tenable®

OVERCOMING CHALLENGES CREATED BY DISPARATE VULNERABILITY MANAGEMENT TOOLS

DITCH YOUR FRAGMENTED TOOL SET AND TACKLE ACTUAL CYBER RISKS FOR YOUR ORGANIZATION

The Fragmented State of Vulnerability Management

Today's security leaders struggle with a patchwork view of the assets and vulnerabilities across their expanding and ever-evolving attack surface.

For decades, organizations that wanted to build defenses to protect their enterprises from cyberattacks have assembled a hodgepodge of disparate solutions. With each new evolution of the network, from cloud computing to web apps to the latest work-from-anywhere paradigm, security teams have bolted on new scanners and other assessment tools to gain visibility into the new environment. But unfortunately, these tools rarely communicate with one another, causing security teams to rely on manually stitched together security data from multiple single-purpose security tools, which make it difficult, if not impossible, to determine what is happening across their attack surface.

With each new evolution of the network, from cloud computing to web apps to the latest work-from-anywhere paradigm, security teams have bolted on new scanners and other assessment tools to gain visibility

These single-purpose tools help eliminate blind spots from across a wide range of network environments, but most are incapable of discovering assets and vulnerabilities outside the specific environment for which they were built. Furthermore, they have their own unique way of displaying and analyzing the vulnerabilities they discover, and frequently even map common fields or aspects differently, making it nearly impossible for teams to gain valuable insights. Instead, teams are relegated to a vicious cycle in which they continually adopt one solution for one problem, another for the next, and over time, are left with a technology stack of siloed data that makes it challenging to scale and evolve to effectively address the latest threats.

For all the money spent on cybersecurity each year – roughly $200 billion and growing[1] – organizations are still looking for better ways to defend their attack surface. The vast majority (94 percent) have experienced a business-impacting cyberattack or compromise over the past 12 months.[2] And more often than not, the root cause of major breaches can be traced back to basic mistakes: unpatched vulnerabilities, misconfigurations and asset blind spots.

[1] Statista Research Department, January 2021

[2] "The Rise of the Business-Aligned Security Executive," a commissioned survey conducted by Forrester Consulting on behalf of Tenable, August 2020

Technology Overload

When we talk about risk-based vulnerability management, we often talk about the challenges of data overload. Security teams get so much information back from their vulnerability assessments, they often struggle to keep up as they manually analyze troves of data to understand their existing vulnerabilities, so they can prioritize which need attention first. Meanwhile, more vulnerabilities come in, faster than they can process what they already had.

We don't often talk about the same challenge as it relates to technology. Across the industry, it's become standard for teams to use single-purpose scanners for each environment, from traditional IT systems and on-prem servers to web apps and cloud assets, and on and on. While these tools help security professionals perform our jobs more effectively, particularly with the support of automation and built-in intelligence, they can also hinder our ability to readily see and address risks across the entire attack surface.

Why? Because when you're constantly shifting back and forth between solutions and dashboards, you can easily miss vulnerabilities that pose an immediate risk to your organization.

These technology challenges compound over time as team members come and go from your organization, taking with them knowledge of why one tool might have been implemented while newcomers may look to procure yet another solution.

Before you know it, you're staring at different dashboards, managing different consoles, and if a critical vulnerability or security incident catches your attention, you're left scrambling to assemble and organize all the data in front of you and decide what to prioritize.

Add to that the hours it can take for a team to research a single vulnerability, and before you know it your team ends up spending more time culling data together than acting on it.

Sidebar Sources:

*Tenable Research, "2020 Threat Landscape Retrospective," January 2021
**Ponemon Institute, "Cybersecurity in Operational Technology: 7 Insights You Need to Know," April 2019
†Verizon, "Data Breach Investigations Report," May 2020
††Gartner, "Container Management Software Forecast," June 2020

What is risk-based vulnerability management?

Rather than trying to fix everything, a risk-based approach to vulnerability management uses machine learning analytics to correlate asset criticality, vulnerability severity and threat actor activity to identify and manage the risks that pose the greatest threat to your organization.

LEARN MORE

Cybersecurity Threats Come From Everywhere...

