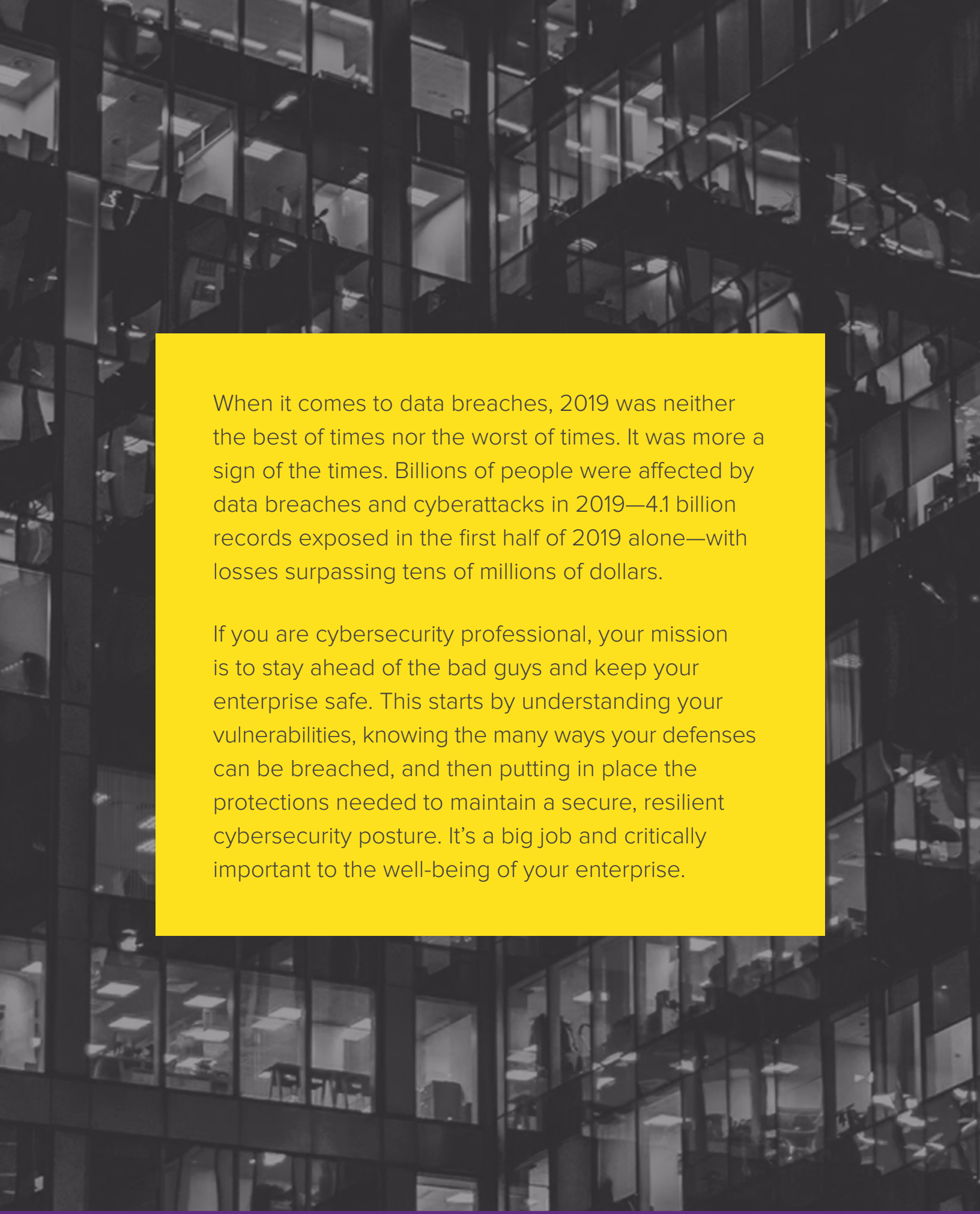
Most Common Cybersecurity Attack Vectors and Breach Methods

Balbix®



When it comes to data breaches, 2019 was neither the best of times nor the worst of times. It was more a sign of the times. Billions of people were affected by data breaches and cyberattacks in 2019—4.1 billion records exposed in the first half of 2019 alone—with losses surpassing tens of millions of dollars.

If you are cybersecurity professional, your mission is to stay ahead of the bad guys and keep your enterprise safe. This starts by understanding your vulnerabilities, knowing the many ways your defenses can be breached, and then putting in place the protections needed to maintain a secure, resilient cybersecurity posture. It's a big job and critically important to the well-being of your enterprise.

Attack surface, attack vectors, and breaches defined

Regardless of business or industry, here are three key terms that lie at the heart of every enterprise's cyber-defenses:

Attack surface—The sum-total of points on a network where attacks can occur where an unauthorized user (the "attacker") can try to manipulate or extract data using a myriad of breach methods (the "***attack vectors***"). If you consider a graph, where the x-axis lists all of the devices and apps on your network (infrastructure, apps, endpoints, IoT, etc.) and the y-axis lists the different breach methods such as weak and default passwords, reused passwords, phishing, social engineering, unpatched software, misconfigurations etc.—the plot is your attack surface.

Attack vector—The method or way by an adversary can breach or infiltrate an entire network/system. Attack vectors enable hackers to exploit system vulnerabilities, including the human element.

