tenable | Datenblatt

Cloud Native Application Protection Platform (CNAPP)

Beheben von Sicherheitslücken in der Cloud mithilfe handlungsfähiger Cloud-Sicherheit

Der schnelle Umstieg auf die Cloud hat zu äußerst komplexen, verteilten Umgebungen und einer wachsenden Angriffsfläche geführt. In Kombination mit bekannten Risiken sind aus neuen cloudbasierten Angriffsvektoren Bedrohungen für Hybrid-Cloud- und Multi-Cloud-Infrastruktur entstanden, die sich in rasendem Tempo weiterentwickeln. Erschwerend kommt hinzu, dass zahlreiche Unternehmen mit isolierten Sicherheitstools und einem Mangel an Cloud-Expertise zu kämpfen haben: Fragmentierte Sichtbarkeit, durch die Sicherheitsteams mit Warnmeldungen überhäuft werden, ist die Folge.

Tenable Cloud Security trägt diesen Herausforderungen Rechnung – mit einer einheitlichen Cloud Native Application Protection Platform (CNAPP), die Teams in die Lage versetzt, kritische Sicherheitslücken in der Cloud zu beheben. Die Lösung deckt schnell Multi-Cloud-Sicherheitslücken wie auch die toxischen Kombinationen von Risiken auf, die durch Fehlkonfigurationen, riskante Berechtigungen, Schwachstellen und unverhältnismäßigen Zugriff auf sensible Daten entstehen. Mit Tenable Cloud Security können Sicherheitsteams sich ein vollständiges Bild von ihren Cloud-Risiken verschaffen – in einer einzigen intuitiven Lösung, die Sicherheit selbst in den komplexesten Umgebungen vereinfacht.

Die Lösung analysiert Ihre gesamten Cloud-Ressourcen, einschließlich Infrastruktur, Workloads, Daten und Identitäten, um die wichtigsten Sicherheitsrisiken zu ermitteln. Gewinnen Sie den notwendigen Kontext, um Verhaltensanomalien zu erkennen, Maßnahmen anhand der wahrscheinlichsten Angriffspfade zu priorisieren und Least-Privilege-Zugriff in großem Maßstab umzusetzen. Weisen Sie die Einhaltung von regulatorischen Rahmenbedingungen mithilfe von intuitiven Reporting-Funktionen nach und veranschaulichen Sie Ihre Fortschritte im Bereich Cloud-Sicherheit im zeitlichen Verlauf.

Wichtige Vorteile

- **Multi-Cloud-Transparenz für Full-Stack-Sicherheit in der Cloud**

  Verschaffen Sie sich einen 360-Grad-Blick auf sämtliche Cloud-Ressourcen, einschließlich Infrastruktur, Identitäten, Workloads und Daten, sowie auf die jeweiligen Gefährdungen über all Ihre Clouds hinweg.

- **Weniger irrelevante Warnmeldungen**

  Machen Sie toxische Kombinationen von Problemen ausfindig und beseitigen Sie die wichtigsten Risiken umgehend. Setzen Sie Full-Stack-Analysen ein, um Risiken im jeweiligen Kontext zu ermitteln.

- **Kontinuierliche Governance**

  Sichern Sie Cloud-Infrastruktur während des gesamten Lebenszyklus ab – von der Entwicklung bis zur Bereitstellung.

- **Vereinfachtes Compliance-Reporting**

  Senken Sie den Zeit- und Arbeitsaufwand bei der Berichterstellung durch automatisiertes Compliance-Reporting mit integrierten und benutzerdefinierten Richtlinien.

- **Risikoempfehlungen und Behebungsmaßnahmen**

  Senken Sie die MTTR durch detaillierte Behebungsempfehlungen und automatisierte Reaktionsmaßnahmen, die Sicherheitslücken beheben.

- **Skalierbare Cloud-Kompetenz**

  „Demokratisieren“ Sie Erkenntnisse und beschleunigen Sie Sicherheitsmaßnahmen im Unternehmen mit einer intuitiven Lösung, die es sämtlichen Beteiligten ermöglicht, sich zu Experten für ihre jeweilige Cloud-Umgebung zu entwickeln.

Wichtige Funktionen

Cloud Security Posture Management (CSPM)

