Whitepaper

Do You (Really) Know Your Breach Risk?

PREDICT AND PREVENT AN ATTACK BEFORE IT HAPPENS

Balbix

Do You (Really) Know Your Breach Risk?

PREDICT AND PREVENT AN ATTACK BEFORE IT HAPPENS.

Across the globe, enterprises face growing breach risk from a vast number of increasingly sophisticated adversaries. Security teams struggle to identify the weakest links and safeguard their valuable systems and data. Despite best efforts, attacks occur with alarming frequency, oftentimes resulting in significant damage.

To predict an attack, security teams need to identify their enterprise's most valuable assets and understand how they can be attacked.

Are such breaches inevitable? We don't think so.

What if you could measure the LIKELIHOOD and IMPACT of a breach for every device, user and application across your entire enterprise? How would you benefit from a self-learning system powered by artificial intelligence that would AUTOMATICALLY predict where and how a breach could occur in the enterprise—before it ever happened?

Do You Have a Risk Heat Map for Your Enterprise?

Given the ever-increasing Attack Surface, enterprises are struggling to fully identify their breach risk. Your security team would greatly benefit from an automated and continuous method of monitoring breach risk for the enterprise across all attack vectors. What you really need is a risk heat map that can show you where your areas of greatest exposure are and how to mitigate the associated risk.

Find devices and users who are vulnerable to Phishing or credential theft with a Google-like search.

How can your PCI network be breached? Find out in the Balbix Risk Dashboard.

Balbix can measure breach resilience for your entire enterprise in hours and provide actionable insights to mitigate risk.

Do you (really) know your network?

The first crucial step in calculating your breach risk heat map is to have an accurate and real time view of all devices and apps that connect to your network. Traditional device inventory systems struggle to identify the proliferation of devices such as BYOD and IoT. Your enterprise needs continuous and real time device and application discovery and classification before you can even begin analyzing your breach risk.

What assets will the attacker go after?

Not all assets are equal. Business critical assets that have sensitive apps or data significantly increase your breach risk. Security teams need an automated way to assess the “breach impact” for every device on the network. This impact can be calculated by examining each device’s type, roles, access and many other attributes.

Where will the attack originate?

Your security team needs to identify the systems that are easiest to attack and can be used as a launch point for the breach. To identify such assets, hundreds of attack vectors need to be continuously analyzed for every device, app and user across your entire network. Key risk factors include phishing, credential exposure, system vulnerabilities, privilege and access abuse, misconfiguration, and malicious behavior.

How will the attack propagate?

Do you know the likely attack propagation paths in your network that can be used for lateral movement? These paths can be calculated by examining each device’s specific connectivity and access to the enterprise's high impact assets such as sensitive networks (PCI), critical network infrastructure (AD), and data center/cloud. Since connectivity and access is constantly changing, the propagation risk calculation must be real time and continuous.

How can you mitigate risk and increase resilience?

You need to be able to not only measure risk for a device, group, site or the whole enterprise but also understand where the risk is coming from and how to mitigate it. Security teams need actionable insights that can help them prioritize their efforts and increase resilience.

Balbix Predictive Breach Risk Platform

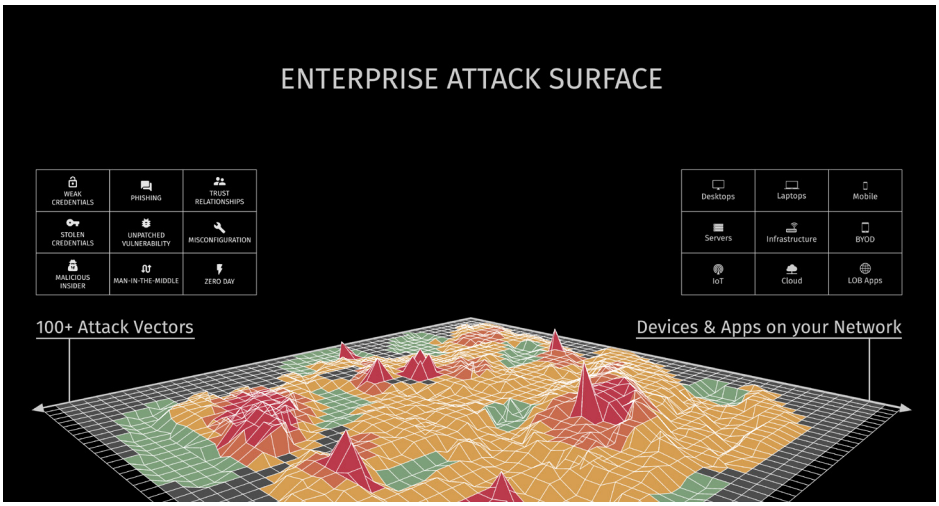
Balbix provides continuous assessment of your breach risk across all devices, apps and users. The risk heat map enables your security team to analyze breach risk at the device level, network level, or across the entire enterprise to predict breach scenarios, prioritize security operations, and mitigate risk. Balbix transforms your security practice from reactive to predictive.