Security breach—Any security incident in which sensitive, protected, or confidential data is accessed or stolen by an unauthorized party, jeopardizing an organization's brand, customers, and assets. Incidents such as DDoS, Bitcoin mining etc. are also security breaches. Data breaches are the most common, but not all security incidents concern data theft.

Cyber-attacks 101

Here is a list of today's most frequently launched attacks and the breach methods they use.

Compromised credentials

Compromised credentials describe a case where user credentials, such as usernames and passwords, are exposed to unauthorized entities. This typically happens when unsuspecting users fall prey to phishing attempts and enter their login credentials on fake websites. Privileged access credentials, which give administrative access to devices and systems, typically pose a higher risk to the enterprise than consumer credentials.

And it is not only humans who hold credentials. Servers, network devices and security tools often have passwords that enable integration and communication between devices. In the hands of an intruder, these machine-to-machine credentials can allow movement throughout the enterprise, both vertically and horizontally, giving almost unfettered access.

DO THIS TO AVOID IT:

- Common usernames and weak passwords can lead to compromised credentials, so it's important that the enterprise has effective password policies that ensure suitable password strength.
- Password sharing across services makes all applications that share credentials vulnerable as a consequence of the breach of one service or application in the cohort. Do not reuse the same password to access multiple apps and systems.
- Using two-factor authentication via a trusted second factor can reduce the number of breaches that occur due to compromised credentials within an organization.

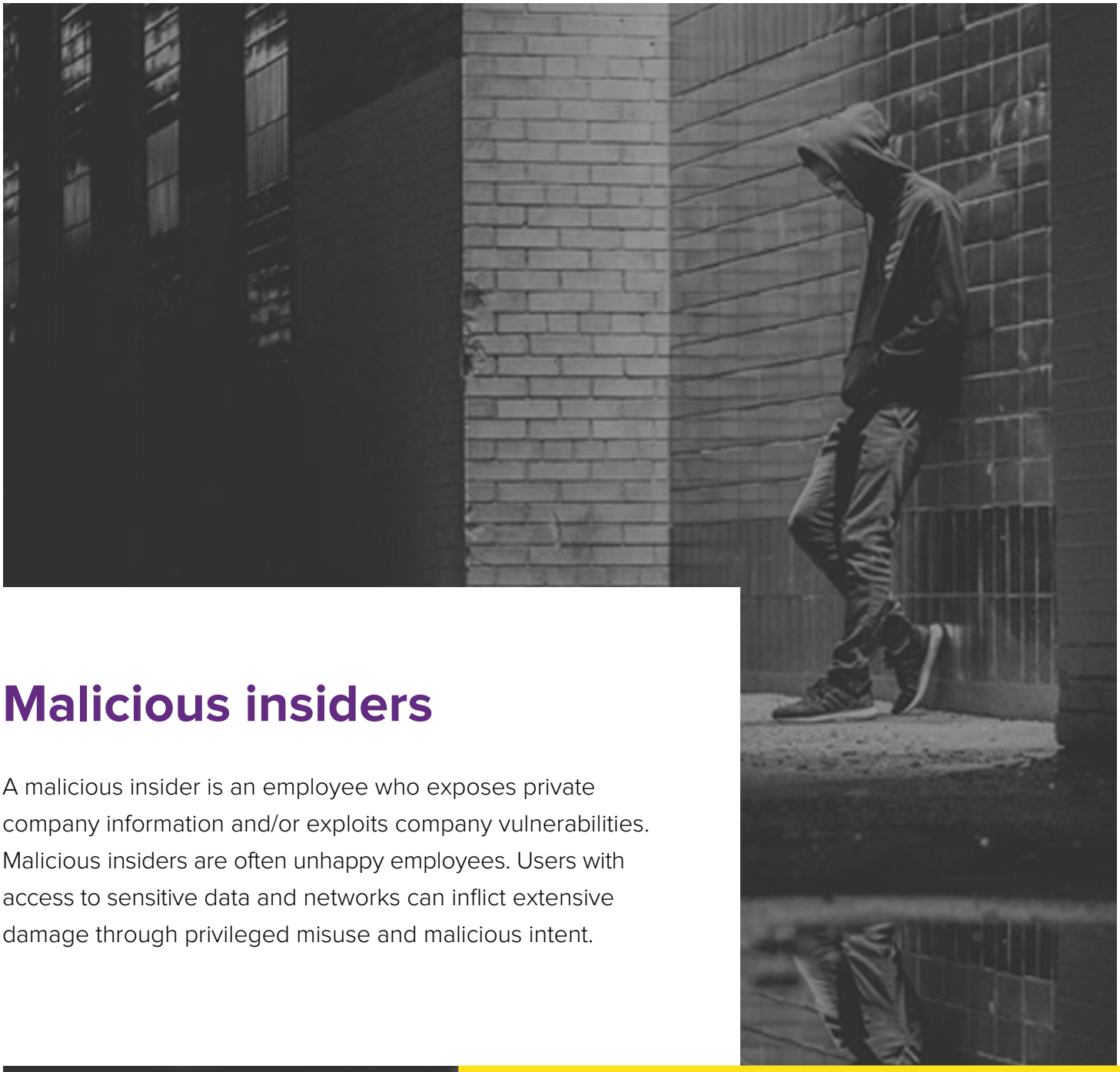
Weak and stolen credentials

Weak passwords and password reuse make credential exposure a gateway for initial attacker access and propagation. Malware attacks such as Mirai highlight this threat not only for managed devices but also IoT connected devices.

