



# Balbix BreachControl™

## AI-Powered Cybersecurity Posture Transformation

Security teams are pulled in many directions—vulnerability management, incidence response, deployment and tuning of security tools, application security, dashboarding and reporting, etc.

- Do you know if you are working on the right projects?
- Where are the riskiest areas of your attack surface?
- Can you quantify the progress you are making?

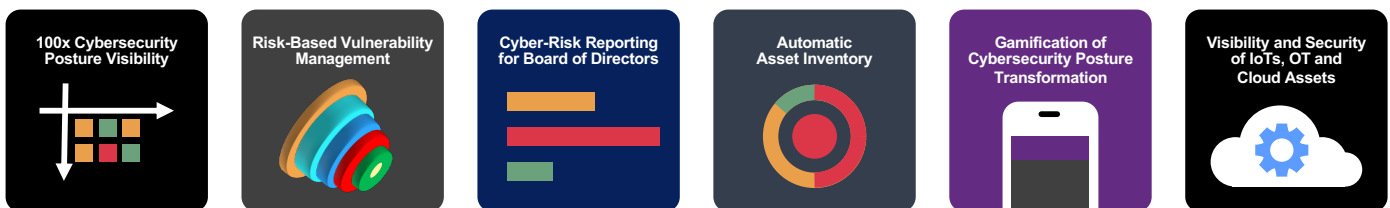
Balbix enables you to address these challenges and make the right decisions in order to transform your cybersecurity posture and reduce breach risk.

The Balbix BreachControl platform uses specialized AI algorithms to discover and analyze the enterprise attack surface to give a 100x more accurate view of breach risk. The platform also provides a prioritized set of actions that you can take to transform your cybersecurity posture and reduce cyber-risk by 95% or more, while making your security team 10x more efficient.



## Use cases

Balbix enables a broad set of vulnerability and risk management use cases that help to transform your enterprise cybersecurity posture.



## Highlights



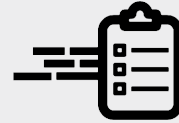
### Continuous discovery and analysis

Sensors, connectors, and collectors deployed across your network continuously discover and monitor your devices, apps, and users across 100+ attack vectors



### Risk insights and prioritization

You can understand your real-time risk with drill-down risk heatmaps and natural-language search.

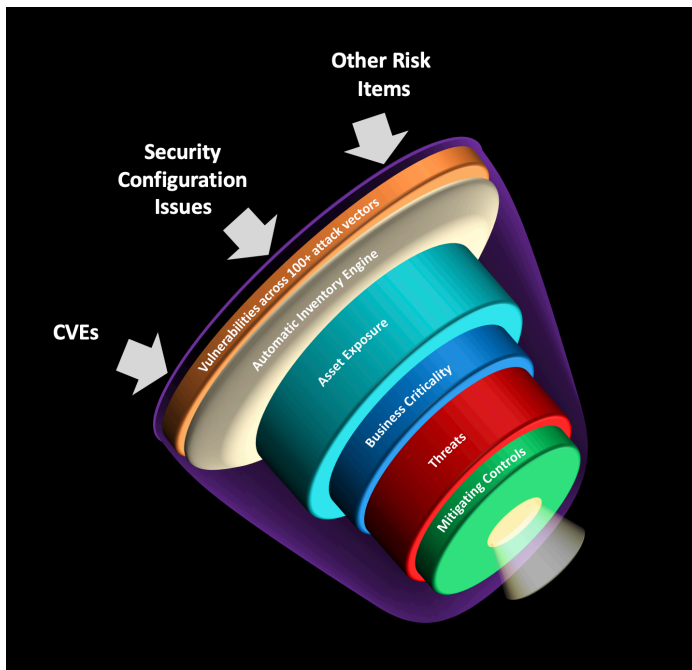


### Cybersecurity posture improvement

Prioritized tickets with relevant context are generated and assigned to the right owners for strategic and tactical mitigating actions.

## 1-hour deployment

- Sensors are placed to span a suitable subset of *north-south* and *east-west* network traffic in your environment
- Connect Balbix to your enterprise data sources such as Active Directory, AWS configuration, logs, etc.
- Within 24 hours, get a 100x more accurate view of cyber-risk including asset inventory, historical patching posture, password-related issues, missing encryption, easily phish-able users, and much more



## Prioritization

Balbix's risk-based prioritization of cybersecurity posture issues incorporates 5 factors:

1. Vulnerability severity level
2. Threat level— is this vulnerability being exploited in the wild
3. Exposure based on usage or configuration
4. Business impact if this asset is compromised
5. Compensating controls that negate risk from this issue

The Balbix platform filters out issues that need immediate attention vs those which can wait a few days, and those which are just noise.