Understanding Your Attack Surface

To uncover your breach risk you must discover where you are vulnerable across your Enterprise. Your Enterprise Attack Surface consists of every device and app, managed and unmanaged, located across your network, along with the various attack vectors that can be used to compromise these assets.

Simply put, your Enterprise Attack Surface can be visualized as a matrix. On the X axis exist all the devices and applications operating on your network. This includes traditional devices such as endpoints and servers, but also infrastructure, mobile, BYOD, IoT, and Cloud. The Y axis represents the hundreds of entry points, or attack vectors, that can be utilized to breach an enterprise, such as phishing, credential exposure, illegal access, data encryption, misconfiguration, and system vulnerabilities just to name a few.

Your Enterprise Attack Surface is rapidly increasing with the proliferation of attack vectors such as phishing, credential exposure and system vulnerabilities.



THE ENTERPRISE ATTACK SURFACE

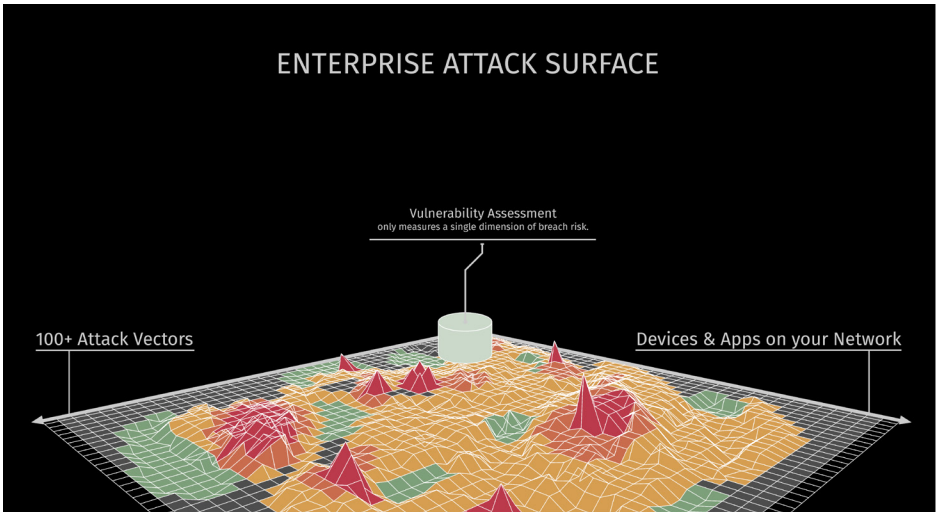
Your Enterprise's Attack Surface is hyper-dimensional and rapidly increasing

Unmanaged devices and apps, such as BYOD & IoT, pose a significant security risk.

As your enterprise devices and applications proliferate, your Enterprise Attack Surface and corresponding breach risk increases exponentially. Every day, an increasing number of unmanaged devices and apps are connecting to your network. In addition, the attack vectors that can lead to a breach continue to grow at a rapid pace. As a result, your Enterprise Attack Surface is now hyper-dimensional and increasingly difficult for your security team to analyze.

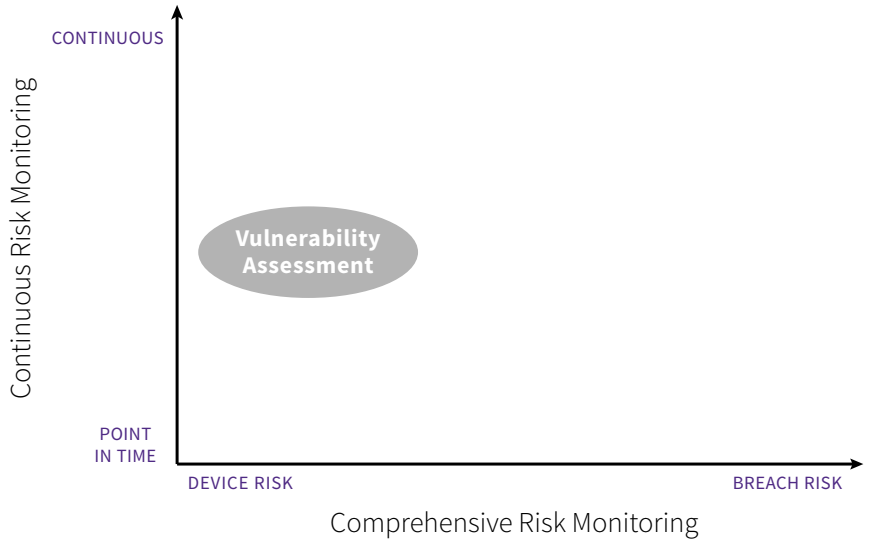
Vulnerability Assessment is Not Enough

Vulnerability Assessment only measures a single dimension of breach risk. Hundreds of risk factors need to be evaluated to calculate the likelihood of a security breach for each device, app or user.



