tenable

OLD PUEBLO
SECURITY GROUP

HACKERS DON'T HONOR SILOS:

Five Steps to Prioritize True Business Exposure

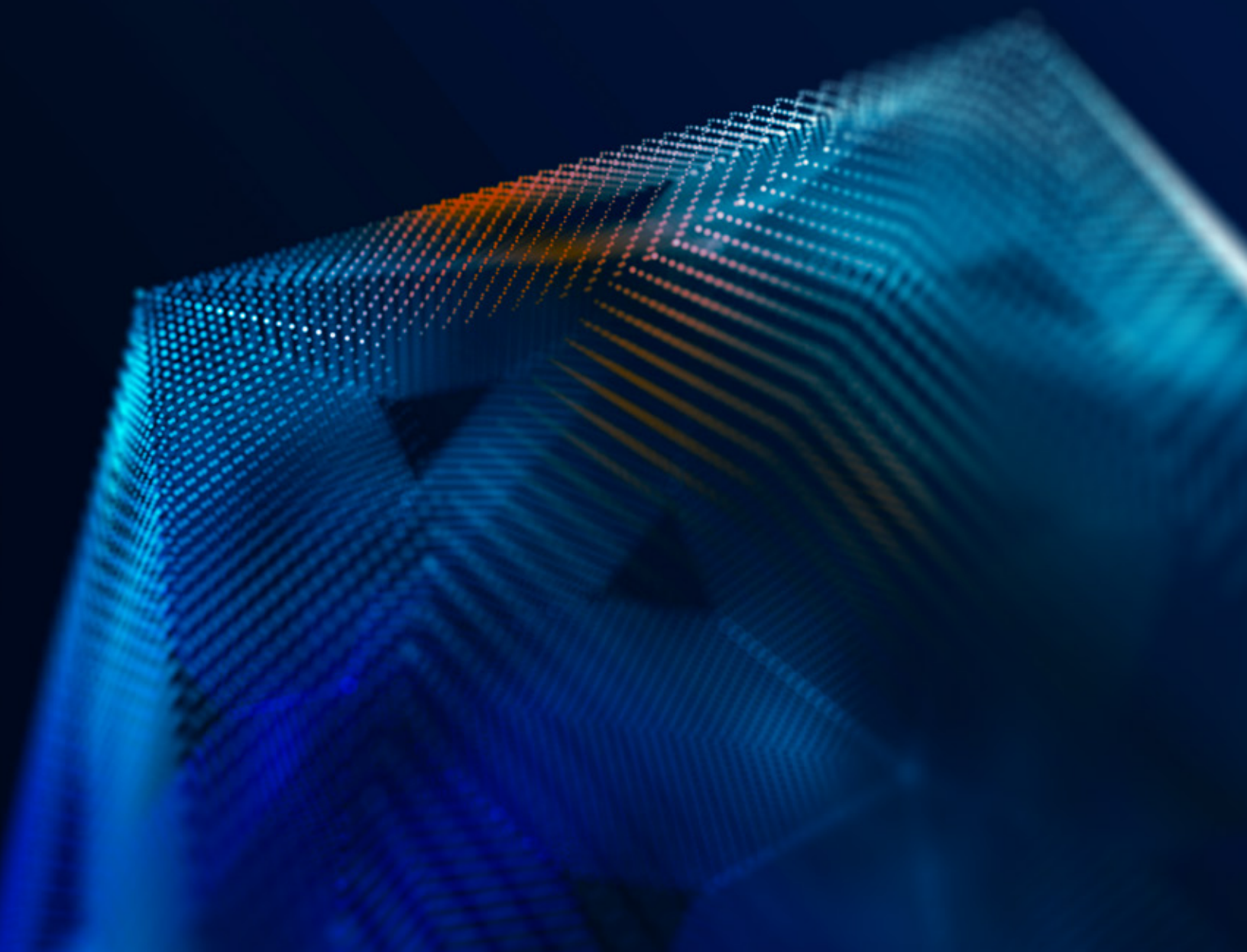


Table of contents

For most organizations, the natural evolution and adoption of technologies including IT, cloud, operation technology, IoT, and diverse applications has led to a multitude of specialized security tools focused on a specific technology or domain of security. By design, these tools are typically strong at a particular flavor or 'silo' of security – for example vulnerability assessment, cloud security posture management, or active directory security. They are not designed to collectively operate as one security solution.

