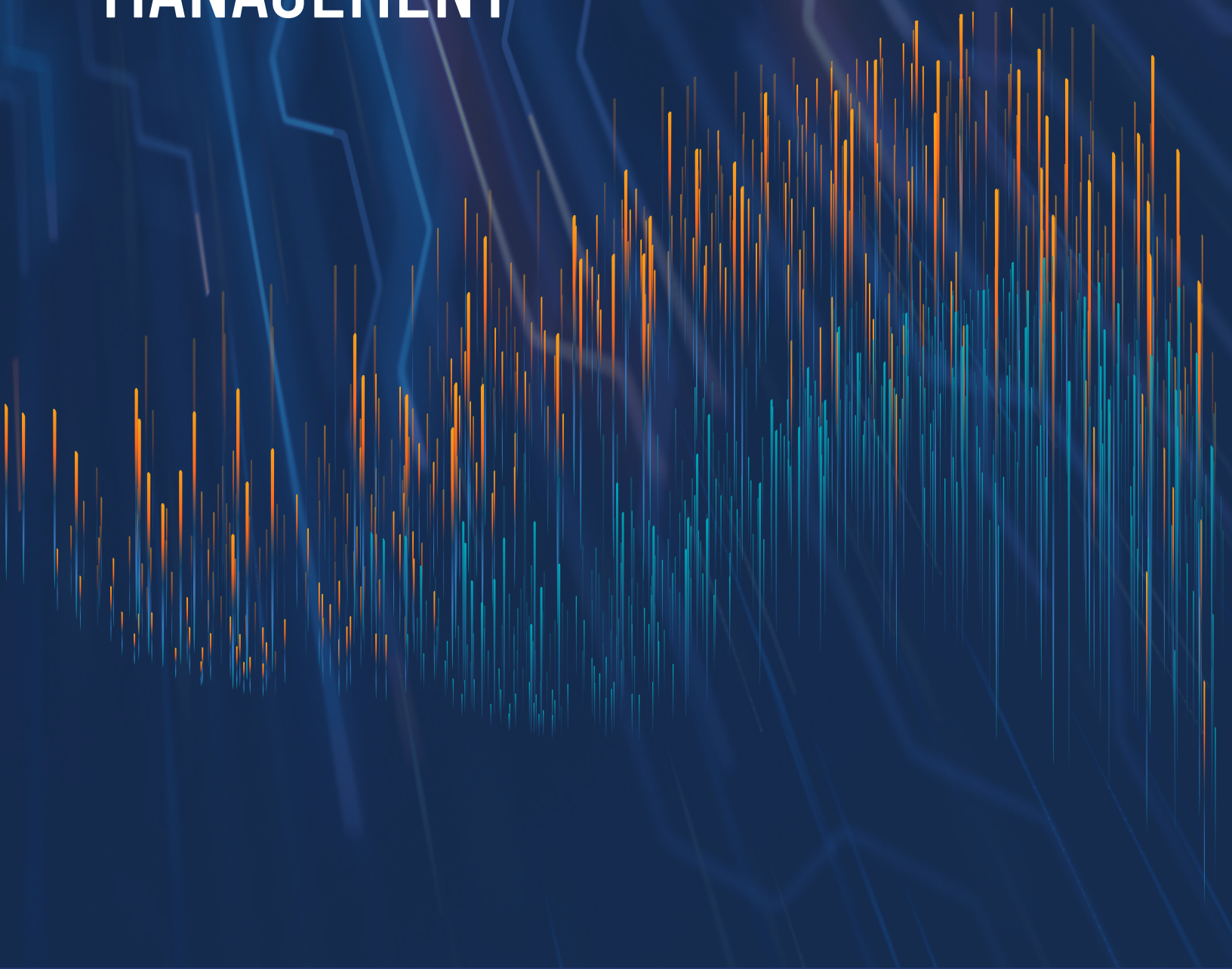
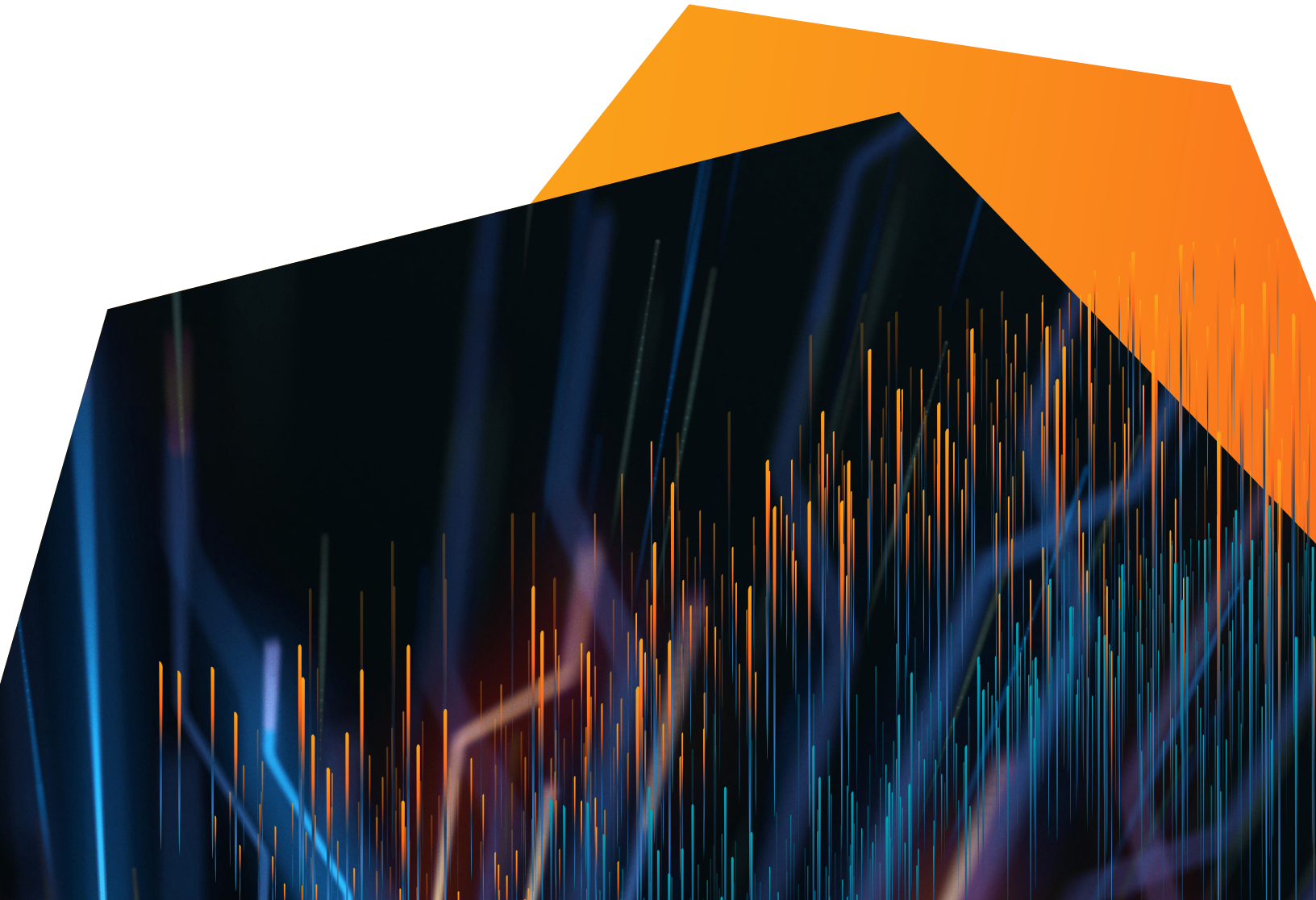
tenable

