Sicherheit

Cloud Insights

NetApp
March 30, 2023

Inhaltsverzeichnis

Sicherheit

Cloud Insights Sicherheit

Die Datensicherheit bei Produkten und Kunden ist bei NetApp von größter Bedeutung. Cloud Insights befolgt während des gesamten Release-Lebenszyklus bewährte Sicherheitsverfahren, um sicherzustellen, dass Kundeninformationen und -Daten bestmöglich gesichert sind.

Sicherheit – Überblick

Physische Sicherheit

Die Produktionsinfrastruktur von Cloud Insights wird in Amazon Web Services (AWS) gehostet. Die physische und umgebungsbedingte Sicherheitskontrollen für Cloud Insights-Produktionsserver, die Gebäude sowie Schlösser oder Schlüssel umfassen, die an Türen verwendet werden, werden von AWS gemanagt. Gemäß AWS: „Der physische Zugang wird sowohl am Perimeter als auch an Einbruchstellen durch professionelles Sicherheitspersonal mithilfe von Videoüberwachung, Intrusion Detection Systemen und anderen elektronischen Mitteln gesteuert. Autorisierte Mitarbeiter nutzen Multi-Faktor-Authentifizierungsmechanismen für den Zugriff auf Datacenter-Stockwerke.“

Cloud Insights folgt den Best Practices des "Modell der gemeinsamen Verantwortung" Beschrieben von AWS.

Produktsicherheit

Cloud Insights folgt einem Entwicklungslebenszyklus gemäß Agile Principles, sodass wir sicherheitsorientierte Softwarefehler schneller beheben können als bei einer längeren Entwicklung des Release-Zyklus. Mithilfe von Methoden zur kontinuierlichen Integration sind wir in der Lage, schnell sowohl auf funktionale als auch auf Sicherheitsänderungen zu reagieren. Die Änderungsmanagementverfahren und -Richtlinien legen fest, wann und wie Änderungen vorgenommen werden, und tragen dazu bei, die Stabilität der Produktionsumgebung zu erhalten. Alle wirkungsvollen Änderungen werden formal kommuniziert, koordiniert, richtig überprüft und vor ihrer Veröffentlichung in der Produktionsumgebung genehmigt.

Netzwerksicherheit

Der Netzwerkzugriff auf Ressourcen in der Cloud Insights-Umgebung wird durch hostbasierte Firewalls gesteuert. Jede Ressource (wie z. B. ein Load Balancer oder eine virtuelle Maschineninstanz) verfügt über eine hostbasierte Firewall, die den eingehenden Datenverkehr auf nur die Ports beschränkt, die für die Ausführung ihrer Funktion benötigt werden.

Cloud Insights nutzt verschiedene Mechanismen wie Intrusion-Detection-Services, um die Produktionsumgebung auf sicherheitsrelevante Anomalien zu überwachen.

Risikoeinschätzung

Das Team von Cloud Insights folgt einem formalisierten Prozess zur Risikobewertung, um Risiken systematisch und wiederholbar zu identifizieren und zu bewerten, sodass sie anhand eines Risikomanagements angemessen gemanagt werden können.

Datensicherung

Die Cloud Insights Produktionsumgebung ist in einer hochredundanten Infrastruktur eingerichtet und nutzt mehrere Verfügbarkeitszonen für alle Services und Komponenten. Neben einer hochverfügbaren und redundanten Computing-Infrastruktur werden wichtige Daten in regelmäßigen Abständen gesichert und Restores regelmäßig getestet. Formelle Backup-Richtlinien und -Verfahren minimieren die Auswirkungen von Unterbrechungen von Geschäftsaktivitäten und schützen Unternehmensprozesse gegen die Auswirkungen von Fehlern in Informationssystemen oder -Ausfällen und stellen einen zeitnahen und adäquaten Wiederaufnahme sicher.

Authentifizierung und Zugriffsmanagement

Der gesamte Kundenzugriff auf Cloud Insights erfolgt über HTTPS über die Browser-UI-Interaktion. Die Authentifizierung erfolgt über den Dienst Auth0 eines Drittanbieters. NetApp hat hier als Authentifizierungsebene für alle Cloud-Datenservices zentralisiert.

Cloud Insights befolgt branchenübliche Best Practices wie „Least Privilege“ und „rollenbasierte Zugriffssteuerung“ für den logischen Zugriff auf die Cloud Insights Produktionsumgebung. Der Zugriff wird streng nach Anforderungen kontrolliert und nur ausgewählten autorisierten Mitarbeitern mit Multi-Faktor-Authentifizierungsmechanismen gewährt.

Erhebung und Schutz von Kundendaten

Alle Kundendaten werden während der Übertragung über öffentliche Netzwerke verschlüsselt und im Ruhezustand verschlüsselt. Cloud Insights nutzt Verschlüsselung an verschiedenen Stellen im System, um Kundendaten mithilfe von Technologien wie Transport Layer Security (TLS) und dem branchenüblichen AES-256-Algorithmus zu sichern.

