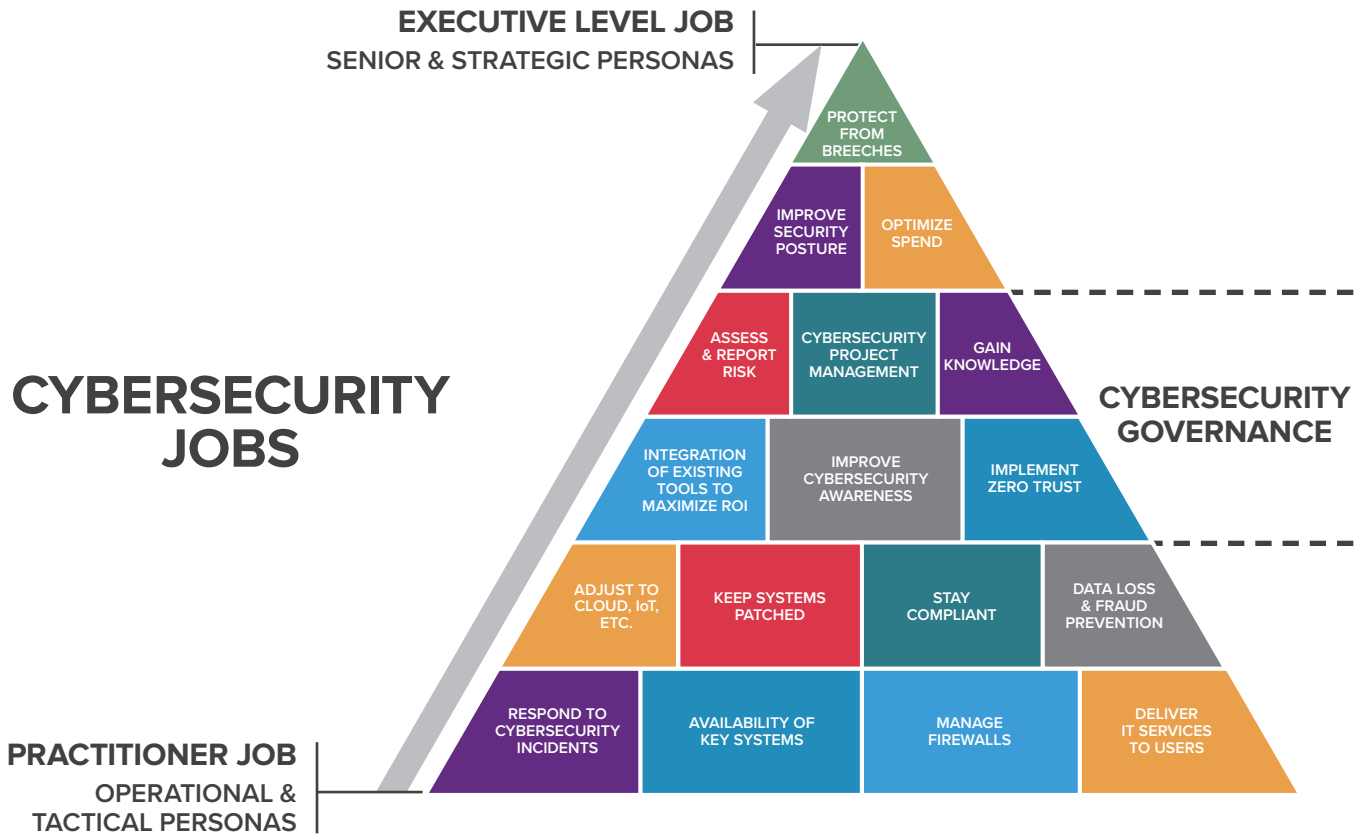
Balbix®

SOLUTION BRIEF

IMPROVE
Overall Security Posture

The primary role of the cybersecurity function in an enterprise is to ensure the safety of the company's data, infrastructure, and technology systems. The CISO is the guardian of the cybersecurity function and to best protect the enterprise from breaches, the CISO and the overall cybersecurity team have a long list of line items that they need to be mindful of. These include incident response, staying compliant, keeping systems patched, preventing fraud, managing firewalls, implementing zero trust, consolidating and integrating tools, reporting to the board, and 23 more items – all these make a CISO's job hard. But perhaps the hardest of job of them all, that all these line items roll up to, is improving overall security posture of the organization.