REFERENCE ARCHITECTURE:
RISK-BASED VULNERABILITY MANAGEMENT



Contents



The Pitfalls of Legacy Vulnerability Management

Legacy vulnerability management (VM) tools are typically limited to a vulnerability scanner and a few open-source technologies such as the Common Vulnerability Scoring System (CVSS). While these tools have been considered the standard for the VM practice for over 15 years, they've failed to keep up with the dramatic changes seen across the modern attack surface, as well as the corresponding increase in the quantity and diversity of today's vulnerabilities.

These outdated methods have led to extraordinary inefficiencies, leading security and IT teams to waste three-quarters of their time on vulnerabilities that don't actually pose any immediate risk, while simultaneously ignoring nearly half of the most dangerous vulnerabilities in their environment. In addition, since legacy VM tools are limited to scanning traditional IT environments, they struggle to discover and assess any vulnerabilities residing in cloud or operational technology (OT) environments.

Why Risk-Based VM?

Legacy VM programs are highly reactive in nature — and therefore inefficient, interrupt-driven, and error-prone. So, to make the best use of their limited security and IT resources, organizations are beginning to adopt a risk-based VM strategy, instead. Unlike legacy methods, risk-based VM is proactive and strategic, so teams can focus on remediating the vulnerabilities that pose the most risk to the organization — therefore enabling them to maximize their efficiency and effectiveness.

Security teams can focus on the vulnerabilities and assets that matter most.

By determining vulnerability severity, threat actor activity and asset criticality, security teams can accurately quantify the organization's true risk. Machine-learning analytics automate this process to provide immediate and accurate answers. The result of this analysis enables security teams to focus on the vulnerabilities and assets that matter most, so they can address the organization's true business risk instead of wasting their valuable time on vulnerabilities that have a low likelihood of being exploited.

Evolving to Risk-Based VM

A risk-based VM strategy is a far more comprehensive solution than what is possible using a legacy VM methodology. As a result, it requires a specific set of tools and technologies at each of five different procedural steps. This paper describes each step and how it compares to legacy methods. It also discusses what you will need at each step and how to make the right purchase decision — including what to look for and which questions to ask.

