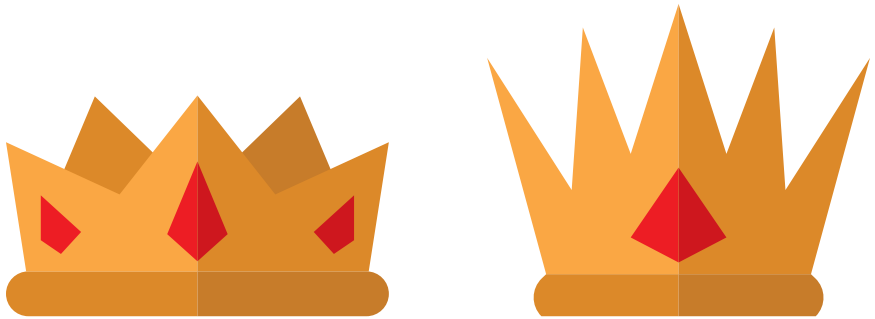
Balbix®

The Definitive Guide to Security Posture

Contents

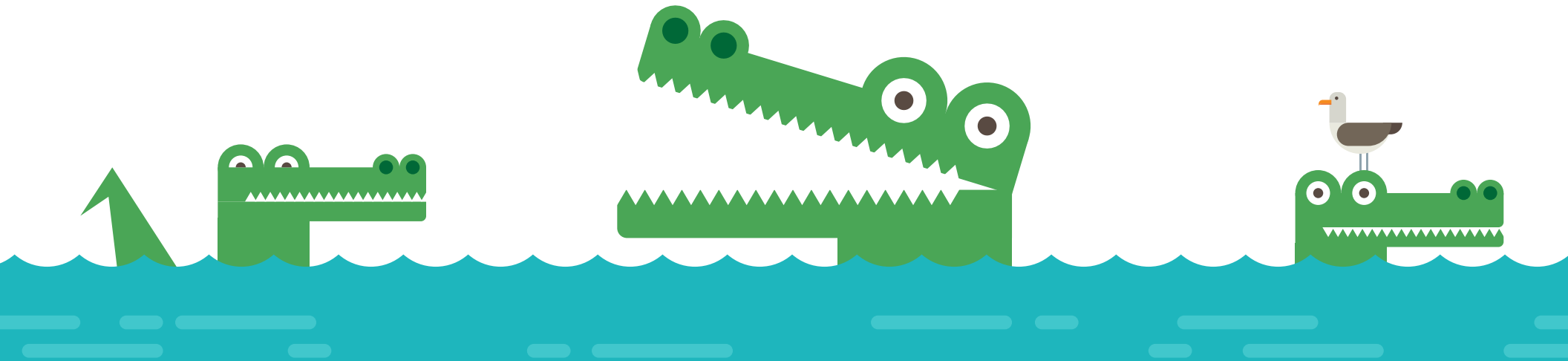


Executive Summary

With thousands of assets in your enterprise and each susceptible to a myriad of different attack vectors, there are millions of ways by which your enterprise can be breached. There is a multifold increase in cybersecurity complexity, security teams are drowning in cybersecurity data with few actionable insights and general poor cybersecurity hygiene, such as a weak password or an unpatched exposed Internet-facing system, all present an open door for attackers.

So how do CISOs wrap their arms around these cybersecurity challenges and protect their enterprise? Your first line of defense against the adversary is a good cybersecurity posture. This Definitive Guide to Security Posture will:

- Define “security posture”
- Delve into the importance, challenges and best practices for getting an accurate asset inventory
- Explain cyber risk and how to measure your attack surface
- Provide strategies to strengthen your security 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. According to a recent McKinsey survey, 75 percent of experts consider cybersecurity to be a top priority. But while there is more awareness on cybersecurity, there is also a lot of confusion. Executives are overwhelmed by the challenge and only 16% say their enterprises are well prepared to deal with cyber risk. And only 1 in 3 say that they are confident that they can avoid breaches. The hard truth is that most organizations only have a vague understanding of their attack surface and overall cybersecurity posture.

While 75% of experts consider cybersecurity to be a top priority, only 16% say they are equipped to deal with cyber risk.

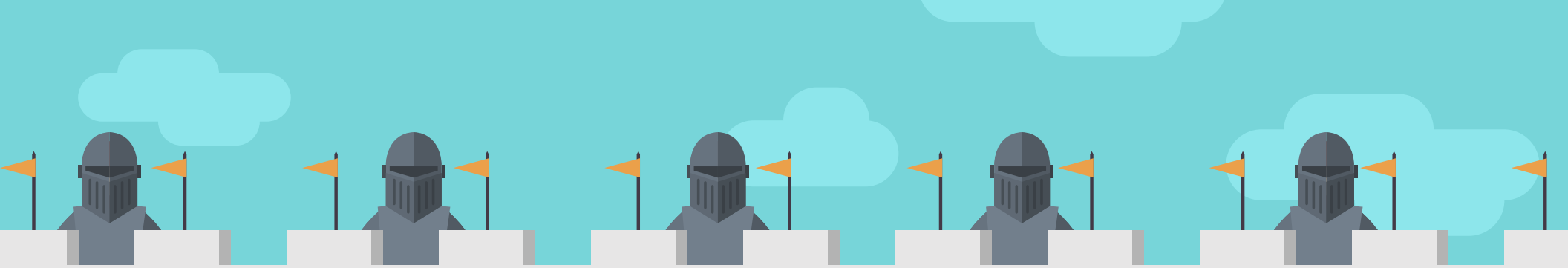
Some sobering statistics

- Around 16 billion records have been exposed in the first half of 2020.
- According to researchers, 8.4 billion records were exposed in the first quarter of 2020 alone, a 273% increase from the first half of 2019 which saw only 4.1 billion exposed.
- According to the 2019 Cost of Data Breach Report from Ponemon Institute, the global average cost of a data breach has grown by 12 percent in the last five years to $3.92 million.
- Damage related to cybercrime is projected to hit $6 trillion annually by 2021

So, what should executives and CISOs do? With a substantial level of threat facing the enterprise and high stakes in terms of revenue and reputation, executives and CISOs must increase their cyber resilience and strengthen their enterprise security posture.

Questions that enterprises must consider

1. What are our most valuable assets?
2. Are our current security controls effective?
3. What are some potential threats we are facing?
4. What is our overall cyber risk exposure?



Defining Security Posture

What is security posture

Your security posture is the overall security status of all your software and hardware assets, networks, services, and information. It also includes the controls and measure you have in place to protect your enterprise from cyber-attacks, your ability to manage your defenses and your readiness and ability to react to and recover from security events.

A conceptual diagram representing your security posture would look something like this:

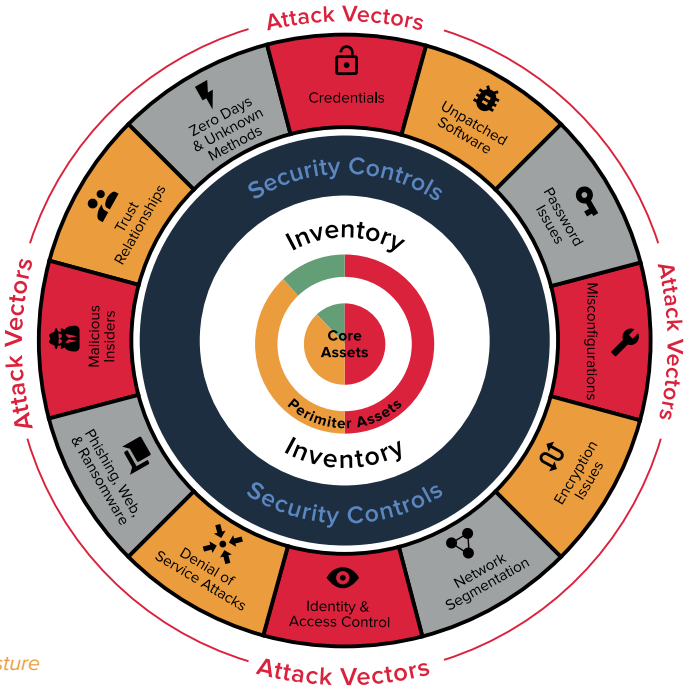


Fig 1:
Security posture

At the very core of understanding your security posture is an accurate inventory of all your assets, including both core and perimeter assets. This includes on-premises, cloud, mobile, and 3rd party assets; managed and unmanaged assets; applications and infrastructure, catalogued based on geographic location. It is important to understand the business criticality of each asset as well, as this is an important component of calculating breach risk.

Surrounding this core is an enumeration of your existing security controls, deployed to manage your defenses. Inherent in this enumeration is also an understanding of how effective these controls are in reducing your cyber risk.

Outside of that circle are the various risk items and attack vectors. Attack vectors are the methods that adversaries use to breach or infiltrate your network. Attack vectors take many different forms, ranging from malware and ransomware, to man-in-the-middle attacks, compromised credentials, and phishing. Some attack vectors target weaknesses in your security and overall infrastructure, others target weaknesses in the humans that have access to your network.

This combination of your inventory, security controls, and defenses against numerous attack vectors makes up your attack surface. Your attack surface is represented by all of the points on your network where an adversary can attempt to gain entry to your information systems. Basically, any technique that a human can use to gain unauthorized access to your company's data via any asset.

And keep in mind that risk extends beyond unpatched software vulnerabilities (CVEs). Your ability to monitor your assets in risk areas such as unpatched software, password issues, misconfigurations, encryption issues, phishing, web and ransomware, denial of service attacks and many others is the mainstay of your security posture.

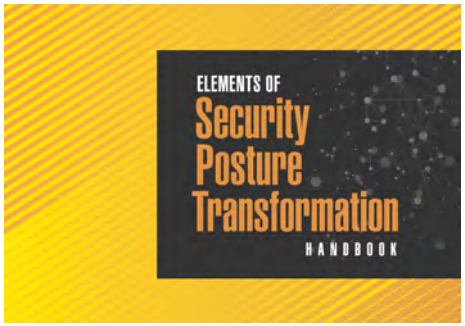
The stronger and more resilient your security posture, the lower your cyber risk and greater your cyber-resilience. Therefore, understanding the full scope of your security posture and correctly prioritizing areas of relevant risk is essential to protecting your organization against breaches.

