WHITE PAPER

Balbix BreachControl™

PREDICT AND PREVENT AN ATTACK BEFORE IT HAPPENS

Balbix

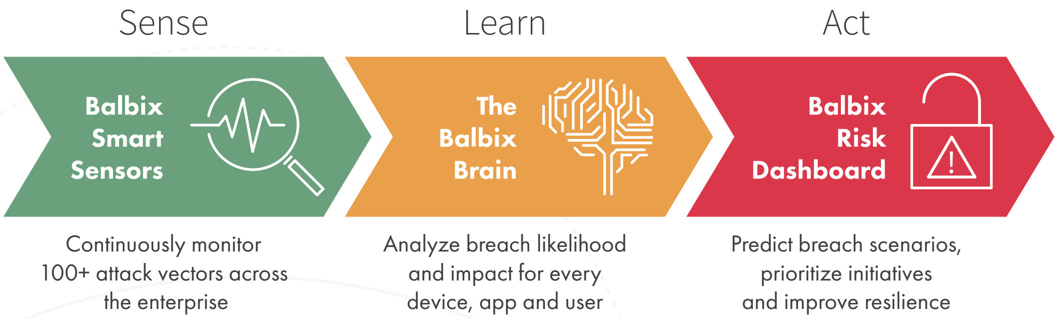
Balbix BreachControl™

PREDICT AND PREVENT AN ATTACK BEFORE IT HAPPENS

The industry's first Breach Avoidance platform

Balbix's Breach Avoidance 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. The robust Balbix "Brain" runs in the cloud and leverages advanced artificial intelligence and self-learning algorithms to calculate risk for every network entity. The Balbix Risk Dashboard provides your security team actionable insights on breach scenarios and optimizing security.

How it works



Sense

Balbix Smart Sensors

Continuously monitor 100+ attack vectors across the enterprise

Learn

The Balbix Brain

Analyze breach likelihood and impact for every device, app and user

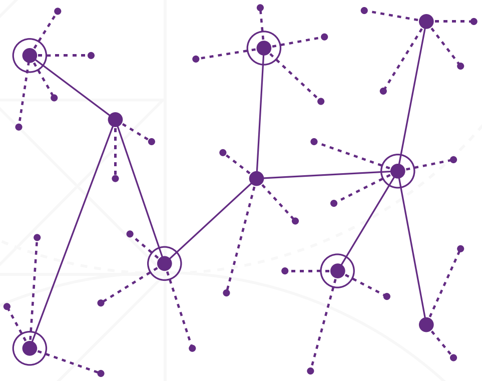
Act

Balbix Risk Dashboard

Predict breach scenarios, prioritize initiatives and improve resilience

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.

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.

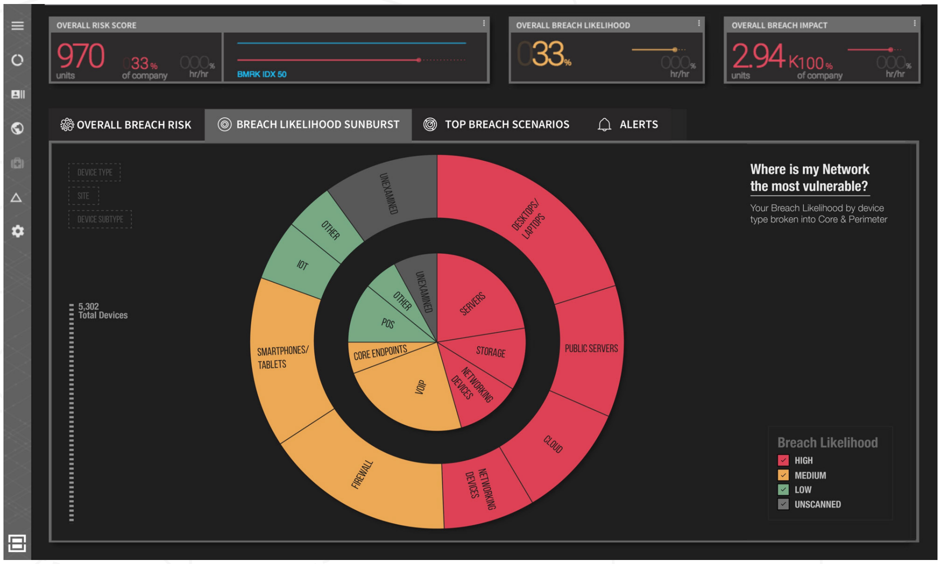
2 **TRAFFIC SENSOR:** This sensor monitors your network traffic in real time to identify breach risks such as browsing to unsafe websites, vulnerability to phishing and man-in-the-middle attacks, and access to sensitive networks and services. The Traffic Sensor connects to the SPAN port on the network 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.

