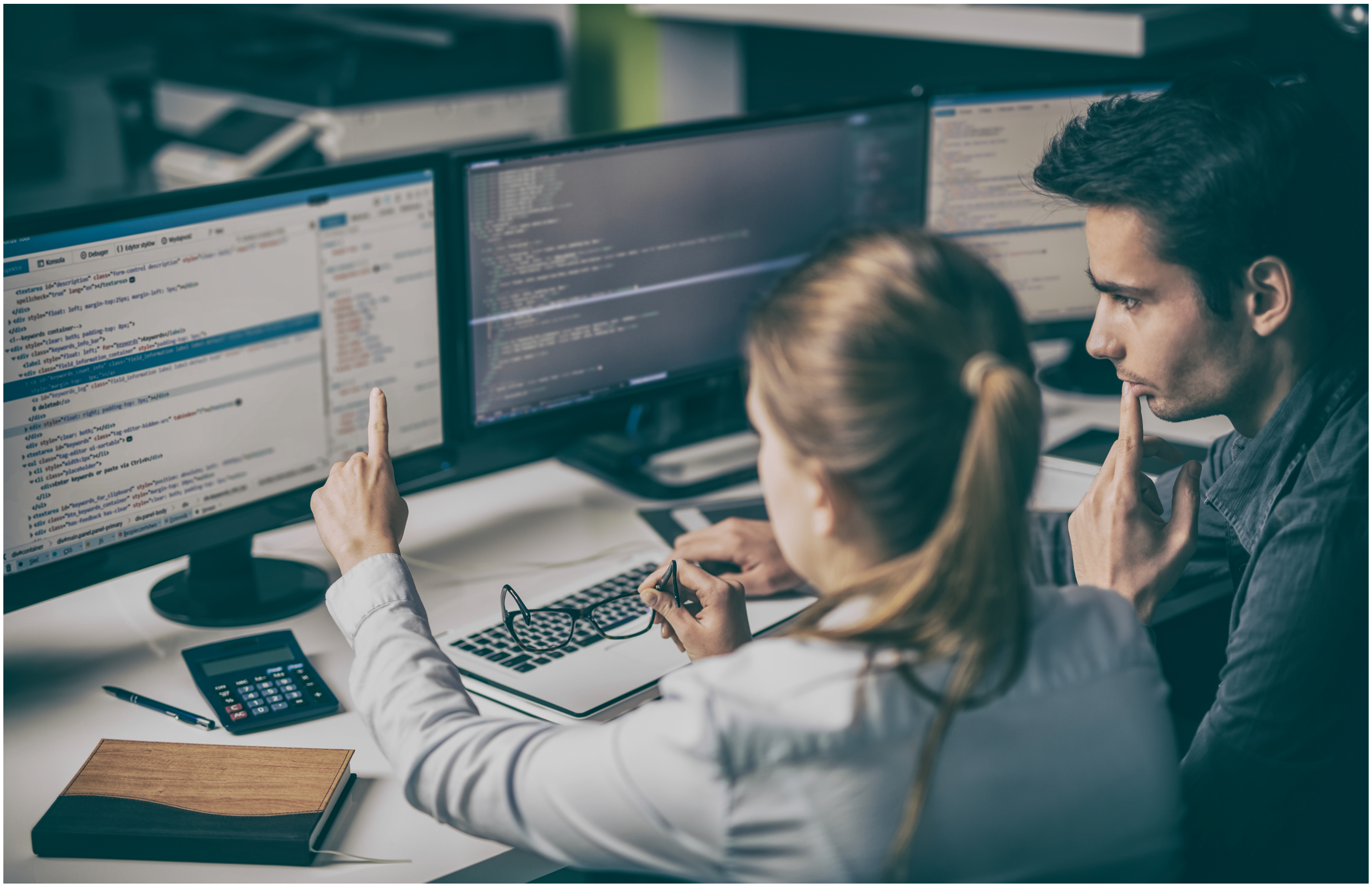


SOLUTION BRIEF

Risk-Based Vulnerability Management

Balbix®

Risk-Based Vulnerability Management

Overview

Your vulnerability management program is supposed to be the cornerstone of your cybersecurity initiatives– how you stay ahead of the adversary. However, traditional vulnerability management has a number of big problems.