Cybersecurity is a complex problem to solve

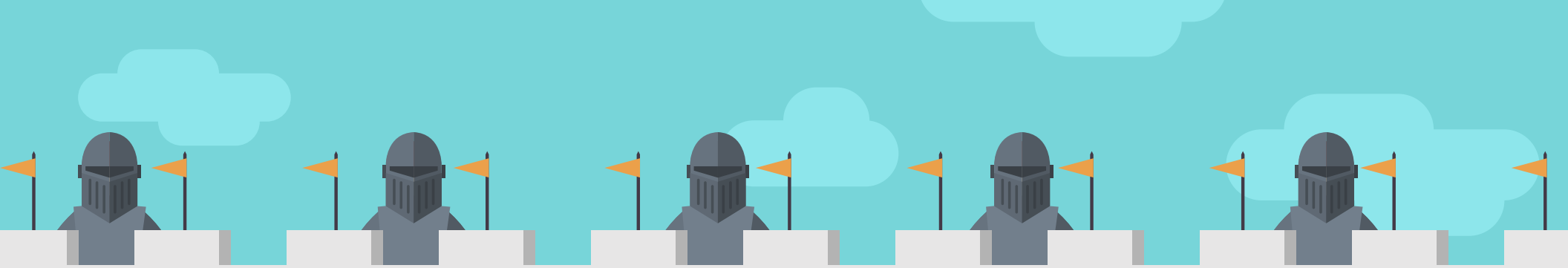
Understanding and defining the full scope of your cybersecurity posture is essential to protecting your business against breaches. To understand, optimize and strengthen your security posture, you need to:

- Analyze your current security posture
- Identify protection gaps that are increasing risk
- Then take action to eliminate those gaps

This guide explains in detail what an organization's security posture is, how you can define and measure it and the steps you need to take to improve it.



Elements of Security Posture Transformation Handbook.



About Asset Inventory

Inventory—the core of your security posture

Asset inventory is an accurate and up to date count of all hardware, software, and network assets in your enterprise. However, being aware of an asset isn't sufficient. You also need to know detailed information about each asset and whether or not that asset is a risk. This involves:

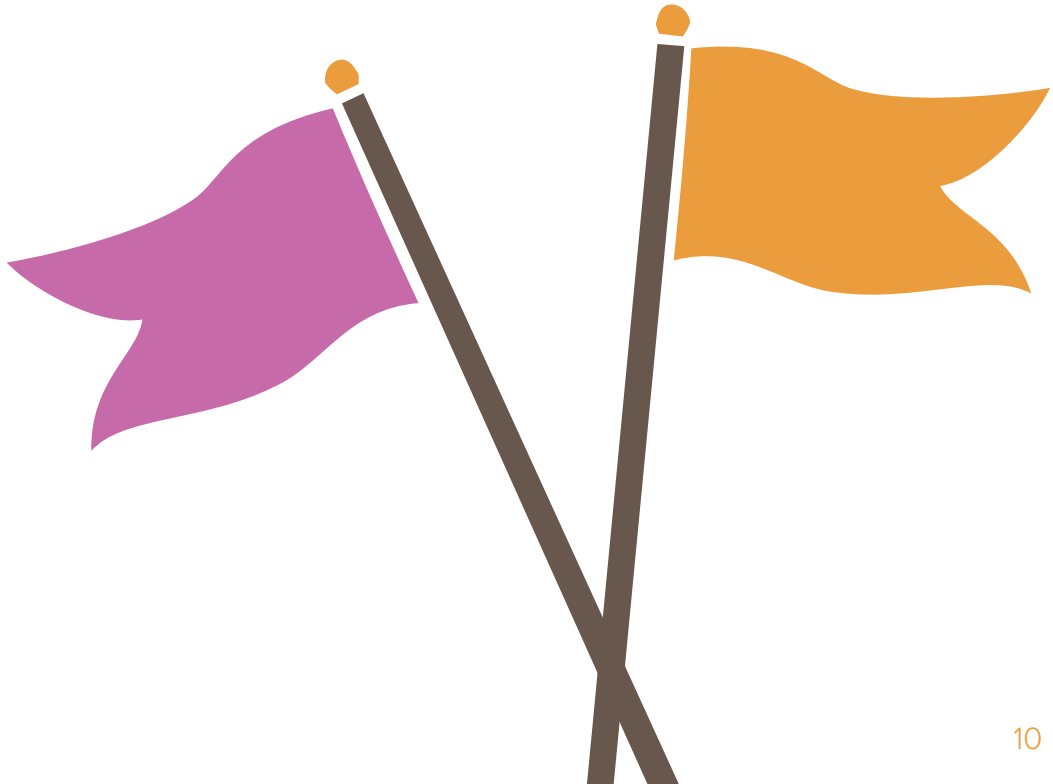
1. Categorizing assets by type of asset, role, and geo location including in-depth information like software and hardware details, status of ports, user accounts, roles, and services linked to that asset
2. Determining business criticality of each asset
3. Ensuring that all assets are running properly licensed and updated software while adhering to overall security policy
4. Continuously monitoring them to get a real time picture of their risk profile and their lifecycle management
5. Creating triggered actions whenever an asset deviates from enterprise security policy
6. Deciding which assets should be decommissioned if no longer updated or being used

What is an IT asset?

It is essentially any device, application, service, or cloud instance that has access to your enterprise network or data.

The importance of inventory

Getting an accurate IT asset inventory is foundational to your security posture. The ability to track and audit your inventory is a baseline requirement for most security standards, including the CIS Top 20, HIPAA, and PCI. Having an accurate, up-to-date asset inventory also ensures your company can keep track of the type and age of hardware in use. By keeping track of this information, you are more easily able to identify technology gaps and refresh cycles. As systems begin to age, and are no longer supported by the manufacturer, they present a security risk to your organization as a whole. Unsupported software that no longer receives updates from the manufacturer brings the risk of not being monitored for new vulnerabilities and implementation of patches.



Inventory challenges

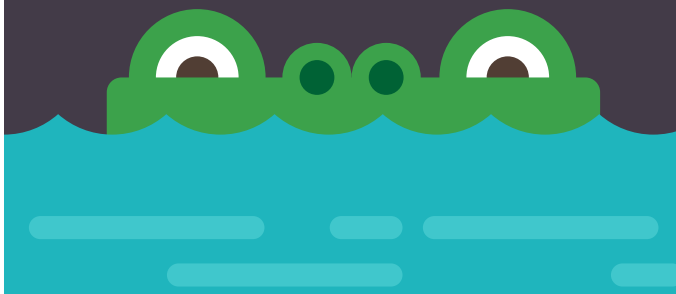
Unfortunately, it is challenging to keep track of the various devices, applications, and services used by enterprise users. As a result, it is difficult to correctly target vulnerability scans and risk assessments. It is particularly problematic to cover non-traditional assets such as bring-your-own devices, IoT, mobile assets, and cloud services.

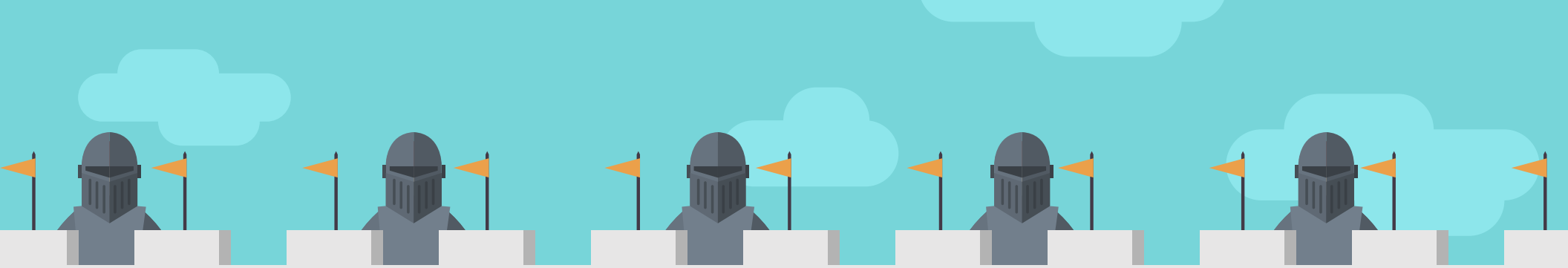
- The set of assets in the enterprise changes constantly with devices being added and retired, physical machines migrating to virtual and various stakeholders constantly installing and updating software (with or without approval).
- Inaccurate inventory makes managing compliance and cyber-risk very difficult.
- An outdated inventory impedes the velocity of business.
- Applying manual effort to keep inventory updated is very time and resource intensive and does not work at scale.
- Enterprise security teams don't often control all assets, which makes the task of understanding Your assets and gathering insights about them even more difficult.

Traditional inventory tools typically only track managed assets. Non-traditional assets like IoT are either left undiscovered or partially tracked by a motley collection of specialized tools, one for each asset category.

Do you know

1. What type of devices are on your network?
2. Where does the sensitive data reside?
3. Who has access to the sensitive data?
4. How many devices are utilizing a particular current security control?
5. What is the OS and distribution of devices on the network?
6. What is the number and type of approved applications on workstations?
7. How many and what types of assets are up to date on OS patches?
8. Which assets are up to date on application patches?





Enterprise Attack Surface

Enterprise attack surface

The second most important aspect of your security posture is measurement and mapping of your attack surface. So, what is your enterprise attack surface and how can you measure it?

Your attack surface is represented by all of the points on your network where an adversary can attempt to gain entry to your information systems. For a medium to large sized enterprise, the attack surface can be gigantic. Hundreds of thousands of assets potentially targeted by hundreds of attack vectors can mean that your attack surface is made up of tens of millions to hundreds of billions of signals that must be monitored at all times.

The graph below represents your attack surface. The x-axis represents all of your assets—everything from traditional infrastructure, servers, databases, switches and routers, etc., and your apps, endpoints—managed, unmanaged, BYOD, mobile phones and tablets, IoTs. This also includes cloud apps—personal applications of employees—Google, Gmail, LinkedIn, etc., official SaaS applications, public facing web sites. At the right end of the x-axis are 3rd party vendors who bring risk into your network because of certain trust relationships.