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

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.



Where is my Network the most vulnerable?

Your Breach Likelihood by device type broken into Core & Perimeter

Balbix smart sensors automatically discover and categorize devices, including IOT and BYOD

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:

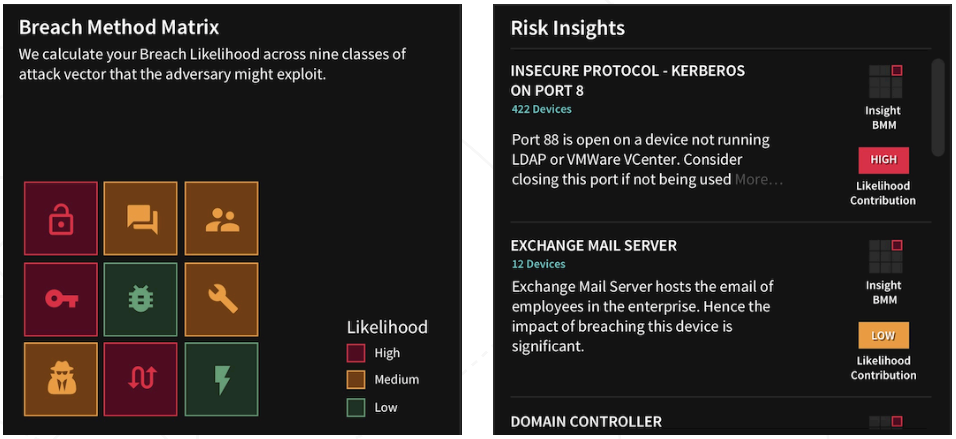
> BMM is like the FICO score for breach risk and is calculated for each device, group, site and the whole enterprise.

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.



Breach Method Matrix

We calculate your Breach Likelihood across nine classes of attack vector that the adversary might exploit.

Risk Insights

INSECURE PROTOCOL - KERBEROS ON PORT 8

422 Devices

Port 88 is open on a device not running LDAP or VMWare VCenter. Consider closing this port if not being used More…

EXCHANGE MAIL SERVER

12 Devices

Exchange Mail Server hosts the email of employees in the enterprise. Hence the impact of breaching this device is significant.

DOMAIN CONTROLLER

The breach method matrix defines the most relevant categories of risk

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.

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

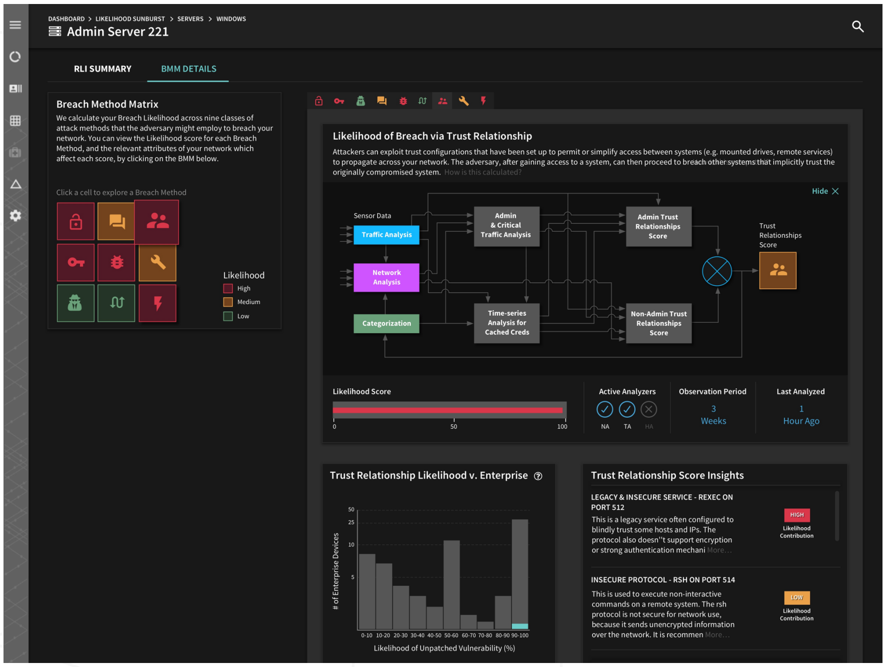
MALICIOUS INSIDER: Users with access to sensitive data and networks can inflict extensive damage through privilege misuse and malicious intent. Monitoring data and network access for every device and user can expose insider risk. Case in point: Wikileaks attributes the recent Vault 7 leak of sensitive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



