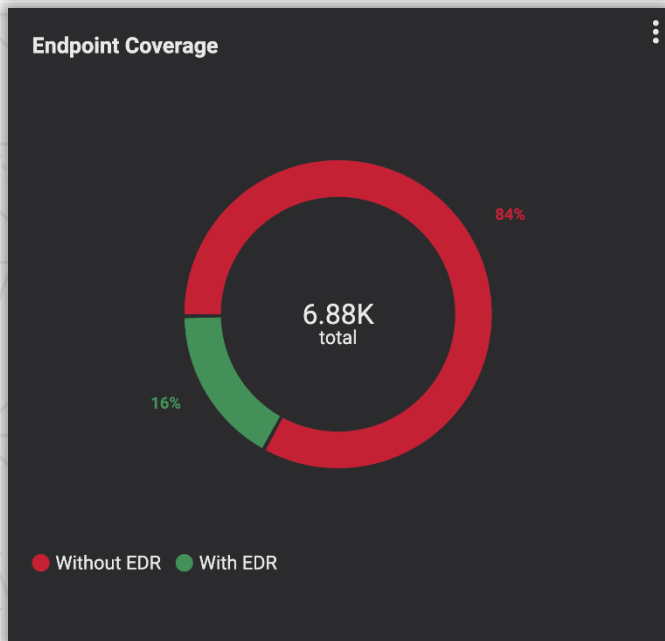
Full Gap and Coverage Analysis

Are you risking your organization's security by neglecting proper monitoring of IT and cybersecurity tools? With so many tools and assets to manage, it becomes challenging to keep track of everything, leaving room for attackers to exploit vulnerabilities. You and your teams worry about situations such as:

- Is your asset inventory data incomplete or outdated, with significant gaps and stale data?
- Are your vulnerability scans covering your entire environment, or do they have blind spots?
- Are your endpoint security controls providing comprehensive coverage ?

The consequences of inaction here can be severe. However, Balbix offers a solution that addresses these critical issues head-on. By providing continuous monitoring and analysis of an organization's assets, Balbix enables you to identify any gaps in coverage across different data sources. You can assess the completeness of your CMDB and pinpoint any gaps that require attention. Balbix also helps you ensure comprehensive vulnerability assessment coverage by your scanners or assessment tools, allowing you to identify overlaps and areas where your environment might be left exposed.

Furthermore, Balbix empowers you to evaluate the coverage of deployed endpoint security controls. You can easily identify any limitations or gaps in your EDR/XDR security infrastructure. Balbix's precise insights at the asset level eliminate guesswork, allowing you to proactively manage your cybersecurity posture and ensure comprehensive protection.





Detailed Software Inventory for Flexible Analysis of all the Deployed Software

Can you really afford the risk of not having a precise and detailed software inventory? What if missing out on a critical software upgrade exposed your organization to a security breach?

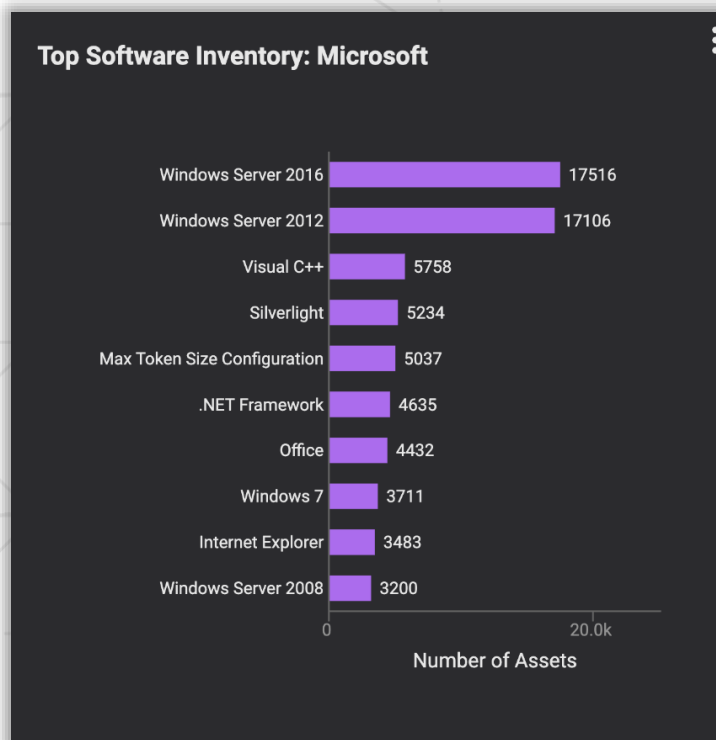
With Balbix, you gain comprehensive visibility into your deployed software, available through a user-friendly dashboard or search UI. You can customize your view, pivoting by software vendor, category (think of application, browser, OS, database or plug-in), version, and product state (like patched, unpatched, end-of-life). The real game-changer with this powerful capability is how Balbix enhances your ability to monitor the software upgrade progress, facilitate new software rollouts, and ensure compliance to corporate policies.

