SiTS

Your Trusted
Cyber Security Partner

Privilegierte Zugriffe sichern

Privileged Access Management as a Service

Einleitung von Brian de Vries, Teamleiter PAM as a Service

SITS freut sich, die Einführung von Privileged Access Management as a Service (PAMaaS) bekannt zu geben. Dieses Angebot basiert auf unserer langjährigen erfolgreichen Zusammenarbeit mit CyberArk – einem führenden Anbieter im „Gartner® Magic Quadrant™ für Privileged Access Management".

In der vernetzten Welt von heute sind privilegierte Zugangskonten die „Schlüssel zum Königreich" für Cyberkriminelle. Sie gewähren umfassenden Zugriff auf Systeme und Daten – und damit sind Konten im Visit für Angreifer. Studien zeigen, dass die meisten Sicherheitsverletzungen privilegierte Konten betreffen und damit robuste PAM-Lösungen unerlässlich machen. Der Anstieg von Cyberangriffen wie Ransomware zeigt, dass ungesicherte privilegierte Identitäten oft eine Lücke sind, die Angreifer nutzen.

Das PAM as a Service-Angebot von SITS nutzt die fortschrittlichen Technologien von CyberArk: Die umfassende Lösung sichert, verwaltet und überwacht privilegierte Zugriffe. So profitieren Unternehmen von modernsten Sicherheitsmaßnahmen, ohne sich um die Verwaltung und Wartung kümmern zu müssen.

„Dies ist wirklich ein Wendepunkt im Bereich der verwalteten IAM-Dienste. Er adressiert die Risiken privilegierter Zugriffe, die bei den meisten Cyberangriffen eine Rolle spielen. Unsere Kunden profitieren von erstklassigen PAM Managed Services – mit unvergleichlicher Skalierbarkeit, Geschwindigkeit und Preis-/Leistungsverhältnis. Ich bin stolz auf das Team, das dies möglich gemacht hat."

„Ich hoffe, Sie erfahren mehr über Privileged Access Management. Zögern Sie nicht, mich zu kontaktieren, falls Sie Fragen haben."

Brian de Vries, Teamleiter PAMaaS

Haben Sie Ihre Privilegierten Konten wirklich im Blick?

Jede Organisation kann Opfer von Datenpannen oder Angriffen werden – sei es durch ahnungslose oder unzufriedene Mitarbeiter, externe Angreifer oder sogar Partnerorganisationen. Heute geht es nicht mehr nur um zufällige Schwachstellen, sondern um gezielte Versuche, Ihre Informationen und Systeme auszunutzen.

Solche Hacks sind regelmäßig in den Schlagzeilen und haben weitreichende Folgen: Verlust oder Veröffentlichung sensibler Daten, Lösegeldzahlungen, um wieder Zugang zu erhalten – oder der endgültige Verlust bei Nichtzahlung. Gesetzliche Meldepflichten bedeuten zudem Bußgelder und mögliche Schadensersatzforderungen, was die Zusammenarbeit mit Kunden gefährdet.

Wie gut haben Sie den Zugang zu Ihren Informationen, IT-Systemen und den Systemen Ihrer Kunden im Blick?

Laut dem Bericht „Identity Security Threat Landscape 2024“ hatten 93 % der Organisationen in den letzten 12 Monaten zwei oder mehr identitätsbezogene Sicherheitsverletzungen. Studien zeigen, dass viele Unternehmen keinen vollständigen Überblick über ihre Zugangsdaten haben – IT-Auditoren stellen regelmäßig Risiken beim Umgang mit diesen fest.

1. https://www.cyberark.com/resources/ebooks/identity-security-threat-landscape-2024-report

Was sind Ihre privilegierten Konten?

Jeder, der mit IT-Systemen arbeitet, nutzt Login-Konten und Zugriffsrechte – diese sind notwendig, um Anwendungen und Kommunikationsmittel wie persönliche E-Mails zu verwenden. Solche Konten sind reguläre Geschäftskonten, die von Identity and Access Management-Lösungen verwaltet werden. Für Mitarbeiter, die IT-Systeme oder die Kommunikation eines Unternehmens verwalten, kommen jedoch spezielle Konten ins Spiel: die privilegierten Konten. Sie werden genutzt, um IT-Systeme, Netzwerke, Server, Workstations und mobile Geräte einzurichten oder zu warten, oder um Inhalte in sozialen Medien für Ihr Unternehmen zu veröffentlichen.

