tenable

Agentless vulnerability management for cloud and hybrid environments

Realize 360-degree visibility of your cloud assets and exposure in minutes

Even with continuous detection of the latest CVEs, traditional vulnerability management solutions leave gaps in cloud security posture. In fact, many of the highest profile breaches, such as the 2019 Capital One data breach1[1], involve cloud misconfigurations[2]. To address these challenges, Tenable One for Cloud Security brings together market-leading vulnerability management (VM) and cloud security posture management (CSPM) capabilities in a single unified approach, providing comprehensive visibility into all cloud exposure, including vulnerabilities, misconfigurations, excess privileges, drift and compliance. With near real-time detection of cloud risks, prescriptive remediations and advanced risk-based scoring, Tenable is uniquely positioned to help you prioritize the risks that poses the highest potential threat to your organization.

1 *Source: Dark Reading, "Capital One Attacker Exploited Misconfigured AWS Databases," June 20, 2022*

2 *Source: Network Computing, "Misconfigurations: Still the Biggest Threat to Cloud Security," August 25, 2021*

Tenable One for cloud security solution highlights

Comprehensive visibility
Provides seamless exposure management across hybrid environments – IT, private cloud and public clouds – in a single unified platform.

Rapid deployment
Deploys in only a few clicks, and begins scanning and delivering visibility into vulnerabilities and misconfigurations in minutes.

Safe
Agentless assessment uses read-only access to cloud provider snapshots, so sensitive data never leaves your environment.

Low overhead
Requires no credentials for setup, with no administrative overhead or system impact.

Reduced risk
Intelligent vulnerability scoring reduces noise and prioritizes risk that has the highest potential impact.

360-degree Views
Provides a unified view of asset details, vulnerabilities, misconfigurations, drift and compliance in a single-pane-of-glass.

Cost-effective
Delivers vulnerability, cloud security posture and exposure management in a single solution for the same price.

Cloud brings new security challenges

If you're like many enterprises, you are strategically moving workloads to the cloud. In fact, most organizations today are using multiple clouds to address unique workload requirements, build scalable cloud native apps using microservices, containers and Kubernetes, and speed time-to-market with continuous delivery practices. The result is highly distributed, rapidly changing hybrid environments that are orders of magnitude more complex — with hundreds to thousands more moving parts than traditional environments running monolithic apps on virtual machines.

And with rapid adoption of cloud, comes rapid growth in the number of developers employed at an organization — often outpacing security teams. In fact, it's not uncommon for developers to outnumber security specialists by as much as 100:1[3]. With more developers continuously delivering code — faster — and greater complexity in the systems being used, comes heightened probability that misconfigurations and drift will be being introduced to production, elevating risk.

"Having two [cloud] environments does not double the complexity… but quadruples it. An organization with three IaaS environments and one on-premises virtualized environment faces 16 times the complexity.[4]"

3 *Source: https://www.devops-certification.org/How_Do_You_Ensure_Your_DevOps_Information_Security.php*

4 *Source: IDC Worldwide Cloud Workload Security Forecast, 2022–2026: Complexity Drives the Market Up and to the Right, Doc #US49522022, Aug 2022*

"The average public container today has 287 vulnerabilities, with the number of high/critical severity instances up 50% in just one year."

—Slim.ai 2022 Public Container Report[5]

5 *Source: Slim.ai, "2022 Public Container Report," Oct. 26, 2022*

All approaches to vulnerability management are not created equal

The ephemeral nature of cloud and continuous delivery practices have made traditional agent and network scanning approaches impractical for cloud security.

Deploying agents on every cloud instance or container brings considerable overhead. And periodic network scanning leaves gaps in visibility that can persist for days. With autoscaling, a single vulnerable image can be replicated in volume, before a scheduled scan can detect it.

And while many cloud security players are adding vulnerability scanning, they lack a deep knowledgebase of known vulnerabilities and remediations, and are not able to provide a complete end-to-end view of risk across hybrid environments.