Discover

The first step in a risk-based VM strategy is to identify, discover and map every asset to gain visibility across your entire attack surface.

1. Understand the Business Environment

First, you'll need to take the time to truly understand the business environment. You'll need this information to determine and prioritize business-critical services and applications, identify service and application owners and other stakeholders, and establish and evaluate existing security and applicable IT policies and processes. After all, you can't protect what you don't know you have.

This is a crucial step, because your environment has likely become more complex than you know. Much of the downfall of legacy VM tools is due to the fact that they failed to recognize and adapt to incremental changes to the attack surface over time. So, take the time to gain in-depth understanding, and then build a VM strategy that can actively detect all assets and identify key processes across the entire attack surface.

2. Define Architecture and Deployment Plan

Next, you'll need to create your sensor deployment strategy. This will obviously include a network scanner to cover your existing, traditional IT infrastructure. But depending on your specific network configuration, it can also include passive monitoring, agents and cloud connectors. If you don't deploy all appropriate sensors for your environment, you'll suffer from blind spots in your VM program. For example, if you have assets in the cloud but you don't have a sensor that can scan that environment, then your cloud assets — and the vulnerabilities that reside on them — will remain invisible to you, therefore leaving you susceptible to threats. Likewise, agent-based sensors help ensure you're detecting vulnerabilities introduced by transient devices, since they aren't regularly connected to the network.

It's critical that you also get buy-in from the rest of the organization for all steps involved in implementing a risk-based VM program. This means C-level approval and sponsorship, for sure. But it should also include your counterparts in other groups or divisions across the company. The reason for the first need is probably pretty obvious; without executive approval (and likely sponsorship, in many cases), a project that aims to fundamentally change the way cyber exposure is measured throughout the organization is unlikely to get very far. Connecting with your peers may not be as obvious—but it's equally as important.

Build a VM strategy that detects all assets and identifies key processes across the entire attack surface.

Unfortunately, all too often other departments are ignored or forgotten, so the risk-based VM strategy is deployed by one group and not the others. This can lead to problems because, as mentioned above, risk-based VM is a fundamentally different way of assessing vulnerabilities, prioritizing remediation efforts and measuring cyber exposure—and the team's effectiveness in reducing that exposure. So, if one group migrates to risk-based VM while the others continue with legacy methods, the reports won't effectively roll up to upper management; in turn, leadership may reject the risk-based way—even if you can prove that it's a superior method.

3. Discover and Map

You also need to identify, discover and map all assets across your entire attack spectrum. This means identifying all subnets throughout your environment and developing a scan strategy to discover all assets located within those subnets. You can then establish scan policies and profiles for each subnet, based on the agreements you made with the individual owners and stakeholders during the initial phases of the Discover step, where you made a concerted effort to understand the business environment.

Once you've done this, you'll want to review and categorize all discovered assets, and then reconcile the results with your configuration management database (CMDB) or other asset management system to ensure that every asset is properly accounted for. With this information in hand, you can review your sensor deployment plan and make any necessary updates to ensure all requirements are met.

Questions to Ask:

Do I have executive buy-in/sponsorship?

Are other groups throughout the organization on board?

Where are all assets located?

What types of environments are the assets in (e.g., traditional IT, OT/IoT, cloud, virtual, containers)?

Which systems, services and applications are business-critical? Who are the owners and key stakeholders for each of them?

Is there a security framework or are there compliance requirements that need to be adhered to?

Do I have the sensors I need to provide visibility across my entire attack surface?

Product Recommendations:

Most legacy scanners weren't designed to handle the modern attack surface and the growing number of threats that come with them. Instead, they typically only deliver visibility into traditional IT environments, so they completely miss any vulnerabilities that are present in the most dynamic aspects of the modern attack surface. Tenable offers a comprehensive solution that delivers active scanning, passive monitoring, connectors and integrations to discover assets across your entire attack surface:

Scanner:

- Nessus Professional (for network scanning)
- Nessus Network Monitor (for passive network monitoring)

Platform:

- Tenable.io (for cloud environments)
- Tenable.sc (for on-premises environments)
- Tenable.ot (for OT environments)
- Integrated sensors and agents

Application Security:

- Tenable.io Container Security
- Tenable.io Web Application Scanning

Tenable Integrations:

- Configuration Management Database (CMDB):
- Axonius
- Microsoft
- ServiceNOW

Assess

Next, you'll need to prepare to fully assess all your assets, regardless of where they reside, what environment they're in, whether or not they are within audit scope, and how frequently they're connected to the network.

1. Scan Discovered Assets for Vulnerabilities

First, you'll need to go beyond your traditional IT network to assess your entire attack surface for vulnerabilities, including any assets you have in cloud, OT and container environments. Transient assets must be included, as well. Having an integrated web app scanner is important too, since the majority of your organization's sensitive data lives in, or runs through, apps — which has made the application layer a primary attack vector.