Privilegierte Konten haben weitaus mehr Rechte als reguläre Konten und gelten als kritische Konten. Benutzer privilegierter Konten haben die Möglichkeit, den Zugriff auf vertrauliche Informationen zu ändern oder geschäftskritische Anwendungen unzugänglich zu machen. Beispiele für privilegierte Konten sind:

- Administrator- und Root-Konten zur Wartung von IT-Systemen;
- Konten zur Veröffentlichung/Bearbeitung von Informationen auf den Social-Media-Konten Ihres Unternehmens;
- Konten zur Anpassung der Stromversorgung (z. B. Windturbinen, Smart Meter und andere IoT-Geräte);
- Konten zur Durchführung von (Zahlungs-)Transaktionen;
- Konten, die innerhalb von Anwendungen oder Robotic Process Automation (RPA) -Software verwendet werden, um Verbindungen zu anderen Anwendungen herzustellen.

Privilegierte Konten: Der Zugang zu den unverzichtbaren Kronjuwelen Ihres Unternehmens gewähren. Um die Nutzung, Verwaltung und den Zugriff auf privilegierte Konten zu regulieren, gibt es spezielle Lösungen, die unter dem Sammelbegriff Privileged Access Management (PAM) zusammengefasst werden.

Probleme mit privilegierten Konten

Privilegierte Konten sind ein begehrtes Ziel für Hacker, da sie Zugang zu wichtigen Systemen und Informationen bieten. Ohne eine PAM-Lösung (Privileged Access Management) sind Nutzer privilegierter Konten gezwungen, selbst Passwörter festzulegen, die schwer zu erraten sind und regelmäßig geändert werden müssen – ein ineffektiver Schutz gegen den Missbrauch durch Unbefugte. Gleichzeitig muss dokumentiert werden, wer welches privilegierte Konto wann genutzt hat, um eine Rückverfolgbarkeit zum Benutzer sicherzustellen.

Um die Kontrolle zu behalten, wird die Anzahl der privilegierten Konten oft eingeschränkt – ein Ansatz, der jedoch das Prinzip der minimalen Privilegien gefährdet. Häufig haben privilegierte Nutzer mehr Rechte, als für ihre Aufgaben notwendig wären, was zu erheblichen Sicherheitslücken führt. Das Prinzip der minimalen Privilegien wird damit aufgegeben: Gewähre nur diejenigen Rechte, die für die jeweilige Aufgabe erforderlich sind, für die das privilegierte Konto bestimmt ist.

Zusätzlich werden privilegierte Konten oft von mehreren Mitarbeitern genutzt, was bedeutet, dass das Passwort vielen bekannt sein muss. Wer ist verantwortlich für regelmäßige Passwortänderungen? Wer dokumentiert, wer das Konto wann genutzt hat? Die Disziplin, diese Prozesse aufrechtzuerhalten, ist oft nicht ausreichend – ein Zustand, den Hacker gerne ausnutzen. Besonders problematisch sind Passwörter, die in Anwendungen und Diensten verwendet werden und nicht ausreichend überwacht werden – hier lauern die größten Risiken!

PAM als „Man-In-The-Middle“ (MITM)

PAM ermöglicht den sicheren Zugriff auf Zielsysteme durch eine **Sitzungsverwaltung**. Sie fungiert Sitzungsverwaltung als Isolationsschicht zwischen dem Arbeitsplatz des Administrators und dem eigentlichen Zielsystem. Der Benutzer verbindet sich zunächst mit einem abgesicherten PAM-Sitzungsproxy, auch bekannt als Steppingstone oder Jump-Host. Dieser Proxy stellt anschließend eine zweite Verbindung zum Zielsystem her, sodass keine direkte Verbindung zwischen dem Arbeitsplatz und dem Zielsystem besteht. So wird verhindert, dass bei einem möglicherweise kompromittierten Arbeitsplatz sensible Daten „abgehört“ werden können.

Der Sitzungsproxy dient nicht nur der Isolierung, sondern ermöglicht auch die Aufzeichnung sämtlicher Aktivitäten auf einem Zielsystem. So können berechtigte Personen – beispielsweise Auditoren oder Problemlöser – im Nachgang nachvollziehen, welche Aktionen durchgeführt wurden. Darüber hinaus besteht die Möglichkeit, eine Sitzung in Echtzeit mitzuverfolgen, was sich besonders dann als nützlich erweist, wenn ein externer Anbieter auf das System zugreift.