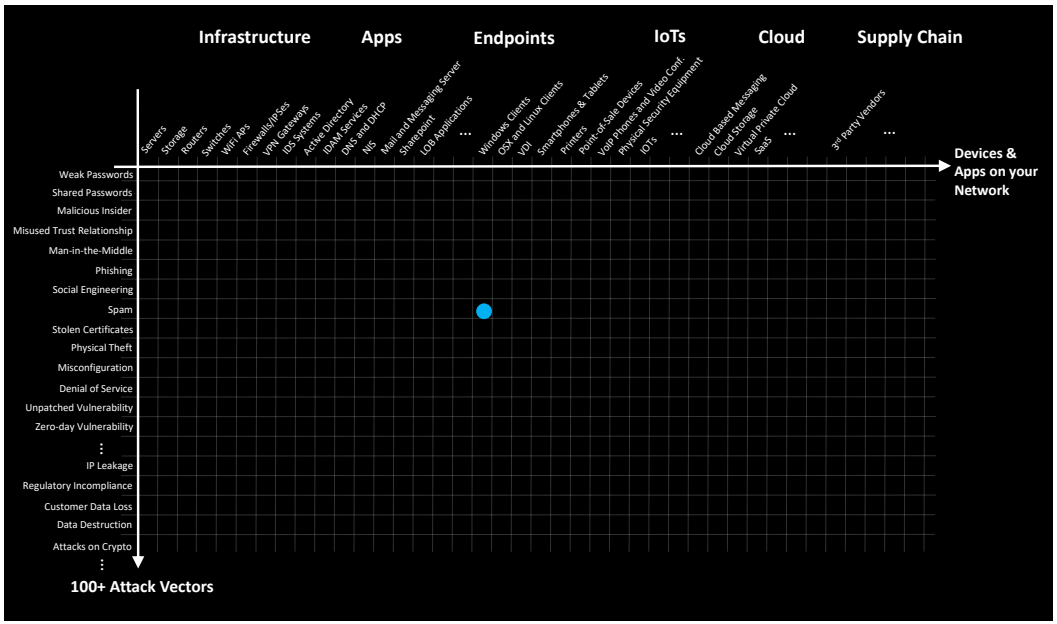


Fig 2:
Enterprise attack surface

What is an Attack Vector?

Attack vectors are the methods that adversaries use to breach or infiltrate your network. Attack vectors take many different forms, ranging from malware and ransomware, to man-in-the-middle attacks, compromised credentials, and phishing. Some attack vectors target weaknesses in your security and overall infrastructure, others target weaknesses in the humans that have access to your network. Some of the common attack vectors are:

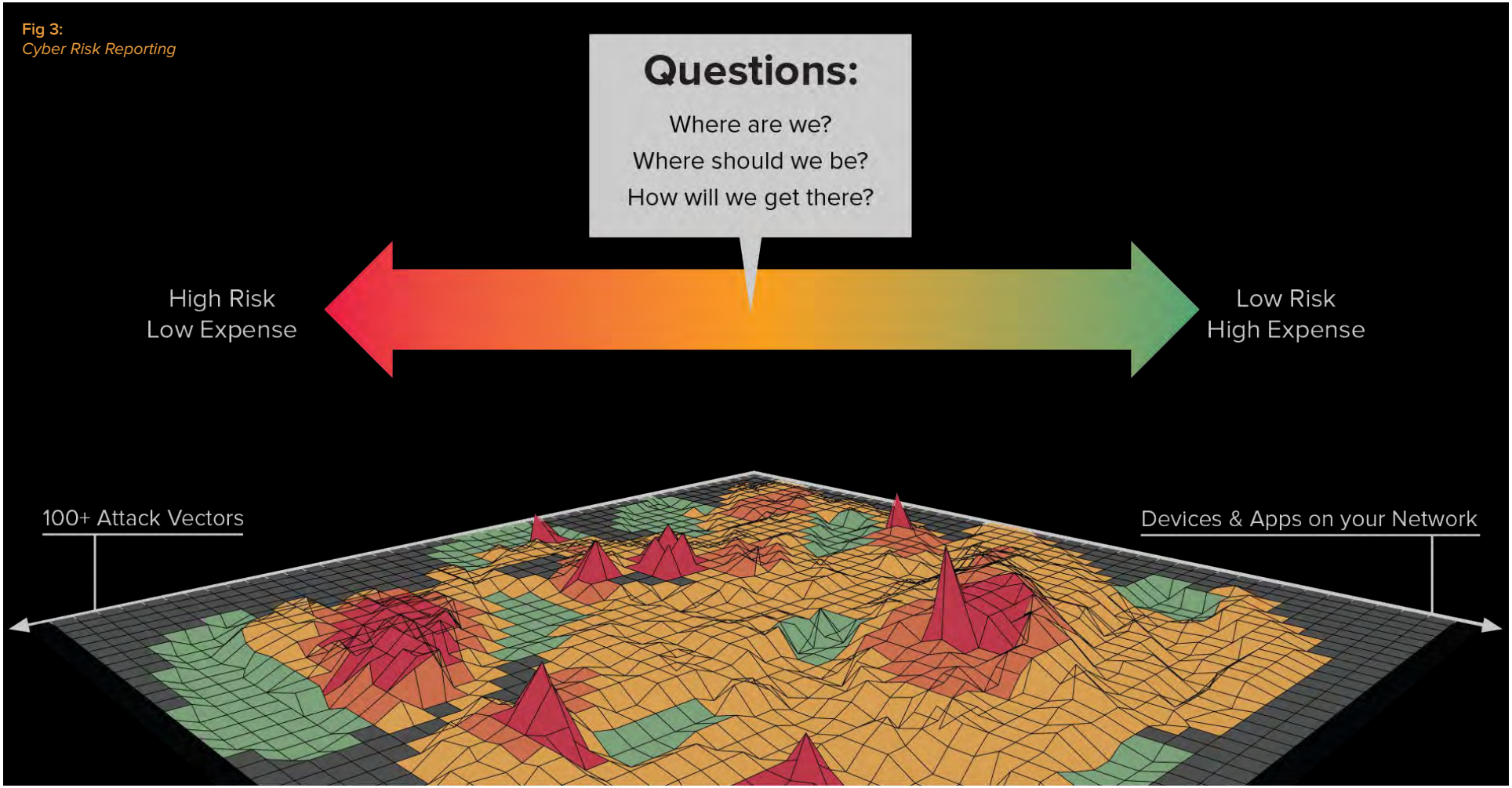
- Compromised Credentials
- Weak & Stolen Credentials
- Malicious Insider
- Missing or Poor Encryption
- Misconfiguration
- Ransomware
- Phishing
- Trust Relationships

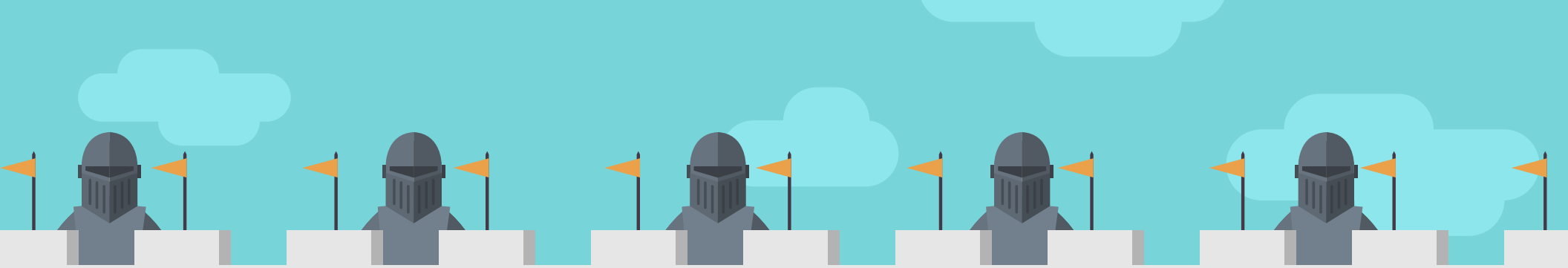
The y-axis represents the hundreds of attack vectors available to your adversaries, ranging from simple things like weak passwords, to more complex things like phishing, unpatched software, encryption issues, misconfiguration, etc. The y-axis also has zero-day vulnerabilities, security bugs that are “unknown” until they are first used by the adversary.

This gigantic x-y plot is your attack surface. In a typical breach, the adversary uses some point on this attack surface to compromise an (Internet facing) asset. Other points are then used to move laterally across the enterprise, compromise some valuable asset, and then to exfiltrate data or do some damage.

The entry point for cyber attackers can be as trivial as a Wi-Fi-enabled camera used to take pictures at the company’s summer picnic.

Fig 3:
Cyber Risk Reporting





Your Enterprise Security Posture

3 truths about your security posture status quo

1. Project oriented approach

Most organizations' current security posture consists of tools that have been deployed as a result of addressing security projects. This project-oriented approach to security is one where teams are focused on completing security projects off of to-do lists without having any real insight into whether or not these projects have a meaningful impact on your organization's security posture. This results in narrowly focused security practices.

2. Reactive tactics

Nearly all new security spending and effort is directed toward detecting an attack in progress or responding to one that has already occurred. While putting out security "fires" is an essential practice; the bulk of your security investments should not be reactive.

3. Misalignment with attack vectors

Are you spending most of your security efforts on fixing indicators of compromise (IoC) alerts, patching, and chasing commitment biases, without really knowing the answers to questions like which of my assets are most critical, what threats are active right now, or which of my assets are most vulnerable?

Continuing to dedicate time, resources, and budget toward fixing problems without having a clear understanding of how those actions reduce the company's overall cyber-risk is not fruitful. Your existing security practices need to be evaluated with a fresh lens to understand your current security posture, find gaps, and then take action to fill those gaps and improve your security posture.

Challenges in accurately understanding your security posture stem from 4 factors:

1. Lack of visibility
2. Lack of structure
3. Lack of clarity
4. Lack of up to date data

4 reasons why your visibility into security posture is inadequate

1. Technology Sprawl

Blind spots appear progressively over time as an organization grows, matures, and adopts new technologies, adds new people, makes acquisitions, and embraces new processes. Cloud computing, mobility, IoT and other aspects of digital transformation have been a major contributing factor in recent years.