Apps and protocols sending login credentials over your network pose a significant security threat. An attacker connected to your network can easily locate and utilize these credentials for lateral movement. For example, in the Target attack, adversaries were able to steal Active Directory credentials and propagate their attack into the enterprise payment network.

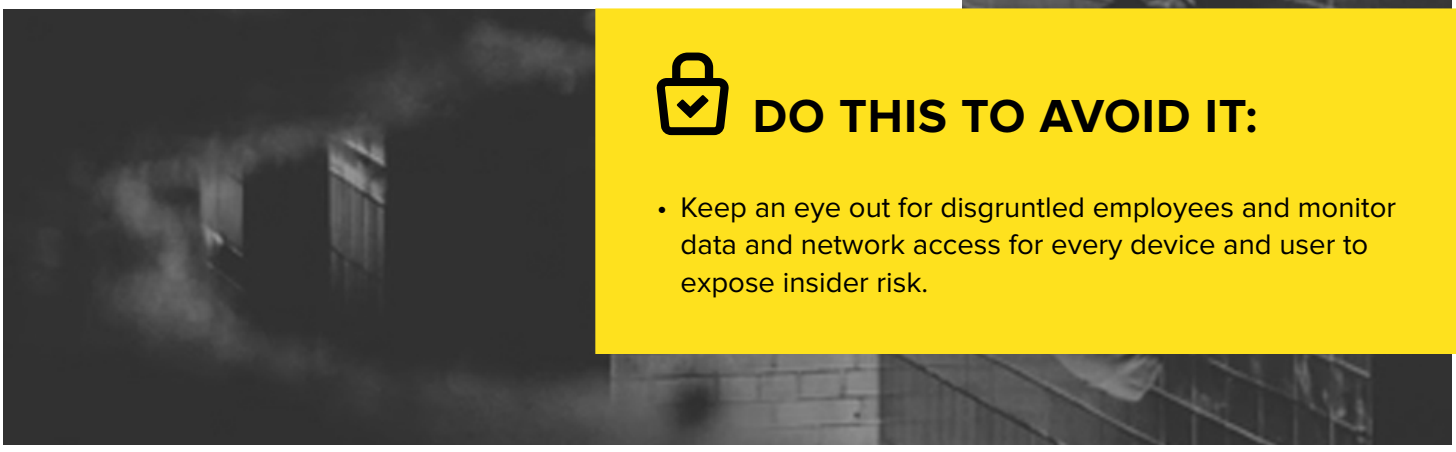
DO THIS TO AVOID IT:

- Track password hygiene and use across your entire enterprise to identify high risk users and their devices.



Malicious insiders

A malicious insider is an employee who exposes private company information and/or exploits company vulnerabilities. Malicious insiders are often unhappy employees. Users with access to sensitive data and networks can inflict extensive damage through privileged misuse and malicious intent.



DO THIS TO AVOID IT:

- Keep an eye out for disgruntled employees and monitor data and network access for every device and user to expose insider risk.