Security at the scale and speed of cloud

To be effective, vulnerability management must keep pace with the rapid change of cloud. It must detect risk as it is introduced, eliminate noise to make staff more productive, and be lightweight, minimizing overhead associated with deploying agents everywhere. It must also address all varieties of vulnerabilities — CVEs, misconfigurations, drift and compliance.

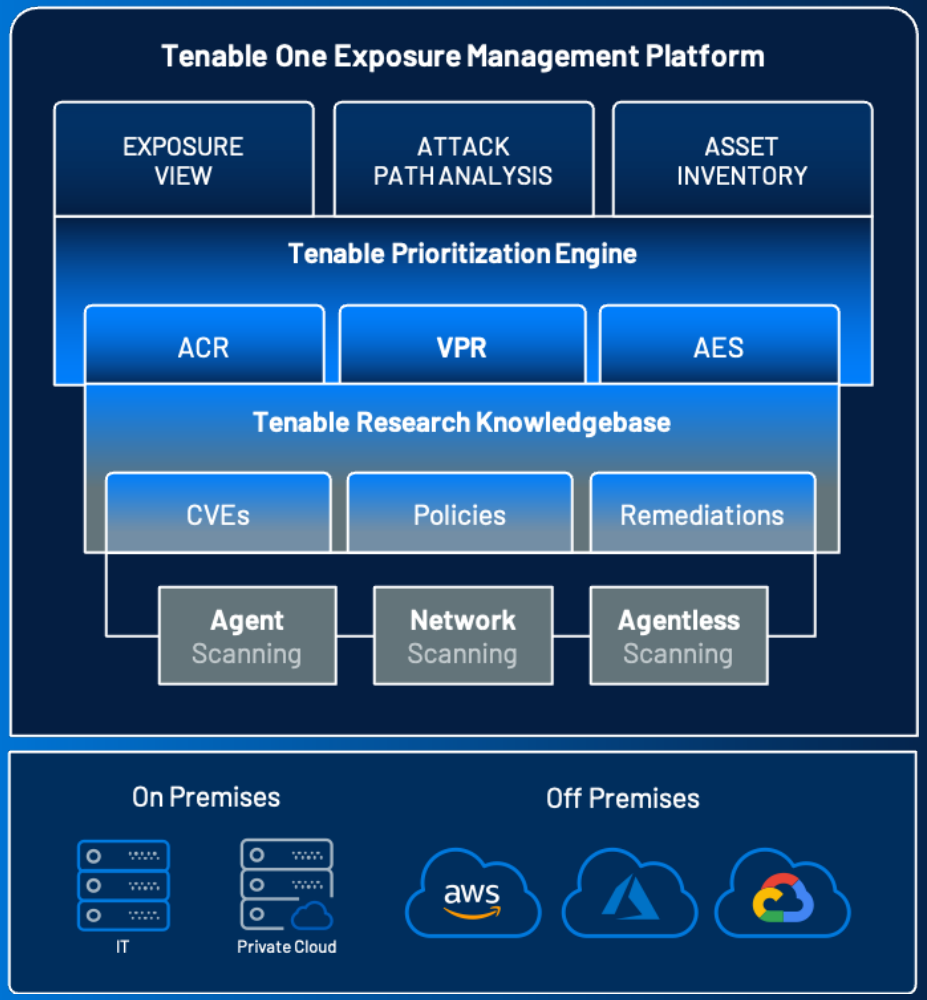
Tenable One for Cloud Security is unified cloud security platform that deploys and delivers value in minutes, providing visibility into every cloud asset and exposure, without the agent overhead and configuration. It leverages Tenable's extensive leadership in zero-day discovery and risk prioritization to deliver the first of its kind, cloud-based vulnerability management solution.

"83% of organizations have had more than one data breach. And nearly half of breaches were cloud based."