VULNERABILITY ASSESSMENT MEASURES ONLY A SMALL AREA OF THE ATTACK SURFACE

Traditionally, enterprises have relied on legacy approaches such as Vulnerability Assessment to measure and reduce their risk of experiencing a breach. While vulnerabilities do represent a serious risk factor, they represent only one category of hundreds of known breach risk vectors. Other factors, such as web browsing behavior, phishing, credential exposure, and access to sensitive networks and data can all provide insight into identifying your breach risk. With the proliferation of unmanaged devices, such as BYOD and IoT, pinpointing risk is an even bigger challenge as Vulnerability Assessment is typically only effective for managed devices. Furthermore, Vulnerability Assessment is constrained to the device level and therefore cannot fully measure the risk of propagation and exfiltration.



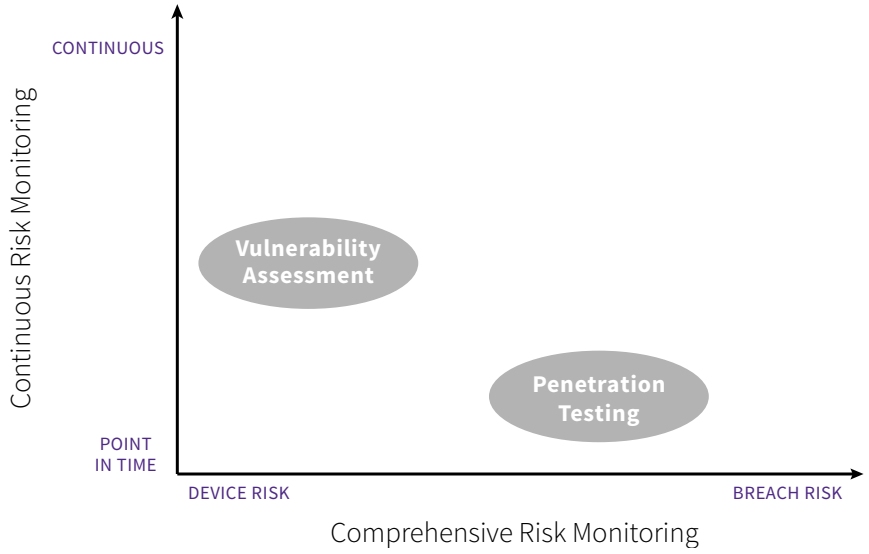
VULNERABILITY ASSESSMENT DOESN'T MEASURE RISK OF PROPAGATION AND BREACH

Penetration Testing = Not Continuous + Falls Short

While penetration testing (pen testing) is a useful tool for assessing your security controls, it is ineffective in adequately mapping the rapidly changing and expanding Enterprise Attack Surface. Most enterprises perform a pen-test once a quarter or on another specific schedule. Because breach risk is constantly adapting and evolving, a much more effective solution is to continuously monitor and evaluate your Enterprise Attack Surface. Additionally, pen-testing usually focuses only on a segment of the overall infrastructure and does not provide comprehensive coverage of the entire enterprise across all attack vectors.

Quarterly pen-testing cannot keep up with your rapidly evolving Enterprise Attack Surface.

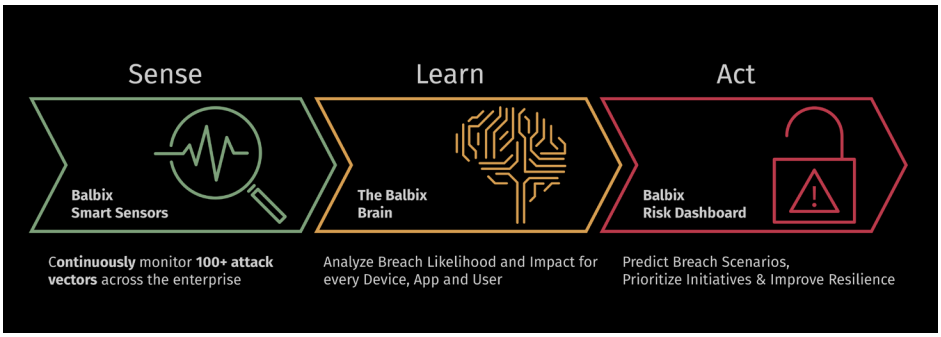
Pen-testing focuses only on a small section of the entire infrastructure and cannot provide coverage across all attack vectors.



PEN TESTING DOESN'T PROVIDE CONTINUOUS BREACH RISK MEASUREMENT

Your Solution: The Balbix Predictive Breach Risk Platform

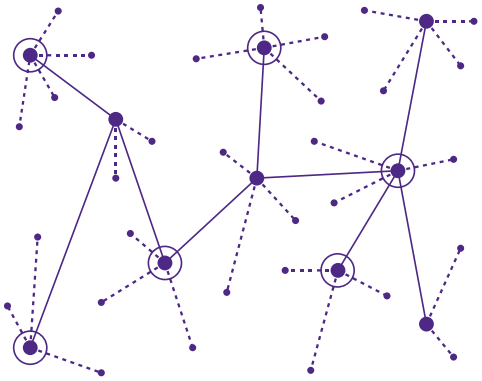
Balbix's Predictive Breach Risk Platform provides your enterprise comprehensive, continuous and automated risk calculation and analysis. Sensors deployed across your entire enterprise network automatically and continuously discover and monitor all devices, apps and users for hundreds of attack vectors. Our robust Balbix "Brain" runs in the cloud and leverages advanced artificial intelligence and self-learning to calculate risk for every network entity. The Balbix Risk Dashboard provides your security team actionable insights on breach scenarios and optimizing security.