Improving overall security posture

The first half of 2020 has documented a 273% increase in exposed data records

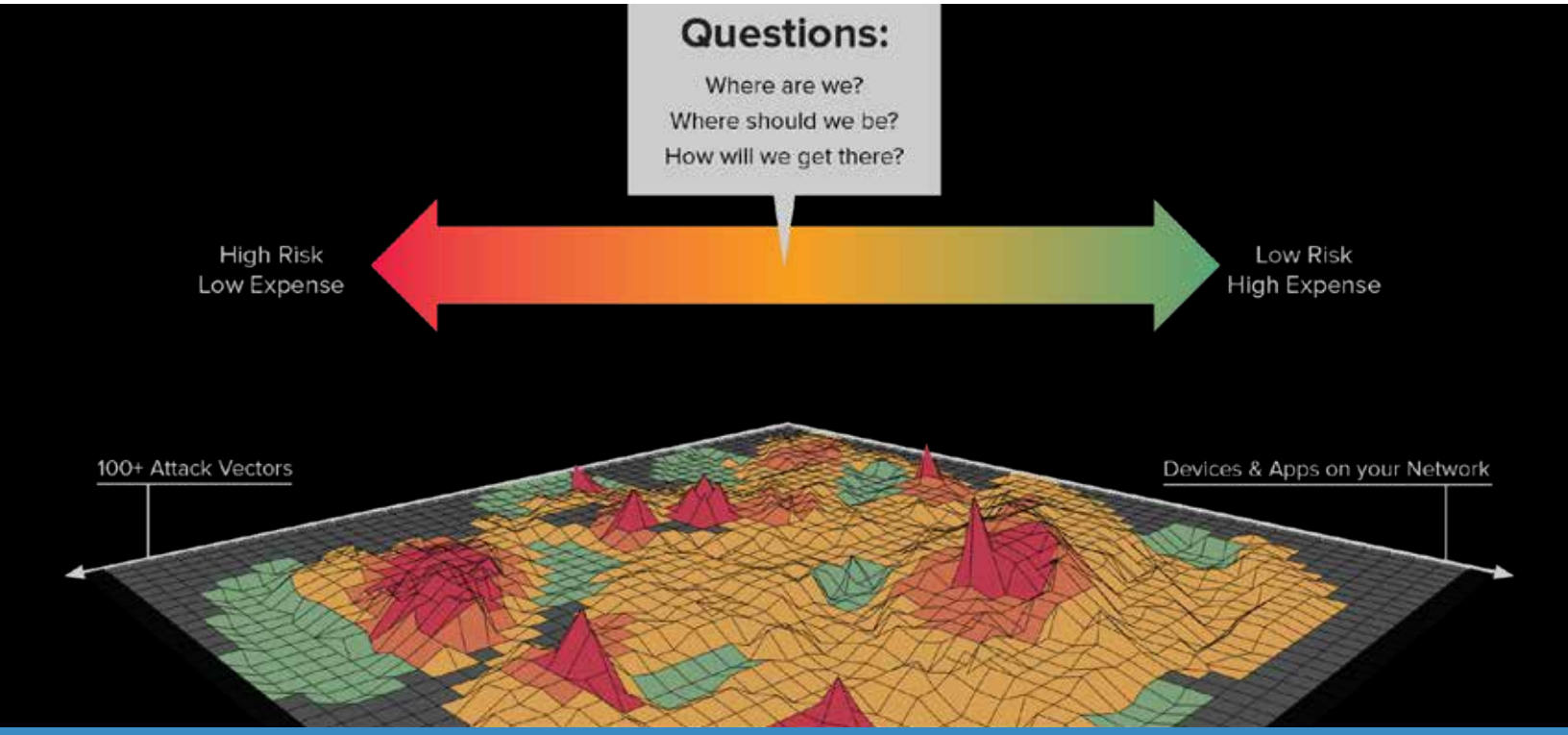
Around 16 billion records have been exposed in the first half of 2020, out of which 8.4 billion records were exposed in the first quarter alone, a 273% increase from the first half of 2019 which saw “only” 4.1 billion exposed. That is a sobering statistic. CISOs and security teams are overwhelmed by the challenge of how to maintain and optimize their security posture and only 1 in 3 say that they are confident that they can avoid breaches.

While there is more awareness amongst top leadership and board members on cybersecurity, the perspective that cybersecurity is just another risk item persists. The board really only has three questions about security posture:

First, they want to know where the organization is on the cyber-risk spectrum.