The simple question is, will bad actors honor these security silos? The safe bet is NO. They will look for an initial weakness and move laterally across domains to achieve an end goal. This makes it exceedingly challenging to identify what constitutes actual business exposure from just any ordinary risk finding.

In this ebook, we will challenge conventional wisdom on security across the attack surface, in order to identify a more viable and scalable approach. We believe that there is perhaps no better way to do this than by approaching security from the attacker's perspective, as after all, it is attackers that we must ***stop***.

Distinguishing exposure from ordinary risk

When optimizing prioritization across silos, it is important to agree on the end game. Certainly the role of virtually every security tool is to identify and control risk. But not all risk is created equal. With this in mind, it is our belief that the purpose of cyber security is to mitigate the risk of a breach, and in turn the resulting exposure - aka the negative consequence – from that breach on an organization - be it a business, government agency, or service provider.

When discerning any risk, from actual exposure there are *three characteristics* we look for:

1. **Preventable**
   Virtually every breach begins with a preventable form of risk: a misconfiguration, a vulnerability, or an excess of privilege.

2. **Exploitable**
   An attacker must be able to discover the risk, and act on it, for example, via existing exploit code for a vulnerability, or through lack of strong password policy or MFA in the case of identities.

3. **Impactful**
   The risk, once exploited, will have a significant and material impact on the organization's mission, be it lost revenue, data, uptime, etc.

Context matters when distinguishing risk findings from Exposure!

Risk **"How do I respond"**	Asset with proxylogon vulnerability	S3 bucket with anonymous download enabled	Asset with chrome CVE-2022-0609 vulnerability
Exposure **"Need to take immediate action"**	Asset with proxylogon vulnerability, externally accessible, with domain-level privileges	S3 bucket with anonymous download enabled, externally accessible, with sensitive client data	Asset with chrome CVE-2022-0609. owned by HR group, with 'create new user' permissions

Exposure is preventable risk, such as a CVE, misconfiguration, or excess of permission, that have a high likelihood to be targeted and exploited by attackers, which also have the potential for material impact on an organization.

The stark reality - *breaches* happen! So why not learn from them?

Lest history repeat itself, let's begin by looking at some examples of high profile breaches crossing multiple industries to gain a more holistic view of how attackers operate.

SolarWinds - projected at $100 Billion in *damages*

With an average cost of $12 million per impacted organization, the Solarwinds breach is arguably the most impactful cyber breach in history. Attackers gained access to and modified the Solarwinds software source code, providing attackers with an initial entry point into over 18,000 organizations. They leveraged these machine privileges to identify misconfigurations and vulnerabilities within the target environments and move laterally, until they gained domain controller privileges within Active Directory. They then used Active Directory Federation Services to modify trust relationships, allowing them to move from on prem to cloud accounts with admin level privileges and without restriction.

Colonial pipeline

Despite its wide recognition as a ransomware attack, the Colonial Pipeline breach actually began with the compromised identity of an employee. Lack of multi-factor authentication allowed attackers to gain entry into the network, exploit additional vulnerabilities in IT systems, and ultimately deploy ransomware.

Boeing

Attackers exploited a known vulnerability to gain initial machine permissions. They then deployed post-exploitation tools such as mimikatz to identify and exploit additional vulnerabilities and misconfigurations and escalate privileges, move laterally and exfiltrate sensitive data with the intent of obtaining ransom.

Uber

Attackers gained initial access to Uber's intranet using compromised credentials. Once inside they scanned and identified what can be classified as a misconfiguration – unsecured administrator credentials – which they used to escalate privileges and access all of Uber's sensitive services.

The anatomy of a breach:

