Balbix®

ELEMENTS OF Security Posture Transformation HANDBOOK

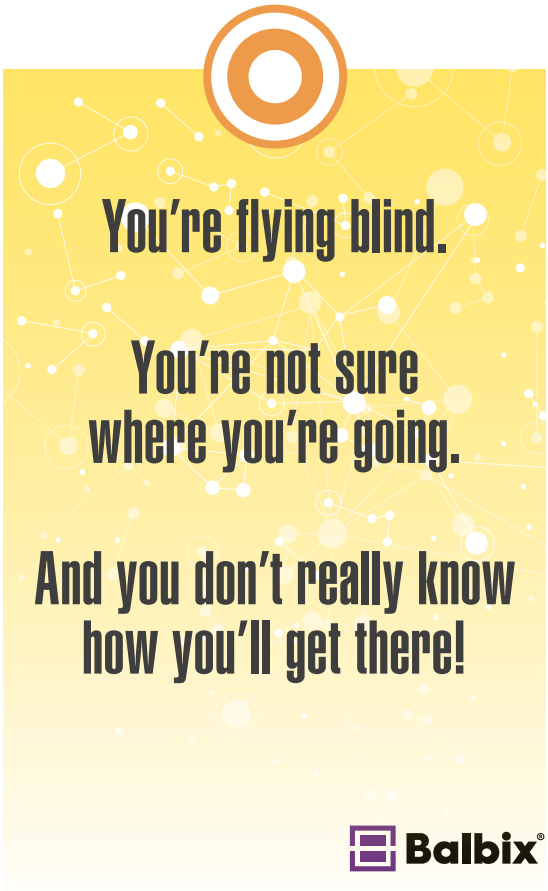
Overview

The enterprise attack surface is massive and growing rapidly. Your extended network has a bewildering variety of assets. Each internet-facing element can be attacked in hundreds of ways. Users can be phished. Weak passwords, software vulnerabilities, misconfigurations and numerous other vectors can be leveraged to compromise some enterprise asset and gain an initial foothold inside your network. Once in, the adversary can rapidly move across the enterprise to locate and compromise an important asset — and you have a major breach. There are quite literally millions of permutations and combinations of methods by which the adversary can attack and compromise your network.

FIGURE 1: Cybersecurity posture spectrum

Most data breaches happen because organizations only have a vague understanding of their attack surface and overall security posture, i.e., your actual readiness to repel cyber-attacks. If your organization is like 99% of all enterprises, you don't really know where you are on the cybersecurity posture spectrum in Figure 1 at right. It is very difficult to reason about the overall likelihood and impact of a successful data breach—i.e., the overall breach risk. You are flying blind!

Furthermore, because of this vague understanding of security posture, you and your colleagues struggle to agree on where in the spectrum your organization ought to be, i.e., to agree on when cybersecurity is "done" for your organization. Many just hope that your security wizards will keep you safe. We can do better!



Balbix

Security Posture Challenges

Let's double click into the notion of security posture. Referring to Figure 2, on the x-axis we have the different parts of your world where things can go wrong from a cybersecurity standpoint. And on the y-axis we have specific ways in which these things will go wrong – aka attack vectors.

On the x-axis we have your traditional infrastructure, servers, databases, switches and routers, etc., and your apps, your endpoints— managed, unmanaged, BYOD, mobile phones and tablets, IoTs. We also have your cloud apps – personal applications of our employees – Google, Gmail, LinkedIn, etc., official SaaS applications, public facing web sites. At the right end of the x-axis, we have your 3rd party vendors who bring risk into your network because of certain trust relationships. It is generally quite difficult for most organizations to even enumerate their x-axis for an accurate and up to date asset inventory.

On the y-axis, we have the different methods of attacks— starting from simple things like weak and default passwords, reused password, passwords stored incorrectly on disk, or transmitted in the clear, to more complex things like phishing, social engineering and unpatched software. Further down the y-axis, we have zero-day vulnerabilities – security bugs that are "unknown" until they are first used. There are quite literally 100s of items on the y-axis in dozens of categories, and each point on the plot is also large vector.

