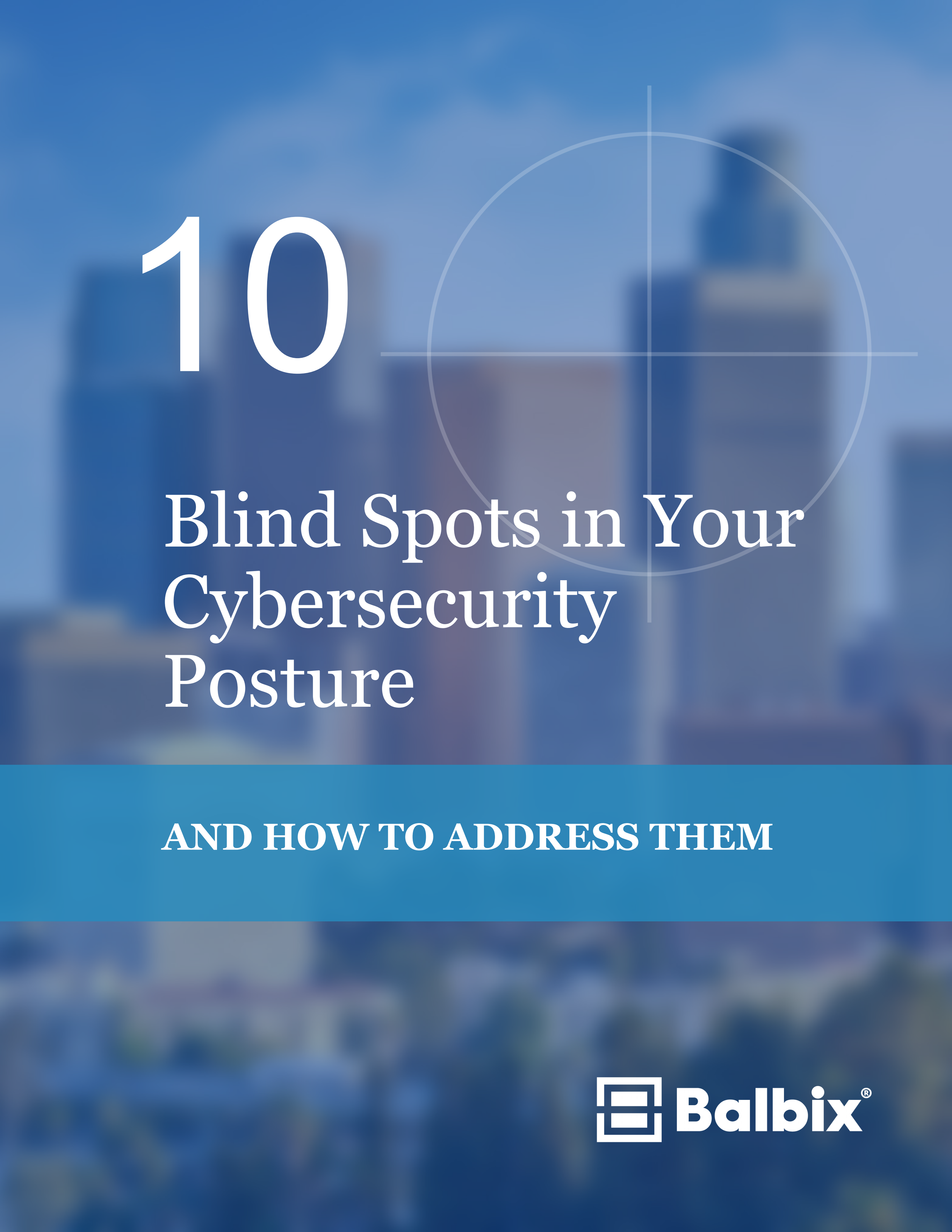


10 Blind Spots in Your Cybersecurity Posture

AND HOW TO ADDRESS THEM

Balbix®

INTRODUCTION

Nearly 90% of all data breaches happen because of poor cybersecurity posture. Unfortunately, organizations only have a vague understanding of their attack surface and cyber-risk. The first step to building a robust security posture is getting visibility into:

- Where you are
- What you have
- Where you need to be
- How you will get there

Any enterprise network is only as secure as its weakest link, so your cybersecurity visibility must extend to all types of assets and all sorts of security issues.

