Doing More With Less in Cybersecurity

8 Key Areas to Increase Efficiency

Balbix®

In an effort to build and support a comprehensive and mature cybersecurity program, organizations have, through no fault of their own, unintentionally assembled dozens of point solutions over the last decade and beyond. While intentions were sound, logic was lost.

During this same stretch of time, astounding technological advancements have led to improved operational efficiencies, competitive differentiation, and convenience for both customers and employees alike. However, the speed of this innovation forced security minded executives to bless a 'check box' mentality for their security toolset, resulting in excessive expenses and clutter.

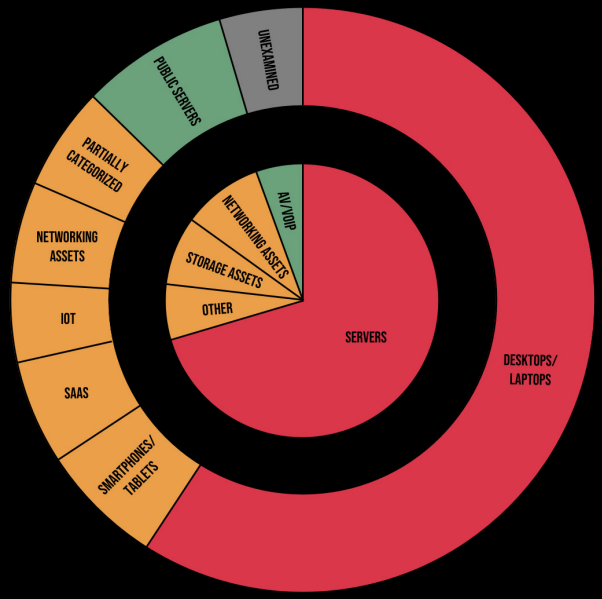
Yet even with such a heavy arsenal at their fingertips, security teams continue to struggle. Answering simple business questions posed by leadership continues to be met with overwhelmingly complex data and directionally ambiguous dialogue. If we stop, zoom out, and think pragmatically about what a security team is intended to do, the answer is fairly simple—enable business while reducing risk by understanding exposure. This should not require 50+ vendor subscriptions.

Security leaders who are being asked to closely evaluate their spending without sacrificing risk levels should start by organizing their breach prevention arsenal into categories. Once identifying these categories and aligning them with larger business goals, look for solutions rather than 'tools' that can accomplish objectives in multiple areas, simplify your workflows, and allow you to cut unnecessary costs.

Let's take a look at 8 key areas of cybersecurity programs where there are opportunities to be more economical and efficient while remaining vigilant and maintaining a strong security posture.

1. Asset Inventory
2. Vulnerability Assessment
3. Threat & Vulnerability Management
4. Network Detection & Response
5. Threat Intelligence
6. Security Information & Event Management
7. Governance, Risk, & Compliance
8. Ticketing (Security Orchestration)

Asset Inventory



Maintaining an up-to-date enterprise inventory system is very challenging. The CIS Top 20 security controls dictate continuous inventory of both hardware and software assets as the top 2 items to address. Many organizations over-rely on their Configuration Management Database (CMDB) for these metrics and yet openly admit inaccuracy due to the manual efforts required and ephemeral nature of the enterprise. 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.

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.