Beim Einsatz der Sitzungsverwaltung sollte jedoch auch geprüft werden, ob es zu datenschutzrechtlichen Konflikten kommt. Zunächst muss geklärt werden, welche Richtlinien für das Monitoring von Mitarbeitern gelten. Zudem können während einer Sitzung vertrauliche Informationen sichtbar werden, weshalb genau festgelegt werden sollte, wer innerhalb der Organisation befugt ist, diese Aufzeichnungen einzusehen. Ebenso ist zu klären, wie lange solche Aufzeichnungen aufbewahrt werden sollen. Bei langfristiger Speicherung muss sichergestellt sein, dass genügend Speicherplatz zur Verfügung steht, um diese Anforderungen zu erfüllen.

Privileged Access Management oder Privileged Account Management?

Eine PAM-Lösung (Privileged Access Management) bietet eine ganze Reihe smarter Funktionen, die Ihnen helfen, den Zugriff auf privilegierte Konten abzusichern und jederzeit nachzuvollziehen. Ihre wertvollen Konten werden in einem digitalen Tresor gespeichert, geschützt durch mehrere Sicherheitsebenen. Dazu zählen: Starke Verschlüsselung, fein abgestufte Zugriffsrechte, lückenlose Protokollierung, Isolierung und Härtung. Sie sorgen dafür, dass kein Unbefugter an die sensiblen Zugänge gelangt.

PAM unterstützt das Passwortmanagement privilegierter Konten und entlastet dadurch die Benutzer dieser Konten. Passwörter können automatisch in regelmäßigen Abständen geändert werden, einschließlich der Durchsetzung erforderlicher Komplexität. Durch die regelmäßige Änderung von Passwörtern wird das Risiko verringert, ein altes, bekanntes Passwort zu verwenden. Es wird außerdem möglich sein, das Prinzip der minimalen Privilegien anzuwenden, sodass spezifischere Konten mit nur den minimal erforderlichen Rechten genutzt werden. Die sichere Speicherung und automatische Verwaltung von Passwörtern wird als Privileged Account Management bezeichnet.

Privileged Access Management sorgt dafür, dass Administratoren auch dann Zugriff auf Zielsysteme haben, wenn sie das Passwort gar nicht kennen. PAM übernimmt hier den Zugang, das Passwort bleibt für den Benutzer unsichtbar und wird einfach im Hintergrund eingegeben. Das ist nicht nur für interne Admins hilfreich, sondern auch für externe Dienstleister, die sicheren Fernzugriff benötigen – und das ohne die üblichen Risiken.

In PAM sind alle Berechtigungen genau definiert: Welche Zielsysteme dürfen Administratoren ansteuern, welche Konten dafür nutzen? Optional kann ein Freigabeprozess eingerichtet werden, der sicherstellt, dass sensible Konten nicht ohne Prüfung genutzt werden. Die komplette Nutzung eines privilegierten Kontos wird protokolliert und bleibt damit jederzeit nachvollziehbar. Bei Bedarf lassen sich sogar alle Aktivitäten aufzeichnen, sodass Auditoren später genau nachverfolgen können, was in einer Sitzung passiert ist – ein wichtiges Feature für die Compliance.

Mit PAM bekommen Sie:

- Zentral gesicherte Speicherung der Passwörter privilegierter Konten.
- Automatische, regelmäßige Passwortänderungen gemäß Ihren Sicherheitsrichtlinien.
- Verwaltung des zentralen Zugriffs auf Zielsysteme und zugehörige Konten.
- Präzise Zugriffssteuerung: Nur die richtigen Leute haben Zugriff auf die richtigen Systeme.
- Bedarfsabhängigen Zugang, wann immer er nötig ist.
- Lückenlose Audit-Trails für alle Aktionen, die mit privilegierten Konten durchgeführt werden.

Von Standing Privileges to Zero Standing Privileges

Traditionell werden privilegierte Konten oft dauerhaft angelegt, was auch als „stehender Zugriff" (Standing Privileges) bezeichnet wird. Das Risiko bei stehendem Zugriff besteht darin, dass diese Konten von Angreifern ausgenutzt und missbraucht werden können, da sie dauerhaft bestehen bleiben. Moderne PAM-Lösungen setzen hingegen auf das „Zero Standing Privileges"-Prinzip, das dem Ansatz der minimalen privilegien entspricht.

