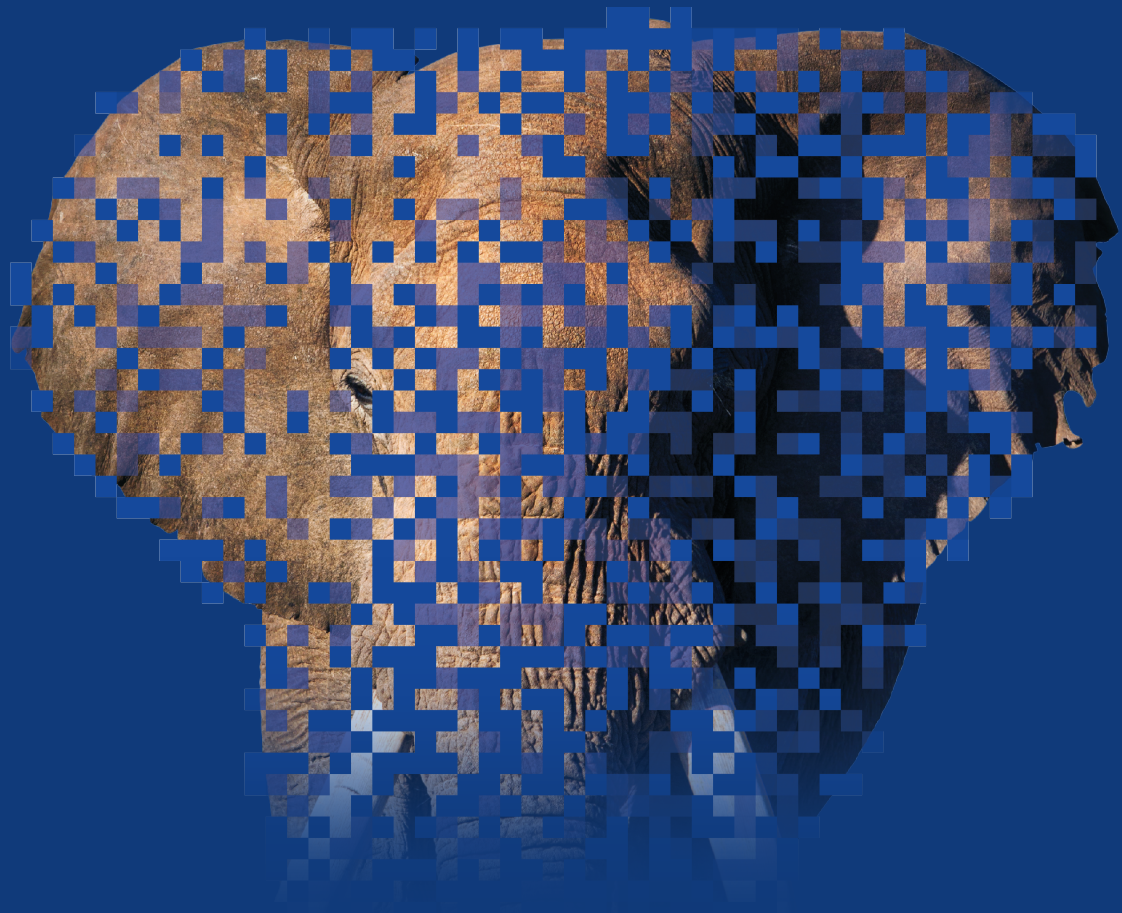
Balbix®

How to Gain 100x Visibility Into Your Cybersecurity Posture



Top-of-mind concern for CISOs:

A robust cybersecurity posture

With thousands of assets in your enterprise and each susceptible to a myriad of different attack vectors, there are millions of ways by which your enterprise can be breached. Poor cybersecurity hygiene, such as a weak password or an unpatched exposed Internet-facing system is an open door for attackers. And yet, many vulnerabilities are purely theoretical and extremely unlikely to ever be exploited.

So how do should CISOs wrap their arms around these cybersecurity challenges and emerge victorious over the adversaries?

Your first line of defense against the adversary is a good cybersecurity posture. Therefore, understanding the full scope of your cybersecurity posture and correctly prioritizing areas of relevant risk is essential to protecting your organization against breaches.

CISO challenges:

- Exploding attack surface, massive increase in security complexity
- Drowning in cybersecurity data, with few actionable insights
- Too many tools

Analyzing and improving cybersecurity posture is not a human scale problem any more

Balbix®

Priorities of an effective CISO

What makes a CISO effective? It is the ability to identify assets that need to be protected, understand and prioritize risks to those assets, and implement appropriate controls to protect those assets.