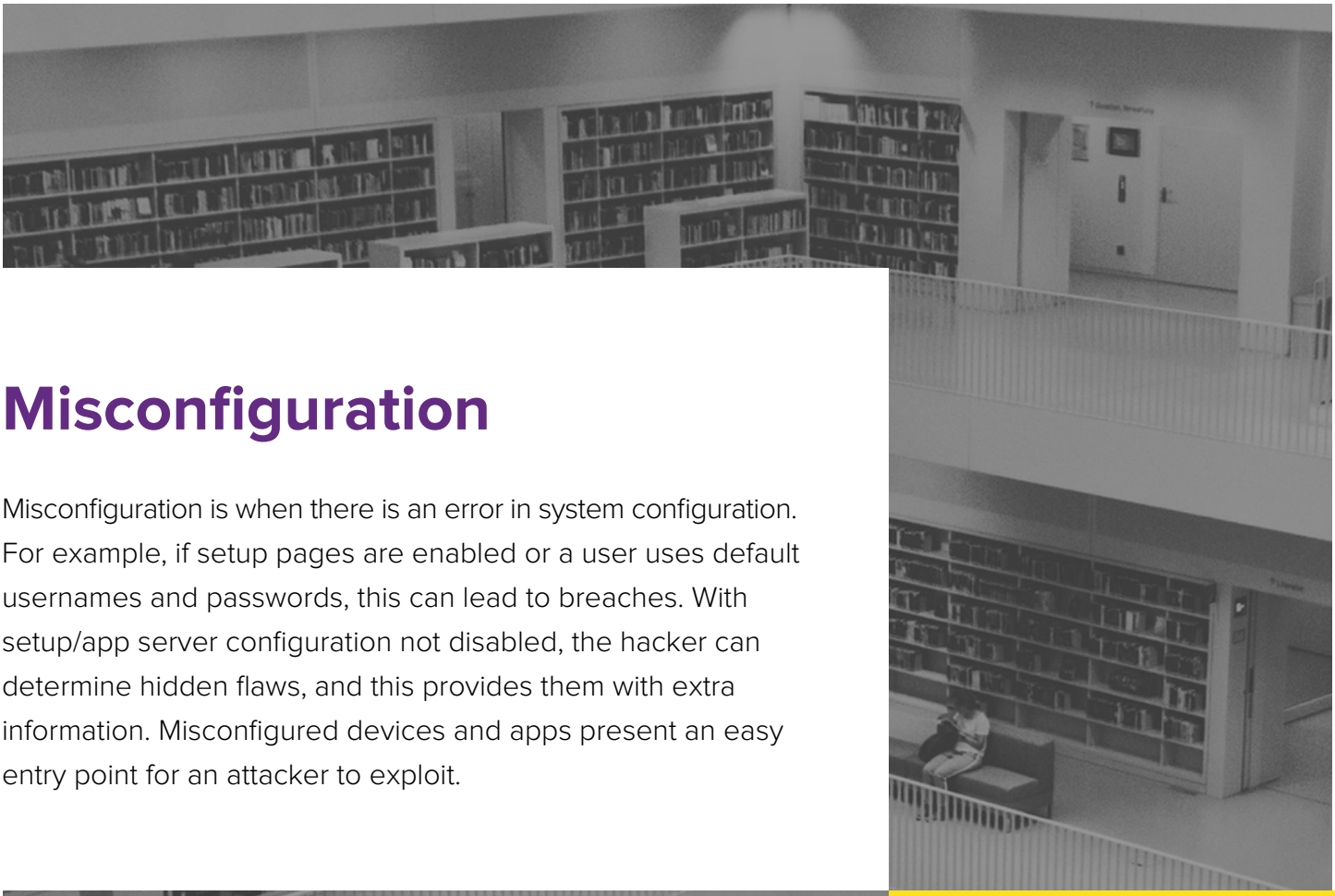
Missing/poor encryption

Data encryption translates data into another form that only people with access to a secret key or password can read. Encrypted data is commonly referred to as ciphertext, while unencrypted data is called plaintext. The purpose of data encryption is to protect digital data confidentiality as it is stored on computer systems and transmitted using the internet or other computer networks. Strong encryption must be applied to data at rest, in-motion, and where suitable, in-processing.

Missing / poor encryption leads to sensitive information including credentials being transmitted either in plaintext, or using weak cryptographic ciphers or protocols. This implies that an adversary intercepting data storage, communication, or processing could get access to sensitive data using brute-force approaches to break weak encryption.

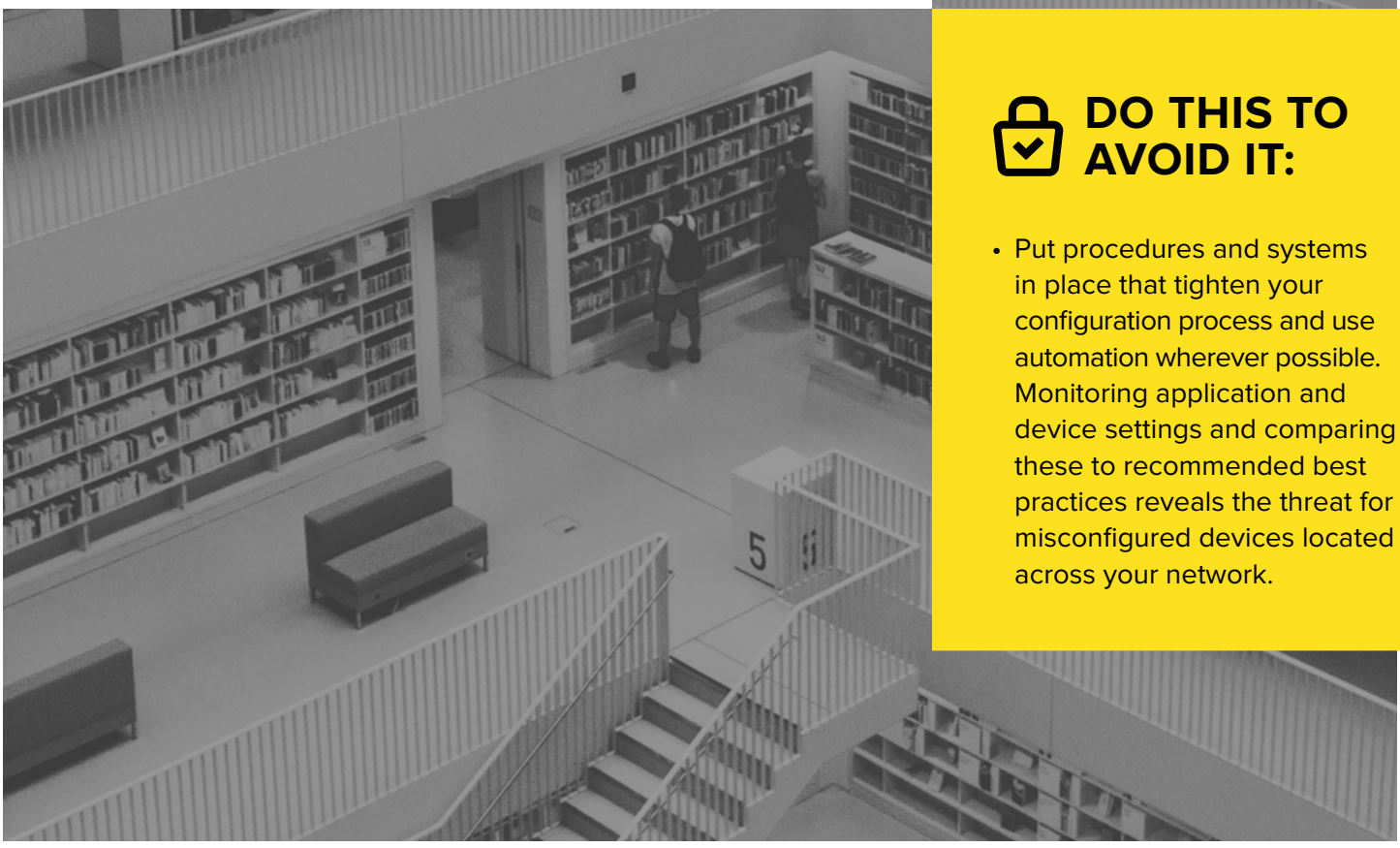
DO THIS TO AVOID IT:

- Don't rely solely on low-level encryption or assume that following compliance means that the data is securely encrypted.
- Ensure that sensitive data is encrypted at rest, in-transit, and in processing.