— IBM Cost of a Data Breach Report 2022[6]

6 *Source: IBM, "Cost of a Data Breach 2022 Report," July 2022*

Security at the scale of cloud requires a unified approach to cloud visibility and exposure management



Scaling vulnerability management for public and hybrid cloud environments

Exposure management

See cloud, on premises and overall cyber exposure score (CES) alongside peer benchmark scores, and drill into asset inventory and role-based views.

Industry-leading prioritization

Apply the same consistent risk-based prioritization (asset criticality rating / vulnerability priority rating / asset exposure score) across hybrid environments.

Unmatched security expertise

Access the extensive knowledgebase of over 73,000 vulnerabilities, 1,500 benchmark policies for configuration and compliance (e.g.CIS), and prescriptive remediations from Tenable Research.

Breadth and depth

Leverage agentless scanning to keep pace with rapidly changing cloud native, public cloud environments. Apply agents or network scanning for deep visibility into persistent IT, and virtual machines in private/hybrid cloud environments.

Unmatched expertise and technology, put to work in the cloud

As both a provider of traditional on-premises software and SaaS-based security solutions, Tenable understands the unique challenges of moving to and securing cloud workloads and we've brought that together to deliver a world class, SaaS-based solution.

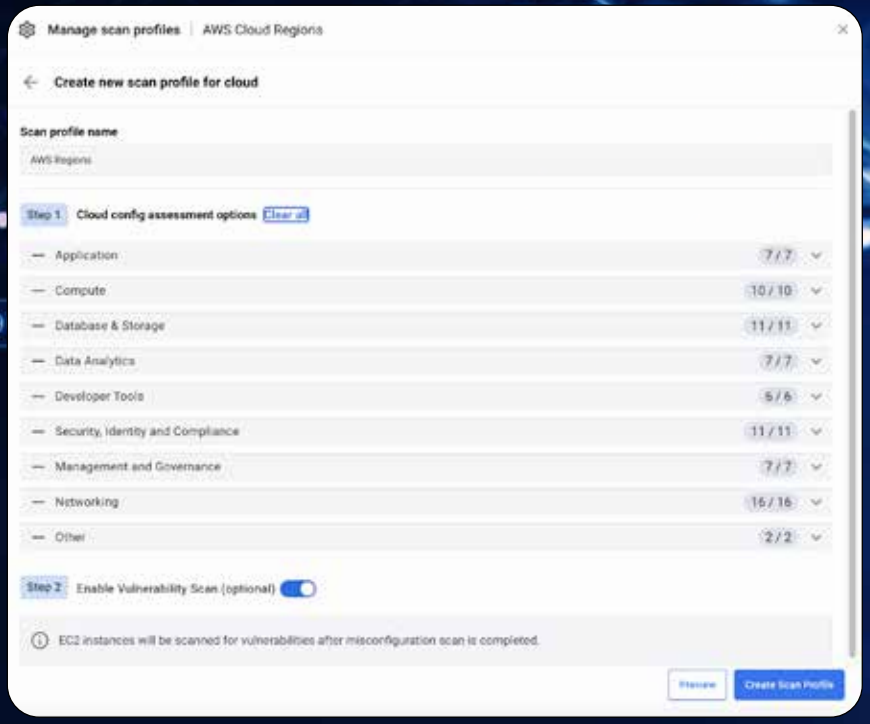
- To ensure deep visibility into CVEs and zero day vulnerabilities, we've built Tenable One for Cloud Security with proven Nessus threat detection, harnessing the extensive knowledgebase of over 73,000 CVEs and remediations from Tenable Research.
- To ensure compliant cloud configurations in runtime, we've leveraged the database of 1,056 audits covering 401 benchmarks from Tenable Research — the same foundation used by Nessus for auditing on prem configurations.
- To prevent risky deployments from reaching production, we've built on the infrastructure as code (IaC) scanning and DevOps integrations provided by Tenable's Accurics acquisition, and the IaC security policies from Terrascan, an open source project led by Tenable with over 200,000 downloads.