Then, they want to know where the organization should be? They rely on the security team to come up with that recommendation.

And if the organization is not where it should be, they want to know the plan to get there.



Your board and senior management rely on the security team to know the answers to these questions. Unfortunately, while these questions look deceptively simple, they are very hard to answer.

10 KEY CHALLENGES

1. There is a significant gap between the business level view of the organization and the IT/security level view, which makes it difficult to align plans with business goals.
2. Mechanisms for asset inventory of the organization are not up to date, require manual effort and offer an incomplete picture, missing several types of IT assets like cloud, mobile, and IoT.
3. There is no easy and systematic way to map business constructs, e.g., factories, business units, profit, and expense to IT/cybersecurity constructs like assets, patch state, security configuration, risk of phishing, password hygiene etc.
4. It is tough to prioritize effectively because there are too many signals to monitor for overall risk with no easy way to tell which methods would be most effective for risk reduction.
5. There is a lack of data or tools to show internal and external benchmarks for breach risk handling and how they trend over time.
6. You don't have the reporting framework that can generate different types of reports appropriate for various scenarios and audiences.
7. There is a lack of a systematic way to prioritize and fix non-patching related vulnerabilities including those related to passwords, phishing, misconfiguration, encryption, malicious insider, attach propagation or lateral movement of adversary once inside the network.
8. There is an explosion in the number of point products that have been deployed for various parts of the attack surface, and there is no way of understanding the effectiveness of all those tools.
9. The various tools are not integrated together so you have a number of places and reports to scan through to get a picture of your security posture. Getting these tools to work together is very complex and resource intensive.
10. Automation of key tasks is missing.

Balbix: A system of record, experience, and intelligence

A SYSTEM OF RECORD

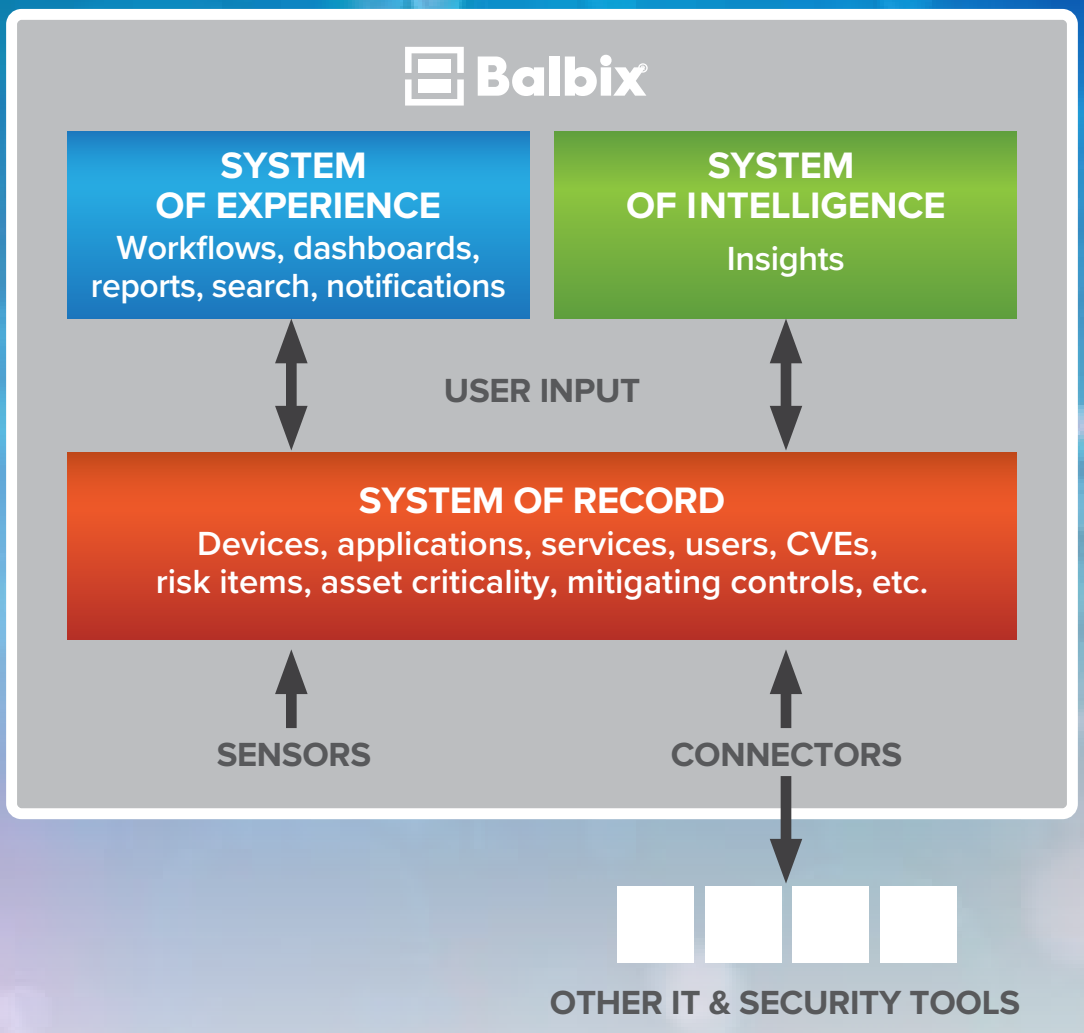
Balbix enables you to understand your inventory including asset criticality, to know what CVEs are open, what your other risk items are, and which compensating controls are effective.