Breach Method Matrix

We calculate your Breach Likelihood across nine classes of attack methods that the adversary might employ to breach your network. You can view the Likelihood score for each Breach Method, and the relevant attributes of your network which affect each score, by clicking on the BMM below.

Likelihood of Breach via Trust Relationship

Attackers can exploit trust configurations that have been set up to permit or simplify access between systems (e.g. mounted drives, remote services) to propagate across your network. The adversary, after gaining access to a system, can then proceed to breach other systems that implicitly trust the originally compromised system. How is this calculated?

Trust Relationship Likelihood v. Enterprise

Trust Relationship Score Insights

LEGACY & INSECURE SERVICE - REXEC ON PORT 512

This is a legacy service often configured to blindly trust some hosts and IPs. The protocol also doesn''t support encryption or strong authentication mechani More...

INSECURE PROTOCOL - RSH ON PORT 514

This is used to execute non-interactive commands on a remote system. The rsh protocol is not secure for network use, because it sends unencrypted information over the network. It is recommen More...

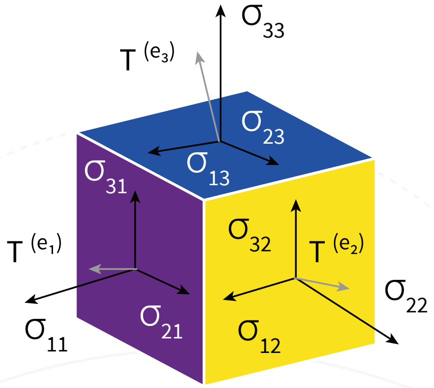
Detailed risk and likelihood information is available for each breach method

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 selflearning and AI, to automatically and continuously calculate your risk and resilience. Here’s how it is done:

Hyper-dimensional risk tensor

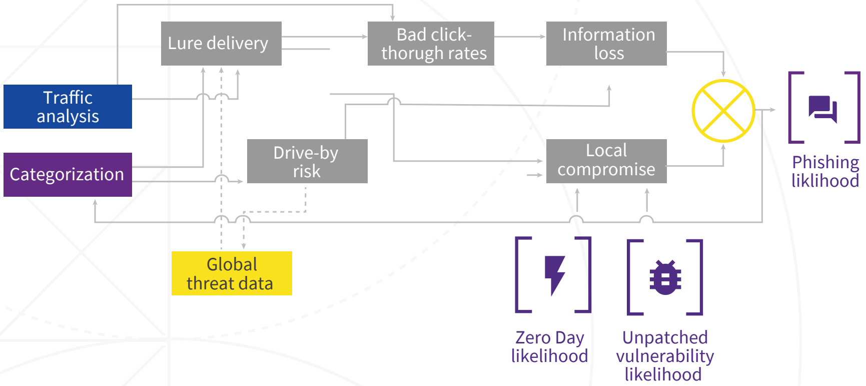
Using collected data, Balbix Brain calculates a hyper-dimensional risk tensor for every discovered device, app and user. This tensor contains hundreds of dimensions, each corresponding to a specific attack vector such as phishing. The risk tensor represents the overall aggregate attack vector measurements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



Breach risk simulation

> 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.

