Acronis Cloud Security

(ehemals 5nine Cloud Security)

Speziell für Microsoft Hyper-V und Microsoft Azure entwickelt und optimiert

EINHEITLICHE HYBRID CLOUD-SICHERHEIT

Unternehmen verlagern ihre Services in die Public Cloud und bauen weitere Hybrid Cloud-Lösungen auf. Dadurch wird die Gewährleistung von Sicherheit immer komplexer, da Administrator:innen möglicherweise keinen Zugriff mehr auf physische Hosts und Netzwerke haben, sodass viele Computing-Services (einschließlich Sicherheit) virtualisiert und remote verwaltet werden müssen. Auch wenn Public Clouds zahlreiche Sicherheitsvorteile bieten, sind die von Microsoft Azure bereitgestellten generischen Lösungen begrenzt und nicht speziell darauf ausgelegt, die sich schnell ändernden Sicherheitsanforderungen heutiger Unternehmen zu erfüllen. Bisher benötigten Unternehmen mehrere externe Anbieter, um ihre virtualisierten Umgebungen durchgängig schützen zu können.

VEREINFACHTE SICHERHEIT FÜR IHRE HYBRID CLOUD

Acronis Cloud Security ist eine umfassende Sicherheitslösung, die alle diese Herausforderungen behebt, indem sie branchenführenden Hyper-V-Schutz auf die Public Cloud ausweitet. Acronis Cloud Security kann als Windows- oder Web-Applikation (eigenständig oder über den Microsoft Azure Marketplace) bereitgestellt werden.

SCHUTZ FÜR ALLE MICROSOFT CLOUD-BEREITSTELLUNGEN

Acronis Cloud Security schützt virtuelle Maschinen (VMs) in allen Microsoft Cloud-Umgebungen. Bei lokalen Hyper-V-Installationen mit einem nativen erweiterbaren Switch schützt Acronis Cloud Security Hosts, Cluster, VMs, Netzwerke und virtuelle Laufwerke. Bei lokalen Hyper-V-Installationen, die SDNv2 nutzen, steht zusätzlich die Virtual Router Security Appliance zum Schutz virtueller Netzwerke zur Verfügung. Bei Azure-Installationen verwendet Acronis Cloud Security ebenfalls die Virtual Router Security Appliance, um VMs, Netzwerke und virtuelle Laufwerke zu schützen, und ermöglicht zusätzlich die Verwaltung der Eigenschaften und Abonnements von Azure-Konten.

VORTEILE

- Automatischer und sofortiger Schutz für neu erstellte VMs durch virtuelle Firewall
- Steigert die Betriebseffizienz und senkt die Gesamtbetriebskosten, da keine Einzellösungen erforderlich sind und die Verwaltung vereinfacht wird
- Integrierte agentenlose Funktionen für Virenschutz (AV) und Ransomware-Schutz (ARW) schützen Ihre Daten ohne Beeinträchtigung der VM-Leistung
- Kontrolle des gesamten ein- und ausgehenden Netzwerkverkehrs und des Datenverkehrs zwischen VMs dank der virtuellen Firewall, die Pakete vor der Übertragung detailliert untersucht
- Intrusion Detection System (IDS) erkennt viele Angriffstypen, einschließlich DoS/DDoS, Angriffe mit Direktzugriff, Cross-Site-Scripting, Brute-Force-Angriffe, Pufferüberlauf, verborgene Port-Scans usw.
- Einfache Sicherheits-Compliance-Audits dank Protokollierung des gesamten Netzwerkverkehrs, aller Änderungen der Infrastrukturkonfiguration sowie aller Administrator-Aktionen
- Zentrale lokale und Azure-basierte Sicherheitsverwaltung, ohne dass sich Administrator:innen beim Azure-Portal anmelden müssen

EINFACH

Einfacher Schutz für alle Microsoft Cloud-Umgebungen: lokal, Cloud, hybrid

- Anwenderfreundliche grafische Benutzeroberfläche bietet Überblick über alle Hyper-V-Cluster und Azure-Instanzen
- Sicherheitsverwaltung der gesamten Microsoft-Hybrid-Cloud (lokal und Azure) von einer zentralen Konsole, ohne dass sich Administrator:innen beim Azure-Portal anmelden müssen
- Erstellung von Sicherheitsgruppen für automatischen Schutz: Push-Übertragung von Regeländerungen an die gesamte VM-Gruppe sowie automatische Anwendung der Sicherheitsfunktionen für VMs, die neu erstellt oder zur Gruppe hinzugefügt werden