Important takeaways

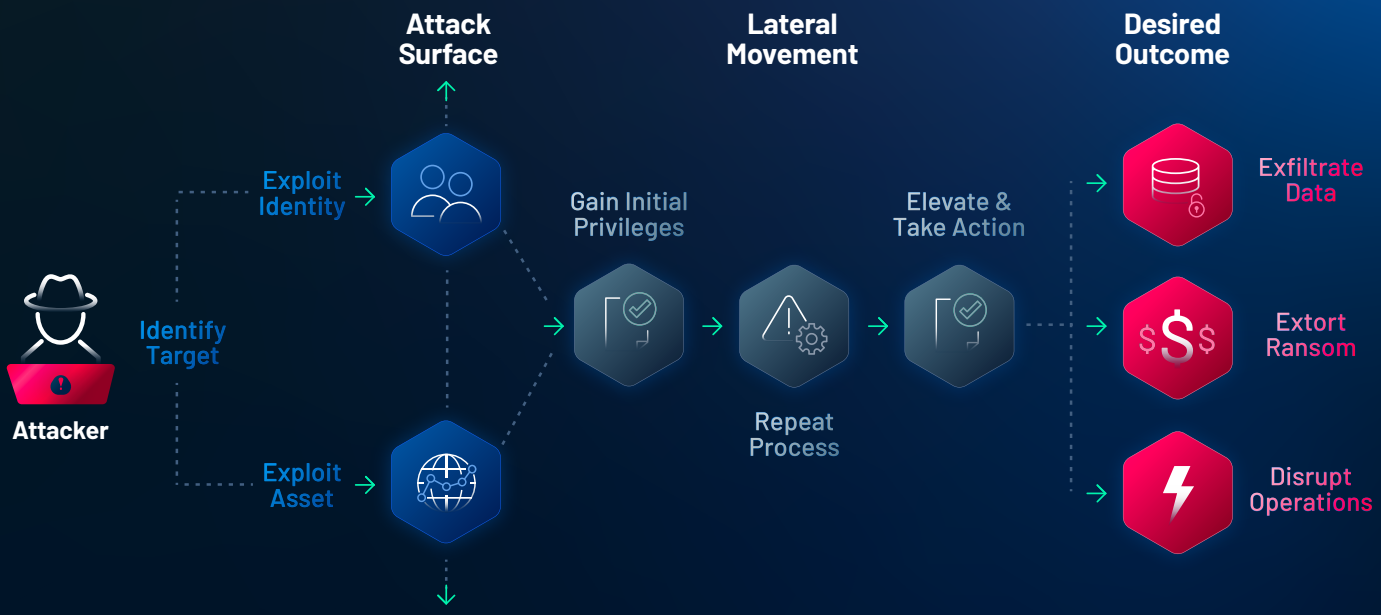
In analyzing the aforementioned breaches, we can begin to see a pattern that is pretty consistent across all of them:

Breaches begin by compromising either an asset or an identity, with the intent of gaining initial human or machine privileges.

Attackers then move laterally by looking for misconfigurations, vulnerabilities and privileges that can further elevate their permissions, and repeating this process.

Once an adequate level of permissions have been achieved, attackers execute an end game like exfiltrating data, demanding ransom, or impacting operations.

The Anatomy of a Breach



What's holding us back?

The problem is that we are not able to approach security in the same way an attacker executes their craft. Let's take a look at the biggest impediments to ***effective preventative security***:

Lack of a holistic view of the attack surface:

Individual tools frequently focus on a specific technology domain: IT, cloud, identity, OT/IoT, apps – or risk: vulnerabilities, misconfigurations, privileges, etc (see figure 1).

Disjointed approaches for scoring risk:

Vendor and tool specific scoring makes it challenging to assess and compare relative risk across domains as well as the total risk presented by a given asset (see figure 1).

Lack of critical technical context:

Fragmented data makes it impossible to understand the relationships between assets, identities, and risks needed to understand viable attack paths which can be exploited by attackers (see figure 2).

Lack of critical business context:

Security tools lack an understanding of the potential for material impact of risk as it relates to the things that matter most to an organization - such as revenue generating services or mission critical data (see figure 2).