Mit „Zero Standing Privileges" werden Aufgaben nach dem Prinzip von Just-in-Time- und Just-Enough-Privilegien zugewiesen. Das bedeutet, dass Zugriffsrechte nur für eine festgelegte Zeit und genau in dem Umfang gültig sind, der für eine spezifische Aufgabe notwendig ist. Ein Administrator, der operative Aufgaben erledigen muss, stellt über das PAM-System eine Anfrage. Wenn der Anfragende die Voraussetzungen erfüllt, erhält er die entsprechenden Administratorrechte für das Asset, die durch attributbasierte Zugriffskontrolle (ABAC) geregelt sind. Sobald die Anfrage (automatisch) genehmigt wird, erstellt das PAM-System ein temporäres privilegiertes Konto, das nur für den festgelegten Zeitraum und das spezifische Asset gültig ist. „Zero Standing Privileges" werden durch ephemeren Zugriff gewährt – nach Ablauf des Zeitraums wird der Benutzer automatisch abgemeldet, und das privilegierte Konto wird gelöscht.

Benutzer automatisch abgemeldet, und das privilegierte Konto wird gelöscht. Das PAM-System zeichnet automatisch auf, wer wann auf welches Asset zugegriffen hat, und erstellt ein vollständiges Audit-Protokoll. Das Fehlen von stehendem Zugriff verhindert Missbrauch, da kein Konto vorhanden ist, das gehackt werden könnte. Das temporäre privilegierte Konto wird so erstellt, dass es in Protokolldateien und im SIEM-System erkennbar ist.

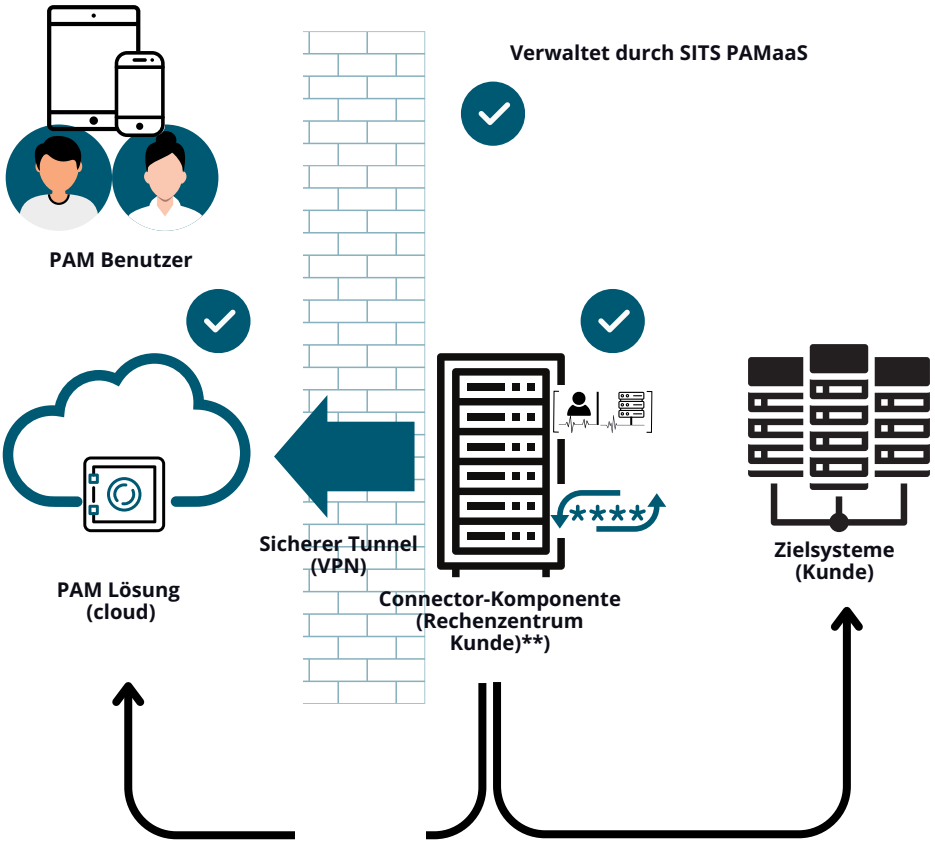
Die Anwendung von „Zero Standing Privileges" auf operative Konten durch ephemeren Zugriff ist der neue Standard im Privileged Access Management. Immer mehr PAM-Lösungen bieten diese Funktion an, sodass Sie Ihre Organisation noch effektiver gegen Cyberangriffe schützen können. Für privilegierte Konten wie Anwendungs- oder integrierte Konten, die weiterhin als stehende Privilegien existieren müssen, kann der PAM-Digitaltresor genutzt werden, um diese zentral zu sichern und zu verwalten.