18,352*
new Common Vulnerabilities and Exposures (CVEs) discovered in 2020

700*
public breach events exposed **22 billion** records

90%**
of operational technology environments that experienced at least one cyberattack in the past 24 months regulary scan for vulns

43%†
of breaches were attacks on web applications

>75%††
of organizations will run containerized apps in production by 2022

Disparate Data Challenges

All of these single-purpose technology solutions may solve specific needs, but the resulting data silos and operational friction create additional challenges for your already over-taxed security teams. They also make it challenging to understand and communicate your security program's effectiveness, let alone its ROI or alignment with key business metrics.

Mapping and Reporting

When your technologies don't connect or communicate, you can't do a quick merge and purge of data. That's because it's likely that field outputs from one tool won't map to field outputs from another. As a result, it's an incredibly manual—and inefficient—process for your teams to pull and synthesize your security data across these disparate tools.

Time Considerations

If you're using separate tools to track all of your assets across multiple environments, it's going to take a lot of time to cull that information for comprehensive insight. And, if those assets are managed across multiple teams, those time considerations only increase exponentially.

Even once you consolidate your data, how can you readily see which security issues are most critical and be confident you haven't missed anything? With separate tools, it's a nightmare. The more manual processes you have, the more time-consuming they become and the more behind your team gets—and stays—against attackers who already have a headstart on you.

Human Error

Vulnerability management approaches that require manually stitched together security intelligence are also prone to human error, which is a significant threat to your ability to successfully manage and mitigate cyber risks. This challenge is compounded if you're using separate solutions or static documents across various teams; one error early in your data-gathering process can have cascading effects on everything that follows, leading to incorrect or suboptimal decisions in your mitigation or incident response efforts.

Most Organizations Are Losing the Remediation Race

On average, it takes organizations about 40 days to remediate all instances of a single vulnerability within their environment. Roughly 73 percent of vulnerabilities still exist within 30 days of an assessment, and almost a third are still unresolved after a year.[3]

[3] Tenable Research, "Persistent Vulnerabilities: Their Causes and the Path Forward," June 2020

Impacts of Technology Overload

Technology overload doesn't just create challenges for security professionals—it can have a significant negative impact on your ability to prioritize risk and defend your entire attack surface.

Missed Vulnerabilities

Attackers are banking on unpatched vulnerabilities and continuously looking for ways to take advantage of them. They know you're overwhelmed with data and don't have clear visibility into every vulnerability they could potentially exploit.

In fact, according to Ponemon, nearly 60 percent of organizations that suffered a breach said it happened because there was a known vulnerability that wasn't yet patched, even though their organization was aware a patch existed prior to the breach.[4]

> **According to Ponemon, nearly 60 percent of organizations that suffered a breach said it happened because there was a known vulnerability that wasn't yet patched**

Lack of Prioritization

Separate solutions and manual processes make it nearly impossible to effectively prioritize your cyber exposures. When you're looking at data from four or five different tools, and you're cobbling the results together, at best your prioritization process is going to be an educated guess.

If you had hundreds, or let's say even a few thousand vulnerabilities to manage, it might be doable, but most organizations have tens to hundreds of thousands, if not millions of vulnerabilities across all their assets and environments. The reality is, it's just not possible to manage these exposures effectively or efficiently if you're doing it piecemeal or manually.

High Operating Expenses

Each new technology solution your organization adds requires additional capital, resources and skilled professionals. This operating expense is even higher when you factor in payroll and benefits for your workforce, as well as the countless hours spent on completing lengthy, manual or repetitive processes that expansive technology stacks and inefficient processes create.

[4] "Costs and Consequences of Gaps in Vulnerability Response," an independent survey conducted by Ponemon Institute LLC on behalf of ServiceNow, October 2019

Disruptions

When a high-profile vulnerability makes headlines, security teams often struggle to understand if it's actually relevant to their environment. That means they have to stop what they're doing and dig into additional research, which can take hours upon hours, before they know if the new vulnerability poses an actual risk.

These disruptions create a panic mode for many teams and, more often than not, fail to identify the actual cyber risks that directly affect your organization. If you're using separate technologies and manual processes, you won't actually know the relative risk posed by a given vulnerability until you stop what you're doing and go through everything. And by then, the process may repeat itself again.

Management Challenges

There are also communication issues that can arise from using single-purpose tools in your vulnerability management program. If it's cumbersome for your team to curate and manage all of this data, imagine how difficult it will be to report on it to your management and executive leadership teams, let alone other key stakeholders like your board.