Balbix Smart Sensors

These sensors conduct automated and ongoing discovery and monitoring of all devices and apps connected to your network across hundreds of attack vectors. Sensors are deployed as physical appliances or software agents and are installed within minutes. Installing multiple sensors can provide complete risk coverage for your entire enterprise. There are three types of Balbix sensors:

Discover managed and unmanaged assets connected to your network in real time.



The Balbix Traffic Sensor examines network traffic in real time to identify risks across hundreds of attack vectors.

1 NETWORK SENSOR

This sensor discovers enterprise assets and services and identifies risks related to open network services and ports. For example, one of your high value servers may be running a vulnerable service, making it an easy target for malicious actors to exploit. The Balbix Network Sensors perform a smart scan of your entire network.

2 TRAFFIC SENSOR

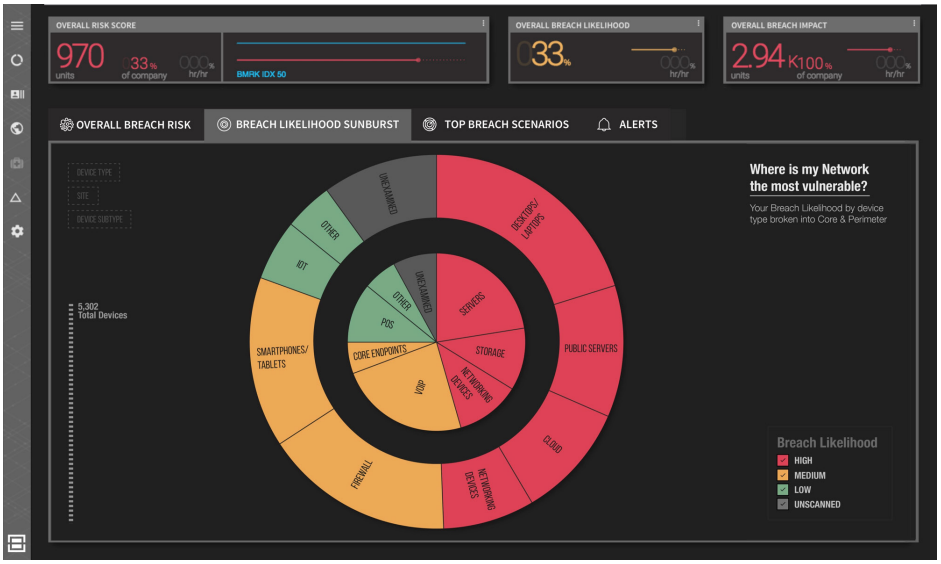
This sensor monitors your network traffic in real time to identify breach risks such as browsing to unsafe websites, vulnerability to phishing and man-in-the-middle attacks, and access to sensitive networks and services. The Traffic Sensor connects to the SPAN port on the network switch, thereby providing comprehensive network visibility without any disruption to the production environment.

3 HOST SENSOR

The Host Sensor gathers real time detailed device and app information such as configuration, policies and software versions. Information is gathered using standard APIs such as WMI, integrations with third party systems, and by optionally installing a light weight agent on the hosts.

Balbix Smart Sensors = Real Time and Comprehensive Discovery

Balbix Smart Sensors automatically discover all devices and apps on your network and measure risk across hundreds of attack vectors. Since the sensors examine all network traffic, devices are discovered in real time without needing to wait for polling intervals. The data collected by the sensors is automatically scrubbed for sensitive information and sent to the Balbix Brain which then applies AI and self-learning to perform automatic and smart categorization of devices and apps in the enterprise.



BALBIX SMART SENSORS AUTOMATICALLY DISCOVER AND CATEGORIZE DEVICES, INCLUDING IOT AND BYOD

Balbix Breach Method Matrix (BMM)

Balbix Smart Sensors monitor every device and app across hundreds of attack vectors such as phishing, credential exposure, privileges, misconfiguration and system vulnerabilities. The risk data is summarized into a 3X3 matrix referred to as the Breach Method Matrix (BMM). BMM is similar to the FICO risk score and is continuously calculated for every enterprise asset, group and the whole enterprise. The key risk categories represented in the BMM are:

BMM is like the FICO score for breach risk and is calculated for each device, group, site and the whole enterprise.

▪ Weak Credentials

Weak passwords and password reuse make credential exposure a gateway for initial attacker access and propagation. Recent malware attacks such as Mirai highlight this threat not only for managed devices but also IoT connected devices. Tracking password hygiene and use across your entire enterprise is key to identifying high risk users and their devices.