Legacy vulnerability tools ***spew out alerts*** in the (tens of) thousands every time a scan completes, leaving your team overwhelmed and struggling with how to proceed. It is hard to tell which of your vulnerabilities are critical, which can wait a day, vs ones that are just noise. You cannot afford to dedicate resources remediating vulnerabilities that pose little or no threat, while ignoring the most critical vulnerabilities which put your organization at real risk of breach.

Another big issue is ***coverage***. Traditional approaches to vulnerability assessment understand and monitor less than 5% of the enterprise attack surface, primarily CVEs (unpatched software vulnerabilities) and some simple security configuration issues mostly across traditional assets.

There are 100+ other ways in which your network can be breached — starting from simple things like weak passwords, default passwords, password reuse, passwords stored incorrectly on disk, or transmitted in the clear on the network. Traditional vulnerability tools will not tell you which of your users are particularly prone to being phished, or which users with privileged access to your enterprise systems have poor cybersecurity hygiene.

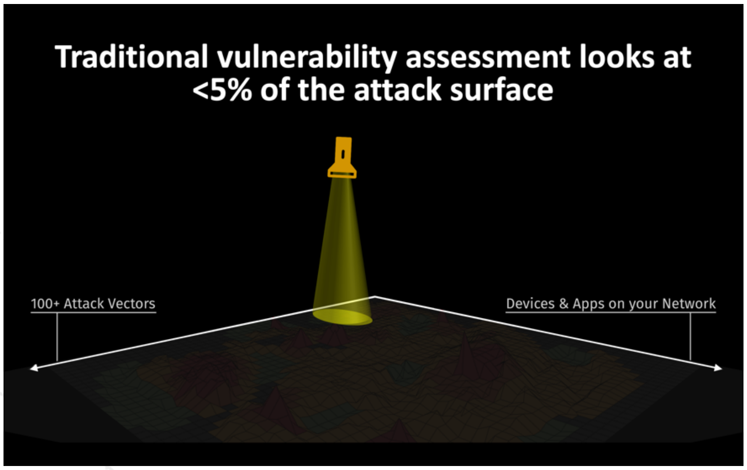

Traditional vulnerability assessment looks at <5% of the attack surface
100+ Attack Vectors
Devices & Apps on your Network

Figure 1: Poor coverage of legacy vulnerability management

In terms of asset coverage, very few organizations have an accurate real-time view of exactly what assets are present in the enterprise. Non-traditional assets such as bring-your-own devices, IOTs, industrial equipment and cloud-services are particularly hard to enumerate and then analyze for risk.

Legacy vulnerability tools do not account for which CVEs are really exploitable, and we know that at any given time less than 20% of CVEs are actually usable by attackers. These vulnerability systems also do not understand the different levels of business criticality of your assets. Nor do these tools account for the degree of exposure of different assets (based on how they are used), or the mitigating impact of your security controls. Much of the work created by legacy tools is simply noise and wasteful.

Consequently, legacy vulnerability management is quite off the mark in proactively managing your organization's cybersecurity posture and breach risk. In a recent survey conducted by the Ponemon institute, only 15% of security teams felt that their patching efforts were highly effective and 67% said that they do not have the time and resources to mitigate all vulnerabilities in order to avoid a data breach.

Risk-based vulnerability management

In order to truly enhance security posture and improve resilience, you need a risk-based approach to vulnerability management that identifies vulnerabilities due to 100+ attack vectors (not just CVEs) across all your assets, and also prioritizes them based on actual risk by understanding the context around each vulnerability and the enterprise asset that it affects.