If you're in an industry that's subject to regulatory compliance, it's tempting to develop your assessment plan around passing audits. But limiting your assessments to assets that are within audit scope often causes other business-critical systems to be ignored. Remember that passing an audit doesn't mean you're secure. But if you're secure, you'll likely pass that portion of the audit, as well.

Including your entire attack surface in your assessment plan is absolutely essential, because adversaries are scanning all of these environments to find the easiest way in. So, any aspect of your environment that you're not regularly assessing leaves a blind spot in your VM strategy — thereby creating a cyber exposure gap that can be exploited by attackers without being detected. Also, to ensure complete coverage of your entire attack surface, plan for any assessments to be done from a credentialed, authenticated state. Local agents or network scans using administrator credentials mean that you'll have complete visibility on the true security posture of each asset no matter where it is in your environment.

In addition to ensuring that your assessment plan is broad enough to cover your entire attack surface, it's also essential to ensure that you're assessing your network frequently enough. All too commonly, assessment plans call for monthly scans; sometimes even less frequently. But if you don't perform assessments frequently enough, you'll be basing your remediation decisions on old, outdated information.

It's important to remember that the threat landscape is dynamic in nature, so to be useful, your security intelligence needs to be dynamic, as well. Using static, point-in-time analyses can lead to late and incomplete remediations. As such, your assessment plan needs to include continuous assessment of all known assets. In addition, your assessment tools need to be capable of dynamically discovering new assets the moment they join the network. This includes transient assets in both physical and virtual environments.

2. Audit Configurations

Next, you'll need to harden your assets to decrease your attack surface to the furthest extent possible. This includes ensuring that operating systems and applications meet industry standards (e.g., PCI, NIST, CIS) to comply with auditing frameworks and baseline configurations. This is an essential step because misconfigurations represent a significant entry point for adversaries and can therefore be employed as an attack vector.

Create a "gold image" standard for all system builds.

Organizations must start by determining what a standard hardened configuration looks like for the various assets identified throughout the network. Starting with frameworks such as the Center for Internet Security (CIS) Benchmarks is a de facto best practice that provides solid security with a well-understood and easily measured set of configuration settings. You'll need to modify these frameworks based on your business needs.

Once a standard configuration is in place, you can use it to create a "gold image" standard for all system builds and deployments to ensure consistency for any new systems deployed. These gold images can be further hardened on a regular basis using a risk-based VM program to determine if any patches are missing or other vulnerabilities are present so they can be remediated before replicating and deploying the image. Additionally, validating whether or not existing systems meet the required configuration settings is a core function of a risk-based VM program, and can be leveraged with the same infrastructure you've deployed to conduct vulnerability scans.

Questions to Ask:

How am I scanning today? What's working well? Where do I need to improve?

Do I have blind spots in my assessment plan?

Am I scanning frequently enough?

Do I support authenticated scanning across my entire network?

Am I actively/passively assessing all in-scope asset types, in all environments (e.g., IT, OT, containers)?

Do I have the tools I need to assess my entire attack surface?

Can my assessment tools dynamically discover new assets and continuously assess existing assets?

Am I auditing configurations today? Is the process working well?

Product Recommendations:

Legacy VM scans are typically performed infrequently and concentrated on a portion of the network. As a result, security teams typically have incomplete data that's old and static, so they don't know what poses the most risk. Instead, they end up waiting until a security event occurs and then go into reactive, incident response mode. What you need is a VM solution that can address the entire attack surface and continuously assess all known assets — plus immediately discover and assess any new assets. Tenable thoroughly assesses the entire attack surface, including on-premises infrastructure, endpoints, cloud infrastructure, web applications, containers, mobile devices and OT:

Scanner:

- Nessus Professional (for network scanning)
- Nessus Network Monitor (for passive network monitoring)

Platform:

- Tenable.io (for cloud environments)
- Tenable.sc (for on-premises environments)
- Tenable.ot (for OT environments)
- Integrated sensors and agents

Application Security:

- Tenable.io Container Security
- Tenable.io Web Application Scanning
- Tenable.io PCI ASV

Tenable Integrations:

Configuration Management Database (CMDB):