Without this insight, the board and management could lose confidence in the team's efforts, and you may struggle to get access to future resources and the support you need to manage and scale your program.

> **If it's cumbersome for your team to curate and manage all of this data, imagine how difficult it will be to report on it to your management and executive leadership teams**

Zerologon Case Study: When Threats Become Reality

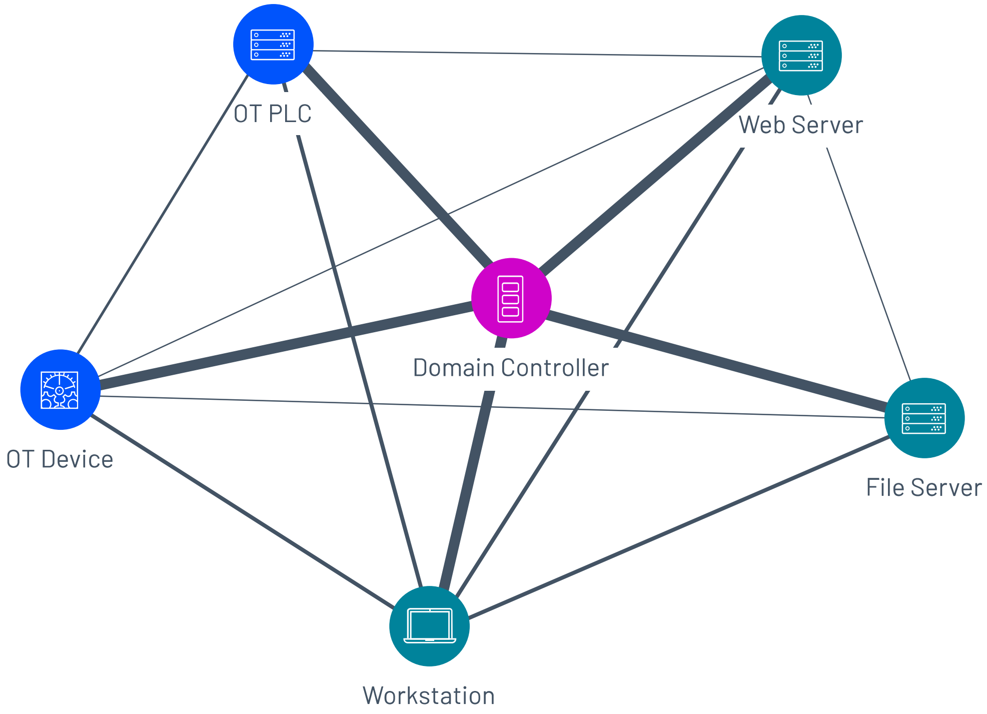
We've talked at a high level about the challenges and impact that single-purpose tools have on vulnerability management programs. But what happens when a potential threat becomes a known exploit observed in the wild? What effects does a fragmented approach have on your ability to discover which of your assets may be exposed?

Let's take a look at a prominent example from 2020: Zerologon (CVE-2020-1472), the privilege-escalation vulnerability in Windows Netlogon that gained the attention of nation-state actors and ransomware groups.[5] (Tenable's Security Response Team designated it as the year's most important vulnerability in its 2020 Threat Landscape Retrospective.)

By exploiting this critical flaw, attackers can gain administrative access to a Windows domain controller—without actual authentication. From there, they can compromise all Active Directory services and escalate privileges to inflict real damage deeper in the network. Within hours of the vulnerability notice, adversaries had already exploited the flaw, quickly moving from a phishing email to executing ransomware such as Ryuk across an entire domain.[6]

Attackers Don't Differentiate Between Assets – So Neither Should You

Zerologon is an example of a security threat that encompasses multiple environments. With privilege escalation, attackers can leverage a foothold on your domain controller as a gateway for lateral movement across your entire network and all of your assets. A vulnerability like Zerologon is not only a risk in itself, but also when it is exploited alongside other vulnerabilities, exposing assets ranging from workstations and file servers to web servers and operational technology (OT) infrastructure.



The proverbial patchwork quilt of security tools is no match for such lateral attack movements, which are increasingly the first step attackers make once they infiltrate a network. Multiple dashboards leave defenders struggling to see the full picture of their potential cyber exposures. Worse yet, a single vulnerability, even with an assigned CVE ID number, may not look the same from one system to another. Disparate tools further widen the chasm when a single vulnerability crosses over into multiple environments.