Misconfiguration

Misconfiguration is when there is an error in system configuration. For example, if setup pages are enabled or a user uses default usernames and passwords, this can lead to breaches. With setup/app server configuration not disabled, the hacker can determine hidden flaws, and this provides them with extra information. Misconfigured devices and apps present an easy entry point for an attacker to exploit.



DO THIS TO AVOID IT:

- Put procedures and systems in place that tighten your configuration process and use automation wherever possible. Monitoring application and device settings and comparing these to recommended best practices reveals the threat for misconfigured devices located across your network.

Ransomware

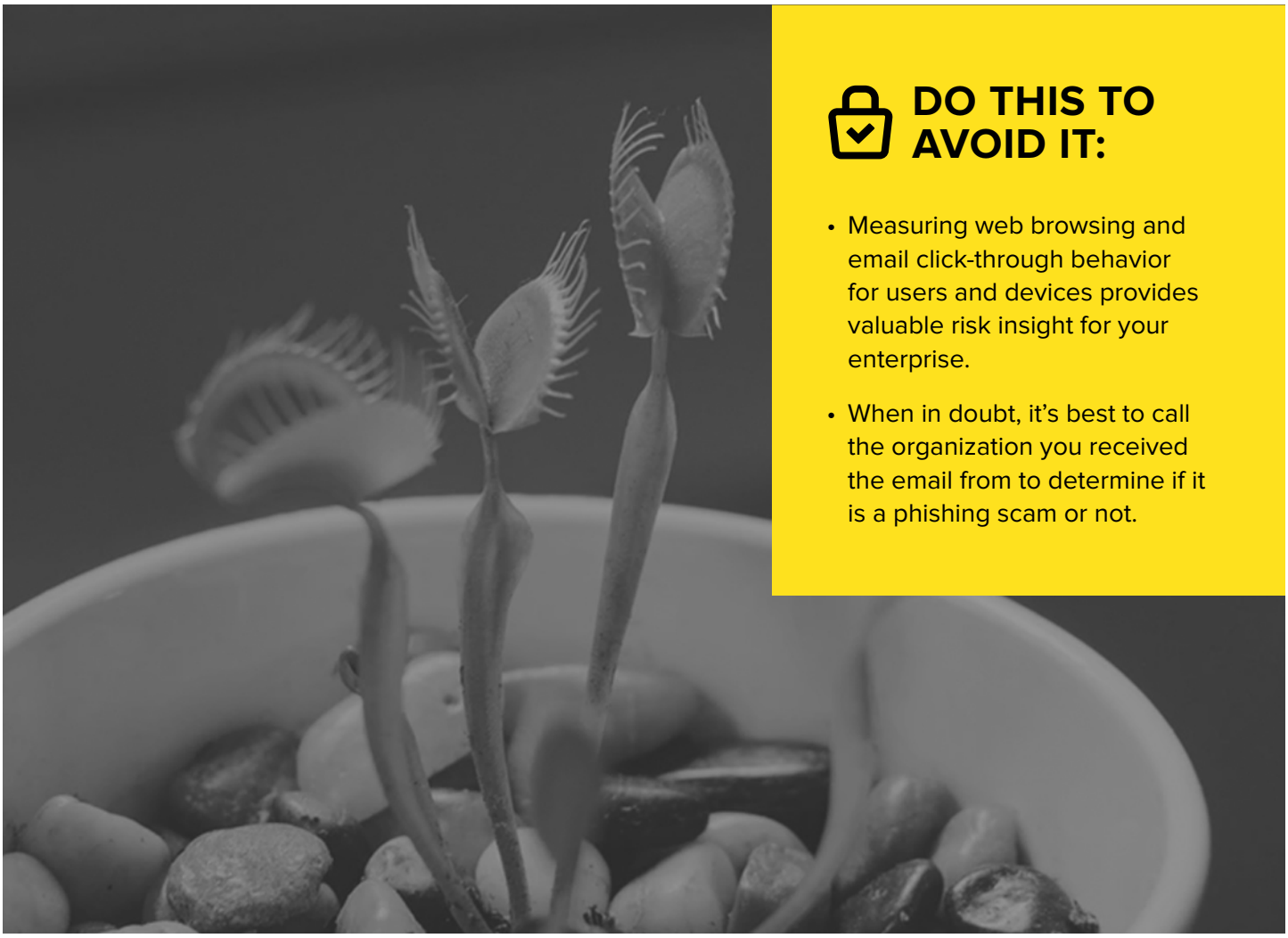
Ransomware is a form of cyber-extortion in which users are unable to access their data until a ransom is paid. Users are shown instructions for how to pay a fee to get the decryption key. The costs can range from a few hundred dollars to thousands, payable to cybercriminals in Bitcoin.