„Zero Standing Privileges" werden durch ephemeren Zugriff ermöglicht. Nach Ablauf des festgelegten Zeitraums wird der Benutzer automatisch abgemeldet und das temporäre privilegierte Konto entfernt.

PAM als sichere Fernzugriffslösung

In der heutigen Welt wird immer mehr Arbeit remote ausgeführt, sowohl von internen Mitarbeitern als auch von externen Mitarbeitern und Anbietern. Die Bereitstellung der richtigen Funktionen für sicheren Fernzugriff und Verwaltungszugriff auf Zielsysteme kann eine Herausforderung sein und teuer werden. Typische Lösungen umfassen Laptops, VPN-Zugänge oder Remote-Desktop-Anwendungen wie Citrix, und auch deren Verwaltung und Sicherung darf nicht vergessen werden.

Das PAM-Sitzungsmanagement in Kombination mit einem zusätzlichen PAM-Fernzugriffsmodul ermöglicht es, sicheren Remote-Verwaltungszugriff auf Zielsysteme bereitzustellen. Der Zugriff kann über den Webbrowser erfolgen, ohne dass VPN- oder Remote-Desktop-Lösungen erforderlich sind. Das Fernzugriffsmodul ist vollständig gesichert, und Multi-Faktor-Authentifizierung ist ein Muss. Nur die nötigen privilegierten Konten, basierend auf den PAM-Berechtigungen, werden bereitgestellt. Dabei werden keine Passwörter der privilegierten Konten an die Nutzer offengelegt. Die gesamte Nutzung wird umfassend protokolliert, um eine vollständige Nachverfolgbarkeit sicherzustellen.



SITS PAM as a Service (PAMaaS)

PAM ist unverzichtbar, wenn es um den Schutz privilegierter Zugriffe auf kritische Systeme geht und um die Einhaltung von Compliance-Anforderungen sicherzustellen. Doch gerade kleine und mittelständische Unternehmen (KMUs) stehen vor großen Herausforderungen, wenn es um die Implementierung geht: Es fehlt oft an Wissen, Ressourcen oder den nötigen Vorabinvestitionen. Das führt dazu, dass PAM-Implementierungen immer wieder verschoben werden – was das Risiko von Sicherheitsvorfällen und die Nichteinhaltung von Standards erhöht.

Für Organisationen, die sich genau diesen Herausforderungen stellen müssen, bietet SITS die Lösung: PAM as a Service (PAMaaS). Das Ziel von PAMaaS ist es, Ihnen die Einführung einer PAM-Lösung einfach zu machen – ohne dass Sie sich über fehlende Expertise oder Ressourcen Gedanken machen müssen. Wir haben unser Wissen und die Best Practices aus jahrelanger Erfahrung standardisiert, sodass Design, Implementierung und Verwaltung reibungslos laufen. Die Vorteile auf einen Blick:

- **Einfache Beschaffung**: Plug & Play – PAM-Lösung sofort nutzbar.
- **Voller Funktionsumfang**: Alle PAM-Anwendungsfälle, inklusive ephemerem Zugriff und sicherem Fernzugriff für Drittanbieter. Basierend auf der branchenführenden CyberArk-Technologie.
- **Schnelle Umsetzung**: Compliance-Anforderungen schnell erfüllen.
- **Weniger interner Aufwand**: Ressourcenengpässe minimieren – wir übernehmen die Verwaltung.
- **Skalierbarkeit**: Perfekt für kleine bis mittelständische Unternehmen.
- **Kalkulierbare Kosten**: Transparente Preisgestaltung, keine Überraschungen.

"Wir freuen uns sehr, dass wir neben großen Unternehmen auch kleinen und mittelständischen Unternehmen den Zugang zur CyberArk-Technologie bieten können. So sichern, kontrollieren und überwachen wir den Zugriff privilegierter Nutzer auf kritische Systeme und sensible Informationen innerhalb Ihres Unternehmens. Wir sind stolz darauf, die Ersten zu sein, die diesen cloud-basierten, vollständig verwalteten Service für KMUs anbieten – einsatzbereit in nur 6 Wochen, zu einem erschwinglichen festen Monatsbeitrag und ohne einmalige Kosten."

