SOLUTION BRIEF

Sichern Sie Ihre Umgebung dank unsichtbarer Sicherheit von Nutanix

Schützen Sie Anwendungen und Daten, um die Verbreitung von Malware in Hybrid Clouds zu verhindern

DIE WESENTLICHEN VORTEILE

Daten schützen und Sicherheitsverletzungen verhindern

- Verschlüsseln Sie Data-at-Rest
- Kontrollieren und beschränken Sie den Zugriff auf sensible Daten
- Analysieren und prüfen Sie Sicherheitskonfigurationen
- Sichern Sie Ihre Hybrid Clouds
- Verhindern Sie die Verbreitung von Ransomware

Netzwerke segmentieren und sichern

- Implementieren Sie Mikrosegmentierung und Netzwerkinspektion in wenigen Minuten
- Separieren Sie regulierte Umgebungen mit automatisierten Softwarekontrollen

Regulierung- und Compliance-Aufwand vereinfachen

- Automatisieren Sie die Basis-Konfiguration der Plattform-Sicherheit
- Überprüfen Sie die Einhaltung gesetzlicher Vorschriften (HIPAA, PCI, NIST, etc.)

DIE SICHERHEIT IN DER HYBRID CLOUD BEGINNT MIT EINER STABILEN INFRASTRUKTURGRUNDLAGE

Die Aufrechterhaltung der Sicherheit in den heutigen Umgebungen ist aus mehreren Gründen eine Herausforderung. Viele herkömmliche Infrastruktur-Stacks bestehen aus Produkten mehrerer Anbieter, die jeweils vom Stack entkoppelt sind – was eine enge und begrenzte Sicht auf die Sicherheit zur Folge hat. Die Validierung und Aufrechterhaltung eines Sicherheitskonzepts durch kontinuierliche Software-Upgrades ist zeitaufwändig und beinhaltet oft fehleranfällige manuelle Prozesse, die Innovation und Produktivität beeinträchtigen.

In der Cloud-Ära muss die Sicherheit in der Unternehmenskultur verankert werden und Sicherheitsüberlegungen müssen ein wesentlicher Bestandteil der Entscheidungsfindung des Unternehmens sein, um die hohen Anforderungen an die Einhaltung gesetzlicher Vorschriften zu erfüllen und die Herausforderungen einer sich permanent weiterentwickelnden Bedrohungslandschaft zu meistern. Unternehmen sollten sich darum bemühen, den Wartungsprozess für die Sicherheit der Infrastruktur zu automatisieren, um menschliche Fehler zu vermeiden und eine nahtlose Skalierbarkeit zu gewährleisten, ohne die Sicherheit in einer sich ständig verändernden Umgebung zu gefährden.

DIE SICHERHEIT FÜR DIE ZUKUNFT DER HYBRID CLOUD ÜBERDENKEN

Sicherheit in der Hybrid Cloud beginnt mit einer robusten Infrastrukturgrundlage. Hier bietet die branchenführende Lösung von Nutanix nicht nur einen operativen und finanziellen Nutzen, sondern hilft auch bei der Verbesserung der Sicherheitslage und der Verhinderung von Datenschutzverletzungen, indem sie einen Defense-in-Depth-Ansatz für die Sicherheit der Hybrid Cloud unterstützt.

Platform Security

Application and Network Security

SecOps and Compliance

NUTANIX™

STANDARDS UND ZERTIFIKATE

Nutanix wendet mehrere Sicherheitsstandards und Validierungsprogramme an. Nutanix erfüllt die strengsten internationalen Standards, einschließlich zahlreicher ISO-, SOC- und FIPS-Standards, und bietet Regierungen und Unternehmen auf der ganzen Welt die Gewissheit, dass Nutanix-Produkte die erwartete Leistung erbringen und mit ihrer bestehenden Technologie zusammenarbeiten.

Besuchen Sie nutanix.com/trust für weitere Informationen.

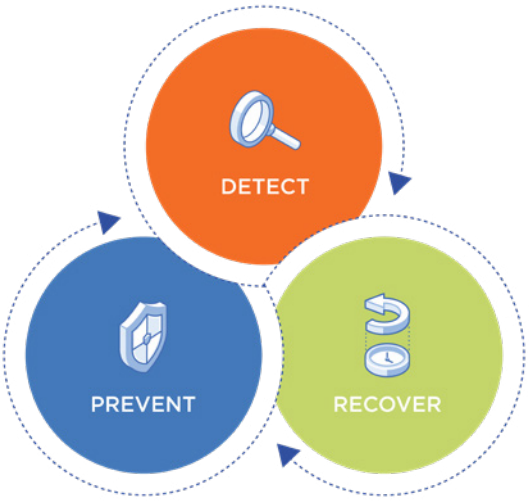
ABWEHR AUF ALLEN EBENEN

Plattform-Sicherheit: Sicherheit ist ein grundlegender Aspekt des Produktdesigns bei Nutanix, beginnend mit den in die Enterprise Cloud Platform integrierten Sicherheitspraktiken (wie Data-at-Rest-Verschlüsselung, umfassende Zugriffskontrollen usw.). Best Practices der Branche und staatliche Standards werden in ein automatisiertes Konfigurationsmonitoring und einen autonomen Selbstheilungsprozess integriert, der die Einhaltung von Compliance-Zielen unterstützt. Strenge Tests auf gängige Schwachstellen und häufige Patch-Veröffentlichungen minimieren das Risiko von Datenschutzverletzungen. Unstimmigkeiten werden protokolliert und auf die Baseline zurückgesetzt, um die Konsistenz der Sicherheitskonfiguration zu gewährleisten.