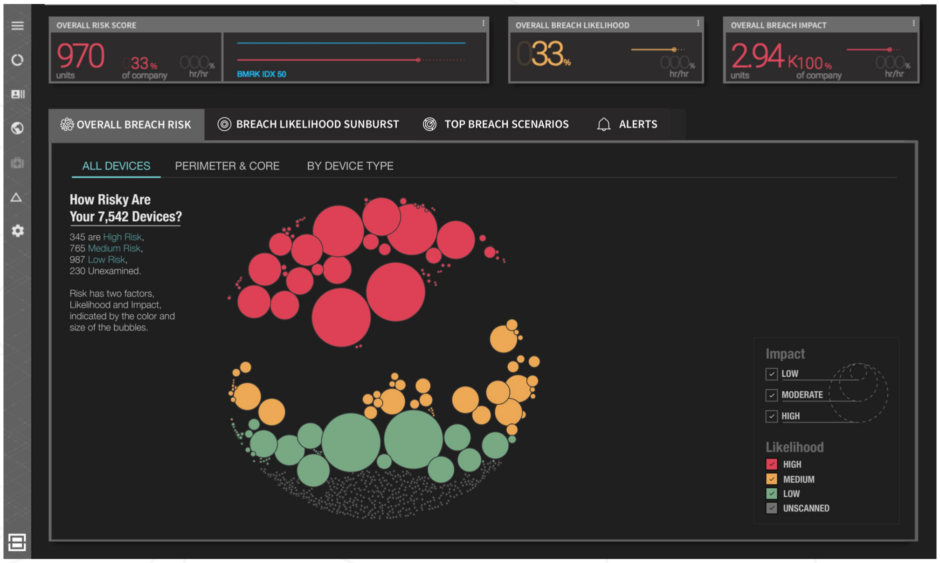
LIKELIHOOD OF BREACH: Your first step in risk calculation is to assess the likelihood of breach for every device, app and user connected to your network. This is calculated by analyzing the risk tensor using AI risk models for each attack vector and aggregating the likelihood score. For example, a laptop 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.

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:



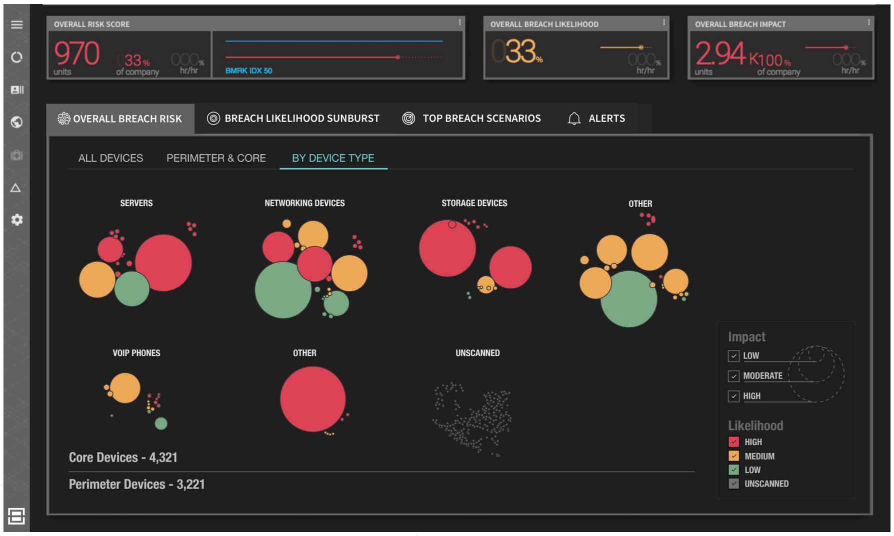
How Risky Are Your 7,542 Devices?

345 are High Risk,
765 Medium Risk,
987 Low Risk,
230 Unexamined.

Risk has two factors, Likelihood and Impact, indicated by the color and size of the bubbles.

The Balbix risk dashboard identifies the most critical security threats that can lead to a breach and provides a clickable risk heat map for your entire enterprise

1 **COMPREHENSIVE AND 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.