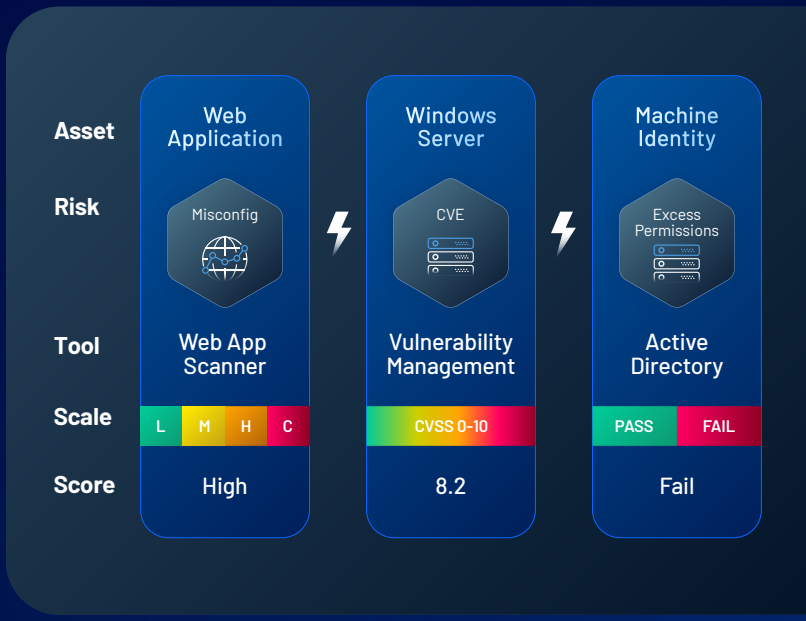


Figure 1: Siloed findings and scoring make prioritization challenging.

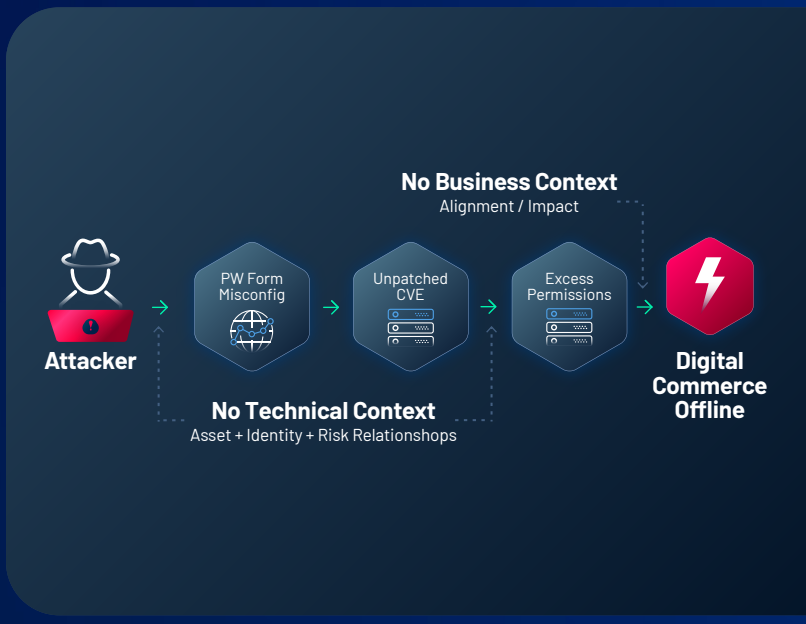


Figure 2: Lack of technical and business context make it impossible to see reality from the attacker's POV.

Moving the goal post

To date, the vast majority of investment in security tools has been made around threat detection and response, which makes sense, as this is where the material impact of breaches actually occurs in the form of compromised client data, brand tarnish, financial penalties and lawsuits, revenue loss, and most recently even personal liability for some CISOs.

However, recent regulations such as those by the Securities and Exchange Commission (SEC) which require the reporting of material impact for publicly traded organizations within 96 hours, and Critical Infrastructure Security Administration (CISA) which require reporting of material impact to critical infrastructure organizations within 72 hours have made transparency a mandate, not a nice to have. The window for action, accountability and disclosure is now days, vs weeks or months. Whereas historically, many breaches went completely unreported.

These mandates increase the need to shift investments towards identification and remediation of risk exposure, prior to occurrence of an active breach and before material impact. Preventative security investments are smaller than the combined cost of a breach in terms of lost revenue, clients, law suits, and penalties. And more importantly, where the risk of personal accountability is vastly reduced.

Evolution, not revolution:

Five steps to optimize prioritization and prevent breaches

Now that we have identified the formula for breaches, the fundamental flaws in traditional siloed security approaches, and the increased need to identify exposure before breaches are underway, we have a more grounded understanding of the problem we must solve.