Are you an IaC developer or cloud security architect?

Try Terrascan in your browser for free.

terrascan by tenable

“Agentless Assessment is truly frictionless. Super easy to onboard, love that it’s scalable with the stacksets, and can’t wait to get it deployed.”



Scan cloud resources for vulnerabilities and misconfigurations with just a click.

Instantly detect new zero day vulnerabilities

Designed for rapid-time-to-value, **Agentless Assessment with Live Results** in Tenable One for Cloud Security onboards cloud accounts using only APIs. Unlike Frictionless Assessment provided by Tenable.io, which requires cloud provider agents, Agentless Assessment with Live Results inventories cloud assets and scans for cloud vulnerabilities without the need to install agents, configure credentials on target hosts or set up scan policies.

Cloud inventory is collected from snapshots of the environment via APIs without any impact on compute speed or costs. When new snapshots are detected, Tenable One for Cloud Security automatically triggers a scan to assess vulnerabilities. As new CVEs are published by Tenable Research, Live Results immediately identifies them without the need to wait for a scheduled scan or manually initiate one.

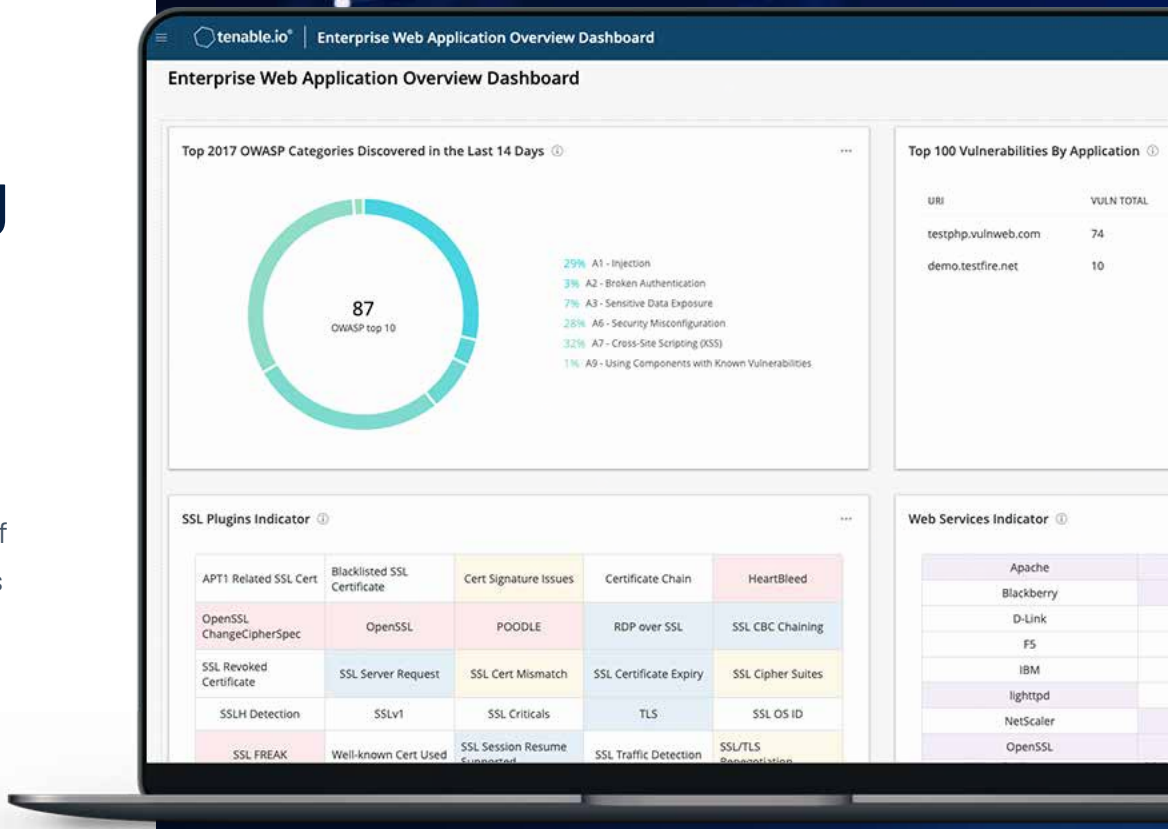
Gain deep hybrid visibility with Nessus agents, network and app scanning

Tenable One for Cloud Security offers optional agent, network and web application scanning to provide deep visibility for hybrid environments.