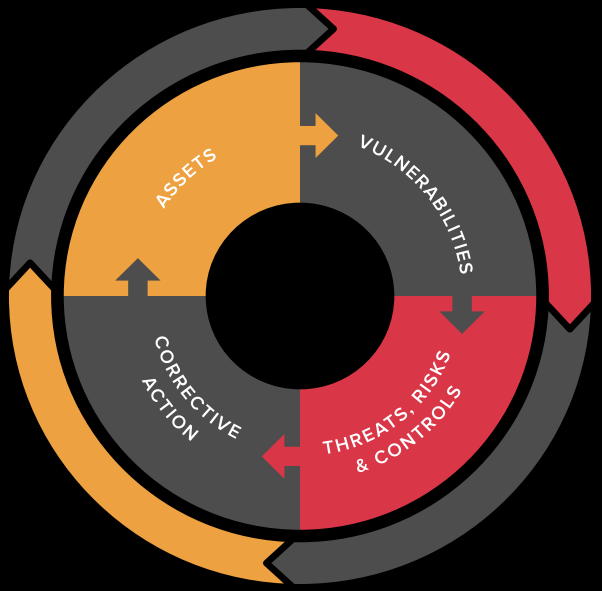
Vulnerability Assessment

- CVE-2018-8174-
- CVE-2018-4878-
- CVE-2017-11882-
- CVE-2017-8750-
- CVE-2017-0199-
- CVE-2016-0189-
- CVE-2017-8570-
- CVE-2018-8373-
- CVE-2012-0158-
- CVE-2015-1805-

Traditional vulnerability assessment tools are often blindly accepted as a cornerstone of any mature security program. While managing unpatched software is certainly a top-tier proactive measure, the collection and analysis of massive outputs require highly qualified security talent to engage in administrative tasks before any action can be taken. By the time the security team digests half of the report, the next scan has been completed and a new pile of vulnerabilities need to be addressed. Furthermore, traditional scanning solutions are unable to discern levels of mission criticality between assets which is necessary for prioritization beyond severity and exploitability.

Balbix analyzes your entire asset inventory continuously, in real-time and provides an active list of vulnerabilities, including and beyond CVE data taking into account issues like password reuse, misconfigurations, and unencrypted communications. Specialized AI categorizes and prioritizes security issues based on risk severity, taking into account breach likelihood and impact for each asset.

Threat & Vulnerability Management



Without vulnerability prioritization capabilities, it is difficult to know where to even begin. Prioritization allows you to base your patching activities on business risk and align your team's efforts with overall business objectives. Asset data, enterprise data, and global threat intelligence should all be factored into prioritization algorithms to paint a complete picture for the context of every risk item and asset owners being tasked with corrective action. Proper prioritization often requires yet another solution beyond your scanning tool, resulting in an additional yearly expense and cumbersome workload for the team toggling between tools.

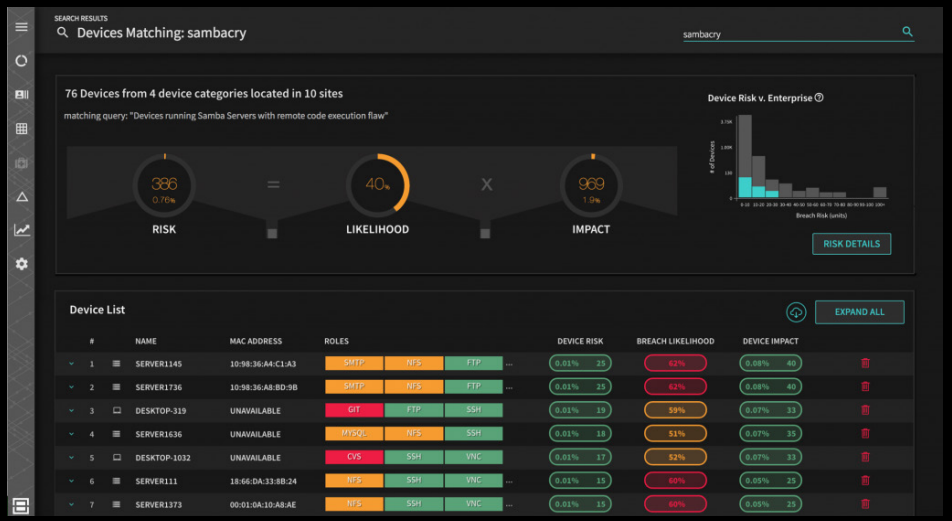
Balbix's specialized algorithms analyze vulnerabilities based on severity, threat level, business criticality, exposure/usage, and compensating controls to prioritize security issues based on risk. Unlike legacy vulnerability assessment products, Balbix provides comprehensive vulnerability assessment across all asset types and 100+ attack vectors. Every risk insight is delivered with impact context and prescriptive fixes.

