



Tenable Solution Comparison Guide

	Vulnerability Management & Security Center	Cloud Security	Identity Exposure	OT Security	Tenable One
Use Case	Vulnerability management for continuous visibility into the assets and vulnerabilities in your organization	Unified cloud security posture management and vulnerability management across multi-cloud and hybrid environments	Secure identity systems to continuously detect and prevent Active Directory and Azure AD attacks	Visibility, security, and control to protect converged IT/OT industrial networks from vulnerabilities and threats	Exposure Management to understand all exposures and communicate cyber risk across the entire attack surface
Target Role	<ul style="list-style-type: none"> → Security Directors → VM Managers → Security Practitioners 	<ul style="list-style-type: none"> → Security Directors → Cloud Security Managers & Architects → Infrastructure Architects/Managers → DevSecOps 	<ul style="list-style-type: none"> → Security Directors → Security Practitioners → AD/Identity Architects 	<ul style="list-style-type: none"> → Compliance/Risk Officer → IT/OT Security Manager → OT/ICS Security Manager 	<ul style="list-style-type: none"> → CISOs → BISOs and Risk Management Leaders → Security Directors → VM Managers
Attack Surface Coverage	<ul style="list-style-type: none"> → IT Assets → Mobile Devices → Remote Assets → Internet-facing Assets 	<ul style="list-style-type: none"> → Cloud Resources → Cloud Workloads → Containers & Kubernetes → Infrastructure as Code (IaC) → Cloud Identities and Entitlements → Cloud Data 	<ul style="list-style-type: none"> → Directory Services → Identities → Cloud Identities (Entra ID) 	<ul style="list-style-type: none"> → Operational Technology (OT)/Industrial Control Systems (ICS) Assets → IT Assets → Internet of Things (IoT) Assets → Building Management Systems (BMS) 	<ul style="list-style-type: none"> → IT Assets → Cloud Workloads → Cloud Resources → Cloud Data → Directory Services → Identities → Cloud Identities (Entra ID) → Web Applications → Containers & Kubernetes Platforms → Infrastructure as Code (IaC) → Mobile Devices → Remote Assets → Internet-facing Assets → OT Assets → IoT Devices
Deployment Model	<ul style="list-style-type: none"> → Cloud-based (Tenable Vulnerability Management Only) → On-prem (Tenable Security Center Only) 	<ul style="list-style-type: none"> → Cloud-based 	<ul style="list-style-type: none"> → Cloud-based → On-prem 	<ul style="list-style-type: none"> → On-prem 	<ul style="list-style-type: none"> → Cloud-based

Key Capabilities	<ul style="list-style-type: none"> → Complete visibility of IT and cloud assets and vulnerabilities → Comprehensive compliance audits and reporting → Risk-based vulnerability prioritization based on threat context → Fully customizable reports and templates 	<ul style="list-style-type: none"> → Visibility into cloud assets, identities and risk across multi-cloud → Agentless vulnerability scanning for container images, virtual machines, serverless functions and Kubernetes clusters → Self-Service Just-in-Time (JIT) access to enforce least privilege at scale → Full stack contextual risk analysis to surface toxic combinations and attack paths → Identity-centric prioritization and guided or automated remediation 	<ul style="list-style-type: none"> → Complete visibility of identity system misconfigurations, weaknesses and changes → Real-time risk prioritization based on current exposure → View all identities across Active Directory and Entra ID → Real-time attack detection with Indicators of Attack (IoA) 	<ul style="list-style-type: none"> → Discovery and visibility of IT and OT assets and all OT network connections → Risk-based VM to reduce the likelihood of a successful cyber attack → Continuously monitoring OT environment for threats and anomalous activity → Identify security risks with baseline snapshots of IT and OT devices 	<ul style="list-style-type: none"> → Unified visibility of all assets and exposures across attack surface → Risk-based prioritization based on asset, exposure and threat context → Cyber risk analytics and SLA performance tracking → Benchmarking against external peers and internal business units → Attack path analysis to anticipate the consequences of a potential attack → External attack surface management to discover all external-facing assets → All capabilities provided in VM, Cloud Security, Identity Exposure and OT Security
Why Tenable?	<ul style="list-style-type: none"> → Greatest CVE coverage with fewest false positives → Industry leading prioritization to focus on the vulnerabilities that matter most → Most comprehensive technology partner integrations → Multiple sensor technologies (agents, local scanners, passive monitoring) → Ability to release new detections in <24 hours for major security events 	<ul style="list-style-type: none"> → Unified CNAPP solution in an intuitive tool → Industry-leading cloud infrastructure entitlement management → Continuously discover, assess, prioritize and remediate all cloud assets and identities without the need to install agents, configure a scan or manage credentials → Automated CI/CD workflow integration with DevOps tools 	<ul style="list-style-type: none"> → Analyze all identity system exposures, Indicators of Attack and Indicators of Exposure in real-time → Visualize identity risk and improve enterprise exposure management → Real-time prioritization and risk scoring → No agents or privileges to deploy 	<ul style="list-style-type: none"> → Complete visibility of IT & OT assets with both active and passive capabilities → Prioritize vulnerabilities with OT-centric threat intelligence → Ability to leverage IT team's knowledge and investment in existing tools → Risk scores align between IT and OT to help better communicate cyber risk → Detailed insight helps organizations move from a run-to-failure to a preventative maintenance strategy 	<ul style="list-style-type: none"> → Broadest asset and exposure support covering IT, cloud, identity and web apps → Single platform to integrate and categorize all asset and exposure data → Industry leading prioritization, including attack path analysis to anticipate threats → Actionable remediation guidance based on total cyber risk reduction → Centralized and business-aligned view of cyber risk with benchmarking

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 approximately 44,000 customers around the globe. Learn more at www.tenable.com.

Contact Us:

Please email us at sales@tenable.com or visit tenable.com/contact