Rather than lose a full day, or longer, every time they assess the vulnerabilities across their attack surface, security teams must maintain continuous visibility into all assets and vulnerabilities, and automate their assessment, so they can quickly prioritize what matters most. When teams discover a critical exploit like Zerologon, front-line practitioners need to quickly know every affected asset across all platforms and environments, before they can successfully triage remediation efforts.

How might that look in practice? A more streamlined approach to vulnerability management would include a technology solution that supports:

Immediate visibility into all of your Zerologon exposures, across assets and environments, consolidated into a single dashboard

Automated workflows that eliminate human error or missed vulnerabilities, and accelerate intelligence gathering and analysis into potential attack vectors that put your Active Directory at risk

Focused remediation that prioritizes critical exposures affecting your most important business units, geographies or asset groups, which attackers could leverage in conjunction with Zerologon or as part of subsequent lateral movement

Dynamic threat intelligence that tracks the evolving landscape of asset and vulnerability risks, including new exploits seen in the wild or additional disclosures from Microsoft and related vendors

Simple cyber risk metrics that communicate your progress in reducing organizational exposure to Zerologon, gaining confidence from leadership and support for additional security resources in the future

Comparison Guide: Fragmented Tools vs. Unified Platform

Here's a quick look at how a unified approach to vulnerability management differs from the fragmented status-quo:

Why Fragmented Tool Sets Slow Down Your Defense	How a Unified Platform Gives You the Upper Hand
Provides Siloed Visibility of Each Environment Within Your Network	**Delivers a Continuous View of Your Entire Attack Surface**
Multiple tools and licenses: on-prem, cloud, web apps, containers, operational technology environments	Comprehensive solution with a unified view of all asset types, managed by a single license
Burdened With Higher Operating Expenses	**Creates a Common Technical Language**
Each tool requires specific installation, maintenance and configuration; expertise can dissipate overnight with staff turnover or role changes	Unified platform requires a single installation and can be utilized by multiple teams across the organization
Subject to Cumbersome Licensing Requirements	**Supports Dynamic Scanning Across Environments**
Rigid licensing and painful procurement process for each additional tool or capability	Flexible asset-based license for reallocating resources as business needs evolve
Plagued With Interoperability Issues	**Streamlines Intelligence Into a Single Dashboard**
Network blind spots, incomplete toolset and incompatible data sets	Complete visibility and continuous access to comprehensive risk-based tools and priority metrics
Lacks Context Into Performance and KPIs	**Calculates Risk and Peer Benchmarks**
No context to understand the relative efficiency and effectiveness of your security program	Automated maturity assessments display risk scores in relation to industry peers and highlight areas for improvement

Say Goodbye to Single-Tool Complexities

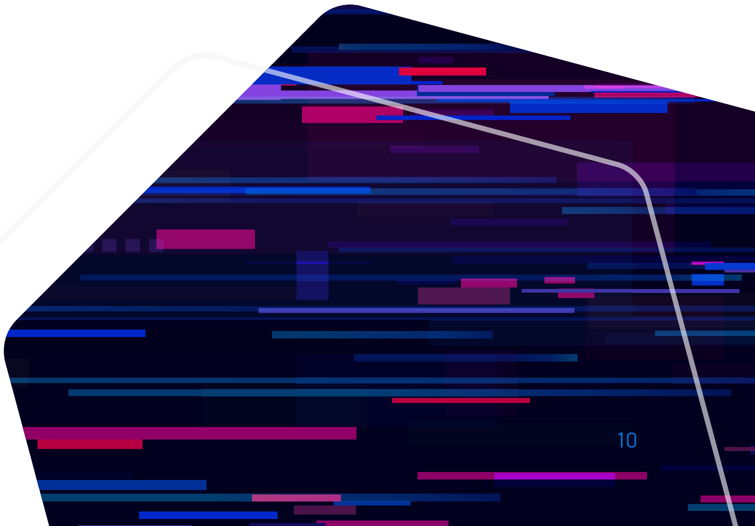
With expanding attack surfaces and increasing attack vectors, cybersecurity professionals face an unprecedented amount of challenges building and maturing effective risk-based vulnerability management programs. These hurdles are further complicated by the proliferation of single-purpose technologies adopted to solve one problem at a time.