- Axonius
- Microsoft
- ServiceNOW

Patch Management

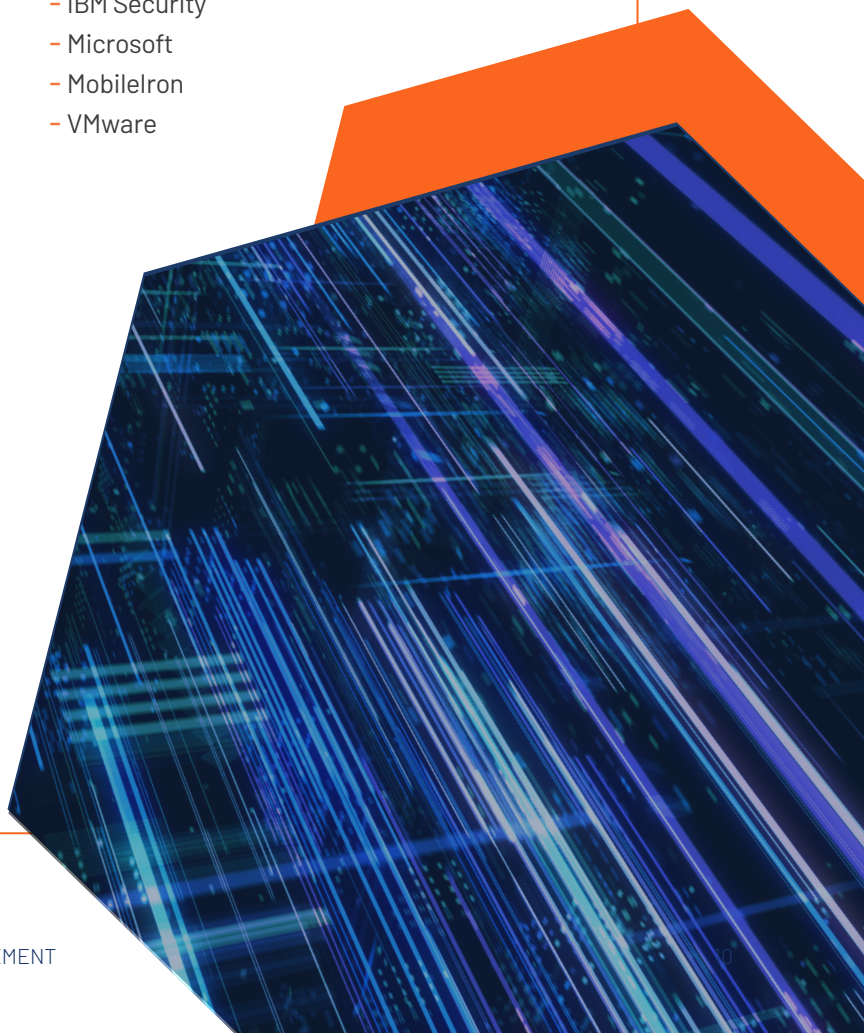
- Autonomic Software
- Dell
- Red Hat
- Symantec

Privileged Access Management (PAM)

- Arcon
- BeyondTrust
- Centrify
- CyberArk
- HashiCorp
- Thycotic

Mobile Device Management (MDM)

- Apple
- BlackBerry
- IBM Security
- Microsoft
- MobileIron
- VMware



Prioritize

Now that you can see all the vulnerabilities across your entire attack surface, you need to understand them in the context of business risk and use that data to prioritize your team's efforts, so you can focus on the vulnerabilities and assets that matter most.

1. Prioritize Vulnerabilities and Assets

Vulnerabilities

Most legacy methods employ the Common Vulnerability Scoring System (CVSS) to prioritize which vulnerabilities to remediate first. For example, a typical organizational policy is to remediate all vulnerabilities with a CVSS score of 7 and above. This method has become commonplace among most security teams, yet it's proven to be inefficient and ineffective when taken in isolation. That's because while v3 of CVSS has certainly made some improvements over past versions, it still suffers from significant problems — not least of which is the fact that it's risk-unaware. Since most CVSS scores are assigned within two weeks of vulnerability discovery, the score only employs a theoretical view of the risk a vulnerability could potentially introduce. That leads security teams to waste the majority of their time chasing after the wrong issues while missing many of the most critical vulnerabilities that pose the greatest risk to the business.

Another major problem is that most teams only use the CVSS base score which never changes, irrespective of the changes in the threat landscape. That's because the base score doesn't have any degree of context from which to understand the actual risk a vulnerability poses to the business. And while CVSSv3 introduced environmental and temporal scores to supplement the base score, these two additional components are often difficult to understand and haven't proven to be terribly effective for measuring risk. As a result, the majority of organizations opt to simply continue to use the base score, exclusively.

Vulnerabilities with the highest risk, residing on your most important assets, makes them highest priority.

Assets

Fully understanding the assets affected by critical vulnerabilities is every bit as important as the vulnerabilities themselves. After all, it's that combination — vulnerabilities with the highest risk, residing on your most important assets — that makes them your highest priority. For example, if you had a vulnerability with a criticality rating of 10.0 (on a scale of 1 to 10) on a secondary file server and another with a criticality rating of 6.5 on the server that houses all of your company financials as well as sensitive customer information, most would likely opt to fix the "6.5" first.

Legacy VM tools lack any sort of asset criticality analysis, causing you to conduct this analysis manually and potentially miss the "6.5" altogether. As a result, that risk would remain on one of your most critical assets while you focused your attention elsewhere. Focusing only on the technical risk of a vulnerability, without taking into account the context of the importance of the asset itself to your business is one of the glaring weaknesses of legacy VM programs. It's why leveraging a risk-based VM program to get more complete visibility on the criticality of your assets and their vulnerabilities means you can get a view of the true risk present in your organization. It's also important to note that even many risk-based VM tools either ignore asset criticality, altogether, deem every asset to be a priority level of 10, or require you to manually enter the criticality level into their system for every one of your assets.