Network Detection & Response

Continuous monitoring of your network and a response plan are must-haves in today's evolving threat environment. Reactive measures, unfortunately, have become a necessity based on the sheer volume of potential entry points. However, defaulting and over-reliance on reactive technology is a flawed approach. Independent research tells us undetected attacks have a dwell time of roughly 200 days. Therefore, alerting is clearly not functioning in a manner that aligns with human capabilities—there's just too much to consider. Instead, by shifting the focus toward rock solid cyber hygiene and surfacing weaknesses across all assets, applications, and users prior to an event, these reactive measures become far more efficient and less resource intensive.

Balbix provides continuous visibility into all servers, workstations, laptops, mobile devices, and IOTs by monitoring real-time network traffic and gathering information from our host analyzers. Security issues being detected in real-time are delivered to the dashboard in a prioritized list based on risk level. Prescriptive fixes are detailed for every risk insight to ensure efficient remediation. Actionable risk insights are prioritized for every issue uncovered to ensure efficient remediation.

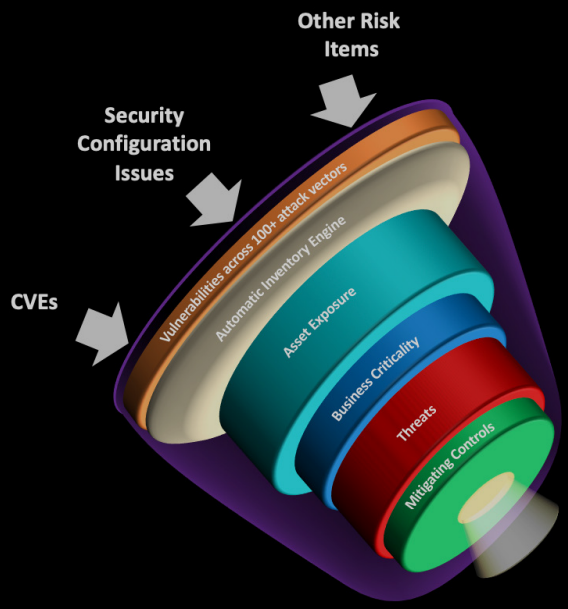
Threat Intelligence



In an effort for software companies to give customers maximum transparency, vulnerabilities are published by the thousands in the form of Common Vulnerabilities and Exposures (CVE). As the threat landscape continues to evolve exponentially, teams are looking for sources of truth, many times residing in the darkest corners of the web, to understand the subset of vulnerabilities that are being actively exploited by attackers. This allows organizations to prioritize exploitable vulnerabilities from theoretical vulnerabilities to maximize risk mitigation. Because there are potentially thousands of sources of threat intelligence, it's simply not a human scale problem to rank and prioritize the best sources of truth that help uncover the most critical exploitable vulnerabilities.

Balbix automates the ingestion of thousands of threat intelligence sources, comparing them to newly published CVEs and the assets within your organization to highlight the most relevant and critical risk insights for an organization. Identify which assets are affected by specific threats using risk heat maps and google-like natural language search. Simply enter a query like "sambacry new york assets" and get risk insights for every asset (both managed and unmanaged) vulnerable to sambacry in New York. Balbix allows you to set up dynamic groups for risk areas of interest and monitor them continuously or assign them to other team members.

Security Information & Event Management



Similar to NDR discussed earlier, security information and event management has become a focal point for acting on security intel and making sense of overwhelming swaths of vulnerability data. SIEM tools typically pull data from other mitigating controls, network devices, servers, and domain controllers and aim to surface meaningful anomalies for necessary action. For that reason, it is not uncommon for a SIEM in a medium-size enterprise to produce 1,000s of security alerts each day.

