Getting Started on Transforming Your Cybersecurity Posture

Introduction

With breaches ever on the rise, cybersecurity is one of the highest priorities for virtually every enterprise. It is a frequent topic of C-suite and board discussions and has a ripple effect throughout the business as organizations look for ways to keep themselves safe. If you were to listen in on these discussions as the proverbial "fly on the wall" however, you would see that they are typically focused on gut feelings and anecdotal observations rather than hard facts and data. The hard truth is that most organizations only have a vague understanding of their attack surface and overall cybersecurity posture.

- *According to a recent report, 945 data breaches led to a staggering 4.5 billion data records being compromised worldwide in the first half of 2018.*
- *2018 Ponemon research reports the global average cost of a data breach is up 6.4 percent over the previous year to $3.86 million.*

Q. Why is there such a wide gap between the cybersecurity measures deployed by enterprises and successful breaches?

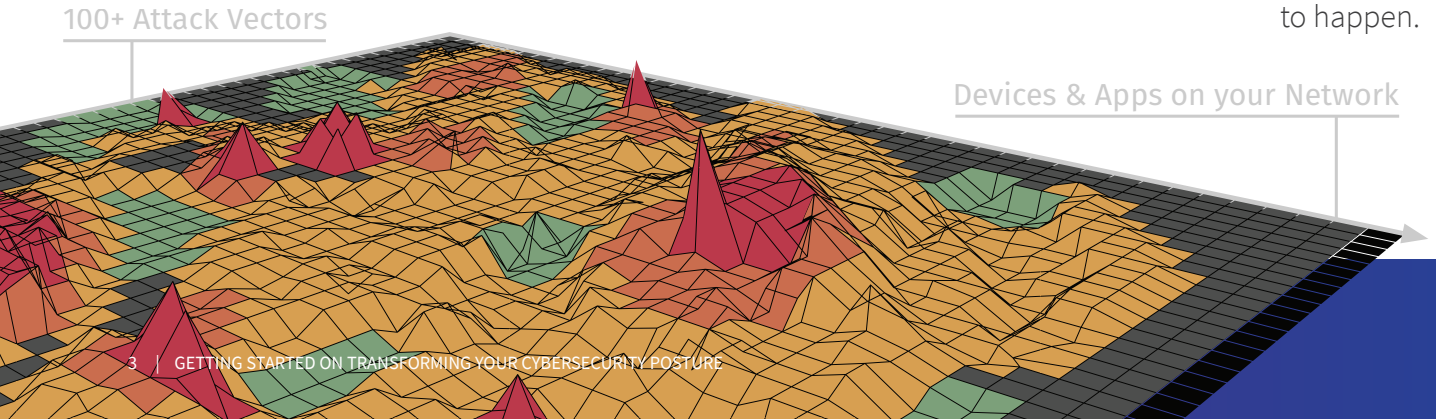
Because organizations have a vague understanding of their current security posture and don't know when it is robust and mature.

Cybersecurity is a complex problem to solve

Attack Surface: All the points of exposure that can potentially be attacked and lead to a cybersecurity breach.

Did you know that analyzing and improving the enterprise security posture is not a human scale problem anymore? For an organization with a thousand employees, there are over 10 million time-varying signals that must be analyzed to accurately predict breach risk. The truth is that the attack surface of a modern enterprise is huge and ever growing, which makes gaining an accurate understanding a big challenge.

The typical enterprise attack surface includes a wide variety of assets spanning across its infrastructure—applications, managed and unmanaged endpoints (fixed and mobile), IoT, and cloud services. Each of these elements can be breached in a myriad of ways. Users and their devices can be leveraged to compromise some enterprise asset and gain an initial foothold inside your network. Once this happens, you are a breach waiting to happen.



Balbix

Understanding your cybersecurity posture

The security status of your enterprise's software and hardware, networks, services, and information; your ability to manage your defenses; and your ability to react to and recover from security events are collectively referred to as your cybersecurity posture. Understanding and defining the full scope of your cybersecurity posture is essential to protecting your business against breaches.

To understand and optimize your cybersecurity posture, you need to:

- *Analyze what it currently looks like*
- *Identify the possible gaps*
- *Then take action to eliminate those gaps*

Balbix®

The starting point

Assessing your current security posture is the first step in identifying where you are in your cybersecurity journey

As with any complex problem, the first order of business is to make sure you're asking the right questions:

- *Do we have a real-time inventory of **all** our assets, including mobile devices, unmanaged assets, cloud services, and IoT?*
- *Are we able to continuously observe all relevant security attributes for our assets?*
- *Assuming some internet-facing asset is compromised, how quickly will the attack propagate before being detected?*
- *What is the likelihood and impact of a major breach?*
- *Are we focusing on the right activities and investments?*
- *Can we quantify our cyber-resilience (i.e., the ability to continuously operate the business despite adverse cyber events)?*
- *Can we estimate the pro forma ROI of our security initiatives, quantifying the expected decrease in breach risks?*

Just the exercise of getting these answers will be a useful first step to help you identify where you are in your cybersecurity journey.

Where you want to be

A mature security posture is where a holistic approach to measuring and mitigating cyber-risk is in place.

When your organization has continuous visibility into what needs protecting based on its business criticality, you can accurately quantify risks, examine holes in security controls, and create short and long term action plans to address your gaps. To properly quantify risk and make it business-centric, a multi-pronged risk model is the best approach. This considers the inherent likelihood and impact of a breach for each asset as it pertains to your business as well as global threats and existing mitigating controls.

This requires:

- *Analyzing millions of time-varying signals to accurately predict where and how breaches might happen*
- *Continually observing relevant security attributes of all enterprise assets, factoring in information about active threats, business criticality, and existing compensating controls*
- *Prioritizing action items using the multi-pronged risk model and addressing the most critical vulnerabilities and issues first*

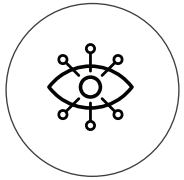
Accurate and contextual risk measurement guides the roadmap of your entire defense strategy and influences your security spending throughout the years.

How to get there

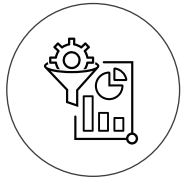
Tranforming your cybersecurity posture will require a collaboration between humans and innovative AI techniques to meet the challenge of the latest cyber threats.

Select an appropriate platform that can provide you with an end-to-end approach to measuring and improving your security posture.

Discover and create a real-time inventory of all of your assets



Continuously observe your inventory across a broad range of attack vectors like unpatched software, passwords, phishing, etc.



Analyze observations to derive risk insights and predict where you are likely to be breached

Prioritize, remediate, and implement fixes

Continually measure and track security posture improvements

Balbix

A mature and resilient security posture is the ultimate goal

As we've seen, cybersecurity presents some unique challenges:

- *A vast attack surface*
- *Ten of thousands of IT assets*
- *A continually moving target*

In order to manage all of these effectively and in real time, organizations need to up their game. Balbix BreachControl™ enables organizations to bring all of this complexity under control by deploying a single platform that continuously discovers and monitors all asset types and attack vectors, analyzes this information to predict likely breach scenarios, prioritizes security issues based on business risk and guides you on the appropriate mitigation steps to address issues.

BreachControl offers:

- *Real-time discovery + inventory of all your assets*
- *Continuous monitoring across a broad range of attack vectors*
- *Comprehensive breach risk assessment and prediction*
- *A prioritized action plan*

By addressing these four essential areas, the Balbix BreachControl™ platform enables you to transform your cybersecurity posture and enhance your enterprise cyber-resilience.

Balbix®