Balbix

# 10 Blind Spots in Your Security Posture

## PASSWORD ISSUES

All enterprises have instances of weak, default, reused passwords, or passwords often stored and/or transferred in the clear.

## NON-TRADITIONAL ASSETS

The foundation of any visibility program is an accurate inventory, including non-traditional assets such as BYOD, IoT, mobile assets, and cloud services.

## CRITICALITY OF UNPATCHED SYSTEMS

Timely security patching is very challenging, due to the volume of new CVEs. However, not everything in your network is equally important.

## PHISHING, WEB AND RANSOMWARE

Do you know which of your users introduce the most cyber risk exposure to your organization due to their browsing behavior?

## POOR IDENTITY AND ACCESS CONTROL

Manual provisioning and de-provisioning process for user access control makes it easy to lose track of who has access to what.

## ENCRYPTION ISSUES

Visibility into unencrypted or improperly encrypted data stored and transmitted in the enterprise brings real security risks.

## MISCONFIGURATIONS

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

## 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.

## MALICIOUS INSIDERS

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

## FLAT NETWORKS

Individual system compromises easily turn into major data breaches if there is no network segmentation.