

# SCHWACHSTELLEN-MANAGEMENT FÜR DIE ON-PREM-VERWALTUNG IHRER IT-, SICHERHEITS- UND COMPLIANCE-LAGE

**Voller Einblick und wirklich relevante Prognosen. Mit On-Prem-Management.**

Die Tenable.sc-Plattform bietet Ihnen einen umfassenden, integrierten Überblick über die Sicherheitsaufstellung Ihres Unternehmens, sodass Sie Schwachstellen On-Prem genau identifizieren, untersuchen und priorisieren können. Tenable.sc ist eine marktführende Vulnerability Management-Lösung, die Einblick in die dynamische Angriffsfläche des Unternehmens gewährt, damit Sie Ihr Cyberrisiko messen und managen können. Dank innovativer Analytik sowie anpassbarer Dashboards, Berichte und Workflows können Sie mithilfe von Tenable.sc ein gründliches Verständnis Ihres Cyberrisikos entwickeln und wissen, welche Schwachstellen zuerst behoben werden müssen. Tenable.sc setzt auf der führenden Nessus-Technologie auf. Die Lösung wertet die Schwachstellendaten von mehreren im Unternehmen verteilten Nessus®-Scannern aus und stellt Schwachstellen-Trends im zeitlichen Verlauf dar, damit Risiken bewertet und Schwachstellen priorisiert werden können.

Tenable.sc enthält Predictive Prioritization, das Daten und Threat-Intelligence aus mehreren Quellen kombiniert und sie anhand eines datenwissenschaftlichen Algorithmus analysiert. Dieser setzt maschinelle Lerntechniken ein, um die Wahrscheinlichkeit der Ausnutzung einer Schwachstelle durch Angreifer vorherzusagen. So erhalten Sie Echtzeit-Informationen, um Ihre Patching-Maßnahmen besser priorisieren zu können und zu erkennen, welche Schwachstellen zuerst behoben werden müssen.

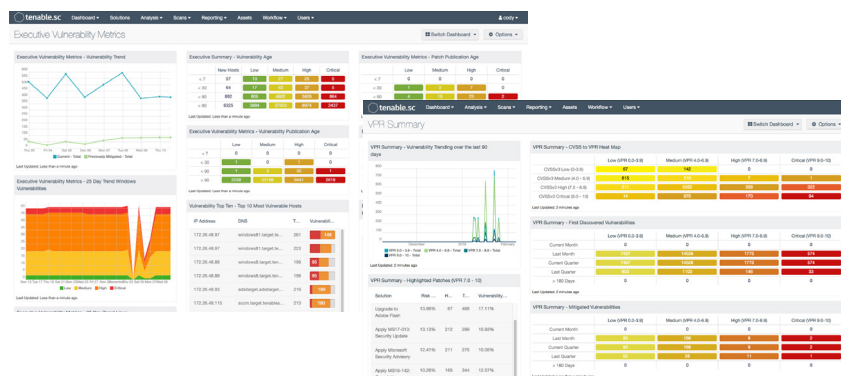


Abbildung 1: Hochgradig anpassbare Dashboards, Berichte, Workflows und Sicherheitsrichtlinien für die spezifischen Anforderungen Ihres Unternehmens

## WICHTIGE VORTEILE

- Kontinuierliche Sichtbarkeit**  
 Verfolgen Sie bekannte Assets kontinuierlich und erfassen Sie unbekannte Assets sowie deren Schwachstellen. Identifizieren Sie Bedrohungen und unerwartete Netzwerkveränderungen, bevor sie zu Sicherheitsverletzungen führen.
- Schwachstellen priorisieren**  
 Die Kombination von Asset- und Schwachstellendaten, Threat-Intelligence und Datenwissenschaft führt zu leicht verständlichen Risikobewertungen. Auf diese Weise lassen sich schnell die Schwachstellen sowie die davon betroffenen kritischsten Assets ermitteln, die das größte Geschäftsrisiko darstellen.
- Reichweite der Abdeckung**  
 Tenable Research arbeitet eng mit der Security-Community zusammen, um neue Schwachstellen aufzudecken und Erkenntnisse bereitzustellen, mit denen Unternehmen ihre Verfahren zur Schwachstellenbewertung optimieren können. Mit mehr als 67.000 Schwachstellen bietet Tenable die branchenweit umfassendste Unterstützung für CVEs und Sicherheitskonfigurationen, damit Sie alle Ihre Risiken nachvollziehen können.
- Prozesse automatisieren**  
 Nutzen Sie eine ausführlich dokumentierte API und vorgefertigte Integrationen zum Importieren von Drittanbieterdaten, Automatisieren von Scans sowie zur Weitergabe von Daten an Ihre IT-Systeme.

