

# Avoid Breaches Through Prediction and Proactive Mitigation

## A THREE STEP APPROACH TO AVOIDING BREACHES IN YOUR ENTERPRISE

Across the globe, enterprises face growing breach risk from a vast number of increasingly sophisticated adversaries, coupled with increased points of entry. Security teams constantly struggle to identify their weakest links and safeguard their most valuable systems and data. Despite best efforts and robust technology investment, breaches occur with alarming frequency, oftentimes resulting in significant damage.

### Are Breaches Avoidable?

What if you could measure the likelihood and impact of a breach for every device, user and application across your entire enterprise? Including the cloud, IoT, mobile and BYOD? How would you benefit from a self-learning system, powered by deep learning and other advanced AI algorithms, that would automatically predict where and how a breach could occur in your enterprise – before it ever happened? And provide your security team with a specific list prioritized by business risk, as well as clear and prescriptive fixes for each predicted breach?

Balbix believes that enterprises can avoid the majority of breaches – not just remediate them once they've occurred and been found – by taking a proactive, three-step approach.

### Three Steps to Breach Avoidance

**1**

#### Predicting Breaches

A proactive approach to breach avoidance starts with putting the right tools in place to comprehensively assess your breach risk internally, across all attack vectors, coupled with understanding external threat risk.

**2**

#### Prioritizing Actions

From there, you need to prioritize the actions you take to proactively mitigate the huge list of potential breaches that comes from mapping your full list of IT assets across the number of potential attack vectors.

**3**

#### Prescribing Fixes

Finally, to maximize security effectiveness and security/IT team efficiency, the security team needs to know exactly how to prescriptively fix each prioritized mitigation action.



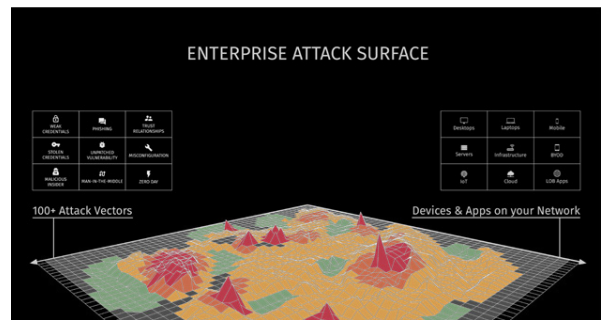
## Step 1: Predicting Breaches

The first crucial step in avoiding breaches is to be able to accurately predict them. That can be accomplished by discovering your full set of IT assets, classifying them based on their business criticality, and mapping them against your external threat environment.

Core to that is having an accurate, continuous and real-time view of all devices and apps that connect to your network, so you can properly map and monitor your full attack surface across internal resources, cloud, mobile, BYOD, IoT and other vectors.

There is also the need to understand the business criticality of each asset, as some sensitive apps or data increase breach risk much more significantly than others – e.g. a DNS server has much more impact if compromised than a team-level file server. Security teams need an automated way to assess the “breach impact” of every asset on the network to properly predict and avoid breaches.

Traditional device inventory systems struggle to identify the proliferation of assets across newer vectors such as cloud, BYOD and IoT, as well as identify an asset’s breach impact.

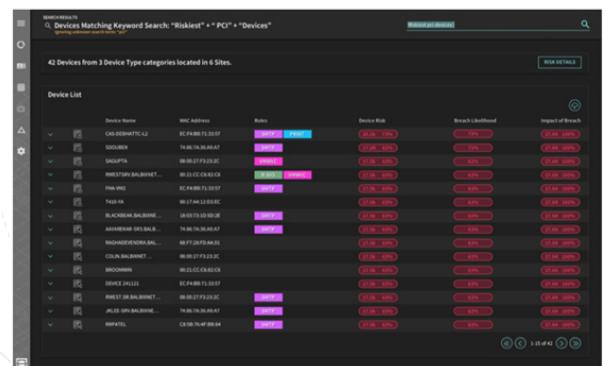


## Step 2: Prioritizing Mitigation Actions

The second crucial step in avoiding breaches is to proactively take action to mitigate them before they occur.

Depending on the size of the enterprise, it is often impossible to mitigate all breaches across all attack vectors, given the sheer volume of potential breaches from 1000s of assets deployed across 100+ attack vectors.