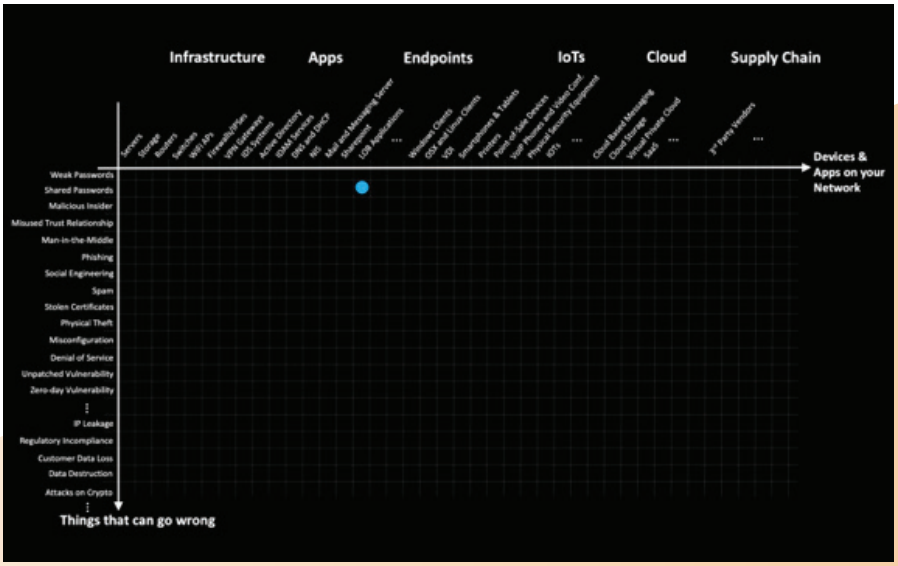


FIGURE 2:
The enterprise attack surface

Balbix

FIGURE 3: The Equifax breach

This gigantic x-y plot is your attack surface. In a typical breach, the adversary uses some point on this attack surface to compromise an (Internet facing) asset. Other points are then used to move laterally across the enterprise, compromise some valuable asset, and then to exfiltrate data or do some damage. Figure 3 shows how the Equifax breach unfolded.

It is not easy to understand what the enterprise risk heatmap for your attack surface looks like (Figure 4). This is critical, because the adversary will generally go after your weakest link. How do you defend what you can't even see properly? It is even harder to figure out what risk is acceptable, and exactly what steps are necessary to change the reds and yellows to greens in the risk heatmap, thereby improving security posture and decreasing breach risk.

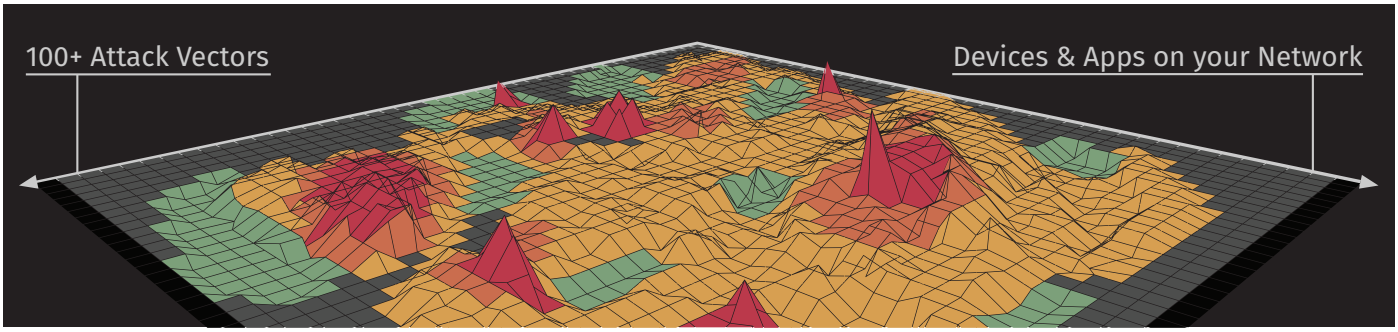


FIGURE 4: The Enterprise risk heat map

Balbix

There are several specific challenges in discovering and analyzing the attack surface:

INACCURATE INVENTORY Most organizations struggle to enumerate their inventory, i.e., the devices, applications and users present in the enterprise network.