▪ Phishing

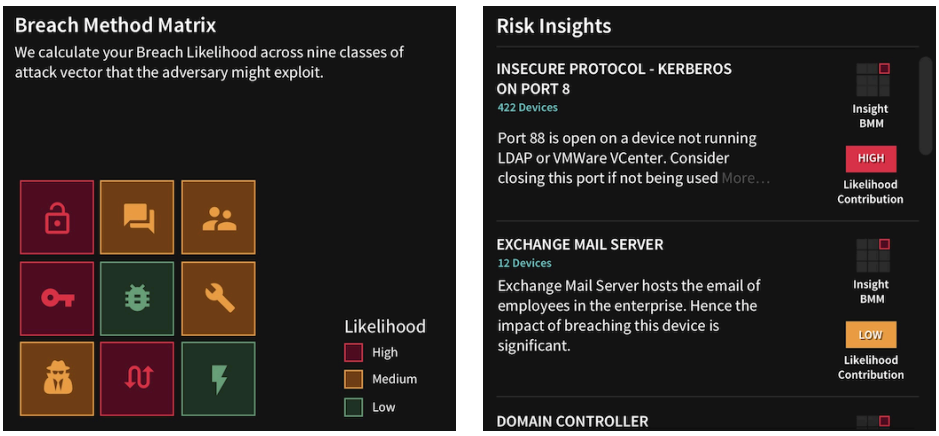
Phishing continues to be one of the most effective social engineering attack vectors. The recent OPM hack demonstrates how phishing can defeat almost all layers of traditional security such as email gateways and endpoint controls. Measuring web browsing and email click through behavior for users and devices provides valuable risk insight for your enterprise.

▪ Trust Relationships

The ultimate goal of adversaries and malicious insiders is to access your high value devices, apps and data. Therefore, devices and users with access to sensitive apps, data and networks pose a significant risk to your enterprise. Discovering trust relationships can identify the impact or damage an attacker can inflict.

▪ Stolen Credentials

Apps and protocols sending login credentials over your network pose a significant security threat. An attacker connected to your network can easily locate and utilize these credentials for lateral movement. For example, in the Target attack, adversaries were able to steal Active Directory credentials and propagate their attack into the enterprise payment network.



THE BREACH METHOD MATRIX DEFINES THE MOST RELEVANT CATEGORIES OF RISK

BMM provides a risk snapshot of every device, group, site, or your entire enterprise.

▪ Unpatched Vulnerability

Unpatched vulnerabilities are easily exploited by malware to infect your endpoint or server. Although vulnerability management products provide a list of devices that need to be patched, the real challenge is to identify high risk devices that can be readily used/hijacked to launch attacks. Vulnerabilities in critical infrastructure or devices with access to sensitive data present a significant risk to your enterprise.

▪ Misconfiguration

Misconfigured devices and apps present an easy entry point for an attacker to exploit. Monitoring application and device settings and comparing these to recommended best practices reveals the threat for misconfigured devices located across your network.

▪ Malicious Insider

Users with access to sensitive data and networks can inflict extensive damage through privilege misuse and malicious intent. Monitoring data and network access for every device and user can expose insider risk. Case in point: Wikileaks attributes the recent Vault 7 leak of sensitive information to a malicious insider.

▪ Man-In-The-Middle

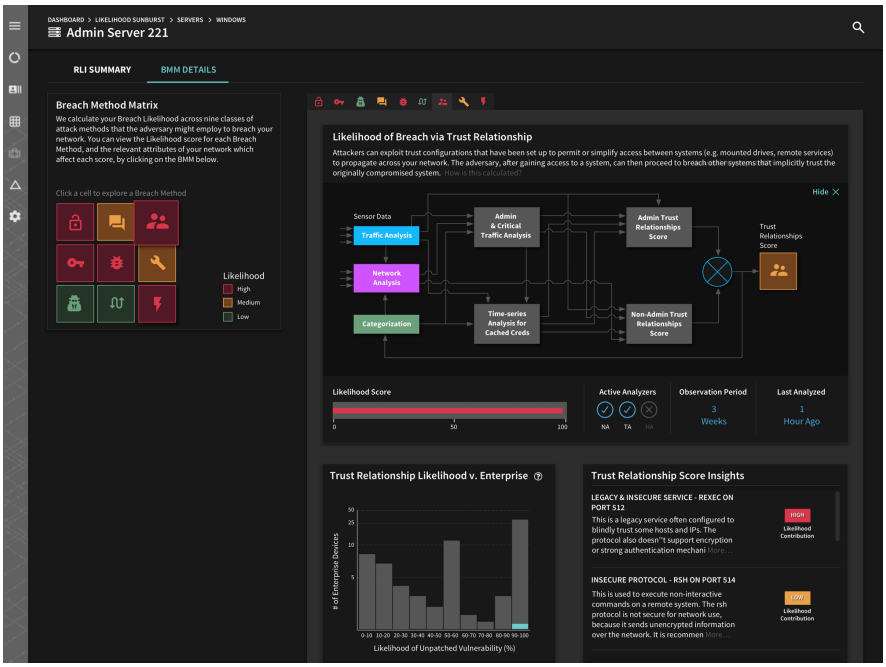
Unencrypted or weakly encrypted network connections and protocols leave your enterprise susceptible to man-in-the-middle attacks. Additionally, devices and users that connect to insecure networks and apps are at risk and can be likewise compromised.

▪ Zero Day

High risk software components such as Java, Flash and IE are prone to zero day attacks due to a large number of inherent vulnerabilities—many of which are not publicly disclosed. Devices containing such high risk software that are actively exposed to the Web are especially prone to attack.