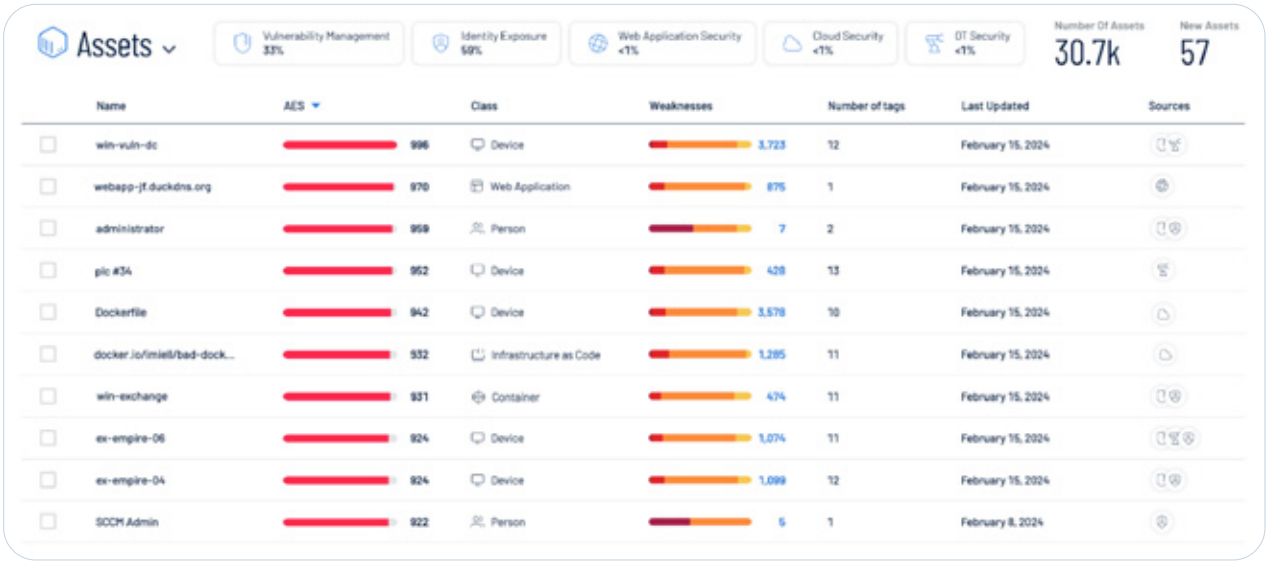
Certainly, the intent is not to over correct our approach to security. We must leverage and continue investments in threat detection and response tools, but we must also increase our focus on preventative security to better understand and prioritize risks that represent actual exposure for the organization before breach and material impact have occurred.

Working with over 44,000 organizations globally, Tenable has identified five critical steps needed to successfully identify and remediate true business exposure and drive better outcomes from your preventative security program.

Step 1

Know your attack surface

As we saw in our real world examples of breaches, attackers gain an initial foothold by compromising an asset or identity and gaining either machine or human privileges. As the traditional perimeter erodes with adoption of cloud, IoT, and remote work, the attack surface continues to grow, as do the number of potential entry points for attackers. Yet it is estimated that only 62% of an organization's attack surface is actually known to cybersecurity teams, according to a recent study. Meanwhile, a single unsecured device, unpatched laptop, or weak password can provide enough initial privileges to start a successful attack. Comprehensive visibility into our entire attack surface, both external and internal is a must. This means aggregating asset and identity information distributed across multiple tools into a unified asset inventory.



Exposure Management platforms, such as Tenable One, discover and aggregate asset data across the entire external and internal attack surface – Cloud, IT, OT, IoT, Identities and Applications, providing a holistic view of the attack surface. Asset data includes asset type, version, configuration, connectivity, weaknesses, and other important asset details. A standardized approach to discovery ensures that asset data can be rationalized across individual scanners and normalized to reflect a single unified source of truth.