IoT Security—challenging but essential

IoT devices are purposefully designed to connect to a network. In large complex enterprises, IoT devices simply end up being connected to the internet with little management or oversight. Some IoT devices may even communicate basic telemetry back to the device manufacturer or have means to receive software updates.

This presents a challenge for security teams because such devices must still be identified, maintained, and monitored. In most cases however, the security teams or security operations center don't know they exist on the network. This means that the potential for security vulnerabilities that can be directly exploited by hackers to breach your critical systems laterally move within your network is immense.

"There were 105 million attacks on IoT devices coming from 276,000 unique IP addresses in the first six months of 2019, compared with just 12 million attacks in the first half of 2018."

Compounding the risk from lack of visibility, there is also the issue that IoT devices often have proprietary interfaces and embedded operating systems. This makes it difficult for security teams to understand if they are running vulnerable software or dealing with misconfigurations.

Security patches are typically not available, and even if they are, the devices themselves may have no built-in ability to be patched remotely. They may be in physically remote or inaccessible locations, or downtime may not be an option. Another issue cited with IoT security is the use of hard-coded or default passwords.

No recent incident more clearly exposed just how vulnerable enterprises are with the security of their IoT hardware than the Mirai botnet attack in 2016. Mirai logged in to devices leveraging frequently used default username/password combos and was able to amass an army of compromised IP cameras and routers, ready to do its bidding. At the time, it was the most powerful DDoS attack the world had seen.

2. Whose job is it, anyway?

Enterprise security teams obviously don't control all aspects of the business and rely heavily on cooperation from other departments and business units to loop security in at the right time before launching new products and buying new software and assets etc.

3. Legacy point products

Large enterprises have a plethora of traditional and legacy tools that don't work together synergistically, leading to a motley collection of specialized tools to do various jobs. It is challenging to get the findings and results of all the tools under one single dashboard thus key data and observations are routinely missed.

4. Not a human-scale problem

Analyzing and understanding the enterprise security posture is no longer a human scale problem because to get an accurate idea of breach risk, security teams need to analyze a lot of data—up to several hundred billion time-varying signals from the extended network of devices, apps and users. This requires the use of AI to automatically identify, monitor, analyze and prioritize action items based on risk and business criticality.

Growing complexity makes your enterprise more vulnerable

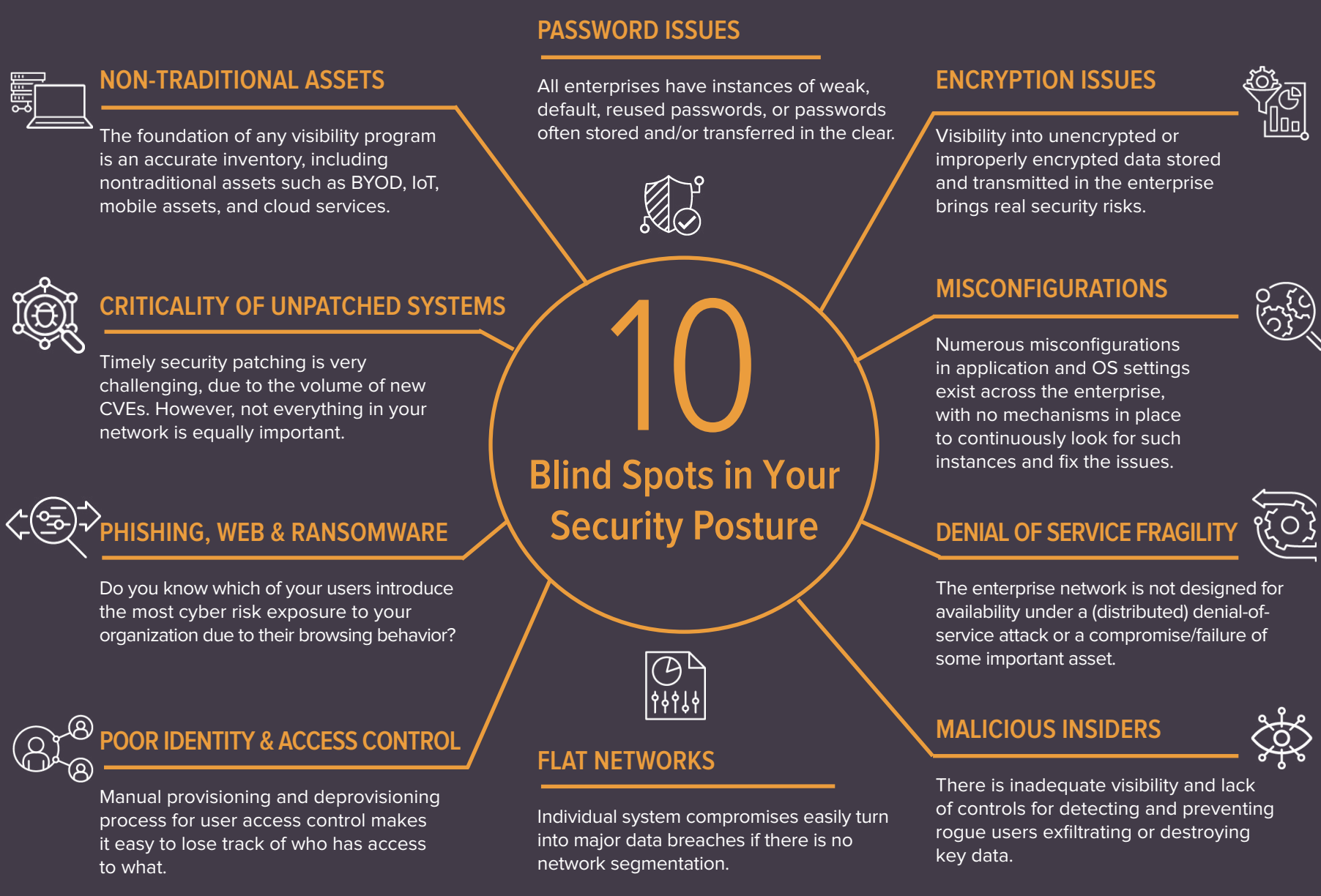
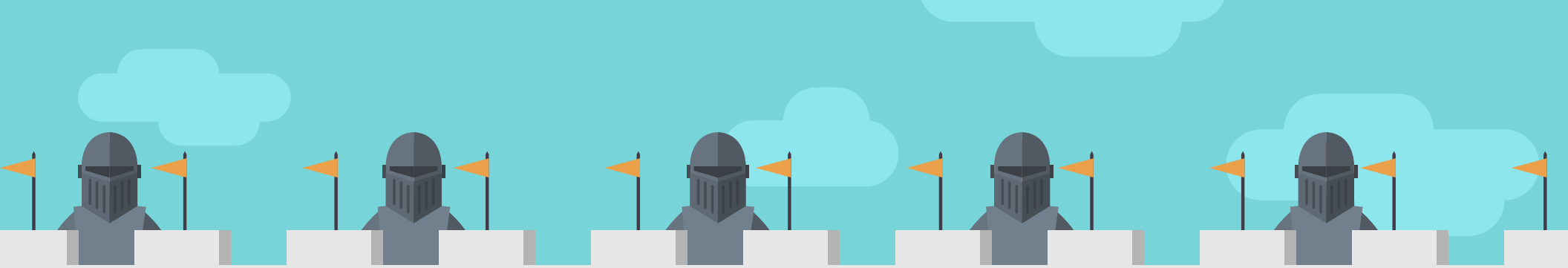


Fig 4:
Security posture blind spots



Understanding Cyber Risk

What is cyber risk

Let's take a detour into understanding cyber risk. Your cyber risk has an inverse relationship with your security posture. As your security posture becomes more robust and stronger, your cyber risk decreases proportionally.

Risk is defined as the probability of a loss event (likelihood) multiplied by the magnitude of loss resulting from that loss event (impact). Cyber risk is the probability of exposure or potential loss resulting from a cyberattack or data breach. Per NIST, cyber risk is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization.

Mathematically, cyber risk can me denoted by multiplying likelihood of breach and it's impact:

risk = likelihood x impact

Where does risk come from?

With digital transformation, increase in globalization, and distributed workforce, there is an interconnected web of employees, customer, and third-party vendors linked to the enterprise network. As described earlier, your IT assets, together with the attack vectors they are susceptible to, make up your attack surface and every point on this attack surface represents a potential area of compromise, and therefore, risk.

The myth of defense in depth

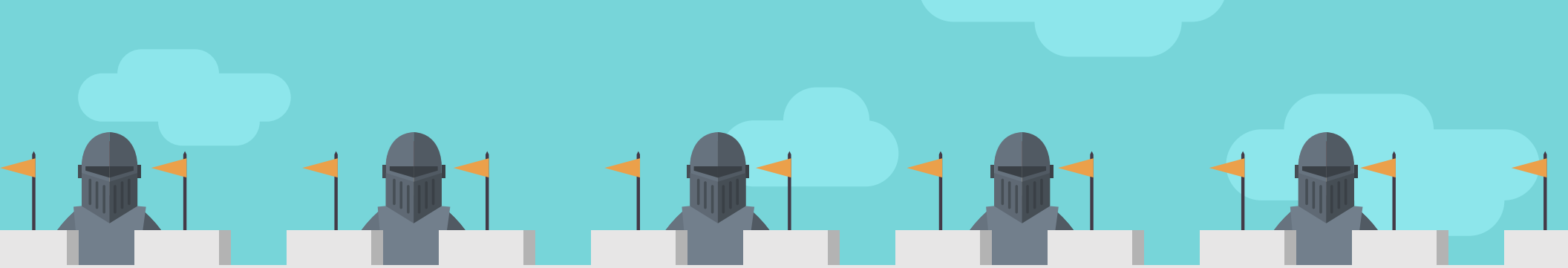
"Defense in depth" is an overused phrase in cybersecurity. It generally really means "spending in depth"—in other words, keep doing what you were doing, but add more security products and services, which invariably increases cost and complexity. While many security programs are underfunded, over the years there has been minimal correlation between the level of security spending and the level of business damage caused by security incidents.