PASSWORD ISSUES In almost all organizations, there are numerous instances of weak, default and reused passwords, often stored and/or transferred in the clear.

UNPATCHED SYSTEMS Timely security patching is very challenging, overwhelmed by the weekly volume of new CVEs. Since, an accurate notion of risk does not exist, and therefore it is very hard to prioritize patches based on risk.

PHISHING, WEB & RANSOMWARE There is often poor security awareness amongst employees and a lack of modern endpoint security tools and controls.

DENIAL OF SERVICE FRAGILITY The enterprise network is not designed for availability under a (distributed) denial-of-service attack or a compromise/failure of some important asset.

POOR IDENTITY & ACCESS CONTROL Identity and access management is sloppy, with many users having excessive system and network privileges.

ENCRYPTION ISSUES There is a large amount of unencrypted or incorrectly encrypted communications. Data is often stored unencrypted or improperly encrypted.

MISCONFIGURATION Numerous misconfigurations in application and OS settings exist across the enterprise. There are no mechanisms in place to continuously look for such instances and fix the issues.

FLAT NETWORKS There is no network segmentation. Attackers can rapidly move across the network from an initial compromised asset. Individual system compromises easily turn into major data breaches. This last issue is key, because in a non-resilient network overall breach risk is determined by its weakest link's breach likelihood.

MALICIOUS INSIDER There is inadequate visibility and controls for detecting and preventing rogue users exfiltrating or destroying key data.

FIGURE 5: The Risk Calculation

To accurately understand security posture, we need to (repeatedly) solve a hyperdimensional math problem involving over the tens of thousands of assets on the x-axis and the 100+ attack vectors in the y-axis of Figure 2. For each point of Figure 2, which is a vector, we need to estimate risk incorporating information about a) threats, b) vulnerabilities, c) mitigating actions, d) business criticality, e) impact elasticity and f) time-to-repair (Figure 5). We must then reason about what actions will bring about the greatest reduction of overall breach risk for the enterprise.

It is worth noting that traditional methods such vulnerability assessment (e.g., Qualys) or penetration testing are able to analyze less than 5% of the enterprise attack surface.

These legacy methods also produce output that is voluminous, unprioritized, and often irrelevant. Due to this lack of a viable proactive security strategy, much effort and money goes into detecting and reacting to security events, albeit unsuccessfully. Numerous surveys peg the average dwell time of undetected attackers in the enterprise at approximately 200 days.

Ultimately, a poor understanding of the massive attack surface results in waste, frustration and anxiety. In spite of millions of dollars of annual security spending, most enterprises are just one bad click, one reused password or a single unpatched system away from a cybersecurity disaster.

In spite of millions of dollars of annual security spending, most enterprises are just one bad click, one reused password or a single unpatched system away from a cybersecurity disaster.

Balbix®

AI-Powered Security Posture Transformation

Balbix uses deep learning and advanced AI algorithms to make this computation feasible. Our platform BreachControl™ enables rapid security posture transformation. There are three major steps in AI-powered security posture transformation:

STEP 1

In step 1, we need to understand your attack surface. Balbix continuously observes your extended enterprise network inside-out and outside-in, to discover the attack surface and analyze the hundreds of millions (or more) of data points that impact your risk.