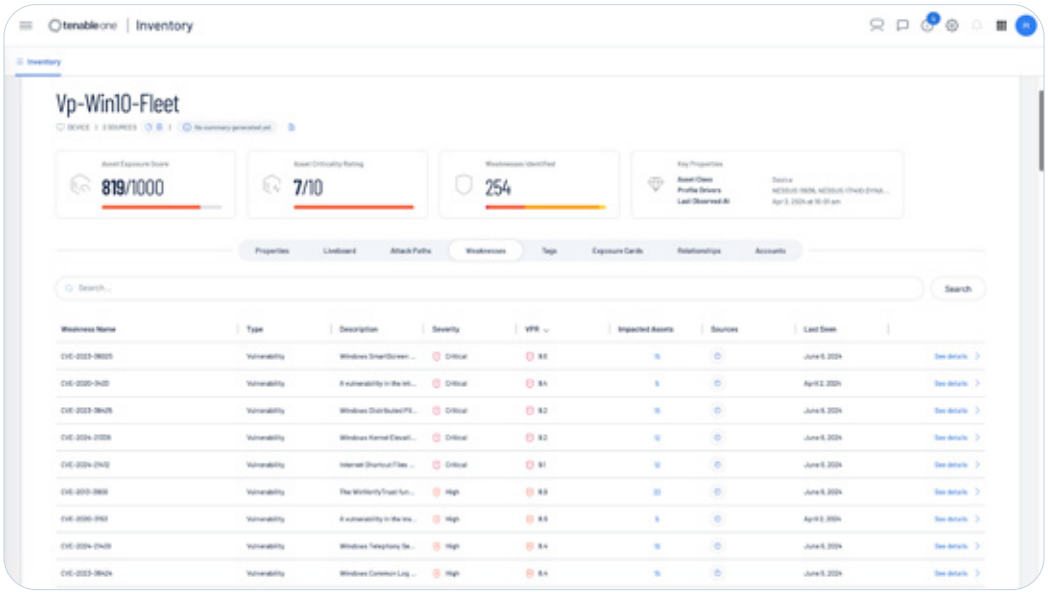
Step 2

Identity all preventable risk

In virtually every attack, the intent is to exploit weaknesses in order to escalate privileges and move laterally. Identifying all preventable forms of risk can be challenging, requiring a mix of techniques and tools often spanning network scanners, agents, passive monitoring, and agentless approaches. Further, these findings remain trapped in individual tools, with their own unique prioritization scores. To effectively measure and manage exposure, we must have a complete and normalized view of all preventable risk - misconfigurations, vulnerabilities and excessive privileges associated with a given asset or identity so we can understand its total exposure.

Platforms such as Tenable One detect the three preventable forms of risk leveraged by all attackers to gain initial access and move laterally: vulnerabilities, misconfiguration and excessive privileges. Findings are aggregated by asset and normalized to calculate an overall Asset Exposure Score (AES) from 1-1000, with 1000 being the highest level of risk. This enables security teams to quickly identify the assets that pose the greatest potential risk to the organization.

AES is calculated using two individual metrics. First, a Vulnerability Priority Rating (VPR), which enables you to focus on the critical few weaknesses that are most exploitable by taking into account a range of dynamic variables, such as severity (e.g. CVSS), availability of exploit code, use by attackers in the wild, and other variables. Second, an Asset Criticality Rating (ACR) which assesses the relative importance of the asset. For example, a database server has a higher ACR than a printer. ACR can be adjusted to reflect crown jewel assets, or to raise or lower the importance of a category of assets.



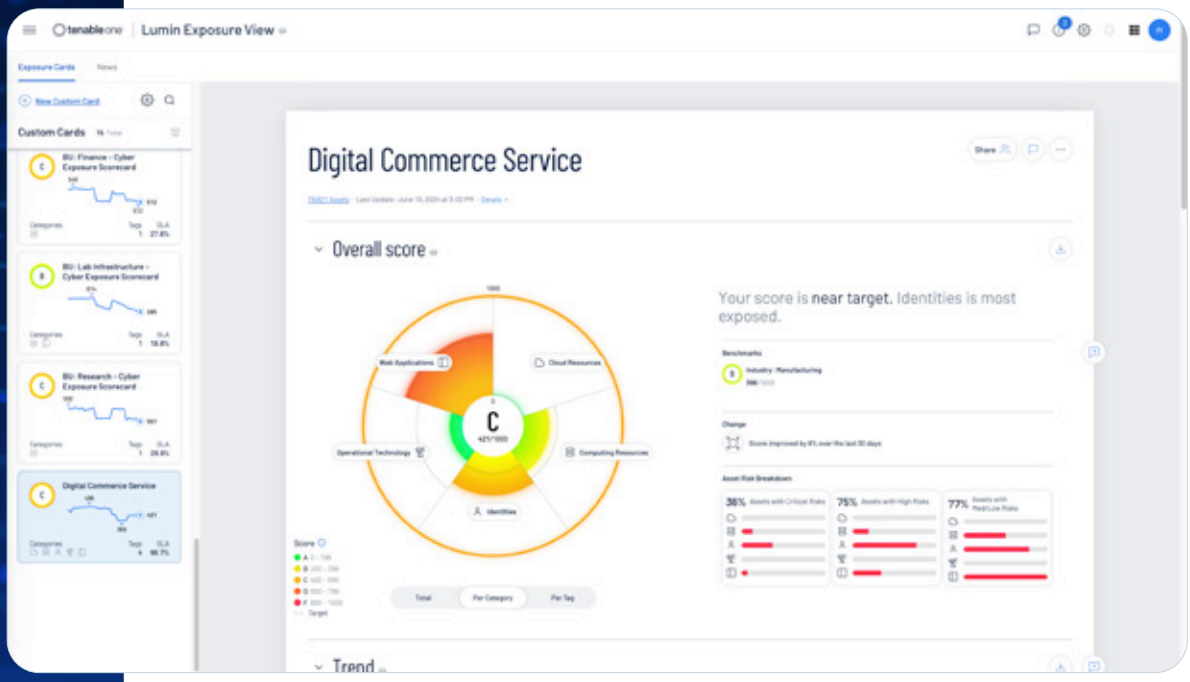
Normalized risk scoring leverages consistent asset criticality and vulnerability scoring to calculate total asset exposure for a given asset across security silos.