A SYSTEM OF EXPERIENCE

Balbix AI analyzes all of data signals across your inventory and attack surface on a continuous, real-time basis to prioritize the most important tasks.

A SYSTEM OF INTELLIGENCE

Balbix provides workflows, notifications, dashboards and reports you need in order to maximize your cybersecurity team efficiency.



FEATURES

AI-Powered Security Posture Transformation

The Balbix platform uses specialized AI algorithms to discover and analyze the enterprise attack surface to enable a broad set of vulnerability and risk management use cases that help to improve your enterprise security posture.

DISCOVERY

- Continuous and automatic discovery of IT assets and monitoring across 100+ attack vectors.
- Comprehensive coverage of all asset types (on-prem, cloud, IoT, mobile, managed and unmanaged) and all attack vectors.
- Discovery of mitigation/compensating controls to understand the effectiveness of your cybersecurity program.

ANALYSIS

AI-powered analysis of observations to derive risk insights and predict where you are likely to be breached.

Calculation and financial quantification of risk using 5 factors – vulnerabilities, threats, asset exposure, business criticality, and compensating controls.

Provide a prioritized set of actions that you can take to transform your security posture and reduce cyber risk by 95% or more, while making your security team 10x more efficient.

Visibility into overall security posture including risk heatmaps by owners, sites, business units.

Dashboard and workflows for various tasks necessary for security posture transformation and reports for various stakeholders to indicate state/progress of risk management.

EXECUTION

- Ability to assign owners and generate prioritized tickets with all relevant context, set goals and show outcomes.
- APIs to enable other security tools take advantage of risk context.
- Gamification to drive all stakeholders to do their part in improving security posture.

BENEFITS

AI-POWERED 100X VISIBILITY	Get a real-time asset inventory and notion of risk.
EXECUTIVE & EMPLOYEE ENGAGEMENT	Involve all stakeholders in the enterprise participate in risk reduction and management with automatically generated notifications and reports, and aligned incentives.
RISK-BASED VULNERABILITY MANAGEMENT	Identify and fix vulnerabilities across 100+ attack vectors proactively and continuously, using prioritized risk insights and actions
VERIFIED PROTECTIVE CONTROLS	Verify whether all necessary endpoint and network-based protective controls are in place and working correctly.
VISIBILITY INTO GAPS	Emerging gaps in protective controls are quickly surfaced for attention and all proposed new controls can be evaluated pro-forma for ROI before deployment.
RISK-BASED ACCESS	Implement risk-based dynamic network segmentation to curtail unauthorized lateral movement in the network.
CONTEXT-AWARE SECURITY OPERATIONS	Identify SOC processes, alarms, and indicators-of-compromise in priority order based on risk and comprehensive context.

SEE BALBIX LIVE

SCHEDULE A 30 MINUTE PRESENTATION

ABOUT BALBIX

Balbix is the world's first cybersecurity platform to leverage specialized AI to provide real-time visibility into an organization's breach risk. The Balbix system predicts where and how breaches are likely to happen, prescribes prioritized mitigating actions, and enables workflows to address the underlying security issues. By using Balbix, CISOs and CIOs can transform their security posture, reducing cyber risk by 95% or more, while making security teams 10 times more efficient. Balbix counts many global 1000 companies among its rapidly growing customer base and was named a "Cool Vendor" by Gartner in 2018.