Armed with this information, your security team will be better equipped to tackle your vulnerabilities in the most efficient manner and increase the effectiveness your cyber-risk management efforts.

Only 15% of security teams say that their patching efforts are highly effective.

Ponemon Report 2019 – The Challenging State of Vulnerability Management Today

Balbix overview

Balbix replaces legacy vulnerability tools and multiple point products to continuously assess your enterprise's cybersecurity posture and prioritize open vulnerabilities based on business risk.

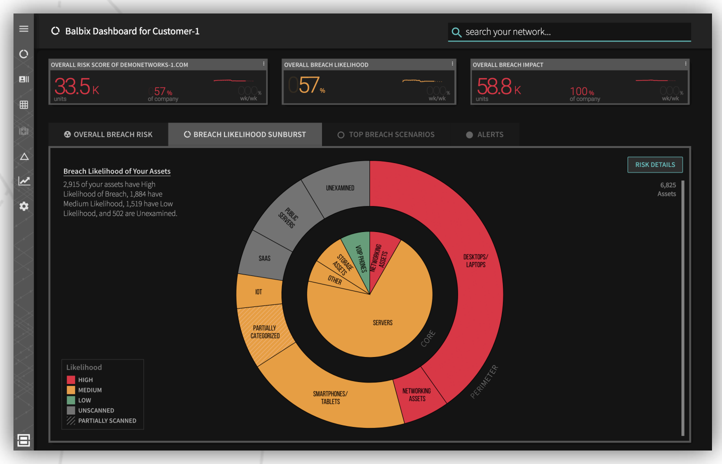
With Balbix you can continuously observe and analyze your enterprise's extended network, *inside-out* and *outside-in,* to discover and identify weaknesses in your defenses. Our system combines information about *open vulnerabilities*, *active threats, real exposure, business criticality* and *your compensating security controls* across all your asset types and 100+ attack vectors to prioritize security issues based on risk.

Balbix helps you align your patching and risk mitigation activities with business risk

Automatic inventory

The first step towards risk-based vulnerability management is actually knowing "what" to scan – i.e. starting with an accurate inventory of all the enterprise assets. Traditional vulnerability management tools can only discover corporate owned and managed assets and lack visibility into non-traditional assets such as bring-your-own devices, IoTs, mobile assets and cloud services.

With Balbix you do not need to specify what to scan as Balbix automatically (and continuously) discovers and categorizes your assets, i.e., any devices, applications and users present on your extended network, and analyzes them for vulnerabilities. Balbix also estimates business criticality for each asset based on analysis of usage and network traffic.



Balbix Dashboard for Customer-1

search your network...

OVERALL RISK SCORE OF DEMONETWORKS-1.COM: 33.5 K units; 57 % of company; 0.00 % wk/wk

OVERALL BREACH LIKELIHOOD: 57 %; 0.00 % wk/wk

OVERALL BREACH IMPACT: 58.8 K units; 100 % of company; 0.00 % wk/wk

Breach Likelihood of Your Assets

2,915 of your assets have High Likelihood of Breach, 1,884 have Medium Likelihood, 1,519 have Low Likelihood, and 502 are Unexamined.