There are several reasons for this:

- Simply adding layers of security products increases complexity, requires security staff skills that are hard to find and often results in more disruption to business operations than to attackers.
- The enterprises with the lowest levels of damage almost invariably are the ones with strong security teams that avoid the most vulnerabilities by proactively driving change in IT operations and procurement to minimize vulnerabilities and misconfigurations in IT systems and applications.
- Because it is impossible to avoid all vulnerabilities, prioritizing staff resources and procurement of security products and services to address the areas of highest risk first and most frequently is key to both effective and efficient cybersecurity.

To address continually evolving threat scenarios and real-world budget and staffing constraints,

well-defined and integrated security processes, backed by "force multiplier" tools, are needed.



Assessing Your Security Posture

Likelihood of breach

The likelihood of a breach, as defined by NIST, is a weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability. An intuitive notion that all security practitioners agree with is that given enough effort, anything can be breached. Graphically, the Breach Likelihood vs Effort concept is depicted below (Figure 5).

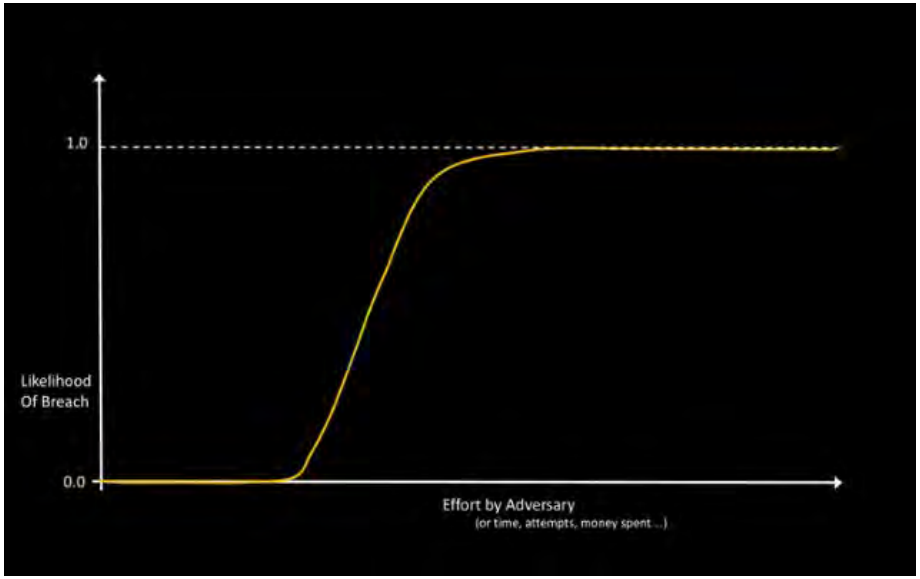


Fig 5:
Breach Likelihood vs Effort

Every enterprise has a Breach Likelihood vs Effort curve like the one shown in Figure 5 above.

However, the placement of the knee of the curve on the x-axis, and the slope of the rise from 0 to 1 may be different. Intuitively, you might think that a security-mature company like a Fortune 500 bank might have the knee of the curve well towards the right of the axis. A smaller company, with a less mature cybersecurity program, might have the knee shifted more towards the left (Figure 6). This is largely true. But there is also a natural entropy in play that tends to move larger, more complex networks closer to the left. All else equal, the larger attack surface makes it easier to break into a network with 10,000 moving parts than it is to break into a network with 10 moving parts.

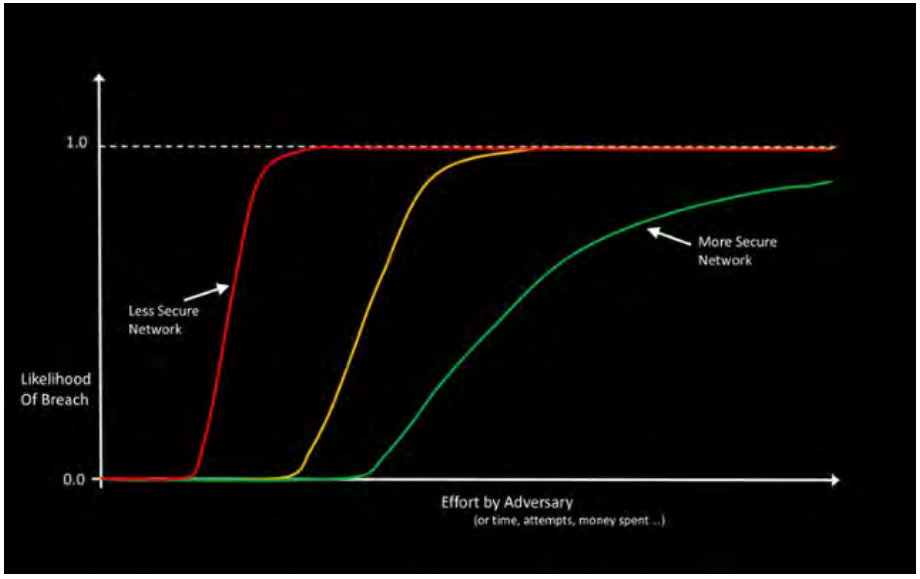


Fig 6:
Breach Likelihood vs Effort for organizations of different security maturity levels

Cyber risk is defined as any risk of financial loss, disruption or damage to the reputation of an organization resulting from the failure of its information technology systems.

Consider this. Would this curve remain the same for your network at all times? The short answer is—no. As you make changes to your network, the curve changes. The deployment of a new security control might push the curve significantly to the right, decreasing the slope. The discovery of a new vulnerability in your network which is being exploited in the wild will move the curve to the left and perhaps make it steeper, until the vulnerability is patched. Given that your network is dynamic with new devices and users, new applications, new configurations and vulnerabilities, upgrades and patches happening continuously, this Likelihood vs Effort curve changes on a daily basis.

4 factors influencing likelihood of breach

Likelihood of breach is a function of 4 factors: vulnerabilities, threats, exposures, and mitigating controls. Let's examine each in further detail.

risk = likelihood x impact

likelihood = *f(vulnerabilities, exposure, threats, mitigating controls)*

#1. Threats

Opportunistic attackers do not care about whom they attack and with new threats emerging on a daily basis, it is key to understand which ones are important from an organization's standpoint. Attackers utilize threats that are either currently fashionable in the underground communities or they standardize attack techniques to enjoy economies of scale when hitting several targets, of whom only a small fraction gets victimized. Unsolicited mass email (spam) is an example for this strategy. Mapping real and emerging threats—what is currently fashionable (or possible) for the adversary—to specific assets and then observing and prioritizing them is critical.

It is also important to keep in mind that not every threat realizes a risk. Threats require vulnerabilities in the target system to become successful attacks. For example, a malformed network packet is only harmful if the software processing the data packet enters an undefined state which allows the attacker to take over control. Such vulnerabilities emerge from common mistakes during coding, which are hard to be fully avoided in the software development. Likewise, the social engineering attempt is only successful if the victim is tricked into sharing credentials with unauthorized parties.

Do You Know?

Which weaknesses are being exploited in the wild?

An exploit is a type of attack that takes advantage of software bugs or vulnerabilities, which cybercriminals use to gain unauthorized access to a system and its data. Commonly exploited software includes operating system, Internet browsers, Adobe applications, and Microsoft Office applications.

#2. Vulnerabilities

A vulnerability, according to the traditional dictionary definition, is anything that exposes you and puts you at risk. So, bad password hygiene—using weak or default passwords, reusing passwords, and not storing passwords correctly—is also a vulnerability. And so are misconfigurations, encryption issues, and risky online behavior of employees. However, a large percentage of organizations running vulnerability management programs utilizing traditional scanners only monitor for unpatched software flaws or CVEs (publicly known infosec vulnerabilities and exposures in publicly released software packages) and don't monitor their attack surface for other risk items. To accurately calculate risk, you must factor in vulnerabilities across a range of attack vectors.

Most common breach methods

- Phishing, Web & Ransomware
- Compromised Credentials
- Weak Passwords
- Trust Relationships & Propagation
- Poor Encryption
- Unpatched Vulnerabilities
- Misconfigurations
- Malicious Insider
- Zero Day & Unknown Methods

Do You Know?

What's your risk from weak or shared passwords, malware, phishing, encryption issues, online behavior of your admins and more?

Vulnerabilities are not just CVEs. Any breach methods that put your enterprise at risk are dangerous.

Read More

#3. Exposure

Exposure due to asset usage is a critical, multi-dimensional factor that influences likelihood of breach. This encompasses items such as duration for which the asset has been present on the network, availability and frequency of use, as well as type of use. In addition to these, it is also important to take into account usage at a different levels of granularity, including individual software and applications, the user profile on the asset (e.g. a Virtual Desktop Interface (VDI) can be used by different users over time), as well as the rate and entropy of credentials used to access a service on the asset.

Do You Know?

Based on how an asset is used, what is its exposure to a particular vulnerability?

Assets that are highly used are likely to be more vulnerable to a breach.

#4. Mitigating Controls

Security organizations typically apply several compensating controls—both products and policies—to mitigate risk from a wide range of vulnerabilities. This investment into security controls like firewalls, anti-phishing systems, and EDR influences the likelihood of breach to a large extent. For example, the presence of a micro-virtualized browsing solution can lower the risk of drive-by phishing considerably, however browsing activity to a malware domain indicates the inefficacy of this mitigation. Similarly, an organization that is effective and timely in its patching behavior decreases its exposure to breach via unpatched vulnerabilities relative to an organization that rarely patches its critical systems.

Do You Know?

Are there any current security controls in use that are reducing risk?

Every year, hackers produce some 120 million new variants of malware.

Calculating impact

Impact of a breach is the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure, modification, destruction, or loss of information, according to NIST.

After calculating breach likelihood, the next step is to assess the breach impact for every device, app and user located within your network. This impact is determined by examining each asset's type, roles, access and many other attributes. Your breach impact is significantly higher for core devices located on sensitive networks or your critical network infrastructure.