Tenable is dedicated to improving customer insight and visibility with innovative and easy-to-understand dashboards that incorporate a growing mix of assets across traditional and modern attack surfaces. While Tenable's individual products will continue to address all of your vulnerability management challenges, you can maximize the efficiency and effectiveness of your security program with our newest offering, the Tenable Exposure Platform (Tenable.ep).

Tenable.ep is the industry's first, comprehensive risk-based vulnerability management platform designed to assess all assets and vulnerabilities across your entire attack surface, all in a unified view. It enables you to know the cyber exposure of every asset, on any platform, at all times, and evolve from compliance-driven attempts to fix everything to a risk-based approach that focuses time and resources on fixing what matters most. No more stitching. No more piecemealing. No more disparate and siloed data.

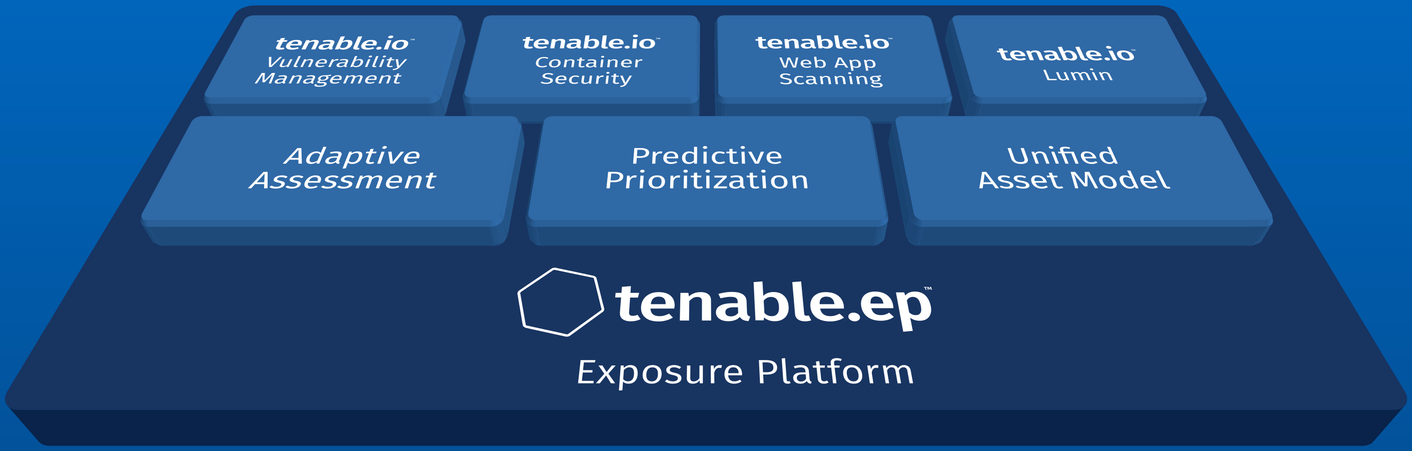
With Tenable.ep, security teams can:

- See every asset and vulnerability across your entire attack surface — all in a unified view
- Predict which vulnerabilities attackers are most likely to exploit in the near future so you can prioritize remediation
- Act to address unacceptable risks affecting your most critical assets
- Allocate resources according to your specific needs, and modify that allocation as your business needs or compliance requirements evolve
- Get deep business insights to calculate, communicate and compare your cyber exposure over time — internally and against your industry peers
- Gain a solid understanding of the effectiveness of your vulnerability management program
- Decrease overhead, time and operational costs
- Assess program maturity and identify gaps for improvement
- Maximize process efficiencies



What’s Included with Tenable.ep

Tenable.ep fully integrates all capabilities as part of a comprehensive solution that’s managed by a single, flexible, asset-based license for simple procurement and easy deployment.


tenable.io Vulnerability Management
tenable.io Container Security
tenable.io Web App Scanning
tenable.io Lumin
Adaptive Assessment
Predictive Prioritization
Unified Asset Model
tenable.ep
Exposure Platform

Experience the Power of a Unified Vulnerability Management Platform:

DOWNLOAD TENABLE.EP DATA SHEET

TRY TENABLE.EP FREE

for 30 Days

tenable®

6100 Merriweather Drive
12th Floor
Columbia, MD 21044

North America +1 (410) 872-0555

www.tenable.com