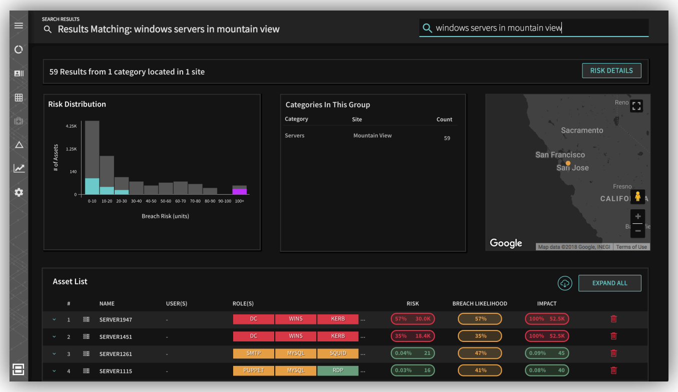
6,825 Assets

Figure 2: Automatic inventory

Real-time and continuous, with natural-language search

Legacy vulnerability tools are cumbersome to operate, and are typically configured to perform periodic (often monthly) scans. As a result, the enterprise's understanding of risk from vulnerabilities is typically several weeks out-of-date. You might recall the superhuman efforts required the last time you had an emergency patch situation, or when the CFO inquired about the risk from *Wannacry*.

Balbix is real-time and operates continuously and automatically. The risk model surfaced by Balbix is usually seconds or less behind the actual on-network conditions.



SEARCH RESULTS

Results Matching: windows servers in mountain view

windows servers in mountain view

59 Results from 1 category located in 1 site

RISK DETAILS

Risk Distribution

Categories In This Group

Category	Site	Count
Servers	Mountain View	59

Asset List

EXPAND ALL

#	NAME	USER(S)	ROLE(S)	RISK	BREACH LIKELIHOOD	IMPACT
1	SERVER1947	-	DC WINS KERB ...	57% 30.0K	57%	100% 52.5K
2	SERVER1451	-	DC WINS KERB ...	35% 18.4K	35%	100% 52.5K
3	SERVER1261	-	SMTP MYSQL SQUID ...	0.04% 21	47%	0.09% 45
4	SERVER1115	-	PUPPET MYSQL RDP ...	0.03% 16	41%	0.08% 40

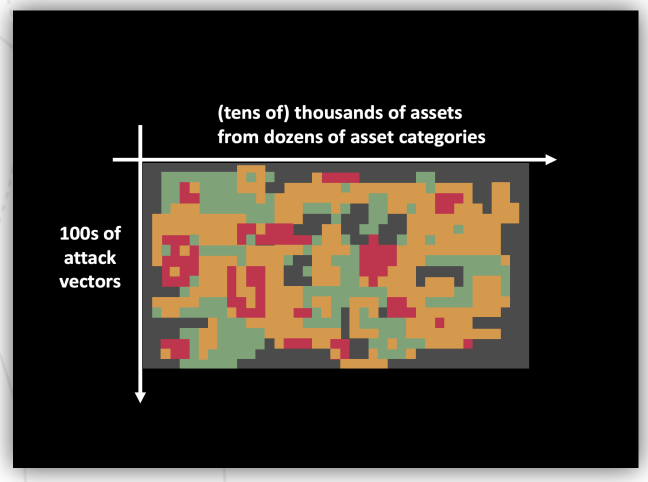
Figure 3: Natural language search to find answers quickly

With Balbix, you can answer questions about your asset inventory, your cybersecurity posture and breach risk using like natural language search. For example, you can query your inventory using IT vocabulary, e.g., *windows servers in mountain view*, and *network admins.* In your search queries*,* you can combine technical terms from security and IT, e.g., *unpatched switches in London, expired certificates, password reuse, phishing,* etc.*,* enter a CVE number *CVE-2017-0144,* or its common name *Wannacry* (if one exists). Balbix also supports higher level queries such as: *where will attacks start*, *what will they go after*, *what assets have intellectual property*, and *cyber-risk to customer data*. Our objective is to give you a Google-like, highly contextual search experience for your cybersecurity and IT data and insights.

Comprehensive visibility across all asset types and attack vectors

As all cyber-defenders know, any enterprise network is only as secure as it's weakest link. An effective vulnerability management program must cover all types of assets and all sorts of security issues beyond unpatched software.

Unlike legacy vulnerability assessment products, Balbix provides comprehensive vulnerability assessment across all asset types: managed and unmanaged, IoTs, infrastructure, on-premises and in the cloud, fixed and mobile. Balbix also analyzes each asset against 100+ attack vectors. For us the word "vulnerability" means something closer to the English definition of "vulnerability", and not just a CVE, and includes issues like password reuse, phishable users, and encryption issues.