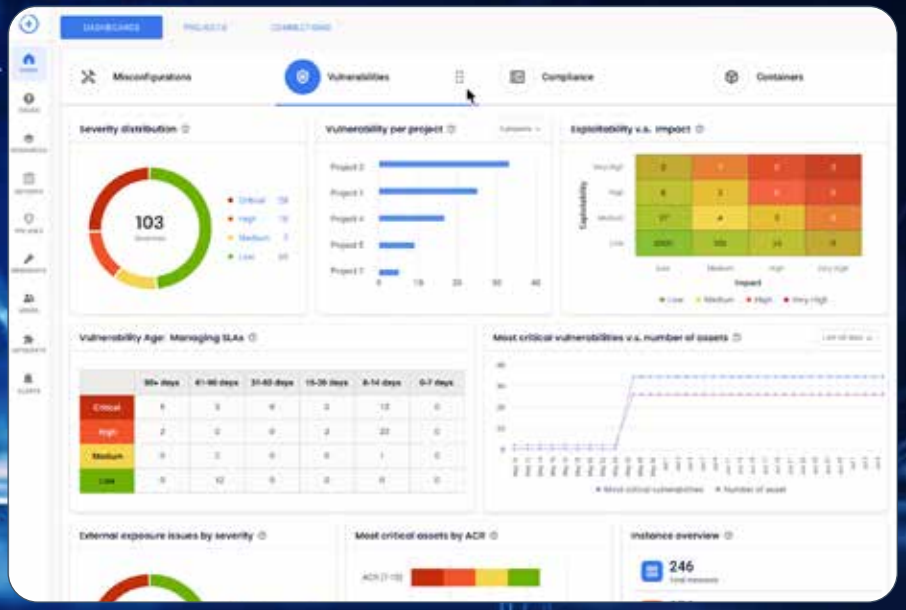
Agent scanning uses a host-based Nessus scanner to actively interrogate virtual machines in the cloud and detect the presence of vulnerabilities. Vulnerabilities include the full library of known CVEs for operating systems and applications, as well as configuration audits from Tenable Research.

Network scanning uses network-based Nessus scanners to actively interrogate virtual machines in the cloud for vulnerabilities. Network scanning can be valuable to extend visibility into assets that come and go, as well as to provide insights into vulnerabilities from the outside in, to understand the external attackers point of view.

Web application scanning uses dynamic application security testing to crawl domains and create a site map of web applications and pages. It identifies any vulnerabilities in application custom code or known vulnerabilities in the third-party components that comprise the bulk of the application.



Easily scan traditional HTML web applications and modern, dynamic web applications built using HTML5, JavaScript and AJAX frameworks.