Kundendeprovisionierung

E-Mail-Benachrichtigungen werden in verschiedenen Abständen versendet, um dem Kunden mitzuteilen, dass das Abonnement abläuft. Nach Ablauf des Abonnements wird die UI eingeschränkt und eine Kulanzzeit beginnt für die Datenerfassung. Der Kunde wird dann per E-Mail benachrichtigt. Bei Testabonnements besteht eine Frist von 14 Tagen. Im Rahmen der bezahlten Abonnements haben Sie eine Frist von 28 Tagen. Nach Ablauf der Kulanzzeit wird der Kunde per E-Mail darüber informiert, dass das Konto innerhalb von 2 Tagen gelöscht wird. Ein zahlter Kunde kann auch direkt beantragen, dass er nicht im Service ist.

Abgelaufene Mieter und alle damit verbundenen Kundendaten werden vom Cloud Insights-Betriebsteam (SRE) am Ende der Kulanzzeit oder nach Bestätigung des Antrags eines Kunden auf Kündigung seines Kontos gelöscht. In beiden Fällen führt das SRE-Team einen API-Aufruf aus, um das Konto zu löschen. Der API-Aufruf löscht die Mandanteninstanz und alle Kundendaten. Die Löschung durch den Kunden wird durch den Aufruf derselben API überprüft und überprüft, ob der Kunde den Status „GELÖSCHT“ hat.

Management von Sicherheitsproblemen

Cloud Insights ist in das PSIRT-Verfahren (Product Security Incident Response Team) von NetApp integriert, um bekannte Schwachstellen zu ermitteln, zu bewerten und zu beheben. PSIRT nutzt Informationen zu Schwachstellen über mehrere Kanäle, darunter Kundenberichte, interne technische Informationen und allgemein anerkannte Quellen wie die CVE-Datenbank.

Sobald ein Problem vom Cloud Insights-Entwicklungsteam erkannt wird, initiiert das Team den PSIRT-Prozess, bewertet und mögliche Abhilfe.

Möglicherweise identifiziert ein Cloud Insights Kunde oder Forscher ein Sicherheitsproblem im Zusammenhang mit dem Cloud Insights Produkt und meldet es direkt an den technischen Support oder an das

NetApp Incident Response Team. In diesen Fällen leitet das Cloud Insights-Team den PSIRT-Prozess ein, bewertet und kann das Problem beheben.

Schwachstellen- und Penetrationstests

Cloud Insights befolgt branchenübliche Best Practices und führt regelmäßig Schwachstellenprüfungen durch, wobei interne und externe Sicherheitsexperten sowie Unternehmen eingesetzt werden.

Schulung zur Sensibilisierung für die Sicherheit

Alle Cloud Insights Mitarbeiter durchlaufen Sicherheitstrainings, die für individuelle Rollen entwickelt wurden, um zu gewährleisten, dass jeder Mitarbeiter in der Lage ist, die spezifischen sicherheitsrelevanten Herausforderungen seiner Rollen zu bewältigen.

Compliance

Cloud Insights führt unabhängige Audits und Validierungen vom externen lizenzierten CPA-Unternehmen für seine Sicherheit, Prozesse und Services durch, einschließlich der Durchführung des SOC 2-Audits.

Informationen und Region

NetApp nimmt die Sicherheit von Kundeninformationen sehr ernst. So und wo Cloud Insights Ihre Informationen speichert:

Welche Informationen speichert Cloud Insights?

Cloud Insights speichert folgende Informationen:

- Performance-Daten

  Performancedaten sind Zeitreihendaten, die Informationen zur Leistung des überwachten Geräts/der überwachten Quelle liefern. Dazu zählen beispielsweise die Anzahl der von einem Speichersystem bereitgestellten iOS, der Durchsatz eines FibreChannel-Ports, die Anzahl der von einem Webserver bereitgestellten Seiten, die Reaktionszeit einer Datenbank und vieles mehr.

- Bestandsdaten

  Bestandsdaten bestehen aus Metadaten, die das überwachte Gerät/die Quelle beschreiben und wie es konfiguriert wird. Dazu gehören beispielsweise installierte Hardware- und Softwareversionen, Festplatten und LUNs in einem Storage-System, CPU-Kerne, RAM und Festplatten einer Virtual Machine, die Tabellen einer Datenbank, die Anzahl und die Art der Ports auf einem SAN Switch, Verzeichnis-/Dateinamen (bei aktivierter Storage Workload Security) usw.

- Konfigurationsdaten

  Dies fasst vom Kunden bereitgestellte Konfigurationsdaten zusammen, die zur Verwaltung von Kundeninventar und -Vorgängen verwendet werden, z. B. Hostnamen oder IP-Adressen der überwachten Geräte, Abfrageintervalle, Zeitlimits usw.