Actionable Enterprise-Wide Risk Measurement

Balbix computes the BMM for every device, group of devices, and across your entire enterprise. By calculating the risk measurement bottom-up, Balbix can accurately measure your enterprise risk and also highlight where the risk originates by revealing the underlying devices and the specific attack vectors contributing to the risk. For each BMM risk category, Balbix also provides actionable mitigation insights to reduce risk and increase resiliency.



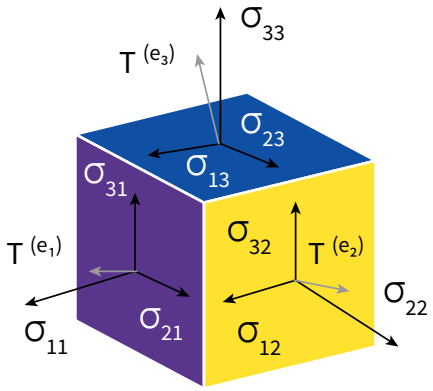
The Balbix "Brain": How it Works

With the Balbix Brain, assessing your breach risk has never been easier, or more accurate. Balbix Smart Sensors provide a constant data stream to the Balbix Brain, which leverages advanced machine self-learning and AI, to automatically and continuously calculate your risk and resilience. Here's how it is done:

Hyper-Dimensional Risk Tensor

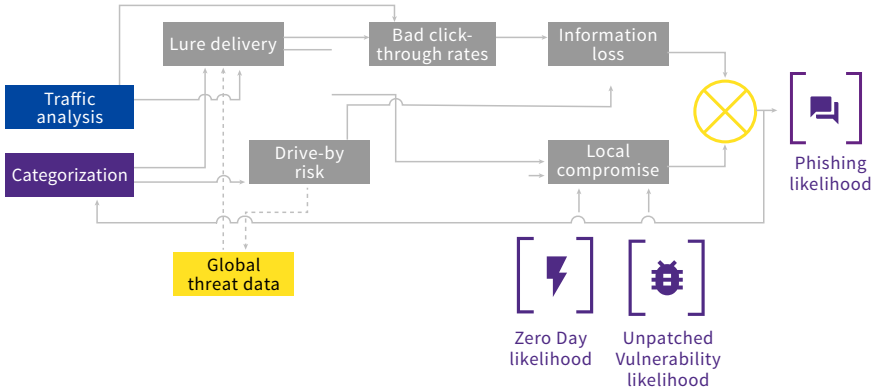
Using collected data, Balbix Brain calculates a hyper-dimensional risk tensor for every discovered device, app and user. This tensor contains hundreds of dimensions, each corresponding to a specific attack vector such as phishing. The risk tensor represents the overall aggregate attack vector measurements from all sensor data.

The Balbix brain applies advanced artificial intelligence and self-learning algorithms to calculate risk across the hyper-dimensional attack surface.



Neural Networks

The Balbix Brain utilizes advanced neural networks to calculate the breach risk. Each risk tensor is continuously evaluated by hundreds of neural networks to predict risk.



Likelihood of Breach

Your first step in risk calculation is to assess the likelihood of breach for every device, app and user connected to your network. This is calculated by analyzing the risk tensor using AI risk models for each attack vector and aggregating the likelihood score. For example, a laptop with a history of risky web browsing behavior may be more likely to be compromised. Similarly, an IoT device using weak encryption in network communication may be susceptible to a man-in-the-middle attack.

Impact of Breach

After calculating breach likelihood, the next step is to assess the breach impact for every device, app and user located within your network. This impact is determined by examining each asset's type, roles, access and many other attributes. Your breach impact is significantly higher for core devices located on sensitive networks or your critical network infrastructure.

The Balbix Brain simulates all possible breach scenarios to identify real risks. Unlike manual pen-testing, our continuous and automated analysis calculates breach risk across your entire enterprise.

