

SINA Cloud als Service

Hochsicher und sofort einsatzbereit

Verschlusssachen bis VS-NfD sicher in der Cloud verarbeiten.
Ohne eigenes Rechenzentrum.



SINA Cloud als Service bietet digitale Souveränität ohne eigenes Rechenzentrum.

SINA Cloud als Service ist die erste VS-fähige Cloud-Infrastruktur als Service. Behörden und geheimschutzbetreute Unternehmen verarbeiten damit Verschlusssachen bis VS-NfD in der Cloud. Ein eigenes VS-fähiges Rechenzentrum und spezialisiertes Fachpersonal für dessen Betrieb sind dafür nicht nötig. secunet betreibt die Infrastruktur in zertifizierten Rechenzentren in Deutschland.

Souverän und rechtssicher

SINA Cloud als Service erfüllt die Anforderungen an eine souveräne Cloud für Verschlusssachen. Vier Punkte machen das aus:

- **IT-Sicherheitsprodukte**
SINA Cloud als Service basiert auf IT-Sicherheitsprodukten mit Einsatzerlaubnis des Bundesamts für Sicherheit in der Informationstechnik (BSI) für Verschlusssachen auf der Stufe VS-NfD.
- **Offene Technologien**
Die Plattform basiert auf Open-Source-Technologien wie Kubernetes und OpenStack. Das schafft Transparenz und reduziert Abhängigkeiten von einzelnen Herstellern.
- **Betrieb in Deutschland**
Die Infrastruktur läuft in zertifizierten secunet Rechenzentren in Deutschland. Anbieter und Betrieb haben ihren Sitz in Deutschland.
- **Planbare Kosten**
Investitionen in Rechenzentrumsflächen und zusätzliches Personal entfallen.

Die sichere Cloud

Verschlusssachen lassen sich mit SINA Cloud als Service bis zur Geheimhaltungsstufe VS-NfD verarbeiten. secunet ist derzeit der einzige Anbieter einer solchen Lösung. Der Betrieb ist nach BSI IT-Grundschutz zertifiziert, erfüllt die Anforderungen der ISO 27001 und ist DSGVO-konform. Die IT-Sicherheitsprodukte verfügen über eine BSI-Einsatzerlaubnis.

Das innovative Architektur-Design

SINA Cloud entkoppelt Sicherheitskomponenten und Cloud-Software. Dieses Design hat zwei entscheidende Vorteile:

1. Zukunftssicherheit: Der Funktionsumfang des Service lässt sich laufend erweitern, ohne die VS-Konformität der Sicherheitskomponenten zu beeinträchtigen.

2. Mandantenfähigkeit: Die Architektur ermöglicht eine hochsichere, kryptografische Trennung unterschiedlicher Kunden auf einer gemeinsamen VS-konformen Infrastruktur mit gemeinsamem Netzwerk, Storage und Ressourcenpool. Das steigert die Ressourceneffizienz gegenüber dedizierten Einzelösungen.

Der Blick in den Betrieb

Die Aufgabenteilung ist klar geregelt. Kunden konzentrieren sich auf ihre Fachanwendungen, secunet sorgt für:

- Bereitstellung der Cloud-Infrastruktur (IaaS) in zertifizierten secunet Rechenzentren
- Betrieb der Infrastruktur und Monitoring rund um die Uhr in zertifizierten Rechenzentren in Deutschland
- Updates und Lifecycle-Management
- Fortlaufende Einhaltung regulatorischer Anforderungen
- Flexible Skalierung bei steigenden Workloads
- Gesicherter Zugang über SINA-Komponenten
- Beratung und Begleitung bei Planung, Testbetrieb und Umsetzung

Für die Anwender ist das Übertragen, Speichern und Verarbeiten von Daten sowie die gemeinsame Nutzung von Ressourcen wie Storage und Netzwerk vollständig transparent und sicher.