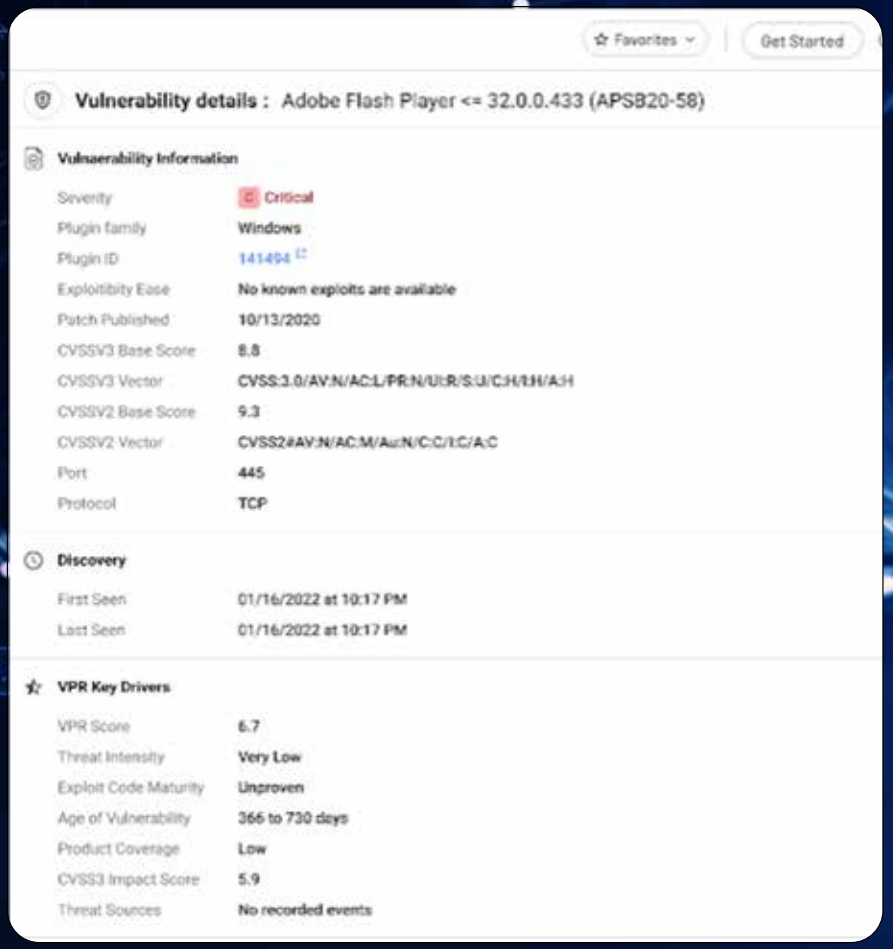
Gain a complete view of cloud vulnerabilities in a single-pane-of-glass alongside other critical asset risk, including misconfigurations, drift, and compliance.

Understand your security and compliance posture

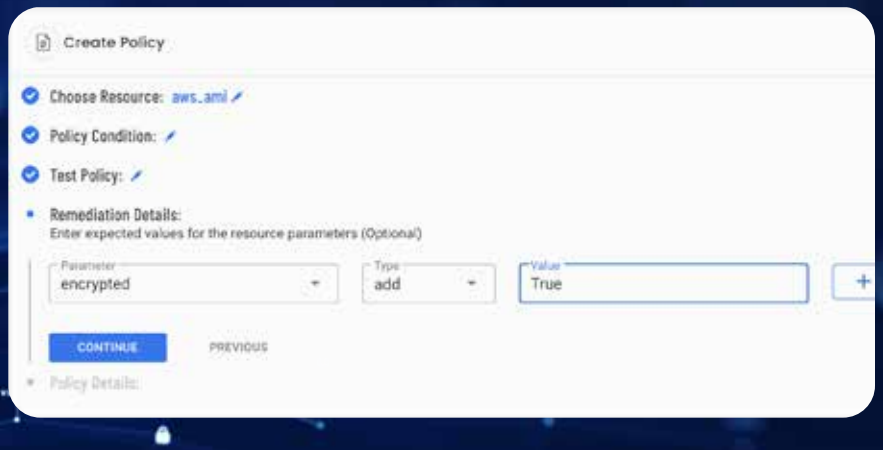
In addition to CVE detection, Tenable One for Cloud Security offers 1,500 out-of-the-box cloud security policies supporting **20 leading benchmarks and regulatory standards**. Quickly detect and remediate misconfigurations, such as excess privileges, unrestricted ports, expired certificates, public access to instances, unencrypted data and configuration drift. Vulnerabilities, misconfigurations and drift are presented in a single-pane-of-glass in role-based views, as well as in contextual views by resource, benchmark or regulatory standard in order to evaluate and report your security and compliance posture.