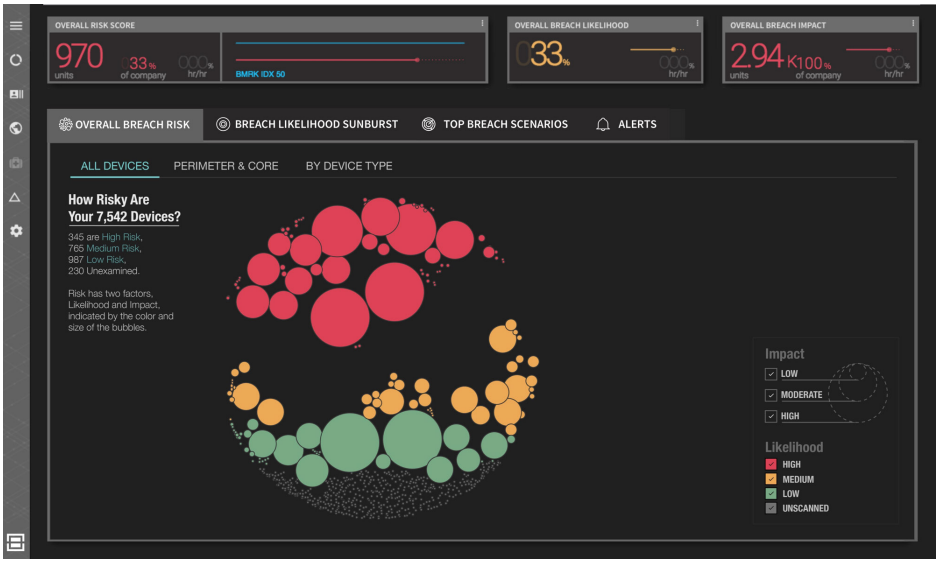
Continuous Breach Simulation

Having calculated breach likelihood and impact for every asset on the network, the Balbix Brain performs millions of breach simulations throughout your entire enterprise network. Every possible breach path is simulated to calculate the risk of an adversary propagating to access high impact assets within your enterprise. Unlike pen-tests that only focus on a specific area of your network and are run point-in-time, our breach simulation is set to run continuously, network-wide.

Balbix Risk Dashboard

The Balbix Risk Dashboard provides an interactive, real time heat map of your enterprise's breach risk. The dashboard enables your security team to predict breach scenarios, mitigate risk by implementing actionable insights, and accurately assess your enterprise-wide breach risk. Here's how:

The Balbix Risk Dashboard provides a clickable risk heat map for your entire enterprise.

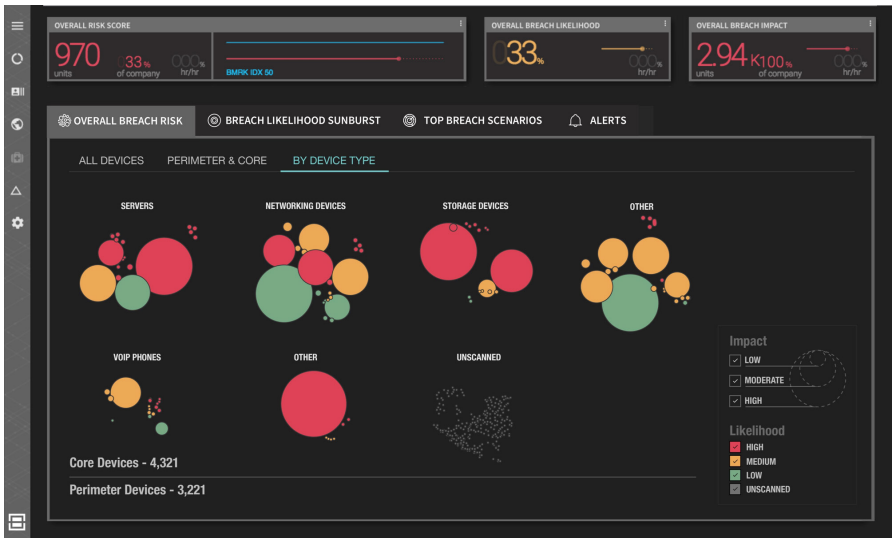


THE BALBIX RISK DASHBOARD IDENTIFIES THE MOST CRITICAL SECURITY THREATS THAT CAN LEAD TO A BREACH

1 COMPREHENSIVE & CONTINUOUS RISK VISIBILITY

The Balbix Risk Dashboard provides a continuous and comprehensive security profile for your entire enterprise—all valuable input for executive or board-level discussions, as well as integral data for your governance, risk and compliance processes.

Find where you are most likely to be breached across all devices, apps and users.



BALBIX MONITORS ALL DEVICES, APPS AND USERS CONTINUOUSLY

2 PREDICT BREACH SCENARIOS

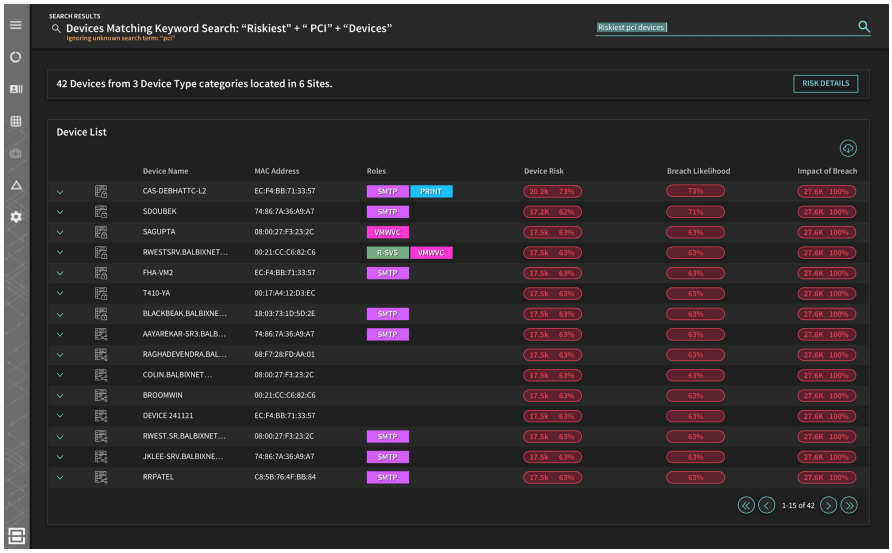
By simulating all possible breach paths, the Balbix Risk Dashboard identifies your enterprise's likeliest breach risk scenarios by highlighting the initial attack point and subsequent lateral movement within the network to reach sensitive networks and data. With the Balbix Risk Dashboard, your security team can now easily evaluate where a specific breach risk could originate in terms of specific devices or networks.