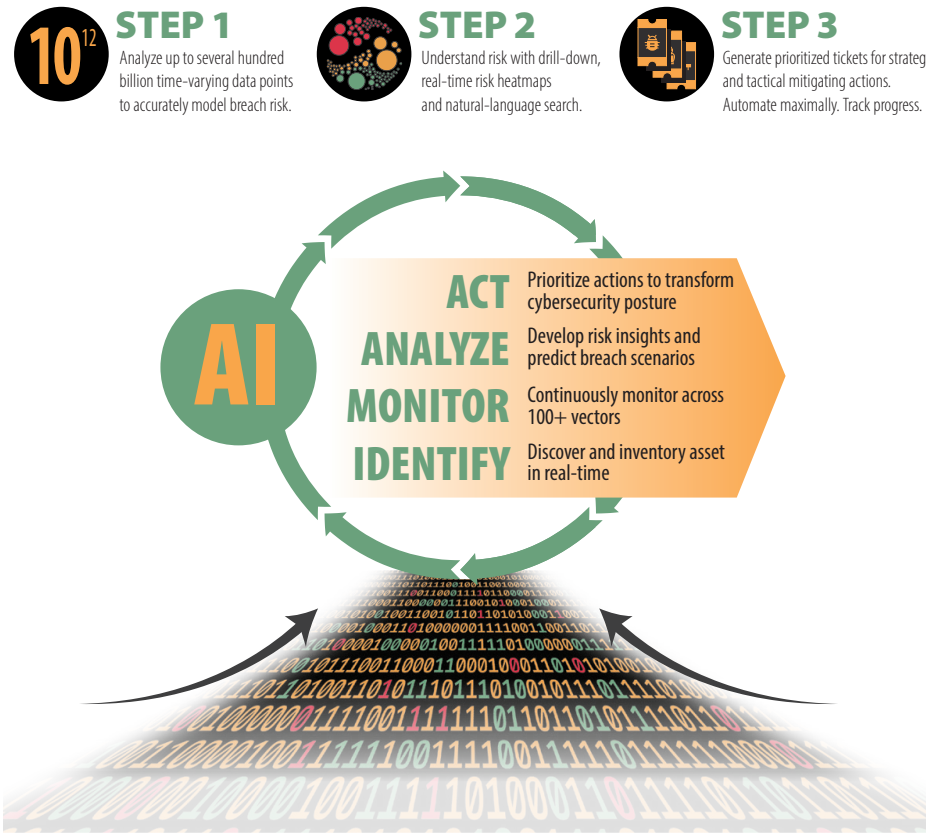
STEP 2

In step 2, Balbix calculates your enterprise's real-time risk, taking into account open vulnerabilities, business criticality, applicable threats and the impact of compensating controls. It is necessary to analyze all possible breach scenarios – the various combinations of attack starting points, target systems and propagation paths – and pinpoint the riskiest scenarios. Balbix surfaces this real-time risk model to relevant stakeholders in the form of highly visual drill-down risk heatmaps and Google-like natural-language search. You can ask questions like "where will attacks start" or "what is the risk to customer data", get a relevant, highly visual answer within milliseconds, and then drill-down into the details.

STEP 3 Step 3 is where we act to change security posture, and this is where all the hard work is.

A. Balbix generates a prioritized list of actions that will affirmably reduce risk. We want to first address security posture issues with the greatest risk before working down the list of smaller contributors.

B. For each issue, Balbix (with a little human supervision) identifies the correct responsible owners for the corresponding assets and then generate prioritized tickets containing all relevant context and assigns them to these owners.



C. Some tickets call for tactical mitigating actions, while other required actions correspond to strategic projects.

D. Wherever possible, we want to automate these required actions, particularly for issues that will come up repeatedly, e.g., installing a Windows patch.

E. Progress is closely tracked and fed back to relevant stakeholders. Balbix enables security teams to distribute the work of driving to and maintaining a good security posture to stakeholders outside the security team—this is critical!

Steps 1-3 are repeated continuously in a loop. At each time instant, Balbix is observing your extended network and recalculating breach risk and what actions are most appropriate to make the security posture better. At some point, the enterprise gets to the desired level of security maturity and resilience.

Balbix®

Mature and Resilient Security Posture

This is what a cyber-resilient enterprise (Figure 6) looks like:

1. AI-POWERED 100X VISIBILITY

You have a real-time asset inventory and notion of risk. The risk calculation incorporates data about vulnerabilities, business criticality, threats and mitigating controls.

2. EXECUTIVE AND EMPLOYEE ENGAGEMENT

With suitable top-down mandate, automatically generated notifications and reports, and aligned incentives all stakeholders in the enterprise participate in risk reduction and management.

3. RISK-BASED VULNERABILITY MANAGEMENT

Vulnerabilities across 100+ attack vectors are proactively and continuously fixed in prioritized order based on risk.