DO THIS TO AVOID IT:

- Make sure you have systems in place that protect all your devices from ransomware including keeping your operating system patched and up-to-date to ensure you have fewer vulnerabilities to exploit and not installing software or giving it administrative privileges unless you know exactly what it is and what it does.

Phishing

Phishing is a cybercrime tactic in which the targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords. It continues to be one of the most effective social engineering attack vectors.



DO THIS TO AVOID IT:

- Measuring web browsing and email click-through behavior for users and devices provides valuable risk insight for your enterprise.
- When in doubt, it's best to call the organization you received the email from to determine if it is a phishing scam or not.

Trust relationships

Trust relationships refer to a certain level of trust that exists between users and systems. For example, trust relationships can connect two domains, so a user only has to log in once in order to access resources. The two domains in a trust relationship are the trusted domain (the domain that authenticates the user the first time), and the trusting domain (the domain that relies on the trusted domain to authenticate users and gives access to its resources without re-authenticating the user). One common breach scenario example is when credentials are cached on the trusted client, which then gets breached, wreaking havoc.

DO THIS TO AVOID IT:

- Managing trust relationships can help you limit or eliminate the impact or damage an attacker can inflict. Google's BeyondCorp is an example of zero-trust security practice.

OTHER BREACH METHODS:

Zero-day vulnerabilities

This is a vulnerability that nobody is aware of until the breach happens (hence the name zero day, as there is no time elapsed between when the attack happens, and the vulnerability is made public). If a developer has not released a patch for the zero-day vulnerability before a hacker exploits that vulnerability, then the following attack is known as a zero-day attack. Having the red team write POC exploits is a way to mitigate zero-day vulnerabilities.

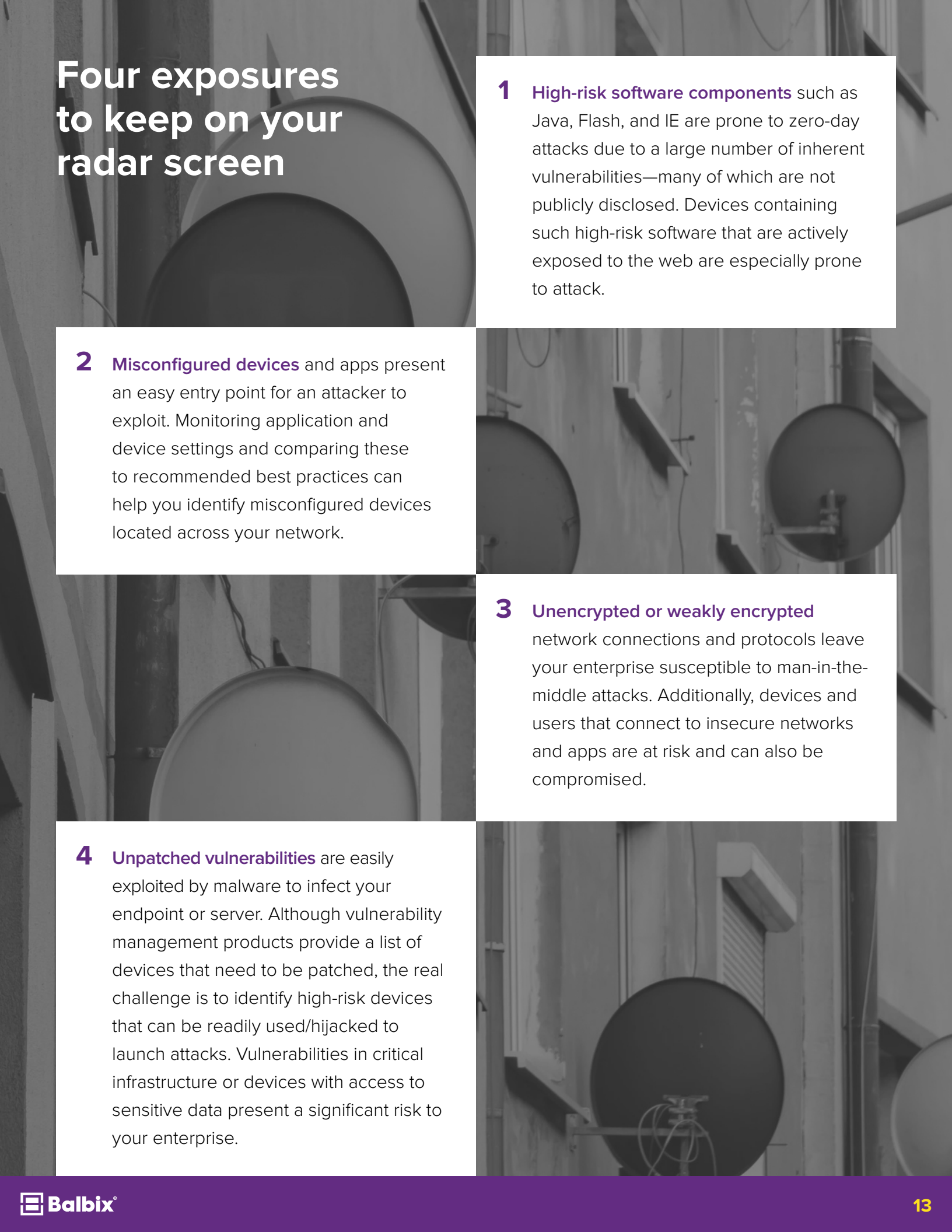
Brute force attack

This is a relentless attack based on trial and error where the hacker attempts to determine passwords or access encrypted data. Similar to the thief who is attempting to crack a safe, the brute force attack tries numerous different combinations until one finally works. Brute force works across all attack vectors described above; including password attacks, breaking weak encryption etc., so it is not technically an attack vector on its own.