Here are 10 common blind spots you need to address to get visibility into your cybersecurity posture and ultimately transform it.

1 NON-TRADITIONAL ASSETS

The most important building block of any visibility program is an accurate inventory of what you are defending. Unfortunately, it is quite hard to keep track of the various devices, applications, and services used by enterprise users. As a result, it is difficult to correctly target vulnerability scans and risk assessments. It is particularly problematic to cover non-traditional assets such as bring-your-own devices, IoT, mobile assets, and cloud services.

2 PASSWORD ISSUES

In almost all organizations, there are numerous instances of weak, default and reused passwords, often stored and/or transferred in the clear. Some CISOs and CIOs try to address this problem with strong and difficult to enforce password policies, but even those can’t address the more problematic issue of password reuse, which frequently extends to platforms and accounts beyond the security team’s control.

3

CRITICALITY OF UNPATCHED SYSTEMS

Timely security patching is very challenging, mostly due to the overwhelming weekly volume of new CVEs. Since an accurate notion of risk does not exist, it is therefore very hard to prioritize patches based on risk. Not everything in your network is equally important, but traditional methods either completely ignore or grossly simplify the business criticality of vulnerabilities.

4

PHISHING, WEB AND RANSOMWARE

There is often poor security awareness amongst employees and a lack of modern endpoint security tools and controls. Keeping your enterprise safe starts with identifying your weakest links and putting measures in place to defend them. The weakest links are always some users. Do you know which of your users introduce the most cyber risk exposure to your organization due to their browsing behavior?

5

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. With these attacks coming from 100+ threat vectors, it is extremely difficult to see where you are most at risk.

6

POOR IDENTITY AND ACCESS CONTROL

Identity and access management is sloppy, with many users having excessive system and network privileges. Many enterprises have a manual provisioning and de-provisioning process, making it easy to lose track of who has access to what.

7

ENCRYPTION ISSUES

In most enterprise networks, there is a large amount of unencrypted or incorrectly encrypted communications. Additionally, data is often stored unencrypted or improperly encrypted. Without real-time visibility into your attack surface, it is impossible to keep up with encryption issues.

8

MISCONFIGURATIONS

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. How many configuration items exist in your enterprise that have a cybersecurity related failure mode?

Balbix®

9

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.

10

MALICIOUS INSIDERS

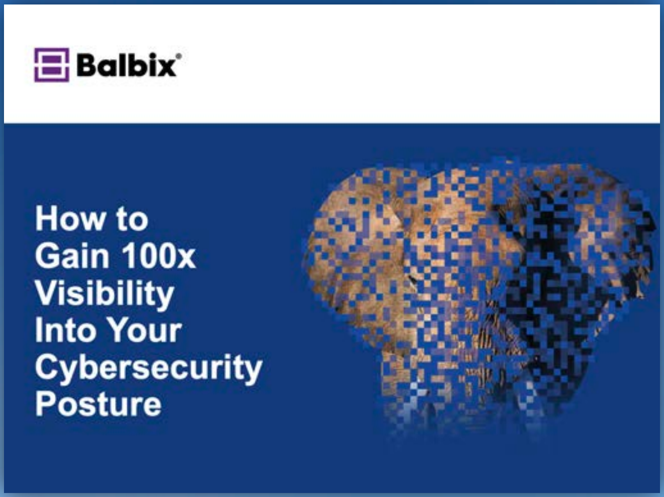
There is inadequate visibility and controls for detecting and preventing rogue users exfiltrating or destroying key data. Most enterprises have trouble detecting and investigating the use of printers, file sharing, or USBs to take IP or data.

Balbix®

ADDRESSING THE BLIND SPOTS

In order to combat the common challenge of blind spots in your cybersecurity posture, CISOs need a way to continuously and comprehensively discover their enterprise attack surface. Analysis of the attack surface should cover on-prem, cloud and mobile assets including unmanaged systems and non-traditional assets. These assets should be monitored continuously and in real-time across 100+ attack vectors.

GAINING CYBERSECURITY POSTURE VISIBILITY WITH BALBIX



Balbix®

How to Gain 100x Visibility Into Your Cybersecurity Posture

Click below to learn more

100x Cybersecurity Posture Visibility

Automatic Asset Inventory