## Automatic inventory

Balbix automatically discovers and analyzes your inventory. This includes all devices, apps and services, managed or unmanaged, infrastructure, on-prem and cloud, mobile, IoTs, ICS, etc. The inventory is available via real-time dashboards and search.

Capabilities include:

- Categorization of assets into core or perimeter assets
- The relationship between assets and users
- Details for each asset, e.g., software and hardware version, open ports, and usage
- Estimated breach impact for each asset

## 100+ attack vectors

Balbix performs continuous monitoring and identification of vulnerabilities and other risk items for each asset across 100+ attack vectors, for example:

- Unpatched software (CVEs)
- Phishing
- Web and ransomware
- Default, weak or reused passwords
- Encryption issues– missing or improper encryption
- Misconfiguration
- Certificate issues

## Google-like search

Get answers to questions about your inventory, cybersecurity posture or breach risk using natural language search.

You can:

- Query your inventory using IT vocabulary, e.g., “windows servers in London”, “security cameras”
- Combine security and IT terms: “unpatched switches in NYC”, “password reuse”, “phishing”
- Search by CVE number, e.g., “CVE-2017-0144”, or its common name “wannacry”
- Use higher level queries like “where will attacks start”, “what will they go after”, “assets with intellectual property”, and “risk to customer data.”



## Discovery and validation of security controls

Balbix considers the risk-negating effect of compensating controls deployed in your enterprise while prioritizing vulnerabilities. Capabilities in this area include:

- Automatic discovery of your existing mitigating controls like firewalls, anti-phishing systems, EDR, etc.
- Analysis to help you understand the effect of specific security controls in reducing enterprise risk
- Calculate proforma ROI of deploying new security controls

## Integrated threat feeds

Balbix incorporates threat intelligence from our partners and public sources. This includes information from the dark web, research forums, govt advisories, exploitDB, pastebin, etc.

- Integrated threat data enables Balbix to prioritize your vulnerabilities based on what is currently fashionable with the adversary vs theoretical CVEs.
- You get to know which of your assets are susceptible to infamous threats like wannacry, sambacry, poodle, broadpwn, etc., and can take mitigating actions quickly.

## Notifications, digests and reports

Balbix provides timely notifications to breach risk owners and stakeholders on important data triggers

- Set up compliance watchdogs using natural language search and the powerful IFTTT framework
- Daily and weekly digests provide stakeholders with timely data
- Generate cyber-risk reports for discussion with your board of directors and senior management

## Take action to transform your cybersecurity posture

### Prioritized action plan

Balbix provides actionable insights with specific steps that you can take to improve cybersecurity posture.



- Suggested risk remediation actions are prioritized based on risk
- Context and tools help you select the order of scheduling mitigating tasks to get maximal reduction of risk
- When appropriate, the system provides options for each risk insight to help you quickly implement a practical fix
- The prescribed mitigating actions can be ticketed to remediation owners automatically or manually

### Integrations

Balbix integrates into your enterprise tools, such as ticketing and security orchestration systems.



- Tickets can be automatically created, assigned to the relevant owners, and tracked
- As your team takes mitigating actions, Balbix automatically discovers and validates each fix
- APIs available for 3<sup>rd</sup> party tools to query Balbix for context about assets and risk

### Customizable

You can define risk areas appropriate for your business and the platform maps them to specific aspects of your cybersecurity posture.



- You can type “risk to intellectual property” in Balbix’s search box, and define this as a risk item of interest
- Balbix can automatically map risk items like “customer data” to the actual on-network assets and their attributes (e.g., patching cadence) that drive the risk
- The system continuously observes, analyzes and reports on the relevant parts of your cybersecurity posture for defined risk areas of concern

### Gamification

To improve cybersecurity posture, CISOs and security teams need stakeholders to act and fix risk items for the systems they own in a timely fashion. This is normally quite hard, but Balbix makes it easier using the power of gamification.



- As gamemaster, the CISO can set up risk focus areas, owners, incentives, target levels and desired SLAs
- Each risk owner gets tasks via tickets assigned to them and notifications
- Balbix ensures that risk owners get all the context, tools and options they need in order to finish the assigned tasks
- Leaderboards and rewards help to get the competitive juices flowing, and rapid security posture transformation