EFFIZIENT

Optimierung der Sicherheitsabläufe für mehrere Hyper-V-Cluster und Azure-Instanzen

- CBT-Technologie (Change Block Tracking) zur Erfassung und Analyse der Datenblöcke, die sich seit dem letzten Scan geändert haben; beschleunigt Scans um das 70-fache
- Dank integrierter Funktionen für Virenschutz (AV) und Ransomware-Schutz (ARW) sind keine separaten Drittanbieterlösungen erforderlich; Scans werden auf Netzwerkebene durchgeführt und erfordern keine Agenten, sodass die VM-Leistung nicht beeinträchtigt wird
- Schutz aller Microsoft Cloud-Ressourcen von einer einzigen Konsole aus, sodass Sie nicht mehr auf mehrere Cyber Security-Tools angewiesen sind

KONTROLLIERT

Einfacher Schutz für alle Microsoft Cloud-Umgebungen: lokal, Cloud, hybrid

- Granulare Benutzer- und Mandanten-Verwaltung durch eine rollenbasierte Zugriffskontrolltechnik (RBAC, Role-Based Access Control), die Benutzer:innen und Ressourcen trennen und so das Risiko einer Kreuzkontamination senken kann
- Kontrolle der Netzwerk-Bandbreitennutzung pro VM ermöglicht die Gewährleistung der Service-Qualität, da verhindert werden kann, dass einzelne VMs zu viel Bandbreite verbrauchen und die Leistung anderer VMs, Services oder der Benutzer:innen beinträchtigen
- Virtuelle Firewall ermöglicht Unternehmen, den gesamten ein- und ausgehenden Datenverkehr und den Verkehr zwischen VMs zu kontrollieren, indem die Pakete analysiert werden, bevor diese die VMs oder virtuellen Netzwerke erreichen

SICHER

Einhaltung strenger Sicherheits-, Datenschutz- und Compliance-Anforderungen, einschließlich einer vollständigen Kontrolle über alle Zugriffe auf Ihre VMs, Hosts, Mandanten und Verwaltungsfunktionen

- Deep Packet Inspection (DPI)-Technik ermöglicht die Untersuchung von Paketen, bevor bestimmt wird, ob Pakete weitergeleitet werden sollten
- Cisco Snort IDS-Regeln (Intrusion Detection System) sind in Acronis Cloud Security integriert und erkennen zahlreiche Netzwerkangriffe, einschließlich DoS/DDoS, Cross-Site-Scripting, Pufferüberlauf, verborgene Port-Scans usw.
- Protokollierung aller Ereignisse und Benutzeraktionen (einschließlich der Ergebnisse von Änderungen) sowie des gesamten Netzwerkverkehrs ermöglicht einfache Audits, um strenge Sicherheits-Compliance-Anforderungen zu erfüllen

ZUVERLÄSSIG

Skalierbare mehrschichtige Cyber Protection ermöglicht auch den Schutz sehr großer und äußerst komplexer Hyper-V- und Azure-Umgebungen

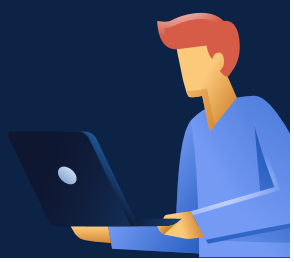
- Cyber Protection und Sicherheitsverwaltung für Hyper-V- und Azure-Workloads mit verschiedenen, auch gemischten Versionen
- Management-Server wird mit Cluster-basierter Konfiguration installiert, um hochzuverlässigen Zugriff auf die Sicherheitsmanagement-Konsole zu ermöglichen
- Sicherheitseinstellungen werden beim Beenden von virtuellen Maschinen und auch bei Nichtverfügbarkeit des Management-Servers beibehalten – für ununterbrochene, kontinuierliche Cyber Protection für Microsoft Cloud

UNTERSTÜTZTE UMGEBUNGEN

Microsoft Azure
Hyper-V

- Windows Server 2019
- Hyper-V Server 2019
- Windows Server 2016
- Windows Server 2012 R2

Hybrid Cloud-Konfigurationen



Acronis

Weitere Informationen unter
www.acronis.com