Effective CISOs are able to:

- Achieve cybersecurity posture visibility by identifying all that needs to be protected and prioritizing areas of greatest risk.
- Transform cybersecurity posture by enhancing current security measures and investing in new areas
- Optimize cybersecurity posture continuously as conditions change
- Communicate breach risk and cybersecurity posture accurately to the board of directors

Click below to learn more

GUIDE

Elements of Cybersecurity Posture Transformation

SOLUTION BRIEF

Cyber-Risk Reporting for Your Board of Directors

100x cybersecurity posture visibility

Great cybersecurity posture visibility means having a complete, accurate and real-time picture of your cybersecurity posture as it relates to areas of business risk. This includes:

This is where effective CISOs win. They have a clear picture of what and where their most critical assets and information reside and they have adequate safeguards to protect these assets. This means first identifying the key systems and data that the enterprise (should) care about, then reviewing your enterprise cybersecurity capabilities and other defenses to ensure that adequate security controls are in place to protect them.

Balbix®

Why is visibility critical?

Managing security is a complex endeavor and traditional security approaches involve multiple point products, manual change processes, monolithic policies and data silos. Because of this, things can fall through the cracks and critical assets can be overlooked resulting in an incomplete and inaccurate picture. This lack of accurate and complete visibility intensifies security challenges.

Visibility is crucial. You cannot monitor or protect devices and information you can't know about. Before security teams can do anything to protect their environment, they need to see and understand the on-network ground truth.

Questions that enterprises must consider:

- What are our most valuable assets?
- Do we know our cybersecurity posture weaknesses?
- Are our current security controls effective?
- What are some potential threats we are facing?
- Are we making the right security investments to ensure cyber-resilience?

How to gain real-time visibility into your attack surface and breach risk

The most important building block of any visibility program is an accurate inventory of what you are defending.

Unfortunately, it is quite hard to keep track of the various devices, applications, and services used by enterprise users. As a result, it is difficult to correctly target vulnerability scans and risk assessments. It is particularly problematic to cover non-traditional assets such as bring-your-own devices, IoT, mobile assets, and cloud services. Any enterprise network is only as secure as its weakest link. Therefore, your cybersecurity visibility must extend all types of assets and all sorts of security issues.

100x cybersecurity posture visibility with Balbix

Balbix continuously discovers your enterprise attack surface and understands your defenses to provide you with comprehensive cybersecurity visibility. This 24×7 analysis covers on-prem, cloud and mobile assets including unmanaged systems and non-traditional assets. Each asset is continuously analyzed for risk across 100+ attack vectors.

With this level of visibility, you gain insights on the weaknesses in your defenses which can help you prioritize and drive remediation actions.

Balbix®

100x better visibility into your cybersecurity posture than traditional methods

All types of assets

Automatic and continuous discovery and categorization of assets to provide a real-time asset inventory.

All types of vulnerabilities

Analysis of each asset against 100+ attack vectors to surface not just unpatched vulnerabilities but also other risk issues like password reuse, easily phishable users, encryption issues, misconfiguration, etc.

Visibility into business criticality of assets

Business criticality for each asset provided based on an analysis of usage and network traffic.

Risk-based prioritization

Risk-based prioritization of vulnerabilities considering 5 factors—vulnerability severity, threat level, business criticality, exposure, and the risk-negating effect of compensating controls.

A deeper dive into asset inventory and its challenges

Maintaining an up-to-date enterprise inventory system is very challenging. The set of assets in the enterprise changes constantly with devices being added and retired, physical machines migrating to virtual and various stakeholders constantly installing and updating software (with or without approval). Inaccurate inventory makes managing compliance and cyber-risk very difficult.

An outdated inventory is also frustrating and impedes the velocity of business. Unfortunately, applying manual effort to keep inventory updated is time and resource intensive and does not work at scale. Enterprise security teams don't often control all assets, which makes the task of understanding assets and gathering insights about them even more difficult.

Traditional inventory tools typically track only managed assets. Non-traditional assets like IoTs are either left undiscovered or partially tracked by a motley collection of specialized tools, one for each asset category.

We know that the best human experts can put together an accurate picture of the type and category of a device on your network by manually looking at a broad variety of data sources.

For example, from Layer 3 packet analysis, an expert might be able to extract media access control (MAC) organizational unit (OU) information that indicates that a device is a Cisco device. At Layer 4, they might see transport headers and protocol behavior that are consistent with the device being a switch with a management portal available at ports 80 and 443. From Layer 7 analysis of protocol behavior and a study of artifacts rendered in the web browser, we might be able to say that port 80 does not automatically redirect to port 443, and that the device is a wireless LAN controller made by Cisco.