Anwendungs- und Netzwerksicherheit: Nutanix Flow bietet fortschrittliche Netzwerksicherheit innerhalb des Rechenzentrums und sorgt so für die Transparenz von Anwendungen und den Schutz vor der Verbreitung von Cyber-Bedrohungen wie Ransomware. Netzwerke und Anwendungen können einfach über eine softwaredefinierte Richtlinie segmentiert werden, ohne dass zusätzliche Hardware oder komplexe Netzwerkkonfigurationen erforderlich sind. Die nativen Funktionen zur Mikrosegmentierung von Netzwerken bieten ein Modell zur Erkennung, Visualisierung und Durchsetzung von Richtlinien, das die Anwendung von granularen Netzwerkrichtlinien (Mikrosegmentierung) zwischen VMs vereinfacht und automatisiert.

SecOps, Compliance und Audit: Flow Security Central bietet Einblick in die Sicherheitslage der Hybrid Cloud, Unterstützung bei der Richtlinienverwaltung, Konfigurationsaudits und Compliance-Validierung für Nutanix HCI. Security Central nutzt eine Reihe automatischer Sicherheitsaudits, um Sicherheitsschwachstellen in der Infrastruktur und Konfigurationsfehler zu erkennen und zu beheben. Sicherheitsadministratoren können automatische Richtlinien erstellen, um Schwachstellen in Echtzeit zu beheben. Security Central hilft auch bei der Überprüfung der Einhaltung gesetzlicher Richtlinien wie PCI-DSS, HIPAA, NIST, etc. – und bietet so eine stets verfügbare Lösung zur Einhaltung von Sicherheitsvorschriften.

Vorbeugen, Erkennen und Wiederherstellen: Es gibt keine einzelne Maßnahme, Softwarelösung oder Sicherheitskontrolle, die Ihr Unternehmen vollständig vor den Bedrohungen durch Malware und Ransomware schützen kann. Die beste Lösung ist ein mehrschichtiger Ansatz, der gemeinhin als „Defense in Depth"-Strategie bezeichnet wird. Um sowohl Ihre operativen als auch Ihre finanziellen Kosten zu minimieren, sollte Ihr ganzheitlicher Plan alle in Nutanix integrierten Funktionen enthalten, die mit den in Ihrem Rechenzentrum vorhandenen Kontrollen und Sicherheitsvorkehrungen zusammenarbeiten.



NUTANIX

VERTRAUEN SIE NUTANIX ALS TEIL IHRER CYBER-VERTEIDIGUNGSSTRATEGIE

HCI-Plattform

- Selbstheilende Konfiguration des Sicherheitskonzeptes
- Speicher-Snapshots und Wiederherstellungspunkte
- Datensicherung, Replikation und Runbook-Automatisierung
- FIPS 140-2-validierte Data-at-Rest-Verschlüsselung
- Segmentierung der Datenebene & der Steuerebene
- Native Virtualisierung – für die Sicherheit entwickelt

Patching und Upgrades

- CVE-Patching, Plattform-Upgrades und Lifecycle-Management „mit einem Klick“
- Verwaltung von Firmware- und BIOS-Upgrades

Verwaltung und Automatisierung

- Rollenbasierte Zugriffskontrolle (RBAC)
- Identitäts- und Zugriffsmanagement
- Ressourcen-Analyse, Einblicke und Aufdeckung von Anomalien
- Codeloses Automatisieren und Starten von Sicherheitsaktionen
- Durchsetzungs- und Automatisierungspläne zur Gewährleistung einer konsequenten Durchsetzung der Richtlinien

Netzwerk und Sicherheit

- Netzwerk- und Anwendungssegmentierung
- Anwendungs- und Netzwerktransparenz
- Tiefgreifende Paketprüfung und Partnerintegration für Bedrohungsanalysen
- Richtlinien- und Ereignisprotokollierung
- Tools für die Einhaltung von Sicherheitsrichtlinien und Audits

Storage-Dienste

- Richtlinien zum Sperren von Dateitypen
- Erkennung anomaler Dateiaktivitäten
- ICAP-Unterstützung für Antivirus-Integration
- Unterstützung unveränderlicher WORM-Richtlinien

Backup, Geschäftskontinuität und Disaster Recovery

- Native Replikation und Datensicherung
- Archivierungs- und Backup-Lösung für Sekundärspeicher
- Cloud-Disaster-Recovery-as-a-Service

NUTANIX™
YOUR ENTERPRISE CLOUD

Tel. +49 89 25552898
info@nutanix.com | www.nutanix.de | @NutanixGermany