DDoS

Distributed Denial of Service (DDoS) is a cyberattack against a network resource (e.g., server, website) by numerous compromised computer systems. The network resource is flooded with extraneous messages, which causes the target to slow down and/or crash, making it inaccessible to authorized users and systems. A DDoS attack normally occurs due to multiple systems being compromised. A potential mitigation method for this is to use CDNs, reverse proxies, HA proxies, etc. that put layers of defense in between systems serving content and clients requesting content.

Four exposures to keep on your radar screen



1 **High-risk software components** such as Java, Flash, and IE are prone to zero-day attacks due to a large number of inherent vulnerabilities—many of which are not publicly disclosed. Devices containing such high-risk software that are actively exposed to the web are especially prone to attack.

2 **Misconfigured devices** and apps present an easy entry point for an attacker to exploit. Monitoring application and device settings and comparing these to recommended best practices can help you identify misconfigured devices located across your network.

3 **Unencrypted or weakly encrypted** network connections and protocols leave your enterprise susceptible to man-in-the-middle attacks. Additionally, devices and users that connect to insecure networks and apps are at risk and can also be compromised.

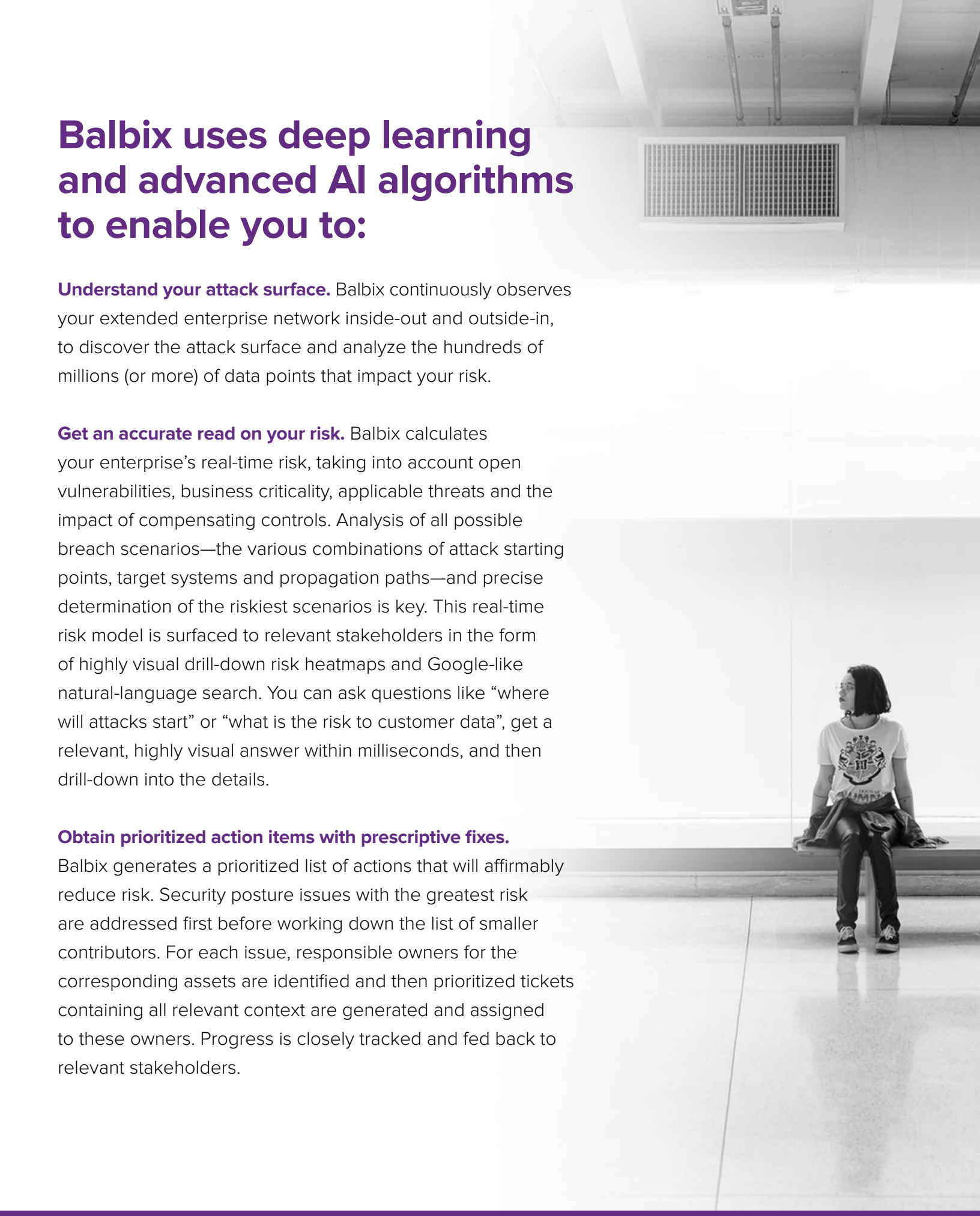
4 **Unpatched vulnerabilities** are easily exploited by malware to infect your endpoint or server. Although vulnerability management products provide a list of devices that need to be patched, the real challenge is to identify high-risk devices that can be readily used/hijacked to launch attacks. Vulnerabilities in critical infrastructure or devices with access to sensitive data present a significant risk to your enterprise.