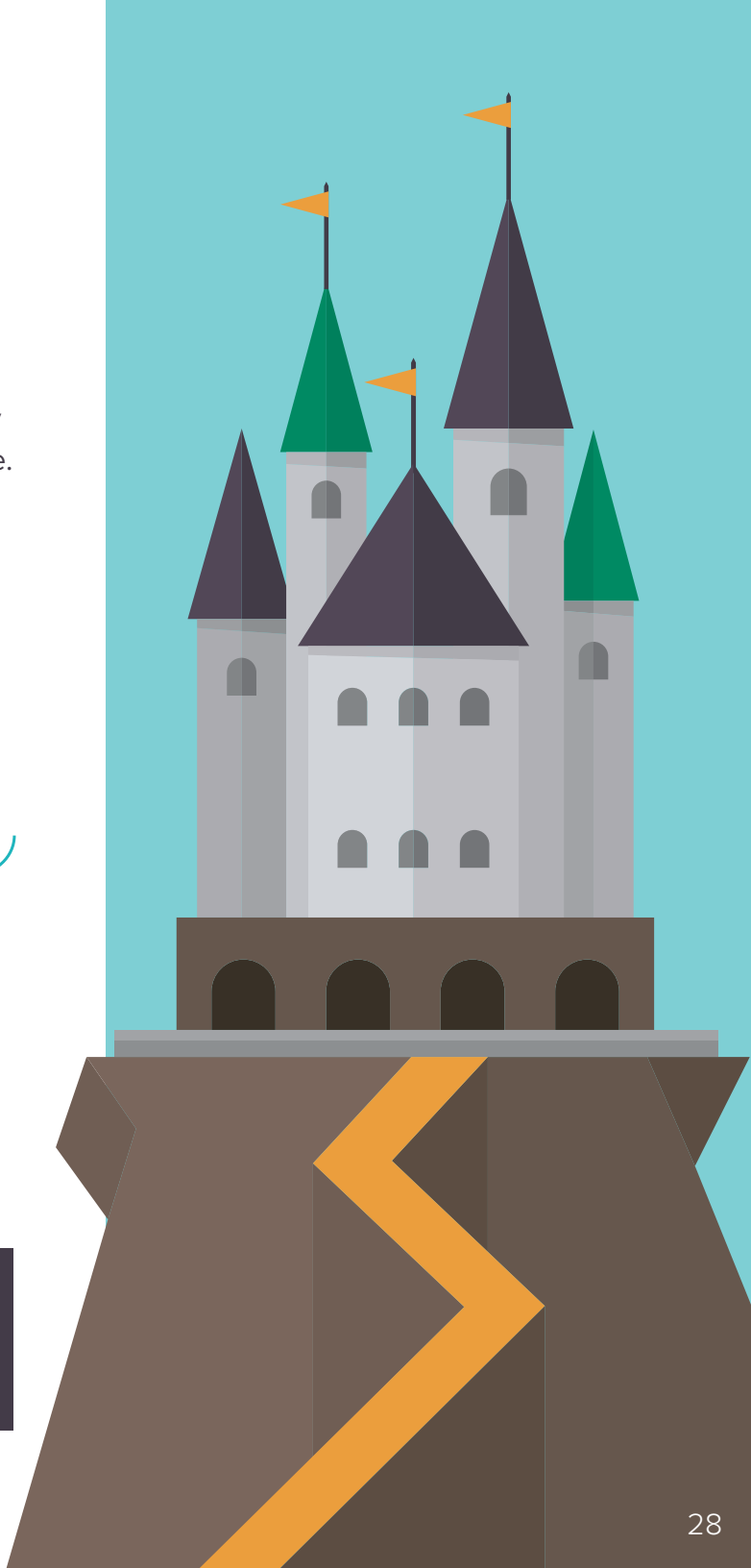
To accurately calculate impact of a breach, you first need to understand what amongst your assets would be potential targets for cyber criminals and then enumerate their importance to your business. Criminals would be potentially interested in your customer, employee, and financial data, intellectual property, contract terms and pricing, strategic planning data, and your third- and fourth-party vendor data.

impact = *g(business criticality)*

risk = likelihood x impact

likelihood = *f(vulnerabilities, exposure, threats, mitigating controls)*

To understand your organization's cyber risk profile and breach impact, you need to determine what information would be valuable to outsiders or cause significant disruption if unavailable or corrupt.



Assessing business criticality

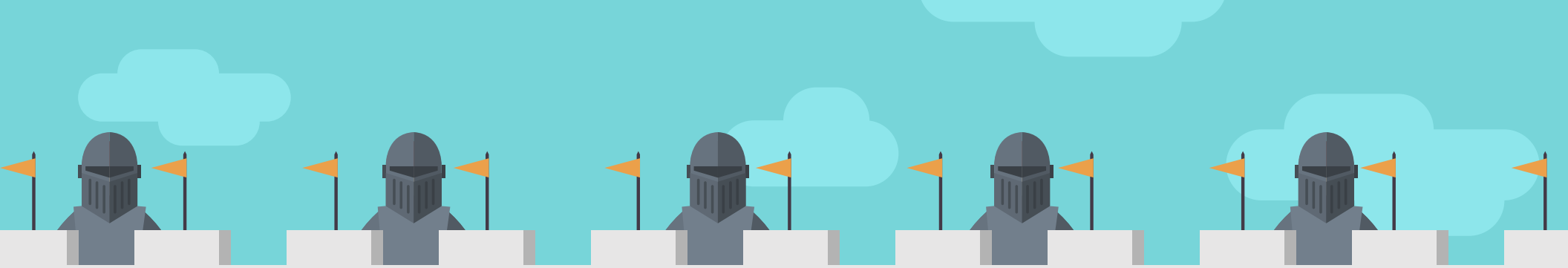
The interaction between threats, vulnerabilities, and controls determines the success of attacks. Attacks turn into incidents if they hit critical assets. Considering the business criticality of assets as an individual risk factor governing impact is important because organizations may use similar technologies and resources to secure assets of very different value and sensitivity. For example, a corporate policy that requires all High/Critical vulns to be patched within 24 hours is much more meaningful for the enterprise when its servers run an online banking portal than a guest login kiosk. While assessing business criticality of an asset, you need to consider both inherent (e.g. asset category, business unit) and contextual properties of the asset (roles, applications, user privilege, and interaction with other assets).

Do You Know?

What is the importance or "business value" of each asset?

The value and criticality of affected assets influences the potential impact of an incident.

Learn More



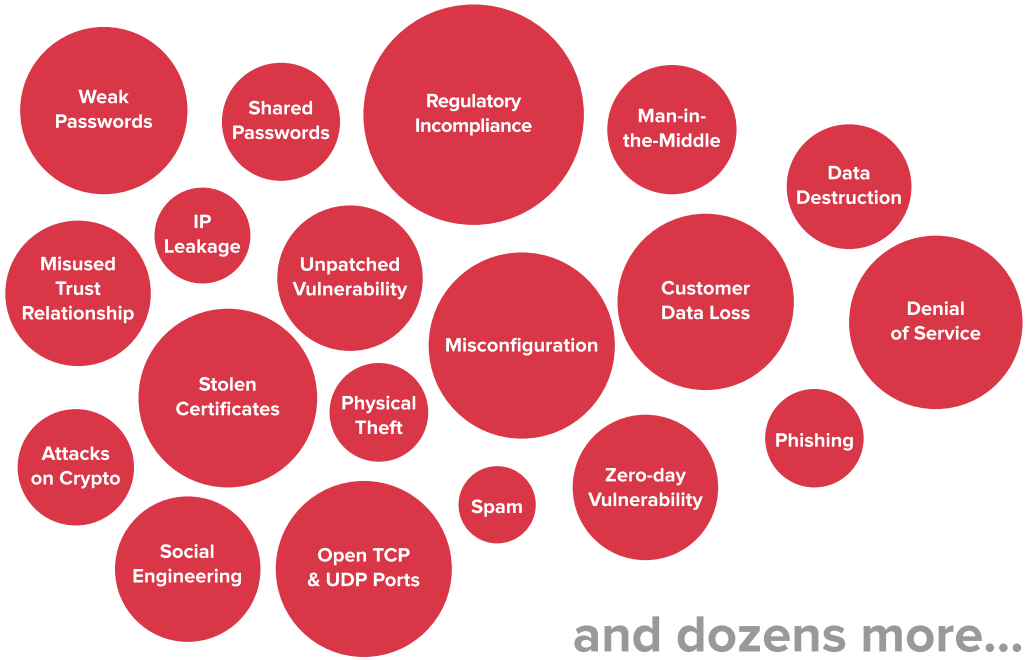
Vulnerability Management

Vulnerability Management

Vulnerability management is widely described as the practice of identifying security vulnerabilities in unpatched systems that if exploited by adversaries, can put your entire enterprise environment at risk. Typically, vulnerability management is a foundational practice, and an integral part of any standard cybersecurity initiative. However, constantly changing device demographics and increasing sophistication in cyberattack techniques, including an increase in recent multi-pronged attacks, are challenging the vulnerability management vendors and the cyber defenders alike.