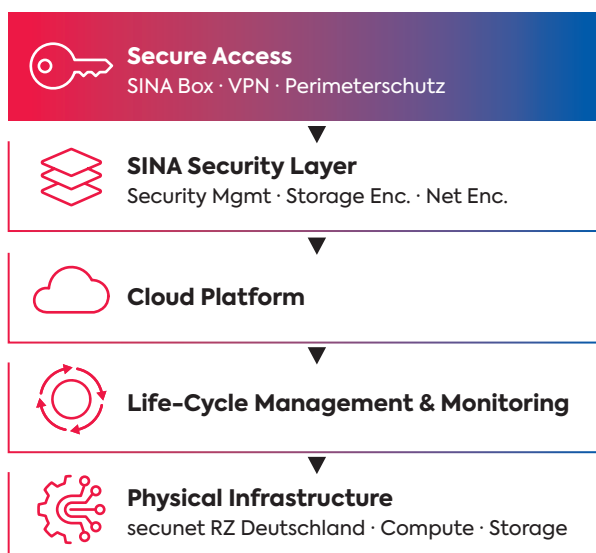
Alles aus einer Hand

secunet begleitet Kunden von der Planung über den Testbetrieb bis zum laufenden Betrieb. Infrastruktur, Sicherheitskomponenten und Betrieb kommen von einem Anbieter. Dadurch gibt es einen Ansprechpartner für alle Fragen und keine Schnittstellen zwischen verschiedenen Dienstleistern. Neue regulatorische Anforderungen setzt secunet fortlaufend um.

Verantwortung: Kunde



Verantwortung: secunet



Highlights

Volumen- und Netzwerkverschlüsselung

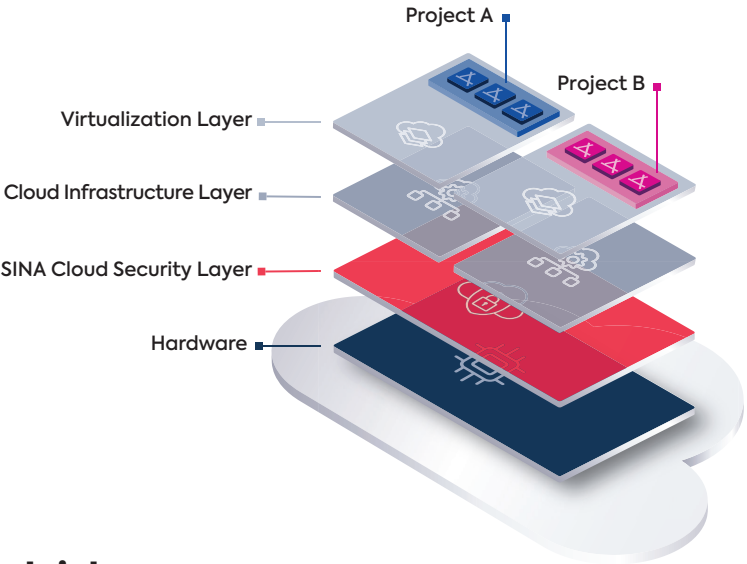
VMs und Volumes werden mandantenspezifisch VS-konform verschlüsselt abgelegt. Das gesamte Netzwerk ist mandantenspezifisch VS-konform verschlüsselt. Die Daten sind damit von der Instanzierung des Dienstes bis zur persistenten Ablage und auf dem Transportweg vor unberechtigter Einsicht und Manipulation geschützt.

Typische Einsatzszenarien

SINA Cloud als Service eignet sich für Kunden, die Anwendungen wie Nextcloud im VS-NfD-Kontext nutzen wollen, ohne eigene VS-Infrastruktur aufzubauen. Auch die Auslagerung von Fachverfahren in die Cloud wird so ermöglicht.

VS-Freigabe

Durch die integrierten IT-Sicherheitsprodukte wird der Weg zur VS-Freigabe deutlich vereinfacht. secunet unterstützt dabei von der Planung bis zur Umsetzung.



Die Bereitstellungsmodelle im Vergleich:

Kriterium	SINA Cloud onPrem	SINA Cloud aaS
Geheimhaltungsstufe	bis GEHEIM möglich	bis VS-NfD
Hosting-Ort	Rechenzentrum des Kunden	Zertifizierte secunet Rechenzentren in Deutschland
Betrieb und Wartung	Eigenständig, volle Kontrolle	Betrieb der Infrastruktur ausgelagert an secunet
Infrastruktur	Dediziert und maßgeschneidert	Geteilte VS-konforme Infrastruktur
Zugang	Lokal, internes Netz und sicherer Zugriff auf die Cloud über zugelassene IT-Sicherheitsprodukte	Sicherer Zugriff auf die Cloud über zugelassene IT-Sicherheitsprodukte
Mandantenfähige Volume- und Netzwerkverschlüsselung	ja	ja
Automatisiertes Life-Cycle-Management	ja	ja, durch secunet
Eigenes Fachpersonal für den Infrastrukturbetrieb erforderlich	ja	nein

Passt SINA Cloud als Service zu Ihren Anforderungen?
Unser Team berät Sie zu Einsatzszenarien und zum Weg zur VS-Freigabe.