Consider a typical Patch Tuesday; identifying critical Microsoft security patches can be a manual, error-prone endeavor. But not with Balbix! It automates the process, enabling teams to identify, deploy necessary fixes, and track installed patches, efficiently addressing large numbers of CVEs. Balbix empowers you with insight, eliminating guesswork and saving valuable time.

Further picture this: Your corporate policy states that all systems within the network must run the latest version of a specific application. Despite this, in a large and complex network, some systems might still be running an outdated version due to oversight or technical issues, posing a significant security risk.

The analysis powered by Balbix's software inventory widget comes to your aid here. By providing a granular view of all software deployed across your network, Balbix enables you to quickly identify systems running the outdated application versions.

Don't just manage your software inventory; excel at it with Balbix.



Automatic Detection of Endpoint Controls

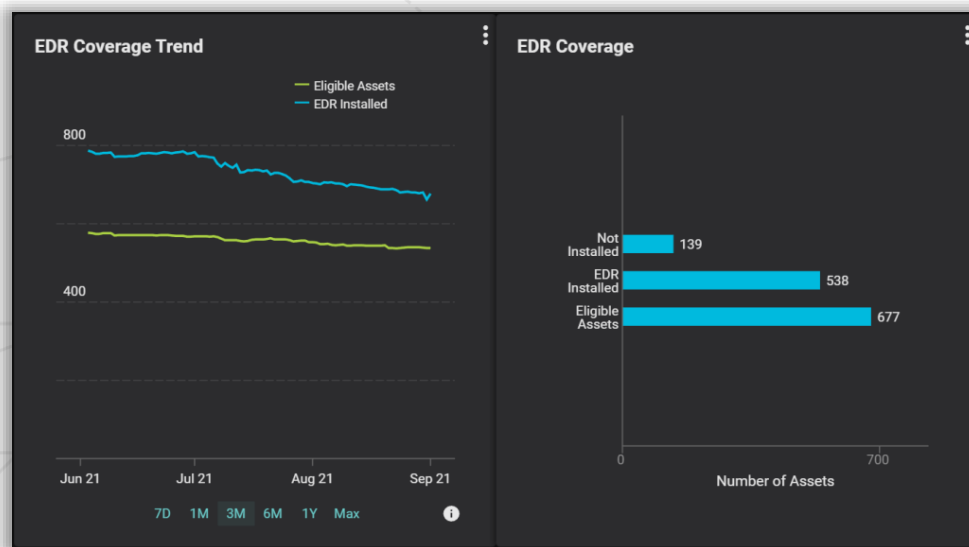
Tracking endpoint controls manually across a complex network can be a cumbersome and error-prone task, with inconsistent detection potentially leading to overlooked security flaws.

Balbix helps you refine your cybersecurity strategy by automating the detection of endpoint controls from your full software inventory and SBOM. This comprehensive view ensures that any coverage gaps are immediately evident, enabling you to swiftly fortify your security.

For instance, you can easily monitor control deployment by displaying a trend chart of systems that have an EDR solution installed, vs. those systems with the control missing. As the EDR rollout progresses across an increasing number of assets, these lines will begin to converge. Balbix allows you to easily generate additional views to highlight and drill into the deployment details.

As a security engineer, you can delve into the group of assets that need attention, obtaining a full list of hostnames, IPs, locations, and more to facilitate your actions.

As a security leader, you gain a better understanding of the full scope of the project and the progress toward completion.