Limitations of traditional vulnerability management

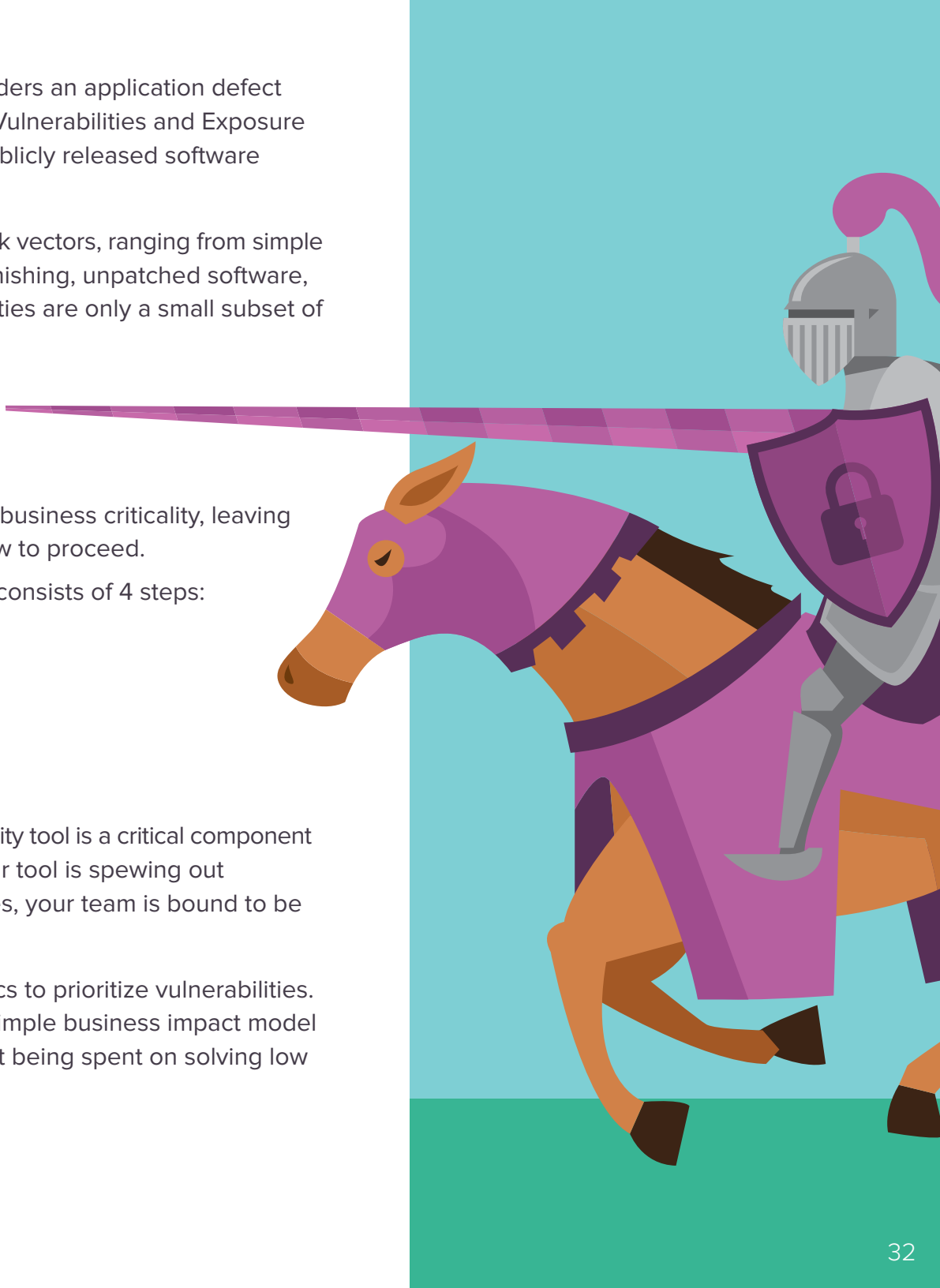
1. Vulnerability management only covers about 5% of your attack surface and misses a number of important risks that should be on your radar.



and dozens more...

Vulnerability management, by its very definition, only considers an application defect as a vulnerability so traditional tools only look at Common Vulnerabilities and Exposure (CVEs)—known security vulnerabilities and exposures in publicly released software packages—due to unpatched software.

However, your enterprise is susceptible to hundreds of attack vectors, ranging from simple things like weak passwords, to more complex things like phishing, unpatched software, encryption and configuration issues, etc. Known vulnerabilities are only a small subset of most enterprises' overall breach risk.



2. Vulnerability management does not prioritize output by business criticality, leaving you drowning in a sea of vulnerabilities with no idea how to proceed.

Conceptually, a typical vulnerability management program consists of 4 steps:

- Identify software vulnerabilities
- Sort them in some order of priority
- Mitigate them by patching or accepting risk
- Rinse and repeat in a continuous cycle

Understanding and acting on data output from your vulnerability tool is a critical component of your vulnerability management program. However, if your tool is spewing out vulnerabilities in the thousands every time a scan completes, your team is bound to be left overwhelmed and struggling with how to proceed.

Moreover, legacy vulnerability tools use primitive risk metrics to prioritize vulnerabilities. Their calculation is typically based on CVSS scores and a simple business impact model (high, medium, low), which leads to untold amounts of effort being spent on solving low impact issues.

3. Vulnerability management output is typically more than 30 days out of date.

Your enterprise asset inventory is dynamic with devices being added and retired, physical machines migrating to virtual and various stakeholders constantly installing and updating software. Traditional vulnerability management scanners are typically configured to run periodically—quarterly, monthly, or weekly—which makes managing compliance and cyber-risk very difficult. Enterprises should strive for continuous monitoring of all assets to keep pace with their dynamic environments. Continuous monitoring not only helps organizations determine whether they are actually fixing the flaws they discover, but also helps security teams identify trends in the performance of the vulnerability management program.

Risk-based vulnerability management

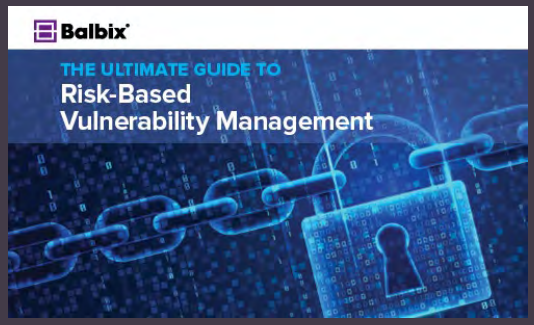
Given that the volume of breaches, from both unpatched systems and other 100s of attack vectors, is continually growing, vulnerability management tools must use risk-based analysis to provide a manageable volume of high-quality alerts. With the hundreds (and growing) of attack vectors and propensity of bad actors to carry out multi-pronged attacks, risk-based vulnerability management is needed. A truly risk-based vulnerability management would have the following key capabilities:

ACCURATE INVENTORY AND CATEGORIZATION

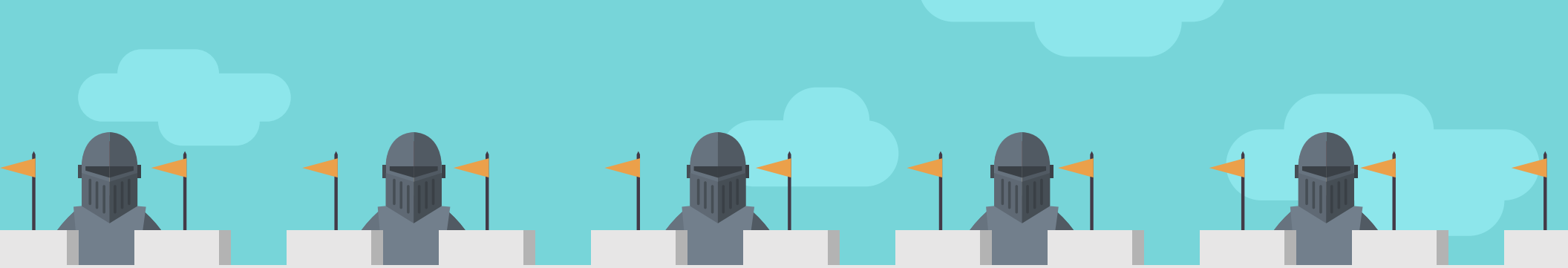
- Comprehensive, automated, and continuous inventory of all existing enterprise assets—managed, unmanaged, cloud, devices, IoT, apps, users
- Categorization of assets including information such as the type of asset geo location, software and hardware details etc.

ASSET CONTEXTUALIZATION BASED ON BUSINESS RISK

Rationalizing mitigation activities becomes an uphill, often unsurmountable task without knowing the context and business risk of each asset. With a risk-based vulnerability management approach, each asset is analyzed using the context of the specific asset, its use in the business, the impact of a potential breach on it, and the likelihood of that happening.



Learn More



Strengthening Your Security Posture

Strengthening your security posture

It is clear that to accurately measure and ultimately strengthen your security posture, you need to first understand and calculate your likelihood of breach (which is a function of threats, vulnerabilities, exposures, mitigations afforded by existing security controls) and secondly, figure out the potential impact of a breach, a function of business criticality of assets. That may sound simple theoretically, but in reality, this translates to several crucial steps.

Learn More

#1. Measure

Comprehensively measure the attack surface

You can do this by first obtaining a real-time inventory of all your IT assets, including managed, and unmanaged servers, laptops and infrastructure, BYODs, IoTs, cloud, third party etc. and automatically discovering any assets newly added to your network in real-time. And then continuously monitoring them across a broad set of attack vectors (unpatched software, phishing and ransomware, misconfigurations, encryption issues etc.)

GET

Continuous, real-time visibility into inventory, vulnerabilities, threats, and mitigations.

#2. Model

Analyze breach risk and predict breach scenarios

In addition to discovering and categorizing your assets, it is imperative to calculate the business impact for each asset by examining its access to sensitive networks, services and data. This coupled with the continuous analysis of indicators of risk across dimensions like weak and shared passwords, misconfiguration, susceptibility to phishing, unpatched software, quality of encryption, etc., produce an inherent likelihood model for the network. Then fold information about the external threat model and the deployed security controls and mitigations to compute the effective risk model for the enterprise.

ALIGN

Your cybersecurity posture with cyber-risk.

#3. Act

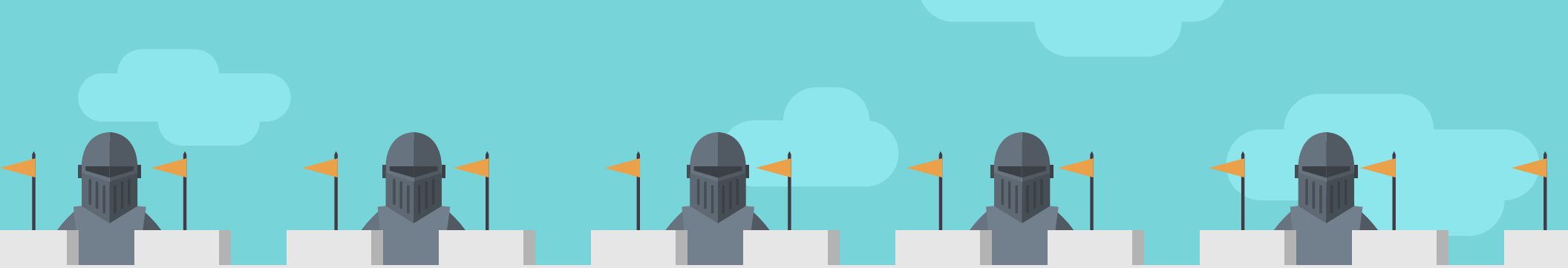
Systematically reduce breach risk

Obviously, there are specific steps you can take to improve your security posture. But the big question is, how do you know what those steps are, in order of priority, and how to take them? Your action items need to be derived directly from your breach risk model. Then these actions will not just be a sweeping list of vulnerabilities, but the result of analysis of your overall attack surface based on actual risk. Some of these insights will be tactical tasks—one-time fixes, such as “change this password” or “patch that system”, while others may point to some strategic actions, e.g. “the mean-time-to-patch for this set of 25 critical assets is too high, it should be 3 days”.