4. VERIFIED PROTECTIVE CONTROLS

All necessary endpoint and network-based protective controls are in place and continuously verified as working correctly. As the enterprise evolves, emerging gaps are quickly surfaced for attention and all proposed new controls can be evaluated pro-forma for ROI before deployment.

5. STRONG IDENTITY

There are mechanisms in place for managing strong user identity.

6. RISK-BASED ACCESS

You have implemented risk-based dynamic network segmentation. As a result, lateral movement is hard for the adversary and attacks don't spread.

7. CONTEXT-AWARE SECURITY OPERATIONS

Your SOC processes alarms and indicators-of-compromise in priority order based on risk and comprehensive context.

8. AI-POWERED AUTOMATED SECURITY ORCHESTRATION

Automated playbooks heal the network as needed.

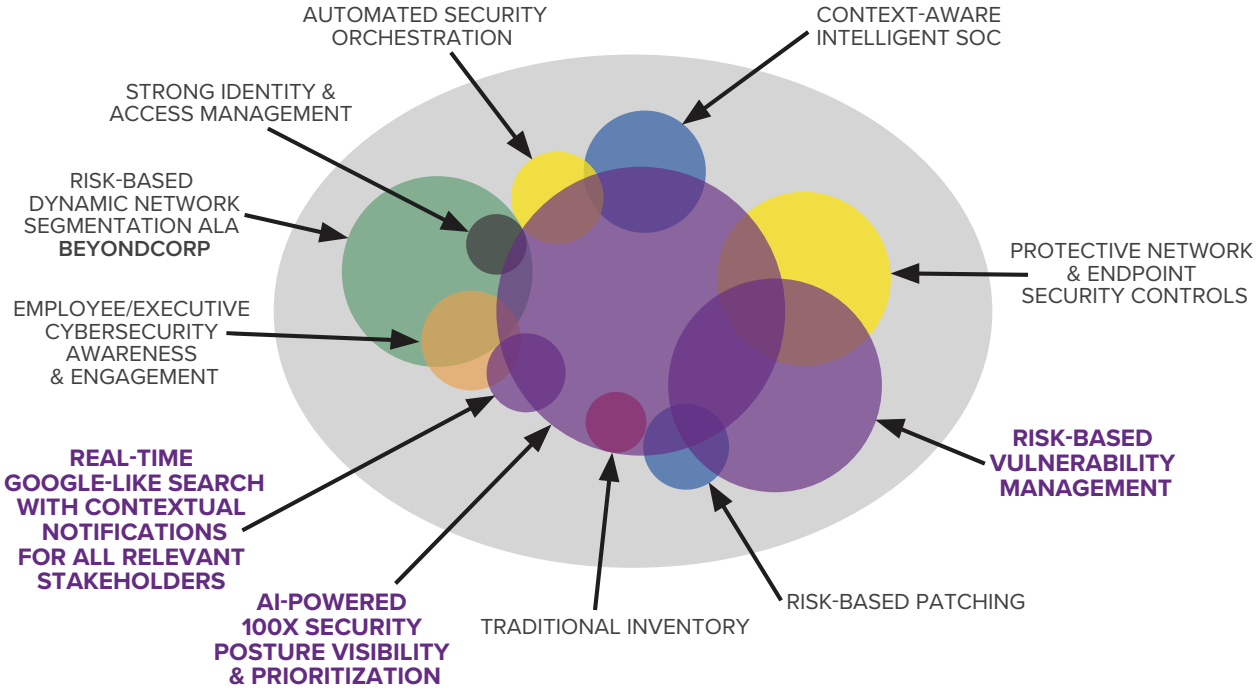


FIGURE 6: A cyber-resilient security posture