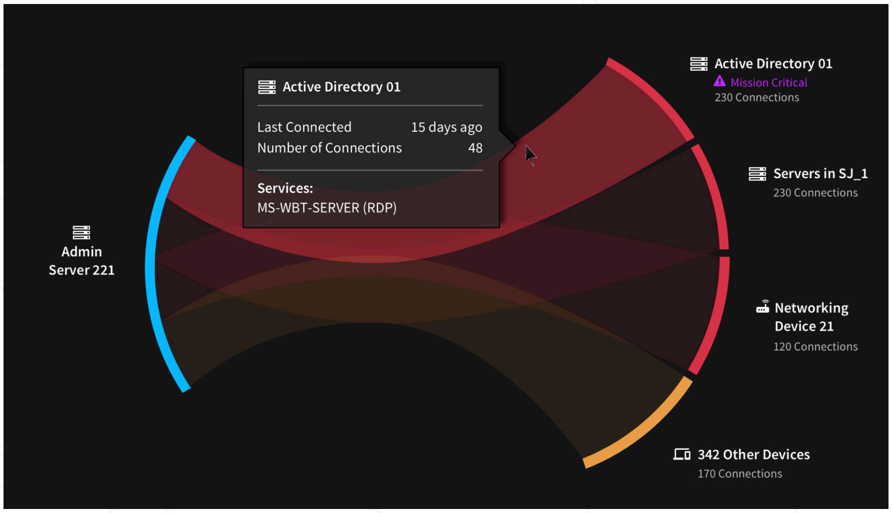


Core Devices - 4,321

Perimeter Devices - 3,221

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

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.



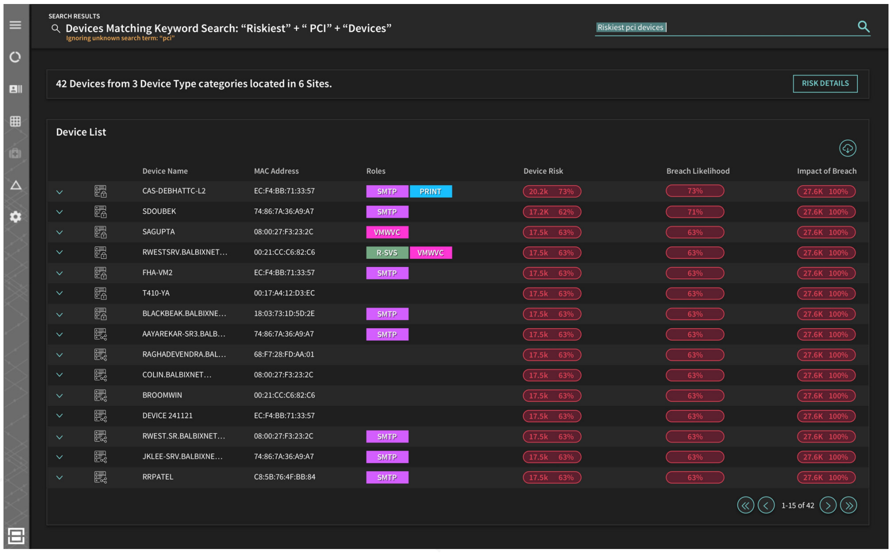
Active Directory 01

Last Connected 15 days ago
Number of Connections 48

Services:
MS-WBT-SERVER (RDP)

Balbix analyzes risk of lateral movement to high impact assets

3 **PRIORITIZE INITIATIVES AND 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.



SEARCH RESULTS

Devices Matching Keyword Search: "Riskiest" + " PCI" + "Devices"

Ignoring unknown search term: "pci"