What is critical to minimizing breach risk is to prioritize mitigation actions based on true business risk (business risk = business impact x likelihood). Your breach avoidance system needs to understand the business impact of each of your IT assets, as well as the likelihood of it being breached, and use the resulting business risk assessment to prioritize all mitigation actions. Ideally your system provides your security and IT teams with a clear, prioritized list of actions to take.



Device Name	IP Address	Risk	Device Risk	Breach Likelihood	Impact of Breach
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical
CL-0000000000000000	10.10.10.10	High	Critical	Critical	Critical

## Step 3: Prescribing Fixes

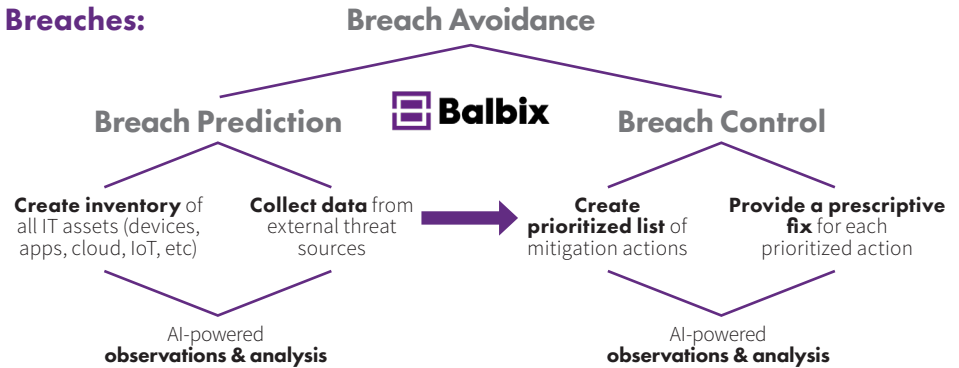
The final step in avoiding breaches is to efficiently implement fixes for each prioritized breach mitigation action.

While this is usually the most time-consuming task to avoiding breaches, as well as remediating existing ones, there are ways to greatly increase the responsiveness of security operations and IT resources.

If your breach avoidance system can generate prescriptive and clear recommendations, that will greatly reduce the time-to-fix for security operations center (SOC) analysts, as well as general IT resources.

## A New Solution for Avoiding Breaches: Balbix BreachControl™

The Balbix breach avoidance platform, BreachControl, helps your enterprise avoid breaches by providing continuous and real-time risk prediction, a prioritized list of mitigation actions, and prescriptive fixes for each action.

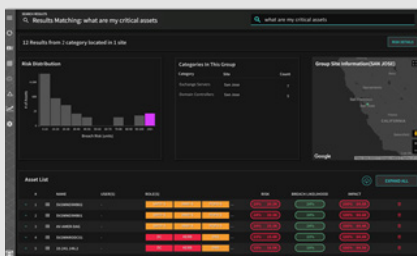


### HOW IT WORKS

Balbix sensors deployed across your entire enterprise network automatically and continuously discover and monitor all your enterprise's devices, apps and users across 100+ attack vectors. In addition, Balbix collects comprehensive data from external threat sources.



Together, this information is processed by the Balbix BreachControl engine in the cloud – leveraging deep learning and other advanced AI algorithms to calculate the business risk for each and every IT asset on your network.



Once the business risk has been established for each IT asset, Balbix BreachControl creates a clear and prioritized list of proactive mitigation actions based on the overall risk heat map.

To optimize effectiveness in avoiding breaches, as well as maximize SOC/IT team responsiveness, Balbix BreachControl provides prescriptive fix recommendations for each mitigation action.

## Balbix Helps Avoid Breaches and Reduces Risk

Rather than spending millions on reactive and largely ineffective shot-in-the-dark efforts at plugging security holes, your enterprise can take a much more predictive and controlled approach to avoiding breaches. Balbix BreachControl not only identifies breach risks ahead of time, but also provides prioritized and prescriptive fixes to prevent a breach from occurring in the first place.



3031 Tisch Way, St 800  
San Jose, CA 95128  
866.936.3180

info@balbix.com  
www.balbix.com