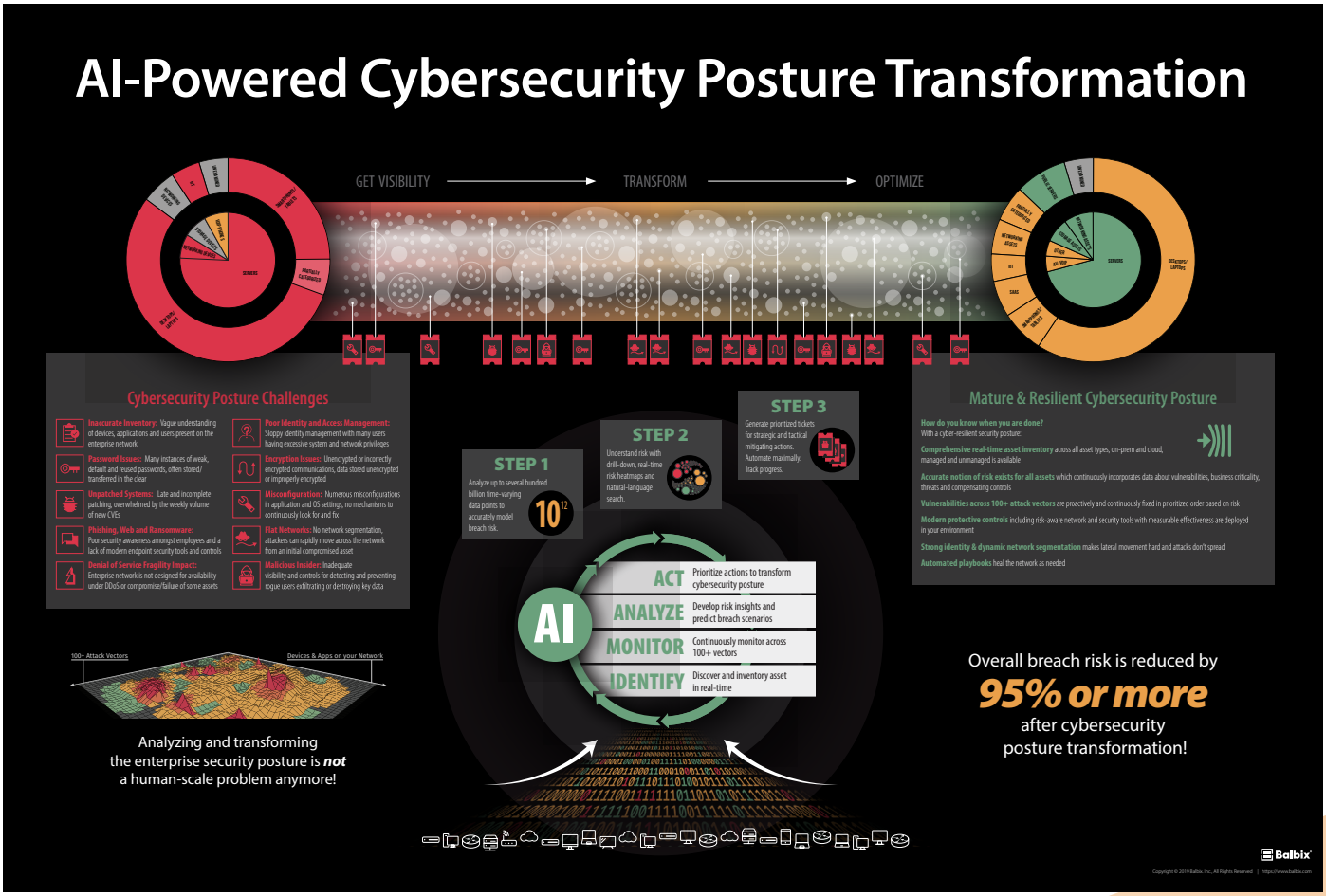
Figure 6 shows the relationship between different elements of a mature and highly resilient cybersecurity posture. The purple items in this picture are core capabilities of Balbix. As you can see, 100x security posture visibility and prioritization is the lynchpin of transforming your security posture. In this picture, we show "Traditional Inventory" and "Risk-based Patching" only for context—their functions are fully subsumed by AI-powered Security Posture Visibility and Risk-based Vulnerability Management.

Balbix®

Summary

We have entered an era where cybersecurity is no longer a human-scale problem. It will require a collaboration between humans and innovative AI techniques to meet the challenge of the latest cyber threats.

Please contact us at info@balbix.com to request a physical copy of the poster below.



Balbix®