Reduce exposure with risk-based prioritization and remediation

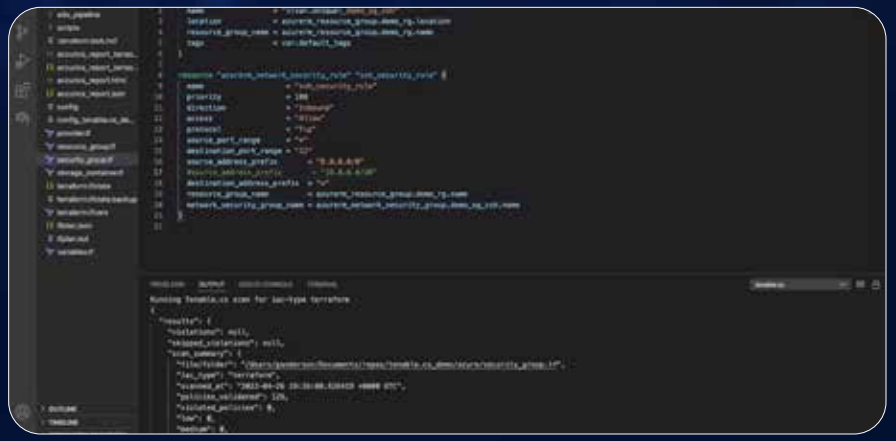
Unlike many VM solutions, Tenable **risk-based prioritization** goes beyond CVSS scores, correlating asset criticality and threat severity using a multitude of dynamic and static variables. For example, prioritization takes into consideration asset connectivity to the internet and exposure of keys and data to determine asset criticality, and CVSS age, impact and exploit maturity to assess threat severity. This same approach is applied to both vulnerabilities and misconfigurations. The result is a reduction in the number of critical severity findings by as much as 23:1 vs CVSSv3, allowing teams to focus on the relatively few vulnerabilities that pose the most risk to your enterprise. DevOps lifecycle integrations and access to step-by-step remediation procedures greatly scale expertise across teams, speeding remediation and improving productivity.



Gain a more accurate understanding of the true risk associated with vulnerabilities for improved prioritization and remediation.



Low-code editor that makes it easy for non-developers to create and edit security policies.



Dev-friendly CLI that makes it easy for developers to run policies and remediate as part of their daily workflows.

Explore policy-as-code in this whitepaper.

Scale security with DevOps friendly workflows

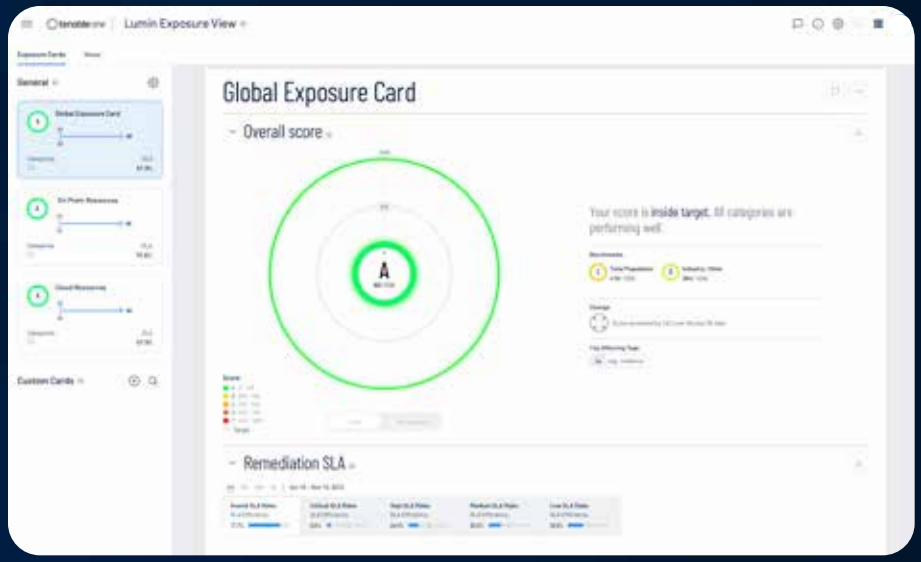
Automated security checks and remediation can greatly impact the speed and productivity of DevOps teams. By translating security policies into codified artifacts, Tenable One for Cloud Security enables cloud security teams to easily automate security checks by directly scanning source code repositories and automating tests as part of CI/CD pipelines. These capabilities ultimately enable security teams to stop vulnerable deployments before reaching production and reducing the number of alerts they need to filter through.