Using a VM program means you can get a view of the true risk present to your organization.

2. Assess Risk

So, to effectively prioritize the vulnerabilities that pose the most risk, you need to understand the full context of each vulnerability. While the CVSS score is a good place to start, before it can be useful it must be fortified with other essential security data, including:

Threat and exploit intelligence:

- Current attacker activity
- Threat sources
- Traffic from suspicious locations or unusual IP addresses

Detailed information about the vulnerability:

- An understanding of how long the vulnerability has been around
- The degree to which the vulnerability is exploitable (e.g., Is authentication required? Is it publicly accessible?)
- How frequently the threat is being seen
- The potential for harm (e.g., exfiltration of sensitive data)

Criticality of the affected assets:

- Where the asset is located and its level of exposure to the Internet
- The type of device for a given asset
- Device functionality

Predictive technology to determine likely future attacker activity

Of course, the above is far from an exhaustive list, but it should provide an idea of the plentitude of security data that's available. It should also serve to illustrate how much in-depth analysis is required in addition to just a one-dimensional score, prior to making prioritization decisions. Armed with the full context of each vulnerability, security teams are able to focus on the assets and vulnerabilities that matter most.

Questions to Ask:

How am I prioritizing my remediation efforts today?

Am I responding appropriately — and in a timely fashion — to my most critical vulnerabilities?

Am I supplementing CVSS with additional security data to assess vulnerabilities in context?

Do my vulnerability scores change with changes in the threat landscape?

Do I have confidence in the scores assigned to my vulnerabilities?

Am I sure I'm prioritizing the correct vulnerabilities?

Product Recommendations:

All of this extra data analysis simply isn't practical to do on your own. Therefore, you'll want your VM platform to employ machine learning automation, so it's capable of rapidly determining the business risk of every vulnerability to help security teams prioritize their remediation efforts. In addition to the CVSS score, Tenable correlates and analyzes other essential contextual elements, including threat and exploit intelligence, an assessment of asset criticality and continuous analysis of a 4.5+ petabyte data lake that includes more than 20 trillion threat, vulnerability and asset data points. All of this data is correlated and processed using machine learning automation to render an accurate risk score for every vulnerability within seconds:

Analytics:

- Tenable Lumin

Integrations:

Security Information and Event Management (SIEM)

- IBM Security (QRadar)
- LogRhythm
- Splunk
- Stellar Cyber
- Swimlane
- Syncurity
- W@tchTower

Configuration Management Database (CMDB)

- Axonius
- Microsoft
- ServiceNOW

Ticketing System:

- Atlassian (Jira)
- ServiceNOW

Remediate

Once you've determined which vulnerabilities are the highest priority, you'll need to take the appropriate action to effectively manage the risk. For each vulnerability, you have three response options — remediate, mitigate, or accept. Which action you choose for each should be in line with what you previously determined during the initial discover phase, as you developed a comprehensive understanding of your environment. But to be sure we're clear on our terminology, here's how we define each of them:

Remediate

Oftentimes, remediation is used interchangeably with patching. And in some cases, patching may be all that's required. But it's important to note that typically, applying a patch is just one part of what's required to remediate a vulnerability. The asset may also require removal or rebuilding, the operating system or specific software components may need to be upgraded, or there could be a configuration error that needs to be corrected. Once the vulnerability is verified to have been fully remediated, the amount of risk associated with the vulnerability is fully removed from the environment.

Mitigate

Mitigation employs other technologies to reduce the risk of a given vulnerability. This is different than remediation, because with mitigation you haven't done anything to actually fix the vulnerability itself. Instead, you're accounting for other mitigating factors that neutralize some or all of the risk posed by the vulnerability. For example, you may have firewall rules in place that effectively block an exploit from accessing sensitive data. To account for this mitigating factor, you would reduce the severity of the vulnerability accordingly.

Accept

Risk acceptance is consciously deciding to not take any action at all. This may be done for a variety of reasons. For example, during the discovery phase, you may have determined that some assets are so business-critical that you can't afford to take them down for maintenance unless the vulnerability is also business-critical. In other cases, the cost of the fix may be greater than the cost associated with a successful exploit. Regardless of the reason, when you choose to accept risk, your VM platform may allow you to remove the risk score from your reports or set it to "0". However, it's important to understand that while it may no longer be immediately visible to you, the actual risk still remains in your environment.

For the vulnerabilities you choose to remediate, you'll want a VM platform that tightly integrates with your ticketing system so you can send tickets directly to IT from your VM platform, pre-populated with the information they'll need to understand what to fix, how to fix it, and why it's a priority. Auto-ticketing capabilities further streamline the effort and maximize the efficiency of the entire process. Communications should also be bi-directional and fully integrate with the ticketing system's workflow so IT can initiate scans to validate their remediations.

Integration with workflow platforms, security information and event management (SIEM) systems, and security orchestration, automation and response (SOAR) tools can also help streamline your efforts to maximize your team's efficiency.