To rigorously calculate and manage risk you need to continuously observe and analyze the enterprise attack surface to surface relevant insights for your security team and the business. These insights will be crucial as you make cyber-security related decisions for the enterprise—such that the right mitigation actions are prioritized and executed. This will also enable you to accurately measure and analyze your exploitable attack surface, increase the impact of your security team and dramatically increase cyber-resilience.

MAKE

Your security practice preventative and proactive instead of reactive.



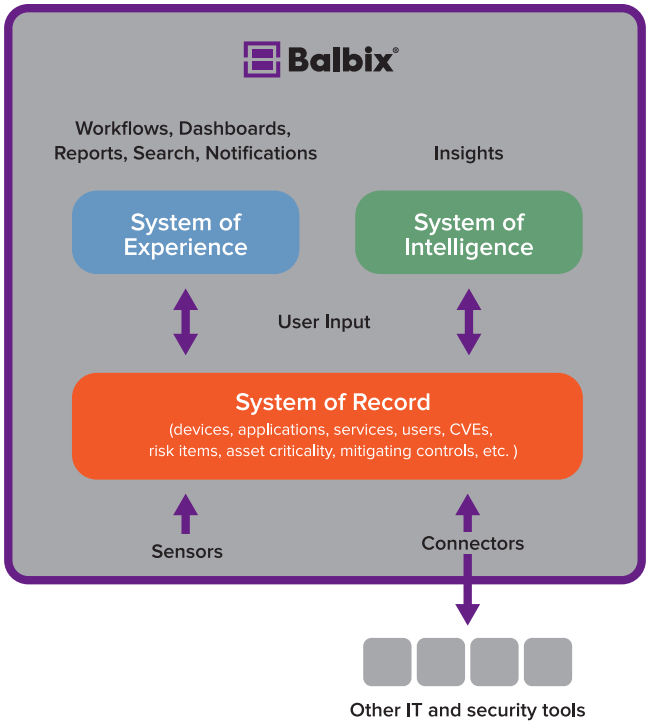
Security Posture Transformation

The Balbix Platform

Imagine if you had a system of record for your security team. This would enable you to understand your inventory including asset criticality, to know what CVEs are open, what your other risk items are, and which compensating controls are effective.

On top of that, if you had a system of Intelligence which enabled you to analyze all of the above on a continuous, real-time basis to prioritize the most important tasks.

And then, add in a system of experience that provides workflows, notifications, dashboards, and reports you need in order to do your job(s) well. That's the Balbix platform, in a nutshell.



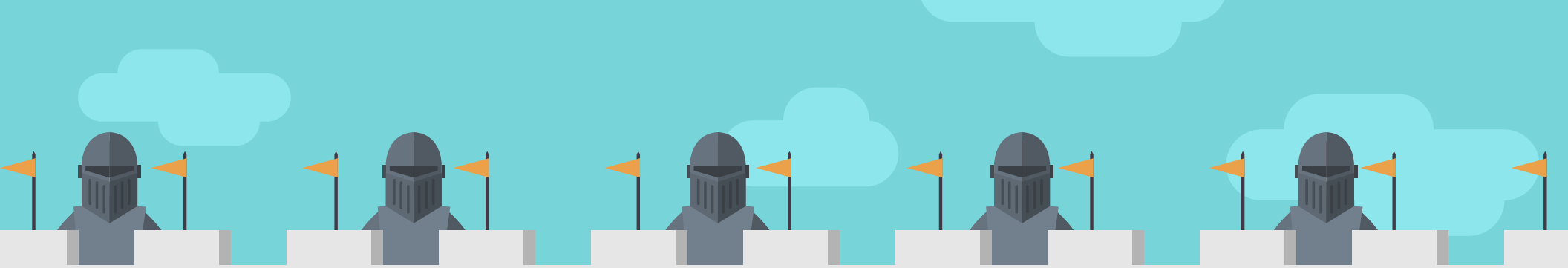
The Balbix platform uses specialized AI algorithms to discover and analyze the enterprise attack surface to enable a broad set of vulnerability and risk management use cases that help to improve your enterprise cybersecurity posture. Balbix offers:

- Continuous and automatic discovery of IT assets and monitoring across 100+ attack vectors.
- Comprehensive coverage of all asset types (on-prem, cloud, IoT, mobile, managed, and unmanaged) and all attack vectors.
- Discovery of mitigation/compensating controls to understand the effectiveness of your cybersecurity program.
- Calculation and financial quantification of risk using 5 factors —vulnerabilities, threats, asset exposure, business criticality, and compensating controls.
- A prioritized set of actions that you can take to transform your cybersecurity posture and reduce cyber risk by 95% or more while making your security team 10x more efficient.
- Visibility into overall cybersecurity posture including risk heatmaps by owners, sites, business units.
- Dashboard and workflows for various tasks necessary for cybersecurity posture transformation and reports for various stakeholders to indicate state/progress of risk management.
- APIs to enable other security tools to take advantage of risk context.
- Gamification to drive all stakeholders to do their part in improving cybersecurity posture.

Dashboard showing the effectiveness of your security controls:

Dashboard that can be used for board updates showing breach risk by division and region and changes over time:

Dashboard showing critical KPIs for improving security posture:



Summary

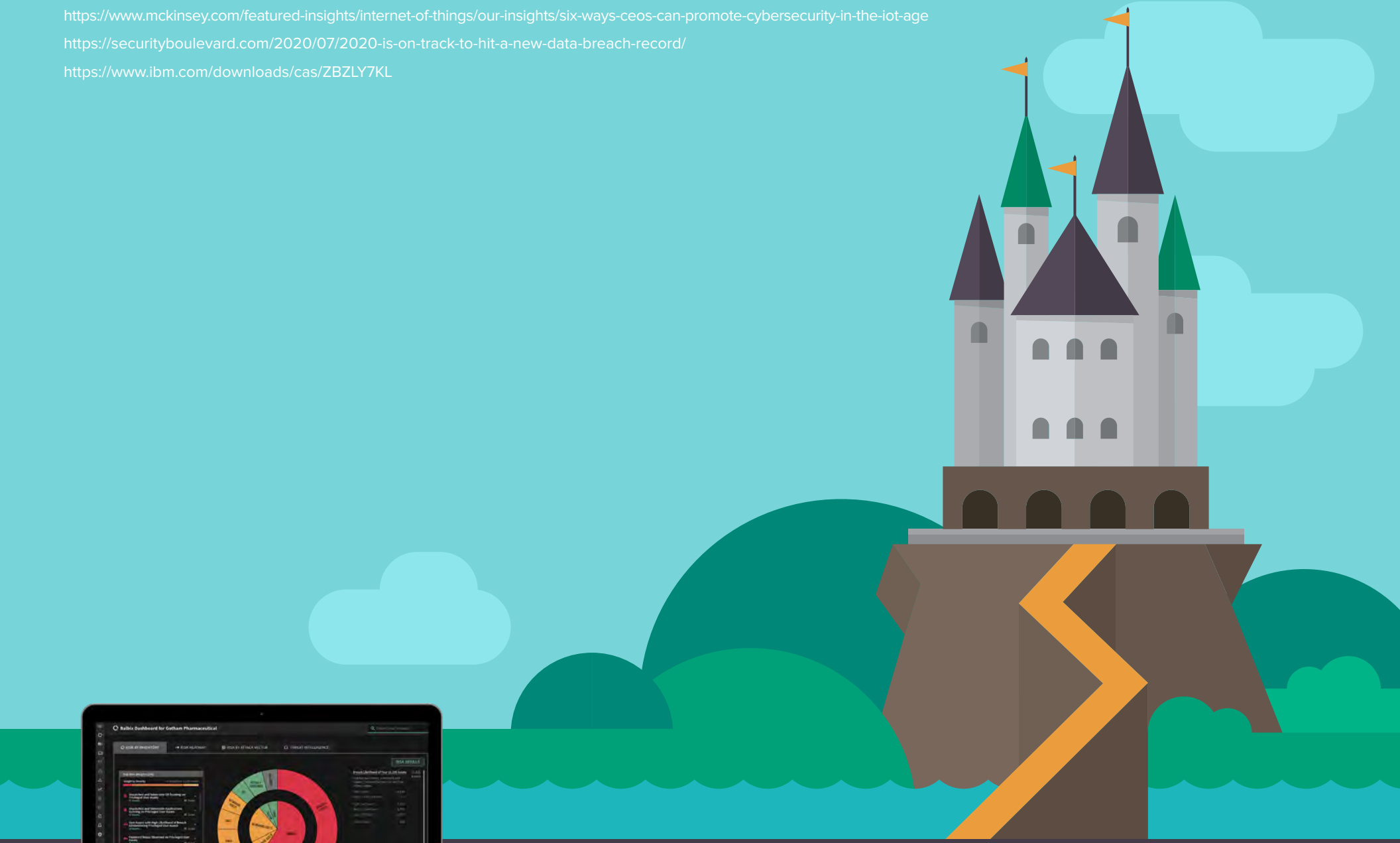
As a CISO, you need to assess and report on your enterprise's security posture in a number of situations. You may be a new CISO trying to get a quick handle on what you have inherited and where to begin. Or you may be a seasoned pro who reports on a periodic basis to your company's audit committee or board of directors. Accurately understanding, assessing, and improving your security posture is the key to understanding your cyber risk and reducing it.

References:

https://www.mckinsey.com/featured-insights/internet-of-things/our-insights/six-ways-ceos-can-promote-cybersecurity-in-the-iot-age

https://securityboulevard.com/2020/07/2020-is-on-track-to-hit-a-new-data-breach-record/

https://www.ibm.com/downloads/cas/ZBZLY7KL



LEARN MORE

Balbix®