Automatically Surface Exposure to End-of-Life Software

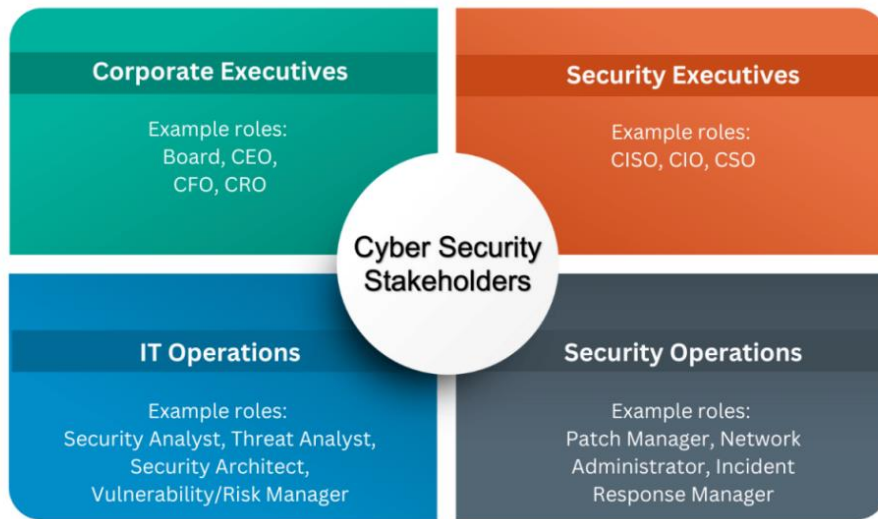
Identifying end-of-life (EOL) software in your environment is essential for effective vulnerability management. These instances are highly vulnerable to attacks as the vendor offers no ongoing security updates or patches.

Balbix makes it easy to identify EOL instances of software across Windows and Linux systems. To do this, all you need to do is search for EOL systems using the native widgets. Since Balbix maintains up-to-date software inventory and version information, you will have the information you are looking for in no time.

4 Enable High Velocity Issue Remediation

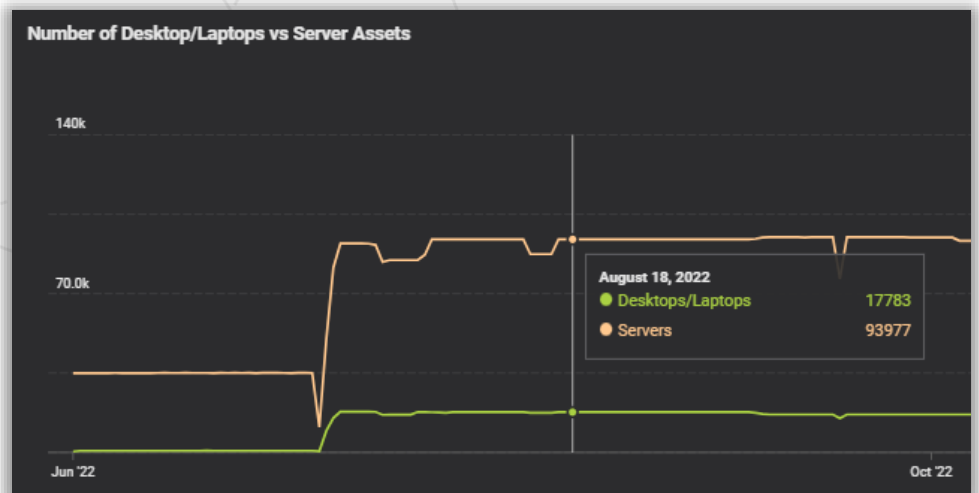
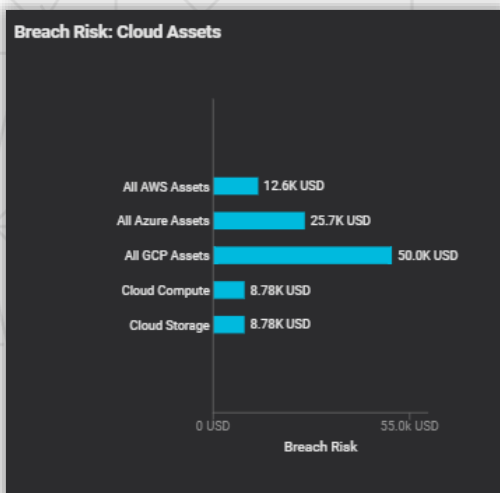
Customizable Dashboards to Easily Communicate Progress and Drive Action

Remember those countless hours spent creating numerous reports to cater to different cybersecurity stakeholders? That worrying feeling of wondering if the vital information you're trying to communicate is getting lost in the sea of data? With Balbix, those worries become a thing of the past.



Balbix's platform allows you to create customizable dashboards, tailored for specific roles—be it Security Executives, Corporate Executives, Security Operations, or IT Operations. Need to show how cyber risk is distributed by line of business, geography, or business owner? A few clicks and you have an executive dashboard ready. Need to prioritize top security risks and enable efficient remediation? An operational dashboard is just minutes away.

With Balbix, dashboards are more than just data; they are collaborative tools. You can choose to share, email, subscribe, or annotate—communicating progress and driving action has never been easier. Shelve the manual methods of reporting and embrace the Balbix way.