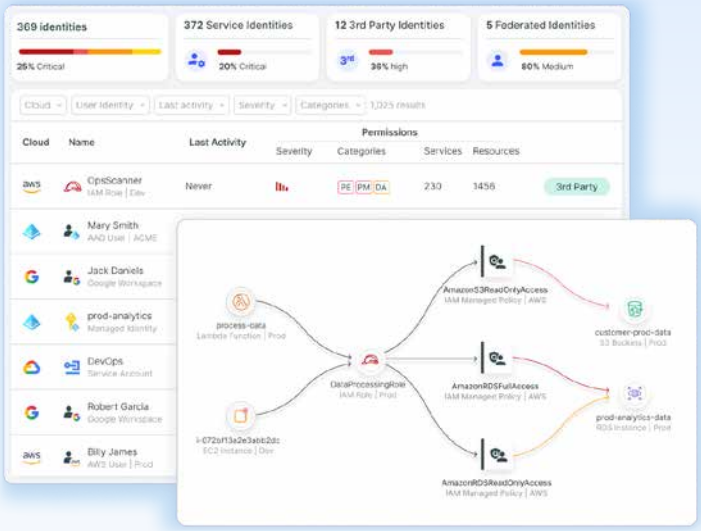
Vereinfachen Sie Cloud-Compliance mit einer einzigen Lösung, die Konfigurationen und Ressourcen in Clouds kontinuierlich scannt, Verstöße identifiziert und die Berichterstattung automatisiert. Nutzen Sie integrierte und benutzerdefinierte Richtlinien und bewerten Sie Risiken dynamisch, um Standards wie NIST, CIS, PCI, SOC 2 und die DSGVO einzuhalten.

Cloud Workload Protection (CWP)

Identifizieren Sie Schwachstellen, offengelegte Secrets, sensible Daten, Malware und Fehlkonfigurationen in virtuellen Maschinen, Containern und Serverless-Funktionen. Profitieren Sie von branchenführender Vulnerability Intelligence von Tenable Research, um Schwachstellen zu isolieren und den jeweiligen Exploit-Reifegrad in deren Code sowie bekannte Ausnutzungen, getaggte Forschung und historische CVSS-, VPR- und EPSS-Scores aufzuschlüsseln.

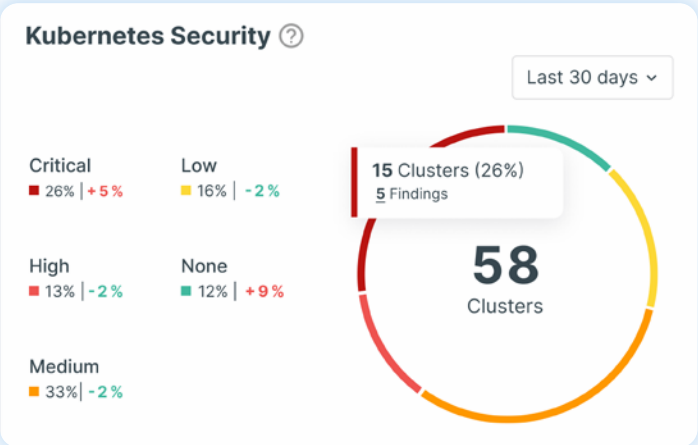
Cloud Infrastructure Entitlement Management (CIEM)

Erfassen Sie alle Cloud-Identitäten, analysieren Sie riskante Berechtigungen und setzen Sie einen Least-Privilege-Zugriff auf kritische Workloads für alle Nutzer durch, einschließlich Personen, Dienste und Maschinen. Profitieren Sie von einer erstklassigen Berechtigungsverwaltung, die sich in führende Identitätsanbieter (IDPs) einbinden lässt. Verbinden Sie Kontextinformationen zu Identitäten mit Workload-bezogenen Risiken wie Fehlkonfigurationen, Schwachstellen und Zugriff auf sensible Daten, um Sicherheitsprobleme besser priorisieren zu können und die Anzahl der Warnmeldungen zu reduzieren.



Kubernetes Security Posture Management (KSPM)

Schützen Sie Kubernetes-Cluster, die in Cloud-verwalteten Services, On-Premises sowie in selbstverwalteten K8s- und OpenShift-Clustern ausgeführt werden. Analysieren Sie sämtliche Container-Komponenten eines Kubernetes-Clusters auf riskante Berechtigungen, Malware, Account-Nutzung und Konfiguration. Profitieren Sie von einem kompletten Bestandsverzeichnis der ausgeführten Ressourcen mitsamt den jeweiligen Schweregraden und leiten Sie Behebungsmaßnahmen an die entsprechenden Verantwortlichen weiter, indem Sie Pull-Requests in der Konsole auslösen.

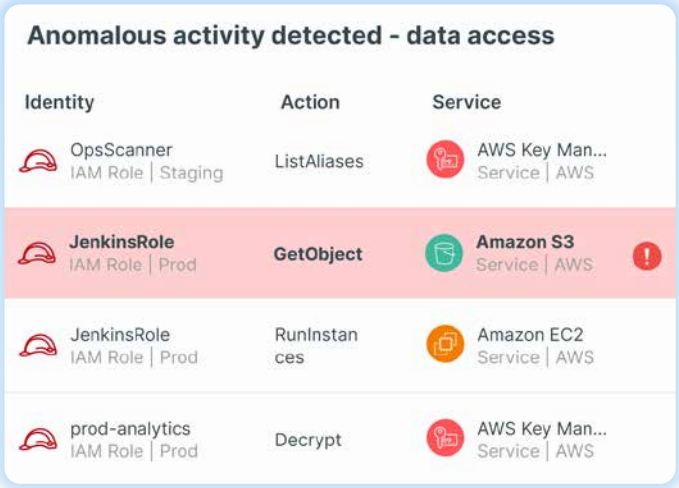


Infrastructure as Code (IaC)-Sicherheit

Scannen Sie Infrastructure as Code (IaC) auf Sicherheitslücken und speisen Sie Tenable-Ergebnisse in bestehende CI/CD-Workflows ein oder nehmen Sie mithilfe von Assistenten direkt automatische Korrekturen vor. Weisen Sie Warnmeldungen und automatisch generierte Least-Privilege-IaC-Snippets über Ticketing-Systeme zu. Führen Sie eine Integration mit Quellcode-Repositorys durch, um Pull-Requests direkt über die Konsole auszulösen.