Send pre-populated tickets directly to IT from your VM platform

Questions to Ask:

What is my process for determining what action to take for high priority vulnerabilities?

What is my authorization process for accepting risk?

How do I confirm that the desired action was performed?

What's my process for opening tickets for vulnerabilities that require remediation?

How do I validate that remediations have been performed — and performed correctly — by IT?

Do I integrate with workflow, SOAR, or SIEM tools to maximize efficiencies? What's working well, and where can improvements be made?

Product Recommendations:

In addition to helping the security team maximize its efficiency, integration with SOAR, SIEM, ticketing and workflow management tools can help you more effectively partner with IT. This is especially the case with ticketing and workflow management tools, which can automate bi-directional communications and intelligence sharing between the two groups. Tenable tightly integrates with myriad remediation tools to facilitate teamwork and seamless handoffs between security and IT to maximize efficient operations:

Platform:

- Tenable.io (for cloud environments)
- Tenable.sc (for on-premises environments)
- Tenable.ot (for OT environments)

Analytics:

- Tenable Lumin

Application Security:

- Tenable.io Container Security
- Tenable.io Web Application Scanning

Tenable Integrations:

Security Information and Event Management (SIEM)

- IBM Security (QRadar)
- LogRhythm
- Splunk
- Stellar Cyber
- Swimlane
- Syncurity
- W@tchTower

Security Orchestration, Automation and Response (SOAR):

- Analyst Platform
- Blackpoint Cyber
- Chronicle
- Cortex XSOAR
- DF Labs
- ForeScout
- Fortinet
- Siemplify
- ZeroNorth

Ticketing System

- Atlassian (Jira)
- ServiceNOW

Patch Management

- Autonomic Software
- Dell
- Red Hat
- Symantec

Measure

Finally, you'll need the ability to measure key performance indicators (KPIs) for process integrity as well as business metrics to understand and communicate the value of your risk-based VM program. That means you'll need to identify:

Process integrity metrics

This includes metrics such as scan coverage, scan frequency, scan depth, mean time to assess (MTTA), and mean time to remediate (MTTR).

Business risk metrics

No matter what, you need to track your organization's overall risk metrics over time so you can clearly see—and articulate—the team's progress. Depending on how granular you want to get, you can maintain separate measurements for each region, office, business unit, or asset group.

Assessment maturity metrics

To ensure that risk metrics are based on highly credible data, you'll need to understand the maturity of your security program. If you're not scanning regularly enough, you may be taking action on outdated information. If your security assessments lack sufficient breadth or depth, you may have blind spots in your network, so the vulnerabilities on key assets may be invisible to you.

Benchmarking metrics

Once you understand how much risk you have across your attack surface, the next step is to assess how that amount relates to the rest of your industry. The ability to compare your level of risk against that of your industry peers delivers a degree of context that helps security teams truly understand how they're doing.

The benefit of these metrics is two-fold. First, they help security teams more deeply understand the effectiveness of their security program and highlight areas for improvement. And second, they can be used to regularly report the team's progress to management and facilitate the ability to articulate clear answers when questions or high-profile exploits occur. In short, having a rich set of reporting and analysis tools enables you to effectively communicate the team's efficiency — to gain and maintain management's confidence in your abilities.

In addition to the tools, themselves, you'll need to work with the various security groups throughout the organization to develop common dashboards that ensure consistent reporting. This will undoubtedly include dashboards that provide a graphical display of each of your KPIs

and other important metrics to enable at-a-glance assessments of the organization's current risk posture, as well as how that posture has changed over time. You'll also need to work with your management to decide when and how often reporting should occur, to ensure expectations are met.

Questions to Ask:

How do I measure the integrity of my VM process?

How do I measure how much risk the business is exposed to?

What KPIs should I be measuring?

How frequently should I be reporting to management?

Do I have a VM platform that's capable of delivering the level of reporting I need?

Is my VM platform flexible enough to deliver specific reports as business needs change?

Product Recommendations:

The need to measure the effectiveness of your security program cannot be overemphasized. A robust reporting system that can deliver timely, accurate results that are produced to your exact specifications enables you to truly understand what's going well and where there are areas for improvement. With full visibility into your team's effectiveness and the integrity of your systems, you'll be capable of making necessary adjustments to ensure the team is maximizing its efficiency. And when high-profile exploits occur, you'll be able to clearly articulate the extent and the location of the exposure.