BALBIX ANALYZES RISK OF LATERAL MOVEMENT TO HIGH IMPACT ASSETS

3 PRIORITIZE INITIATIVES & MITIGATE RISK

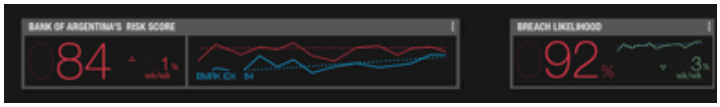
The Balbix Risk Dashboard provides clear and actionable insights to prioritize your security team's initiatives and mitigate your breach risk. Your security team not only sees what actions are necessary to improve security, but also understands why.

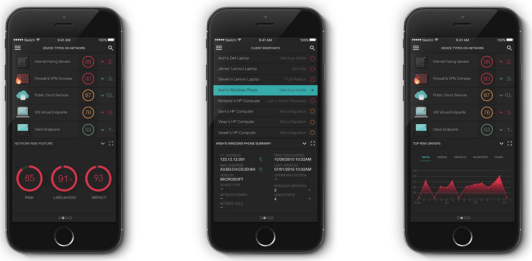
The Balbix Risk Dashboard provides proactive security insights that can predict and prevent security breaches.



THE BALBIX RISK DASHBOARD GIVES SECURITY TEAMS INSIGHT NEEDED TO PRIORITIZE ACTION

The Balbix Risk Dashboard provides accurate breach risk visibility to your management, board and auditors to enable security planning.



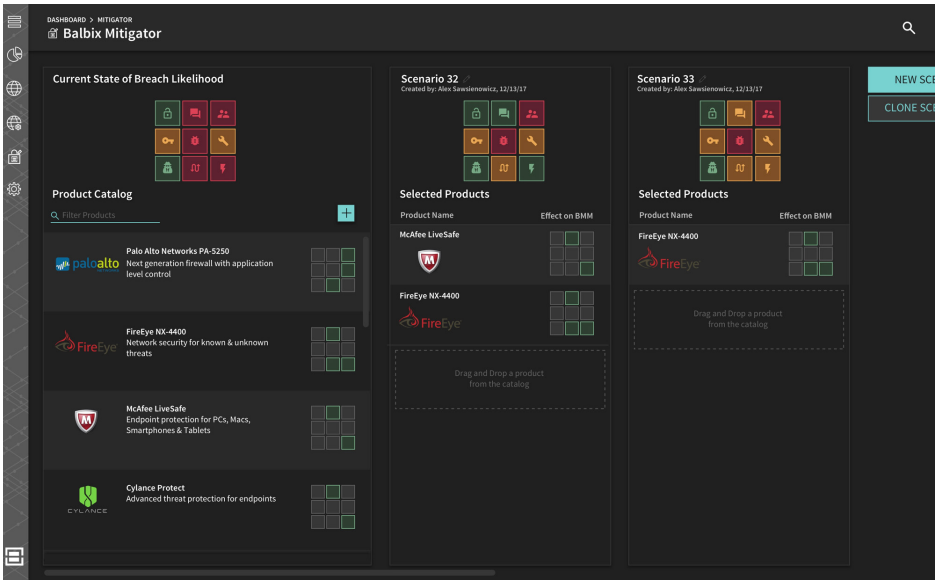


The Balbix Risk Dashboard provides accurate breach risk visibility to your management, board and auditors to enable security planning.

Natural language search allows you to query for devices and assets that are most vulnerable to a specific attack.

4 SECURITY EFFECTIVENESS & RESILIENCE

Security teams find themselves in a constant struggle to stay on top of a deluge of security controls deployed within their enterprise. Yet, despite product proliferation, security teams are often left in the dark over which security controls are actually working. The Balbix Risk Dashboard enables your security leadership to clearly identify those security controls that are meaningfully reducing risk, and locate any gaps.



THE BALBIX RISK DASHBOARD ALLOWS YOU MEASURE AND OPTIMIZE SECURITY INITIATIVES

In Conclusion: Balbix Increases Resilience and Reduces Risk

Rather than spending millions on reactive and largely ineffective shot-in-the-dark efforts at plugging security holes, your enterprise can take a much more predictive approach. Balbix's comprehensive and automated risk assessment tool not only identifies security breach and attack risks in real time, but also provides solutions to prevent a breach from occurring in the first place.

With Balbix, your enterprise's security team has the on-demand risk assessment information they need to prioritize their efforts and initiatives. Your management team and board also gain invaluable insight of your enterprise's risk profile to better plan future investments and projects to both increase resilience and reduce overall operating costs.

Reduce your risk and gain resilience with Balbix.
Contact us for a free demo today.

Balbix

Balbix
3031 Tisch Way, Suite 800
San Jose, CA 95128
info@balbix.com
866 936 3180

www.balbix.com