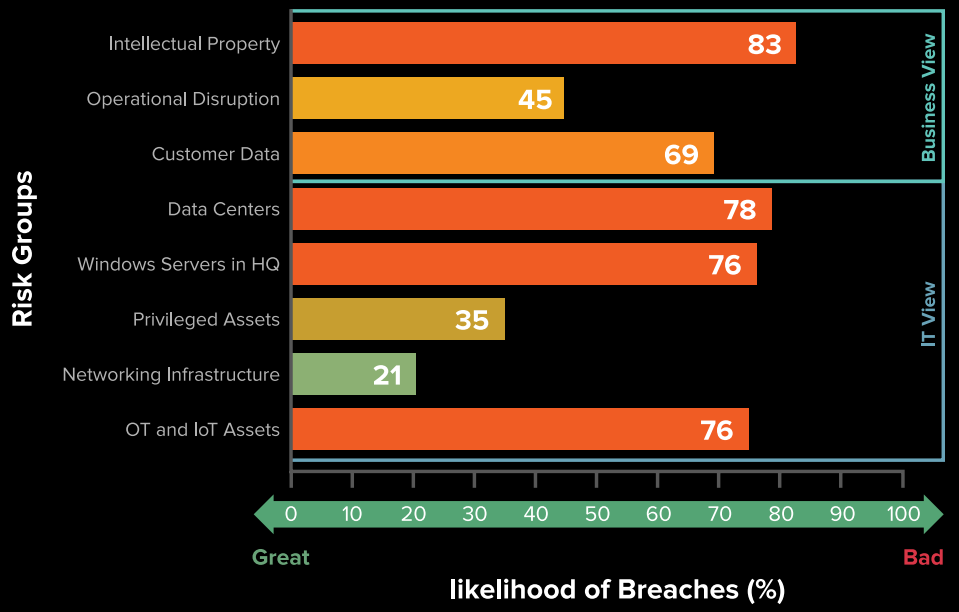
Balbix allows SIEM solutions to serve their intended purpose as a backstop for identifying and actioning oversights. By automatically gathering threat intelligence from global threat feeds in addition to host and traffic analyzers deployed throughout an organization, Balbix provides a prioritized list of risk insights so that you can proactively fix security issues before they become mission critical. CISOs and CIOs can drill down on specific areas of risk with heat maps that allow for detailed context on business criticality and breach likelihood for every asset in an organization.

Governance, Risk, & Compliance

Key to effective data governance and compliance management is an accurate and up-to-date inventory of all your enterprise's data, categorized by departments and/or risk owners. Furthermore, you need to know which assets are holding highly sensitive information like customer PII or intellectual property. Mapping these items of risk toward an acceptable framework adopted by the business is how many decisions are being made. This means the accuracy of your data governance is driving the high-level understanding of risk and resource allocation.

Obsolete and out-of-policy software on employee assets is a very difficult and costly problem for organizations. Balbix allows you to simplify and accelerate regulatory compliance, providing real-time visibility into the security of all IT assets, apps, and users in your environment. This goes beyond standard GRC tools, monitoring the likelihood of compromise for each asset across 100+ attack vectors.

Ticketing (Security Orchestration)