Brian de Vries, Teamleiter PAMaaS

PAMaaS - Vollständig standardisiert und verwaltet

Mit den Standardisierungen von SITS wird PAMaaS zu einer schlanken und effizienten Lösung für Unternehmen, die ihre IT-Ressourcen und das nötige Fachwissen schonen wollen. Diese Standardisierung minimiert mögliche Verzögerungen bei der Implementierung, sodass Sicherheitsteams sich auf ihre eigentlichen Aufgaben konzentrieren können. Hier die wichtigsten Elemente:

- **Architektur;** Ein dedizierter Cloud-Tenant für die sichere Speicherung und den Zugriff auf privilegierte Anmeldeinformationen, mit Connectors auf der Kundeninfrastruktur für sichere Kommunikation und Integrationen, wie z. B. Zielsysteme, LDAPs und SIEM. Die Architektur und alle erforderlichen Voraussetzungen sind vollständig dokumentiert und für den Kunden verfügbar.
- **Onboarding und Konfiguration:** Während das Onboarding auf die effizienteste Weise durchgeführt wird, sind alle damit verbundenen Konfigurationen basierend auf den über die Jahre entwickelten Best Practices vordefiniert. Der Kunde muss sich keine Sorgen über logische Benennungsstandards, Berechtigungsmodelle und Verbindungskomponenten machen. Alle Konfigurationen werden automatisiert angewendet.
- **Dokumentation:** Als Teil der standardisierten Dokumentation erhält der Kunde eine Liste der Voraussetzungen, ein Lösungsdesign, einen Service Level Agreement (SLA), Quick Reference Cards (QRCs) und Berichte.
- **Prozesse:** Ein sehr wichtiger Aspekt einer erfolgreichen PAM-Implementierung sind die Prozesse rund um die Verwaltung und Nutzung der PAM-Lösung. Mit unseren standardisierten Prozessen wird eine transparente Arbeitsweise für das Onboarding und Offboarding von Benutzern/Teams sowie für andere Serviceanfragen oder die Behandlung von Vorfällen geschaffen, wenn dies erforderlich ist. Und nicht zu vergessen, auch das Software-Lifecycle-Management wird über einen standardisierten Prozess durchgeführt und von SITS als Teil von PAMaaS vollständig umgesetzt.

"Wir freuen uns auf die Zusammenarbeit mit SITS, einem führenden Unternehmen im Bereich Cybersicherheit. Diese Zusammenarbeit – unsere Expertise als Managed Services Provider kombiniert mit dem einzigartigen PAM-as-a-Service-Angebot von SITS – markiert einen wichtigen Schritt, um erstklassige PAM-Dienstleistungen für Unternehmen jeder Größe bereitzustellen.Da die meisten Sicherheitsverletzungen privilegierte Konten betreffen, unterstreicht diese Zusammenarbeit unser Engagement, Sicherheitsmaßnahmen zu verbessern, um das Risiko von Datenverletzungen zu verringern und die Einhaltung regulatorischer Standards sicherzustellen."

Renske Galema, Area Vice President Northern Europe at CyberArk

CYBERARK®

Auf einen Blick

Minimieren Sie das Risiko von Datenverletzungen und stellen Sie die Einhaltung regulatorischer Standards sicher. PAM as a Service bietet Ihnen die bewährte Technologie von CyberArk, um privilegierten Zugriff effizient als Dienstleistung zu sichern, zu verwalten und zu überwachen – ideal für kleine, mittelständische und große Unternehmen.

Vorteile von PAM as a Service:

- Vollständig verwaltet von SITS (MSP) Cloud-basierte PAM-Lösung von CyberArk.
- In 6 Wochen betriebsbereit.
- Keine Einrichtungskosten, nur eine feste monatliche Gebühr.
- Standardisierte Prozesse und vollständig verwaltet von zertifizierten Spezialisten.
- Hoch skalierbar, geeignet für kleine und mittelständische Unternehmen.

Loslegen!

Fordern Sie Ihre Demo oder Ihr Webinar an!

Melden Sie sich jetzt für eine Demo oder ein Webinar an und entdecken Sie, wie Sie Ihre Sicherheitsmaßnahmen verbessern können. Reduzieren Sie das Risiko von Datenverletzungen und gewährleisten Sie die Einhaltung regulatorischer Standards.

Erhalten Sie Ihr Preisangebot innerhalb von 48 Stunden!

- Keine Einrichtungskosten;
- Nur eine feste monatliche Gebühr;
- Skalierbar in Benutzerzahlen;
- Transparent und vorhersehbar.

info.de@sits.com
info.ch@sits.com
info.dk@sits.com
info.nl@sits.com

www.sits.com

SITS