“Our inventory process was a mess. We were unable to identify and categorize assets properly. Yes, we had dozens of tools and some ad-hoc integration, but it was very difficult to correlate the data from these sources into a single, comprehensive inventory...Thanks to Balbix, we have real-time asset inventory with continuous monitoring. We get actionable insights for IT and risk every day”

– VP of Cybersecurity, **Fortune 50 Telco**

Exports and Reporting

Do you need a simpler way to handle large amounts of asset data, generate valuable insights, and meet compliance reporting requirements? Balbix provides a straightforward solution to these problems.

Balbix allows for bulk exports of comprehensive asset inventory, enabling your security team to delve into data analysis, or supply other systems as necessary. This feature lets you easily export data on your assets, software, and more, regardless of the report size, simplifying your asset management workflows and compliance reporting.

Furthermore, Balbix's dashboard provides a range of reporting options. If you require a specific compliance report, such as the percentage of endpoint controls deployed, it can be delivered directly to your email. Balbix replaces time-consuming manual reporting processes, helping you to save time, decrease risk, and improve your security operations efficiency.

CMDB Update

Maintaining an up-to-date Configuration Management Database (CMDB) such as ServiceNow can be a challenging task, especially when dealing with outdated or inaccurate data. Balbix provides a straightforward solution to address this common issue.

Balbix automatically correlates and deduplicates data, offering near-real-time, cleansed asset information. If your organization utilizes a separate CMDB, Balbix's up-to-date, enriched asset data can infuse it with much-needed freshness.

Through Balbix, your CMDB evolves from a static, outdated archive into a dynamic, constantly updated source of truth for your entire enterprise. This process allows easy access to real-time asset data, effectively addressing a common pain point in data management and enabling you to achieve the promised ROI (return on investment) from your CMDB.



Drive Actionable Risk Reduction with Risk-Based Vulnerability Management

While building an effective cybersecurity posture, visibility becomes your compass. The maxim "You can't protect what you can't see" holds true, and Balbix's CAASM solution serves as a foundational pillar of your cybersecurity strategy. It provides clear sightlines of your assets, paving the way for effective risk mitigation.

Astute business leaders understand the importance of reducing risk, and they seek a plan to address it. To develop this plan, we must address the "where, why, how, who, and when" questions. Where does the underlying vulnerability lie that drives each risk? Why does it exist? How should it be addressed and prioritized, focusing on the highest-risk items first? Who is responsible for remediation? When should it be remediated according to enterprise policy and SLAs?

This is where Risk-Based Vulnerability Management (RBVM) comes into play. It forms a core foundation of your proactive cybersecurity efforts, keeping you ahead of potential threats and efficiently reducing identified risks in an optimal manner.

Balbix goes far beyond providing just the asset visibility focus of other CAASM tools. It seamlessly integrates RBVM into the platform, automating the discovery, prioritization, remediation, and reporting of vulnerabilities. You gain continuous, unified asset inventory and vulnerability visibility. Risk-based vulnerability prioritization allows you to focus on the most critical items first. Balbix streamlines your remediation workflows and provides comprehensive vulnerability management metrics. It's not just about quantifying risk; it's about driving actionable risk reduction.



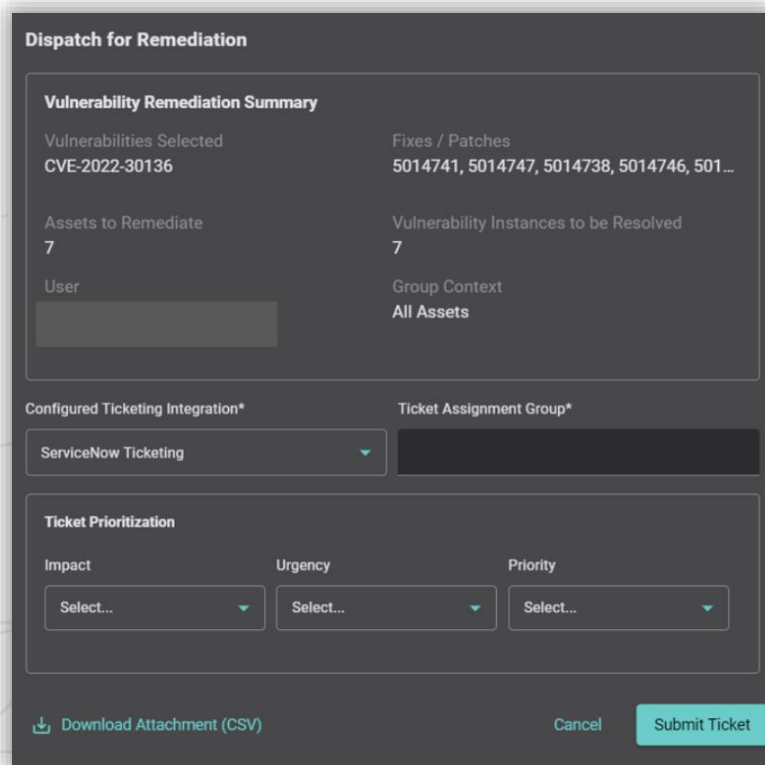
With Balbix, you have the power to proactively mitigate risks, safeguard your organization, and stay one step ahead in the ever-evolving cybersecurity landscape.