Tenable delivers clear visibility and in-depth reporting capabilities to empower security leaders with the knowledge they need to make the right decisions — and to stand by those decisions when questions are raised. This visibility also enables them to keep the board and other executives out of "panic mode" during times of high-profile threats. And Tenable's peer benchmarking and maturity assessments help you understand how your security program compares to the rest of the industry, so you know if improvements are required:

Platform:

- Tenable.io (for cloud environments)
- Tenable.sc (for on-premises environments)
- Tenable.ot (for OT environments)

Analytics:

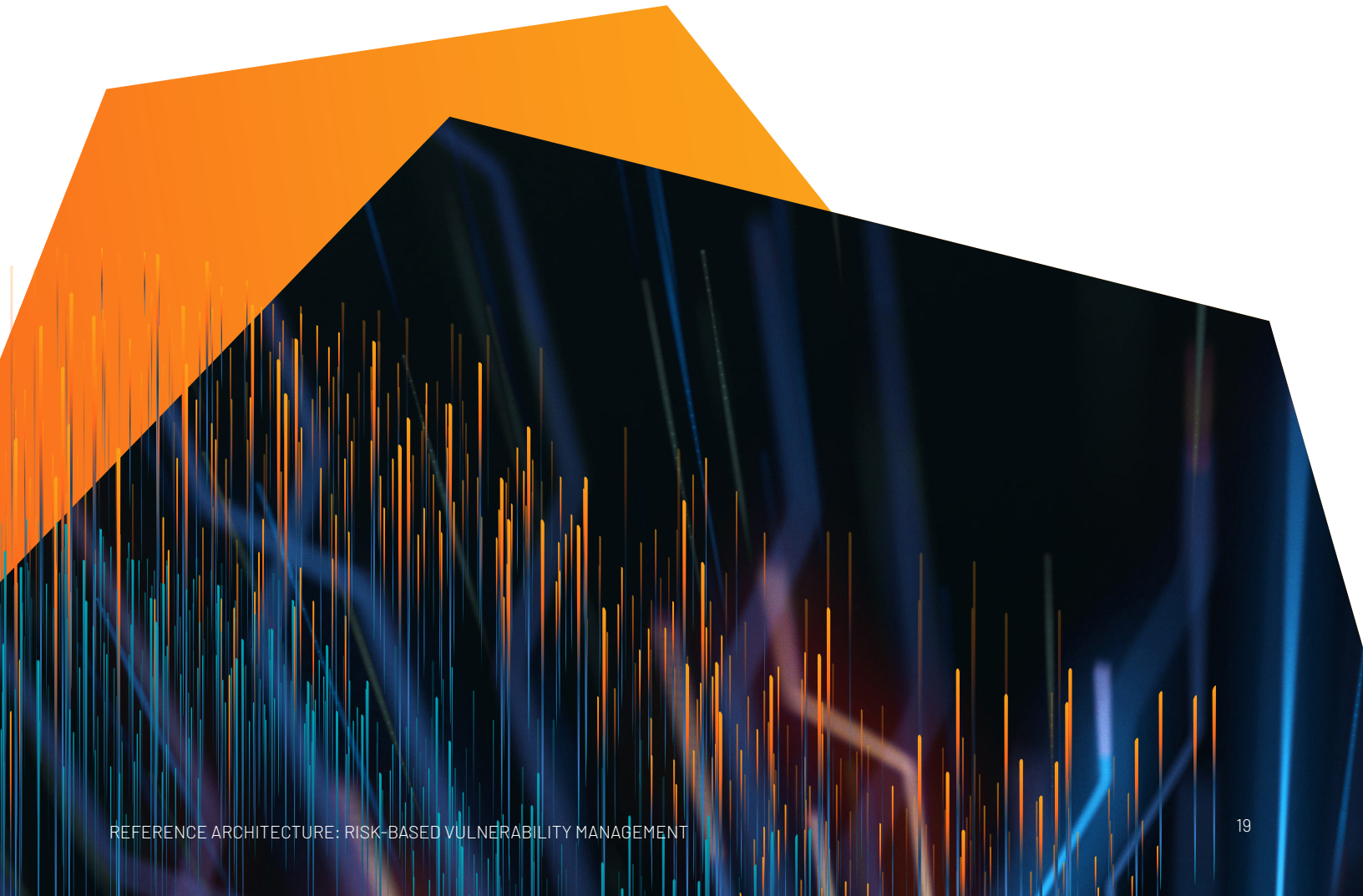
- Tenable Lumin

Commit to Improving Your VM Capabilities

While the evolution to risk-based VM admitedly contains a number of steps, it's actually easier to implement than you think. And, once you move to this proactive, strategic methodology, you can immediately begin reaping the benefits of a VM program that delivers the dynamic, continuous visibility you need to proactively manage risk and make strategic decisions.

Risk-based VM eliminates the blind spots that plague legacy tools and enables you to prioritize your remediation efforts so you can focus on the critical vulnerabilities affecting your most important assets. This, in turn, helps you make the most efficient use of your limited security resources by producing the greatest reduction in risk with the least amount of effort.

While this reference architecture provides a comprehensive overview of the tools, technologies and processes you need to implement a risk-based VM program, the migration can still be challenging if you attempt to do it on your own. Tenable can help you achieve your goals, quickly and efficiently. We have technical specialists that can work with you every step of the way to help you maximize your success.



7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046

North America +1 (410) 872-0555

www.tenable.com

070620 R01 V06