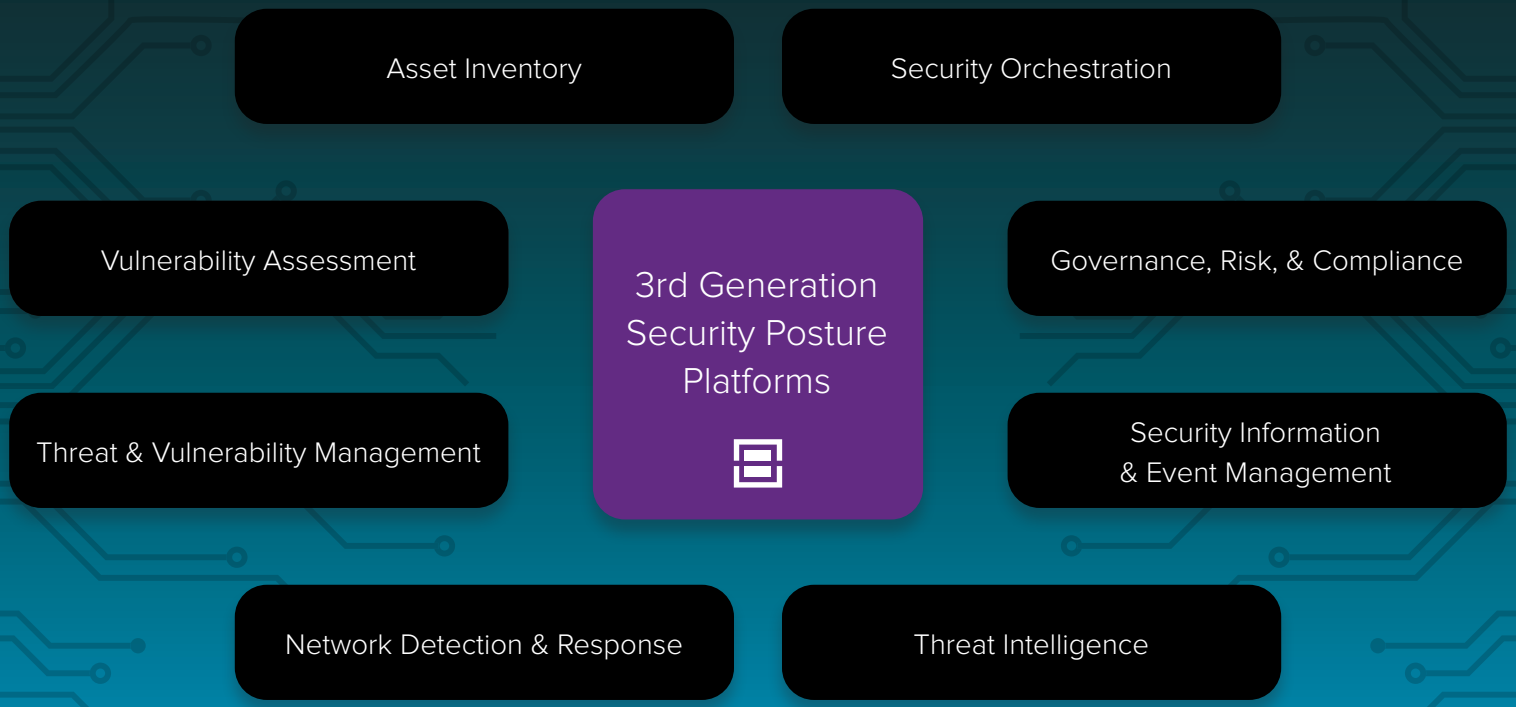


Cyber risk insights are only valuable if they are both accurate and acted on appropriately with little delay. Too much time and energy is wasted debating what is and is not in need of attention without an agreeable source of truth in place. What security teams really need are clear risk insights delivered to specific owners with context and prioritized by severity. Proper security orchestration and ticketing should enable security teams to align their effort with results.

Balbix has direct integration with the most well used service desk solutions and generates prioritized tickets with relevant context assigned to the right owners for strategic and tactical mitigating actions. These tickets go beyond simple CVE numbers and detail prescriptive fixes for remediating each vulnerability. Notifications, leaderboards and incentives can be set up for a gamified approach to drive cyber-risk reduction.

Balbix BreachControl™

Balbix enables you to do all this and more, bringing your cybersecurity posture programs together in one place.



Understand your attack surface and complete asset inventory

Balbix continuously observes your extended enterprise network inside-out and outside-in to discover the attack surface and analyze hundreds of millions (or more) of data points that impact your risk. Organizations can track their inventories in real-time and stay current on security issues affecting business critical devices, software, and other assets.

Get an accurate read on your risk

Balbix calculates your enterprise's real-time risk, taking into account open vulnerabilities, business criticality, applicable threats and the impact of compensating controls. Analysis of all possible breach scenarios—the various combinations of attack starting points, target systems and propagation paths—and precise determination of the riskiest scenarios is key. This real-time risk model is surfaced to relevant stakeholders in the form of highly visual drill-down risk heat maps and Google-like natural-language search. You can ask questions like "where will attacks start" or "what is the risk to customer data," and get a relevant, highly visual answer, along with drill-down details on how to mitigate the risk.

Obtain prioritized action items with prescriptive fixes

Balbix generates a prioritized list of actions that will affirmably reduce risk. Security posture issues with the greatest risk are addressed first before working down the list of smaller contributors. For each issue, responsible owners for the corresponding assets are identified and then prioritized tickets containing all relevant context are generated and assigned to these owners. Progress is closely tracked and fed back to relevant stakeholders.

Balbix®

Leading an Economical and Efficient InfoSec Program

Read the Blog

Elements of Security Posture Transformation

Get the Handbook