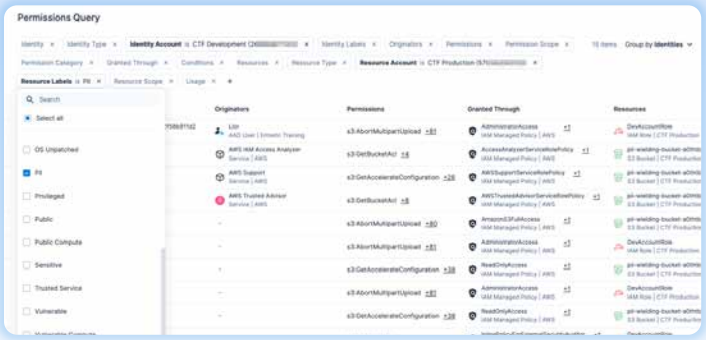
Cloud Detection and Response (CDR)

Reichern Sie Cloud-Aktivitätsprotokolle mit ressourcenspezifischen Daten zu identitätsbasierten Bedrohungen an und beschleunigen Sie die Anomalie-Erkennung und Reaktion mit kontextbezogenen und handlungsrelevanten Erkenntnissen zu ausgeweiteten Zugriffsrechten, Änderungen an der Netzwerkkonfiguration sowie zu unbefugter Nutzung bzw. Diebstahl von Zugriffsschlüsseln.



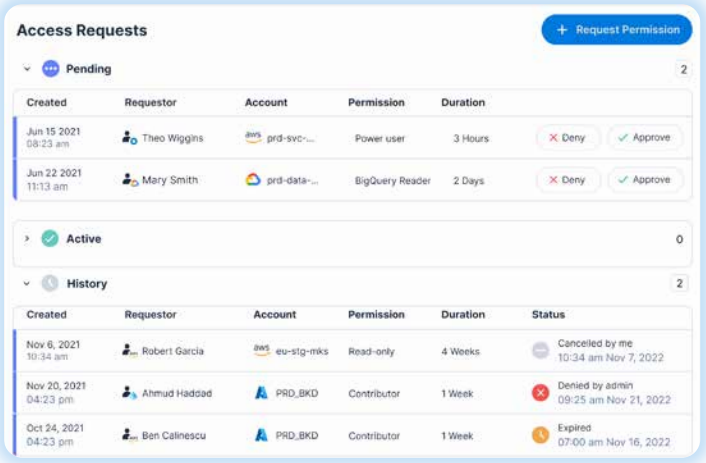
Data Security Posture Management (DSPM)

Bringen Sie in Erfahrung, welche Arten von sensiblen Daten wo genau in Ihrer Cloud gespeichert sind, einschließlich personenbezogener Daten, geschützter Gesundheitsdaten und Betriebsgeheimnisse. Vollziehen Sie nach, welches Exposure-Risiko für Daten von übermäßigen Zugriffsrechten, Fehlkonfigurationen und Schwachstellen ausgeht. Halten Sie Datensicherheitsvorschriften und Branchenstandards ein.



Just-in-Time(JIT)-Zugriff per Self-Service

Gewähren Sie schnelle Genehmigungen für einen zeitlich befristeten und bedarfsgerechten Zugriff auf Cloud-Ressourcen – und über IdP-Gruppen auch auf SaaS-Apps. Entziehen Sie Berechtigungen automatisch und stellen Sie sicher, dass sämtliche Zugriffsanfragen zu Auditzwecken protokolliert werden.



Über Tenable

Tenable®, das Unternehmen für Exposure Management, identifiziert und schließt Sicherheitslücken, die den Wert, die Reputation und die Vertrauenswürdigkeit von Unternehmen gefährden. Die KI-gestützte Exposure Management-Plattform von Tenable bietet umfassende Sichtbarkeit und handlungsrelevante Erkenntnisse entlang der gesamten Angriffsfläche und ermöglicht es Unternehmen, sich vor Cyberangriffen zu schützen – von IT-Infrastrukturen über Cloud-Umgebungen bis hin zu kritischen Infrastrukturen und allen dazwischen liegenden Bereichen. Mehr als 44.000 Kunden weltweit verlassen sich auf Tenable, wenn es darum geht, Sicherheits- und Geschäftsrisiken zu minimieren. Weitere Informationen finden Sie auf de.tenable.com.

Kontakt

Bitte senden Sie eine E-Mail an sales-de@tenable.com oder besuchen Sie de.tenable.com/contact.

08/19/24