# WICHTIGE FUNKTIONEN

## Daten managen, auf Ihre Weise

Tenable.sc ist die führende On-Prem-Option für Schwachstellen-Management. Verwalten Sie Ihre Daten nach Ihren Vorstellungen mit On-Premises- oder hybriden Implementierungsoptionen, die auf Ihre komplexesten Bereitstellungsanforderungen abgestimmt sind, und reduzieren Sie gleichzeitig das Risiko für Ihr Unternehmen.

## Umfassende Bewertungsoptionen

Tenable.sc bietet Ihnen eine einheitliche Transparenz über Ihre gesamte Angriffsfläche. Die Lösung setzt Nessus-Sensoren sowie eine Kombination aus aktiven Scannern, Agents, passivem Netzwerk-Monitoring und CMDB-Integrationen ein, um die Scan-Abdeckung in der gesamten Infrastruktur zu maximieren und blinde Flecken bei Schwachstellen zu reduzieren. Dieser Mix aus verschiedenen Datensensoren hilft Ihnen, sowohl bekannte als auch unbekannte Assets sowie deren Schwachstellen zu verfolgen und zu bewerten.

## Passive Asset-Erfassung

Erfassen und identifizieren Sie IT-Assets in Ihrem Netzwerk, darunter Server, Desktops, Laptops, Netzwerkgeräte, Webanwendungen, virtuelle Maschinen, Mobilgeräte und die Cloud.

## Priorisierung von Schwachstellen anhand des tatsächlichen Risikos

Tenable.sc kombiniert Schwachstellendaten, Threat-Intelligence und Data Science, um Ihnen eine leicht verständliche Risikobewertung zu liefern, damit Sie Schwachstellen priorisieren können und wissen, was Sie zuerst beheben müssen. So können Sie Risiken schnell beurteilen und die Schwachstellen identifizieren, die die größten Auswirkungen auf Ihr Unternehmen haben.

## Vereinfachtes Schwachstellen-Management

Durch intuitive Berichte, Dashboard-Visualisierungen und eine benutzerfreundliche Oberfläche werden gängige Aufgaben wie das Konfigurieren von Scans, Durchführen von Bewertungen und Analysieren von Ergebnissen mit Tenable.sc leichter denn je. Dank vordefinierter Scan-Vorlagen, Konfigurationsprüfungen und Checks für Compliance-Audits, die sich an Best-Practices-Frameworks orientieren, benötigen Sie nur noch einen Bruchteil des bisherigen Aufwands, um Ihr Unternehmen zu schützen. Passen Sie Ihre Berichte und Analysen mit vorkonfigurierten, einsatzfertigen Dashboards an oder erstellen Sie mithilfe von Vorlagen eigene Dashboards, die den Anforderungen des Unternehmens gerecht werden.

## Optimierte Compliance

Mithilfe von vordefinierten Checks, Metriken und proaktiven Warnmeldungen bei Verstößen gegen Branchenstandards und gesetzliche Auflagen können Sie sich ein Bild der Compliance machen und entsprechende Berichte erstellen. Zu den Branchenstandards gehören CERT, NIST, DISA STIG, DHS CDM, FISMA, PCI DSS, HIPAA/HITECH und viele weitere mehr.

## Tenable Research

Tenable.sc wird von Tenable Research unterstützt. Unser Forschungsbereich liefert erstklassige Cyber Exposure-Informationen, datenwissenschaftliche Erkenntnisse, Warnmeldungen und Sicherheitsempfehlungen. Dank häufiger Updates von Tenable Research sind die neuesten Schwachstellen-Checks, Zero-Day-Forschungsergebnisse und Konfigurations-Benchmarks zum Schutz Ihres Unternehmens unmittelbar verfügbar.

## Einsatz von Tenable.sc Director

Tenable.sc Director ist ein Add-on, mit dem Sie Ihre Risikolage von zentraler Stelle aus verwalten und überblicken können. Dadurch reduzieren Sie Komplexität und erzielen vollständige Sichtbarkeit – konsolenübergreifend innerhalb Ihrer gesamten Bereitstellung.

## Vorgefertigte Integrationen sowie eine dokumentierte API und ein integriertes SDK

Tenable.io verfügt über sofort einsetzbare Integrationen für Credentialed Scanning, SIEM, SOAR, Ticketing- und Patching-Systeme sowie weitere ergänzende Lösungen, sodass Sie Ihren Schwachstellen-Management-Prozess ganz einfach optimieren können. Eine vollständige Auflistung finden Sie [hier](#). Dank einer umfassend dokumentierten API können Sie mit Tenable.sc zudem ganz einfach eigene Integrationen erstellen. Diese Tools verursachen keine zusätzlichen Kosten, maximieren jedoch den Nutzwert Ihrer spezifischen Anwendungsfälle im Bereich Schwachstellen-Management.

---

**Weitere Informationen:** Besuchen Sie [de.tenable.com](https://de.tenable.com)

**Kontakt:** Bitte senden Sie eine E-Mail an [sales-de@tenable.com](mailto:sales-de@tenable.com) oder besuchen Sie [de.tenable.com/contact](https://de.tenable.com/contact)