Step 3

Align with business context

In reality, most security teams remain understaffed. Partly because of a limited talent pool in the market, but more so for some organizations, due to limited budgets preventing adequate staffing. This, plus the overwhelming number of assets and findings can leave many security teams struggling to keep pace. The result is alert fatigue. To overcome alert fatigue and scale security, we must have visibility into the things that matter most – the critical services, processes, and data that support the mission of the organization. These can be a digital commerce service that generates revenue, client data that stores personally identifiable information (PII), or a process such as a manufacturing line. By aligning assets to these mission critical functions, we can prioritize crown jewel assets, and deprioritize those that are not aligned to critical functions.

In the Tenable One platform, for example, asset tagging allows security staff to logically group assets across technology domains and align them to a dedicated Exposure Card corresponding to an important business function, service, process, etc. Exposure Cards aggregate associated AES scores for each asset to calculate an overall Cyber Exposure Score (CES) for any critical business function or grouping. CES scores provide an at a glance view of overall exposure, but more importantly, they lay the foundation to track and understand changes in exposure over time.



Exposure cards provide a 35,000 foot view of cyber exposure aligned to the things that matter most to the organization - mission critical services, processes, functions and data.

Step 4

Remediate true exposure

The goal of attackers is to identify viable attack paths which can enable desired outcomes, be it exfiltrating data, disrupting operations, or demanding payment of ransom. Because even a single open port on an asset can provide an initial foothold leading to 'n' number of potential attack paths, it is important to understand the relationships between assets, identities and risk which together allow attackers to move laterally and achieve their objectives. With an understanding of these toxic relationships, we can then see which attack paths actually lead to crown jewels, and prioritize remediation accordingly.

Exposure Management platforms such as Tenable One leverage the detailed asset, identity, and risk relationship information discovered and maintained within its asset inventory, along with business context provided by tagging and exposure views to create business-aligned asset views with corresponding AES. This allows security staff to see the highest risk assets, and more importantly, pull up all related attack paths for a high risk asset which can lead to crown jewels (See figure 1). In this way, organizations can prioritize remediation of the highest risk attack paths. Further, because even a single asset can give way to 'n' number of potential derivative attack paths, we can quickly identify the choke point which when remediated can mitigate numerous related attack paths, greatly scaling productivity. In other words, rather than remediate every weakness in every attack path, which can be 10s to 100s or even thousands of steps, we can prioritize specific choke points spanning many attack paths, massively scaling remediation and improving staff productivity and effectiveness (See image 2).

Image 1: Tenable One provides visibility into high risk attack paths, along with AI insights that make it easy for any staff to operate at an expert level.