Enabling Remediation Workflows and Integrations

Efficient vulnerability remediation is critical for effective vulnerability management yet can often be slowed down by disjointed systems and manual efforts.

Balbix removes this friction through seamless integration with ticketing platforms such as ServiceNow ITSM or Jira Service Management. This facilitates the creation of remediation tickets by directly pushing detailed fix information and all relevant context, thereby enabling teams to quickly address high-priority vulnerabilities with reduced manual intervention.

These ticketing integrations not only maximize the potential of your established systems but also enhance the efficiency of your security and IT teams, creating a more streamlined and effective remediation workflow.



Dispatch for Remediation

Vulnerability Remediation Summary

Vulnerabilities Selected CVE-2022-30136	Fixes / Patches 5014741, 5014747, 5014738, 5014746, 501...
Assets to Remediate 7	Vulnerability Instances to be Resolved 7
User [Redacted]	Group Context All Assets

Configured Ticketing Integration*
ServiceNow Ticketing

Ticket Assignment Group*
[Redacted]

Ticket Prioritization

Impact Select...	Urgency Select...	Priority Select...
---------------------	----------------------	-----------------------

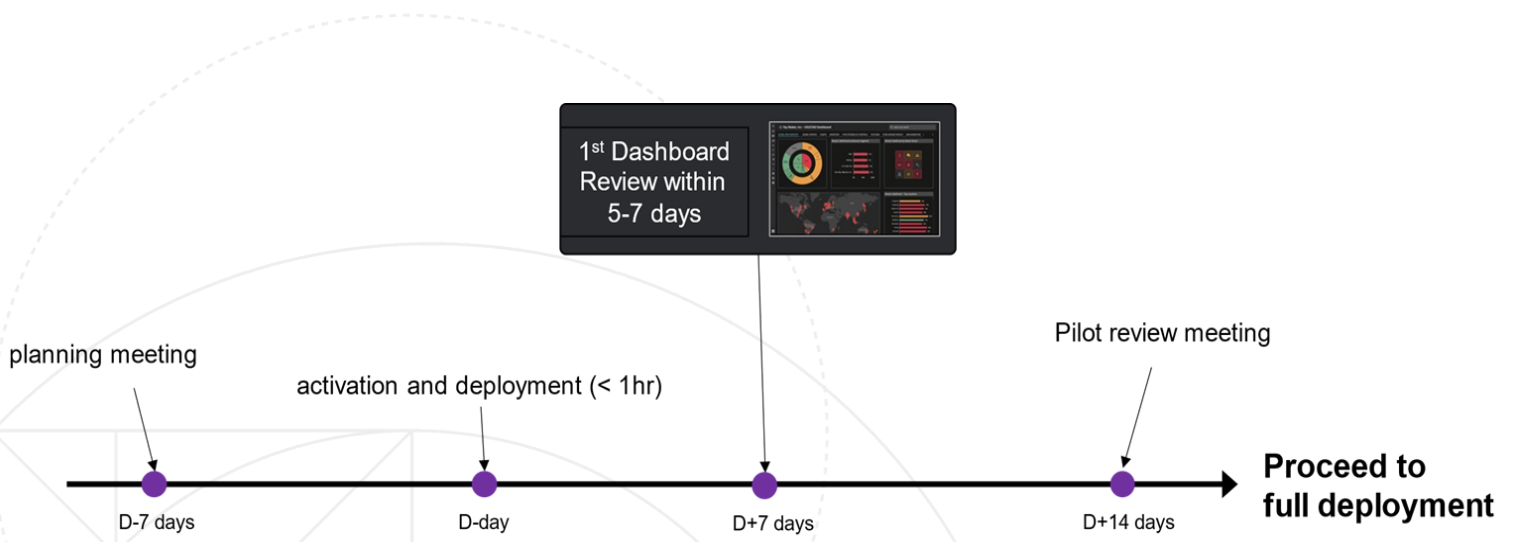
Download Attachment (CSV) Cancel Submit Ticket



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.