Riskiest pci devices

42 Devices from 3 Device Type categories located in 6 Sites.

Device List

Device Name	MAC Address	Roles	Device Risk	Breach Likelihood	Impact of Breach
CAS-DEBHATTC-L2	EC:F4:BB:71:33:57	SMTP PRINT	20.2k 73%	73%	27.6K 100%
SDOUBEK	74:86:7A:36:A9:A7	SMTP	17.2K 62%	71%	27.6K 100%
SAGUPTA	08:00:27:F3:23:2C	VMWVC	17.5k 63%	63%	27.6K 100%
RWESTSRV.BALBIXNET…	00:21:CC:C6:82:C6	R-SVS VMWVC	17.5k 63%	63%	27.6K 100%
FHA-VM2	EC:F4:BB:71:33:57	SMTP	17.5k 63%	63%	27.6K 100%
T410-YA	00:17:A4:12:D3:EC		17.5k 63%	63%	27.6K 100%
BLACKBEAK.BALBIXNE…	18:03:73:1D:5D:2E	SMTP	17.5k 63%	63%	27.6K 100%
AAYAREKAR-SR3.BALB…	74:86:7A:36:A9:A7	SMTP	17.5k 63%	63%	27.6K 100%
RAGHADEVENDRA.BAL…	68:F7:28:FD:AA:01		17.5k 63%	63%	27.6K 100%
COLIN.BALBIXNET…	08:00:27:F3:23:2C		17.5k 63%	63%	27.6K 100%
BROOMWIN	00:21:CC:C6:82:C6		17.5k 63%	63%	27.6K 100%
DEVICE 241121	EC:F4:BB:71:33:57		17.5k 63%	63%	27.6K 100%
RWEST.SR.BALBIXNET…	08:00:27:F3:23:2C	SMTP	17.5k 63%	63%	27.6K 100%
JKLEE-SRV.BALBIXNE…	74:86:7A:36:A9:A7	SMTP	17.5k 63%	63%	27.6K 100%
RRPATEL	C8:5B:76:4F:BB:84	SMTP	17.5k 63%	63%	27.6K 100%

1-15 of 42

The Balbix risk dashboard gives security teams insight needed to prioritize action

Balbix breach risk dashboard provides:

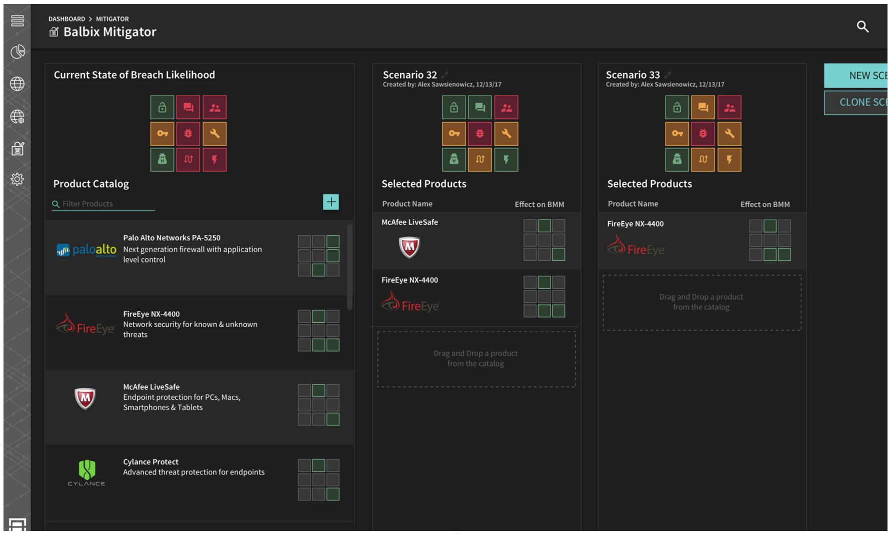
Information on where you are most likely to be breached across all devices, apps, and users

Proactive **security insights** that can predict and prevent security breaches

Accurate **breach risk visibility** to your management, board, and auditors

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

4 **SECURITY EFFECTIVENESS AND 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.



DASHBOARD > MITIGATOR
Balbix Mitigator

Current State of Breach Likelihood

Product Catalog

Filter Products

Palo Alto Networks PA-5250
Next generation firewall with application level control

FireEye NX-4400
Network security for known & unknown threats

McAfee LiveSafe
Endpoint protection for PCs, Macs, Smartphones & Tablets

Cylance Protect
Advanced threat protection for endpoints

Scenario 32
Created by: Alex Sawsienowicz, 12/13/17

Selected Products

Product Name	Effect on BMM
McAfee LiveSafe	
FireEye NX-4400	

Drag and Drop a product from the catalog

Scenario 33
Created by: Alex Sawsienowicz, 12/13/17

Selected Products

Product Name	Effect on BMM
FireEye NX-4400	

Drag and Drop a product from the catalog

The Balbix risk dashboard allows you measure and optimize security initiatives

Increase resilience and reduce 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.

Balbix

3031 Tisch Way, St 800
San Jose, CA 95128
866.936.3180

info@balbix.com
www.balbix.com