At the enterprise level, however, relying on humans to do this type of analysis on a continuous basis does not scale.

Addressing the problems of inventory with AI

At Balbix, we use AI to mimic this type of intelligent analysis by throwing L3, L4, and L7 data from different vantage points on your network into a sequence-to-sequence deep neural network which discovers, inventories and categorizes all devices, users, and applications. The system is real time, with entities analyzed the second they show up on your extended network.

Specialized AI is very effective for addressing the challenges of inventory. Consider the challenge of associating users with devices. Typically, you can identify users associated with managed laptops and desktops either by linking them with Kerberos authentication or domain logon sessions of users. As you can imagine, this approach does not work well for unmanaged bring-your-own devices.

Balbix uses time-domain correlation of Dynamic Host Configuration Protocol (DHCP) lease renewals, beginning-of-day traffic time, on-off times, and timing of Gmail push notifications to different devices to figure out if a smartphone and a laptop/desktop have the same owner. The effectiveness of this AI algorithm is very high.

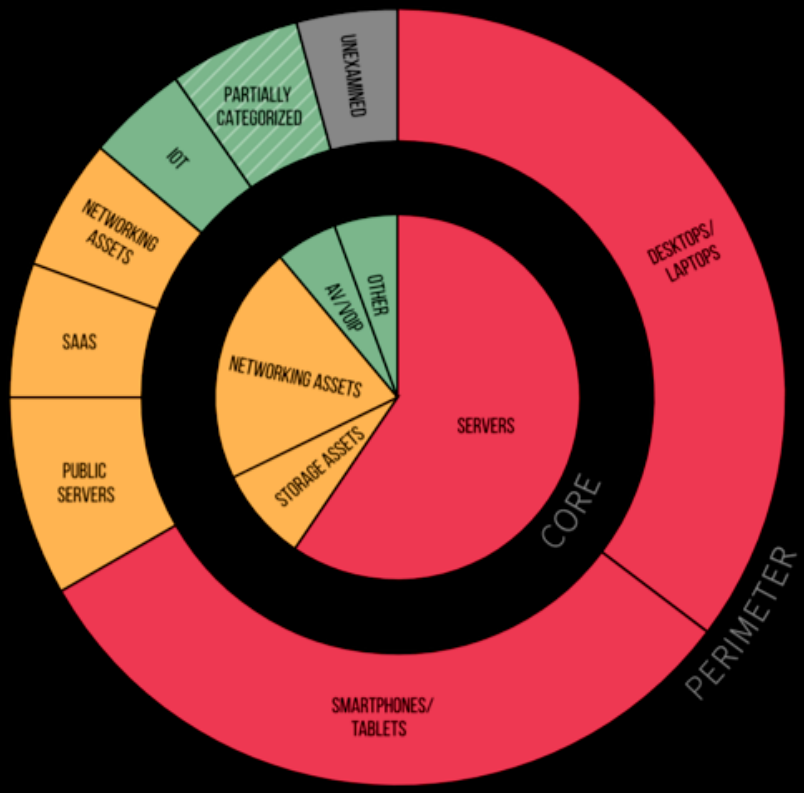
Click below to learn more

Balbix®

Use AI to automatically discover and inventory all your assets with Balbix

Balbix enables enterprises to maintain an accurate and up-to-date inventory of the organization's assets. This includes all devices, apps, and services; managed and unmanaged infrastructure; on-prem and cloud; fixed and mobile; IoT, ICS, etc., and how they are used by your users. This inventory is available via real-time dashboards and search.

Asset are also analyzed across 100+ attack vectors to identify ones that are most likely to be compromised. You can also set up automatic and continuous compliance watchdogs.



"After deploying Balbix for the first time, we discovered between 25% and 35% more assets than we thought we had."

Balbix®

Track and manage your asset inventory in real time with AI and search

Real time and continuous

Track assets in real-time through automatic discovery and continuous updates so you can stay current, with an up-to-date inventory.

Coverage and categorization

Automatic discovery, analysis and categorization of all devices, apps and services including infrastructure, on-prem and cloud, fixed and mobile, IoT, ICS, etc.

Google-like search

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

Align with your business

Customize your inventory and risk model based on your specific business needs. Define risk areas appropriate for your business using natural language search.

Balbix

Balbix BreachControl™

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.

Balbix enables a broad set of vulnerability and risk management use cases that help to transform your enterprise cybersecurity posture, reducing cyber-risk by 95% or more, while making your security team 10x more efficient.

Learn more

www.balbix.com
info@balbix.com

Click below to explore use cases

Balbix®