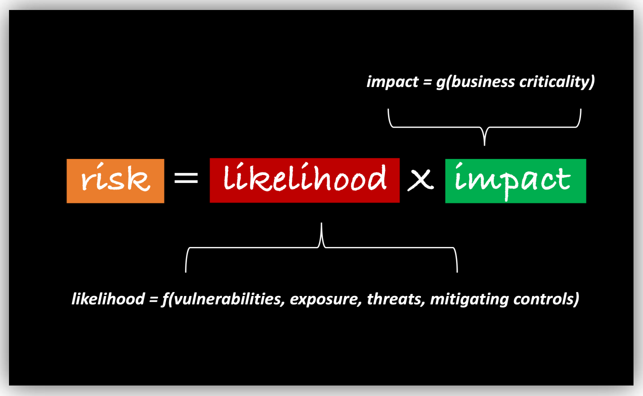
(tens of) thousands of assets
from dozens of asset categories
100s of
attack
vectors

Figure 4: Comprehensive vulnerability assessment

Five-pronged risk calculation

Legacy vulnerability and patching tools use primitive risk metrics to prioritize vulnerabilities. Their calculation is typically based on CVE score and a simple business impact model (high, medium, low), and leads to priority inversion and wasted effort.

Balbix's risk-based prioritization of vulnerabilities considers in 5 factors — vulnerability severity, threat level, business criticality, exposure/usage and the risk-negating effect of compensating controls. This results in very accurate prioritization and helps you avoid needless busy work fixing low priority issues.



impact = g(business criticality)

risk = likelihood × impact

likelihood = f(vulnerabilities, exposure, threats, mitigating controls)

Figure 5: Five-pronged risk calculation

Customizable notion of risk

Organizations have different top risk concerns based on the nature of their business. Legacy vulnerability management treats all security issues the same way.

Balbix lets you to define risk areas appropriate for your business using natural language search, and then maps your vulnerabilities to these areas. For example, one such risk area can be "intellectual property", and Balbix will let you analyze, prioritize and remediate vulnerable assets that contain intellectual property. In a specific quarter, for example, you may choose to focus on reducing risk to one of these areas, and show real progress.

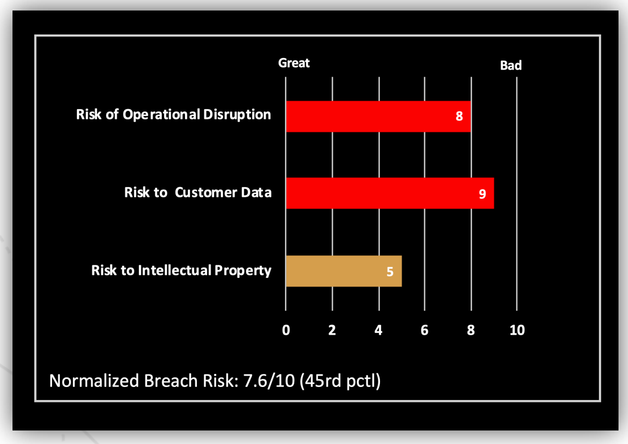
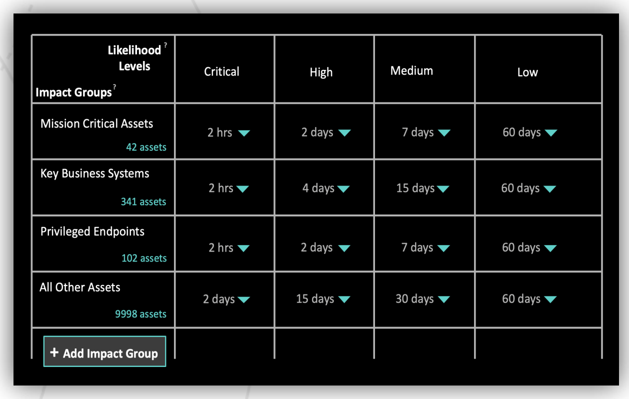


Figure 6: Cyber-risk metrics aligned to business concerns

Implement MTTP SLAs

Patching systems periodically is a big portion of enterprise vulnerability management. With legacy tools, most organization have a normal patching cadence and a separate process for dealing with emergency patching. This leads to many important enterprise assets being unpatched for weeks on end.