Balbix uses deep learning and advanced AI algorithms to enable you 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.

Get an accurate read on your risk. Balbix calculates your enterprise's real-time risk, taking into account open vulnerabilities, business criticality, applicable threats and the impact of compensating controls. Analysis of all possible breach scenarios—the various combinations of attack starting points, target systems and propagation paths—and precise determination of the riskiest scenarios is key. This real-time risk model is surfaced 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.

Obtain prioritized action items with prescriptive fixes. Balbix generates a prioritized list of actions that will affirmably reduce risk. Security posture issues with the greatest risk are addressed first before working down the list of smaller contributors. For each issue, responsible owners for the corresponding assets are identified and then prioritized tickets containing all relevant context are generated and assigned to these owners. Progress is closely tracked and fed back to relevant stakeholders.

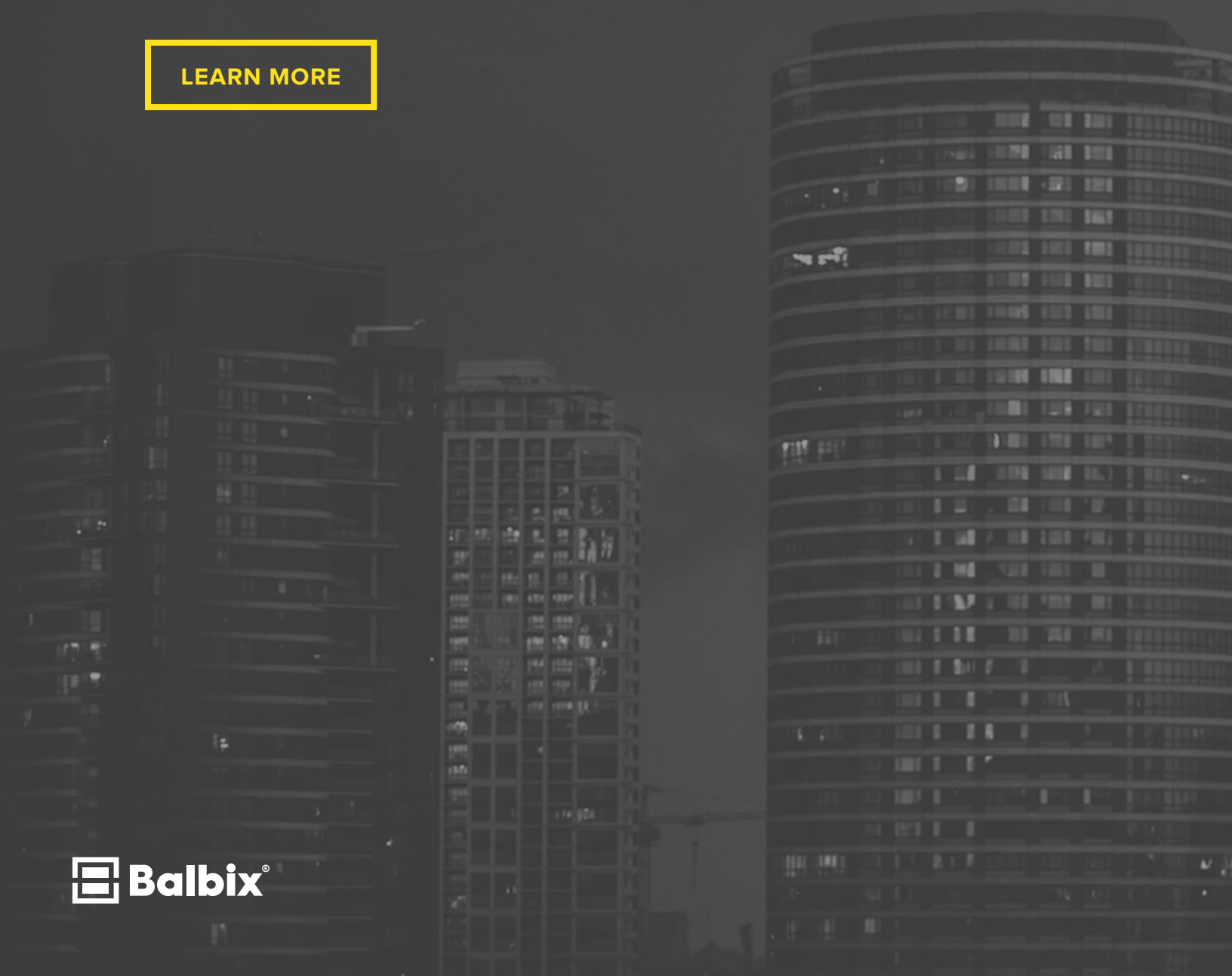


Stay ahead of the game

The ultimate goal of adversaries and malicious insiders is to access your high value devices, apps, and data. Left unsecured, devices and users with access to sensitive apps, data, and networks will pose a significant risk to your enterprise.

To stay ahead of the bad guys, you need to start by understanding your vulnerabilities, knowing the many ways your defenses can be breached, and then putting in place the protections needed to maintain a secure, resilient cybersecurity posture. Keeping the attack surface as small as possible should be considered a basic security measure. Also managing trust relationships can help you limit or eliminate the impact or damage an attacker can inflict.

LEARN MORE



Balbix®