The same codified policies can then be run as part of local development workflows. By doing so, developers can quickly and easily identify and fix policy violations as part of existing workflows, thereby reducing the number of rework requests they have to deal with.

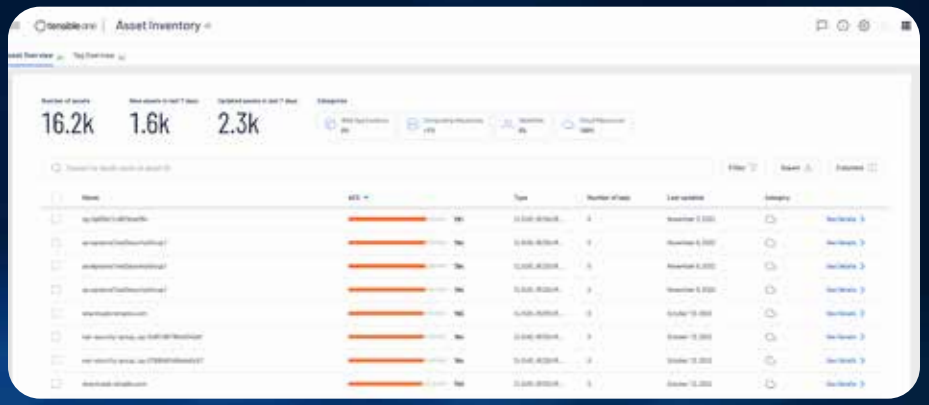
Exposure Management across hybrid environments

Data from Tenable.io, Tenable.cs, Tenable.asm and other Tenable offerings is automatically surfaced within Tenable One for Cloud Security, providing end-to-end visibility into all assets and their vulnerabilities across the entire attack surface.

Exposure Cards for cloud and other domains, along with peer benchmarking, make it easy to assess security posture against industry peers, see trends and determine where and when to make key staff and financial investments.



Quickly assess your overall cloud security posture against industry peer benchmarks and prioritize investments.



Tenable calculates a dynamic asset exposure score (AES) for each asset on your network to represent the asset's relative exposure as an integer between 0 and 1000. A higher AES indicates higher exposure.

“Great for comprehensive visibility. Tenable delivers amazing insights into the vulnerabilities which may impact your company. Not many other products deliver this across so many cloud providers and on-premises.”

— Cloud security architect, entertainment industry organization

“The centralized dashboard helps govern overall organizational risk. The CISO community would benefit from using Tenable’s quantified Cyber Exposure Score (CES) to prioritize mitigation.”

— Chief information security officer, a large enterprise

The Tenable One for Cloud Security advantage

To get ahead of exponential growth in cyberattacks1, enterprises need a scalable approach to security. A unified approach.

Only Tenable One for Cloud Security combines comprehensive discovery of assets and risk, with the industry’s most extensive knowledgebase from Tenable Research, and advanced risk-based scoring and remediations. With Tenable One for Cloud Security, you can operationalize prevention from code to cloud, better utilize limited resources, and pinpoint potential exposures before they impact your business.

Reign in cloud risk. Get started today with a FREE Trial of Tenable Cloud Security .

1Source: Accenture, “Triple Digit Increase in Cyber Attacks,” August 4, 2021

tenable®

01/23 v1