With Balbix, you can set up target mean-time-to-patch SLAs for vulnerabilities of different likelihood values for asset groups of different business impact levels. These SLAs can be used to create tickets and drive patching workflows in a prioritized fashion to minimize cyber-risk exposure due to unpatched systems.



Likelihood ? Levels Impact Groups ?	Critical	High	Medium	Low
Mission Critical Assets 42 assets	2 hrs ▾	2 days ▾	7 days ▾	60 days ▾
Key Business Systems 341 assets	2 hrs ▾	4 days ▾	15 days ▾	60 days ▾
Privileged Endpoints 102 assets	2 hrs ▾	2 days ▾	7 days ▾	60 days ▾
All Other Assets 9998 assets	2 days ▾	15 days ▾	30 days ▾	60 days ▾
+ Add Impact Group				

Figure 7: Target SLAs for mean-time-to-patch

End-to-end identification, prioritization and resolution of vulnerabilities

Ultimately, Balbix allows you set up your business risk areas and manage how vulnerabilities in these areas are automatically mapped to their asset-group owners with risk-based priority. Based on desired SLAs, tickets are automatically created, assigned to the relevant owners and tracked. Ticket owners are offered alternatives between fixing the vulnerability (e.g., by patching) or implementing some compensating control. Balbix continuously monitors the network for fixes and mitigating controls.

Balbix also enables the comparative benchmarking and reporting of different groups' vulnerability management practices.

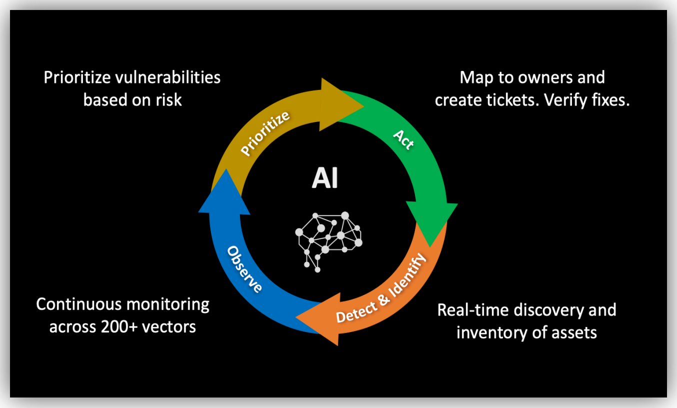

Prioritize vulnerabilities based on risk
Map to owners and create tickets. Verify fixes.
Prioritize
Act
AI
Observe
Detect & Identify
Continuous monitoring across 200+ vectors
Real-time discovery and inventory of assets

Figure 8: End-to-end vulnerability management

Balbix's unique risk-based vulnerability management

Real-time and continuous

Comprehensive across asset types and 100+ attack vectors

SLA based end-to-end vulnerability management

Natural language search

Prioritization based on vulnerabilities, exposure, threats, business criticality and compensating controls

Customizable to align with your business

Automatic inventory and business criticality

Replaces and consolidates existing tools

Deep learning and other advanced AI algorithms

Pilot deployment in less than 1 hour

Know which of your vulnerabilities are critical, those which can wait a day, vs. ones that are just noise…

3031 Tisch Way, Ste 800
San Jose, CA 95128
866.936.3180
info@balbix.com
www.balbix.com

Scan me