- Secrets

  Secrets bestehen aus den Anmeldeinformationen, die von der Cloud Insights-Erfassungseinheit für den Zugriff auf Kundengeräte und -Dienste verwendet werden. Diese Anmeldedaten werden mit AES-256 verschlüsselt, die privaten Schlüssel werden nur in den Acquisition Units gespeichert und verlassen nie die

Kundenumgebung. Selbst privilegierte Cloud Insights SREs können aufgrund dieses Designs nicht in Klartext auf Kundengeheimnisse zugreifen.

- Funktionale Daten

  Diese Daten werden durch die Bereitstellung des Cloud Data Service durch NetApp generiert, der NetApp über die Entwicklung, Implementierung, den Betrieb, die Wartung und die Sicherung des Cloud Data Service informiert. Funktionale Daten enthalten weder Kundendaten noch personenbezogene Daten.

- Benutzerdaten

  Authentifizierung und Zugriffsinformationen, mit denen NetApp Cloud Central mit regionalen Cloud Insights-Standorten kommunizieren kann, einschließlich Daten, die sich auf die Benutzerautorisierung beziehen.

- Sicherheitsdaten Des Benutzerverzeichnisses Für Storage-Workloads

  In Fällen, in denen die Workload-Sicherheitsfunktion aktiviert ist UND der Kunde den Benutzer-Directory-Collector aktivieren möchte, speichert das System Anzeigenamen, Unternehmens-E-Mail-Adressen und andere Informationen, die aus Active Directory gesammelt wurden.

Benutzerdaten im Benutzerverzeichnis beziehen sich auf Benutzerverzeichnisdaten, die vom Datensammler des Workload Security User Directory erfasst werden, nicht auf Daten der Benutzer von Cloud Insights/Workload Security selbst.

Es werden keine expliziten personenbezogenen Daten aus Infrastruktur- und Dienstleistungsressourcen erhoben. Die erfassten Daten bestehen aus Performance-Kennzahlen, Konfigurationsdaten und Infrastrukturmetadaten, ähnlich wie viele Telefonanbieter mit NetApp Auto-Support und ActiveIQ. Abhängig von den Namenskonventionen des Kunden werden jedoch Daten für Shares, Volumes, VMs, qtrees, Anwendungen usw. können personenbezogene Informationen enthalten.

Wenn Workload Security aktiviert ist, untersucht das System außerdem Datei- und Verzeichnisnamen auf SMB- oder anderen Freigaben, die personenbezogene Informationen enthalten können. Wenn Kunden den Workload Security User Directory Collector (der im Wesentlichen Windows SIDs über Active Directory Nutzernamen zu Benutzernamen einordnet) aktivieren, werden der Anzeigename, die Unternehmens-E-Mail-Adresse und alle ausgewählten zusätzlichen Attribute von Cloud Insights erfasst und gespeichert.

Darüber hinaus werden Zugriffsprotokolle an Cloud Insights erstellt und enthalten die IP- und E-Mail-Adressen der Benutzer, die bei der Anmeldung beim Service verwendet werden.

Wo werden meine Informationen gespeichert?

Cloud Insights speichert Informationen je nach Region, in der Ihre Umgebung erstellt wird.

Folgende Informationen werden in der Host-Region gespeichert:

- Telemetrie- und Asset-/Objektdaten, einschließlich Zähler und Performance-Kennzahlen
- Informationen zu den Erfassungseinheiten
- Funktionale Daten
- Audit-Informationen zu Benutzeraktivitäten in Cloud Insights
- Active Directory-Informationen zu Workload-Sicherheit

- Informationen zur Workload Security Audit

Die folgenden Informationen befinden sich in den USA, unabhängig davon, in welcher Region Sie Ihre Cloud Insights-Umgebung hosten:

- Angaben zum Umgebungsstandort (manchmal auch „Mandant“ genannt), z. B. Standort-/Kontoinhaber.
- Informationen, über die NetApp Cloud Central mit regionalen Cloud Insights-Standorten kommunizieren kann, einschließlich Hinweisen zur Benutzerautorisierung.
- Informationen in Bezug auf die Beziehung zwischen dem Cloud Insights-Benutzer und dem Mandanten.

Host-Regionen

Host-Regionen sind:

- USA: USA-Osten-1
- EMEA: EU-Mitte-1
- APAC: ap-Südost-2

Weitere Informationen

Weitere Informationen zu Datenschutz und Sicherheit von NetApp finden Sie unter folgenden Links:

- "Trust Center"
- "Grenzüberschreitende Datenübertragungen"
- "Binding Corporate Rules"
- "Reaktion auf Datenanfragen von Drittanbietern"
- "NetApp Datenschutzgrundsätze"