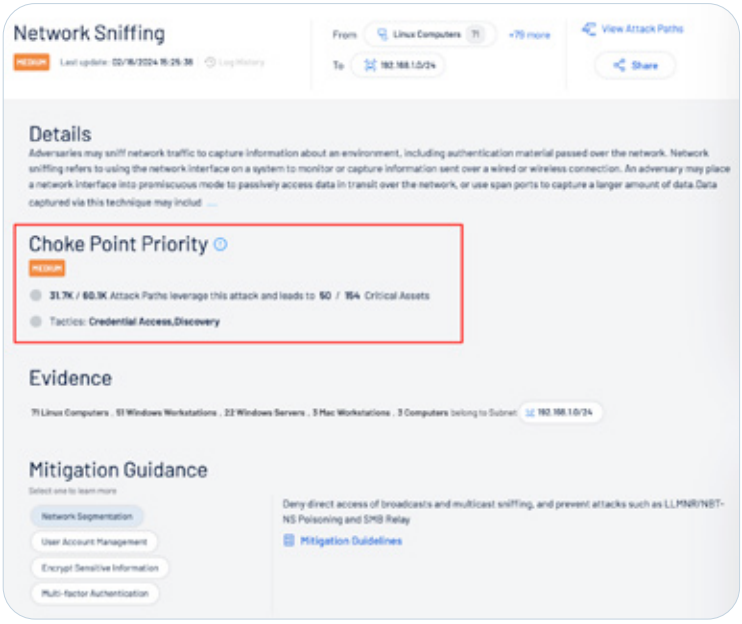


Image 2: Identification of choke point priority based on impact to critical assets simplifies and scales remediation.

Step 5

Continuously optimize investments

While tremendous investments have been made in security tools, with trillions of data and telemetry details around every potential risk, the reality is most security leaders today struggle to answer the fundamental question, 'How secure are we?" – which is increasingly the interest of Boards of directors, C-suites and lines of business, alike. Further, with tight budgets and staffing constraints, the ability to understand and prioritize investments where they can have the biggest impact is vital.

For this reason, it is critical to measure and communicate exposure along numerous axes, including overall cyber exposure for an organization, exposure by business function or line of business, by technology domain, by administrator, or even compliance aligned to specific regulatory mandates. In steps 1-4, we broke down data silos to achieve complete visibility into all assets and risk, their relationship to each other, and to the things that matter most. Armed with this holistic view of the attack surface and true exposure, we can now track all varieties of cyber exposure and the potential impact, and align people, budget, and other investments in a way that best supports organizational objectives.

For example, the Global Exposure Card in Tenable One lets us visualize our overall cyber exposure score as an organization over time, but more importantly, compare that to peers in our industry or across industries. With this unique insight, we can demonstrate whether further investment is required to keep pace with peers in our market. Similarly, domain specific and custom exposure cards allow us to identify which technologies and business functions pose the greatest risk of exposure – allowing shifting of funds and staff where needed. Further, tracking of security controls aligned to industry benchmarks such as the Center for Internet Security (CIS), allow us to measure compliance with regulatory requirements, right down to the specific framework controls, allowing for prioritization of resources to ensure ongoing compliance.

Tenable One provides realtime and historical visibility into key performance and risk indicators, including trend, SLA, and remediation insights.

Realize better outcomes with exposure management

These five steps offer a prescriptive approach that transcends siloed security, providing unique insight into true business exposure through the lens of an attacker. Exposure Management platforms such as Tenable One can streamline and accelerate this journey to integrated exposure management across the attack surface with measurable benefits.

Tenable One clients have reported:

Up to 10X
improvement
in asset visibility

identifying and fingerprinting unknown and unmanaged assets across the attack surface.

Up to 75%
time savings
aggregating and normalizing

risk data and scoring across historically siloed security domains.

Up to 82%
reduction
in new tickets

by identifying toxic risk combinations, and prioritizing remediation of shared choke points that disrupt multiple attack paths.

Up to 80%
reduction
in licensing costs

by eliminating multiple expensive point security tools and leveraging a unified licensing approach across the attack surface.

About Tenable

Tenable is the exposure management company, exposing and closing the cybersecurity gaps that erode business value, reputation and trust. The company's AI-powered exposure management platform radically unifies security visibility, insight and action across the attack surface, equipping modern organizations to protect against attacks from IT infrastructure to cloud environments to critical infrastructure and everywhere in between. By protecting enterprises from security exposure, Tenable reduces business risk for more than 44,000 customers around the globe.

Learn more at www.tenable.com.

In conclusion, the modern threat landscape demands a shift in how we approach security. Siloed security is no longer sufficient to address the sophistication of today's threat attackers that are looking for visibility gaps and weaknesses exploit, move laterally and escalate privileges. By adopting a holistic and attacker-centric strategy, organizations can gain comprehensive visibility into their assets, identities and risks aligned to the things that matter most, and prioritize remediation of true exposure that can have a material impact on the organization. Armed with enhanced visibility and context, organizations can continuously optimize security investments. Exposure management platforms streamline the process of breaking down silos. They provide a robust framework for prioritizing true business exposure, ensuring that security measures are not only effective, but also scalable and aligned with the organization's mission.

Contact us:

Please email us at sales@oldpueblosecuritygroup.com or visitwww.oldpueblosecuritygroup.com