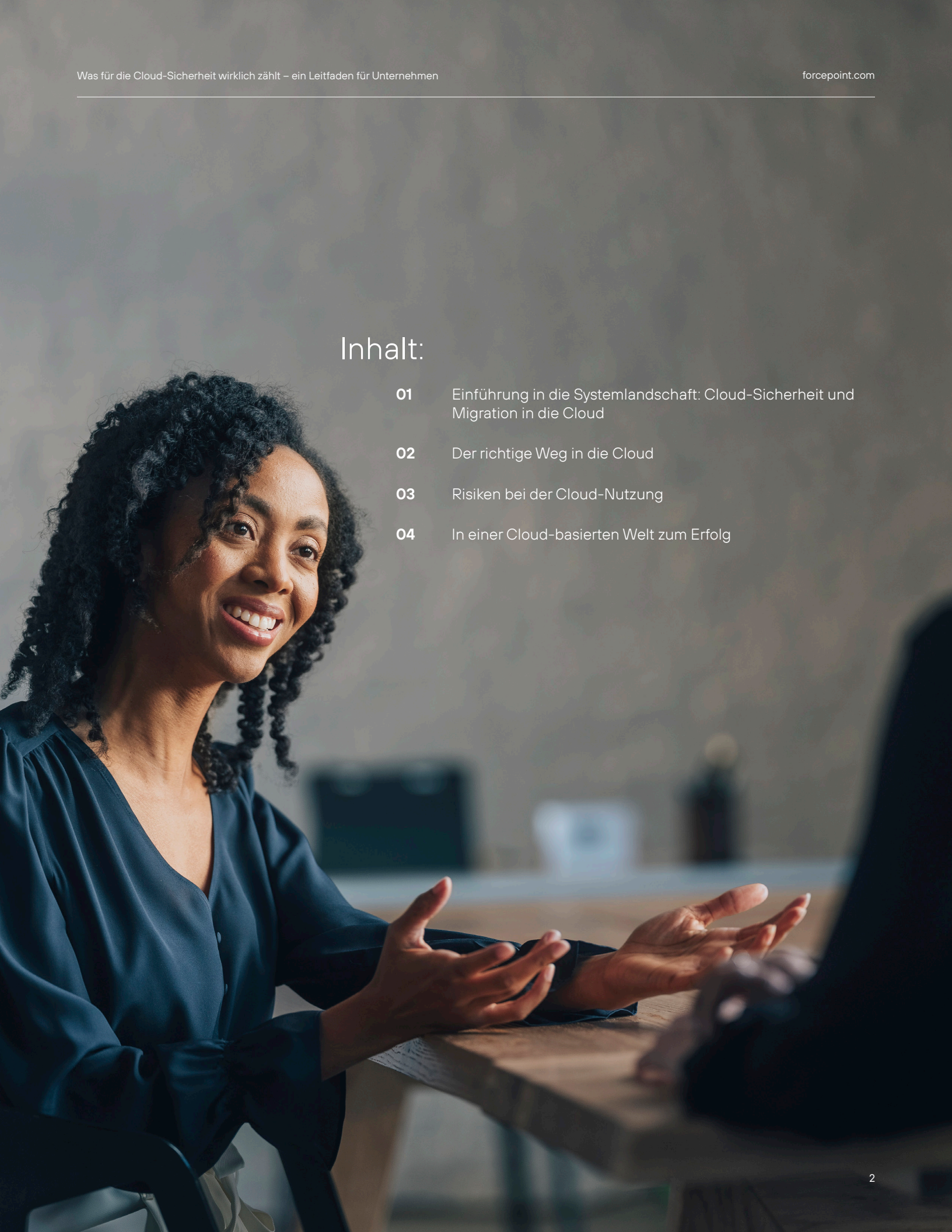
Was für die Cloud-Sicherheit wirklich zählt – ein Leitfaden für Unternehmen

Forcepoint

Broschüre

Inhalt:



Einführung in die Systemlandschaft: Cloud-Sicherheit und Migration in die Cloud

Wenn Sie das Gefühl haben, dass in der heutigen Welt kein Weg mehr um die Cloud herumführt, liegen Sie richtig. Aber warum wird in einem immer höheren Tempo alles in die Cloud verlagert? Die treibende Kraft ist der Konsum. Genauer gesagt geht es um die Business-to-Consumer-Beziehung.

Wie Unternehmen die Cloud anpassen und schützen, orientiert sich am Nutzungsverhalten der Menschen.

Cloud-Sicherheit wird vom Menschen gesteuert.

Die Cloud steht für direkten Zugriff.

Und die Cloud weckt Erwartungen.

Die Cloud ist aus unserem täglichen Leben nicht mehr wegzudenken. Zu jedem Zeitpunkt können wir unterbrechungsfrei auf Inhalte, Anwendungen und Geräte zugreifen, die nahtlos miteinander verbunden sind. Insgesamt ist die Cloud exakt daran orientiert, wie der moderne Mensch unterbewusst funktioniert und handelt. Am Arbeitsplatz ist die Erwartungshaltung dieselbe. Man möchte die benötigten Komponenten zu jedem beliebigen Zeitpunkt nutzen können. Man erwartet eine reibungslose Arbeitserfahrung, die die Produktivität nicht einschränkt, sondern fördert. Wie kann die Cloud Ihre Produktivität steigern? Wie kann man mit weniger mehr erreichen? Die Cloud bedeutet nicht nur Komfort, sondern auch Verletzbarkeit.

Arbeitskräfte sind im Grunde Verbraucher. Wie Unternehmen ihre Organisationen, Daten und Mitarbeiter schützen, muss denselben Erwartungen und Erfahrungen entsprechen wie unser Alltag. Damit wir reibungslos arbeiten und den immer neuen Bedrohungen trotzen können, die unweigerlich mit dieser Freiheit und diesem Komfort verbunden sind, müssen Sicherheitsmaßnahmen stetig weiterentwickelt werden.

Das macht die Cloud-Kultur aus. Doch welche Umstände regen zum Handeln an und motivieren Unternehmen dazu, in Bezug auf Cloud und Sicherheit umzudenken? Hier einige Beispiele:

- Die digitale Transformation seit der Einführung und Implementierung von Office 365
- Die Verlagerung von langjährig genutzten bzw. benutzerspezifischen Anwendungen in die Cloud, wie z. B. EHR- oder ERP-Systeme
- Mitarbeiter außerhalb des Büros, des Unternehmensnetzwerks oder jenseits anderer Schutzmaßnahmen
- Globale Unternehmen, die in weit verzweigten Umgebungen und darüber hinaus agieren und deren Außenstellen dasselbe Sicherheitsniveau erfordern wie die Zentrale – ohne dass an jedem Standort ein teures, hardwarebasiertes Backhaul-Netzwerk nötig ist
- Optimierungsmaßnahmen – ob Konsolidierung von Security Stacks, optimierte Workflows für Teams oder Reduzierung von Investitions- und Betriebskosten
- Verlagerung der Infrastruktur in eine öffentliche Cloud, wie z. B. Amazon Web Services oder Microsoft Azure

Der richtige Weg in die Cloud

Jeder hat ein anderes Verständnis von „Cloud-Sicherheit". Noch dazu verändert sich die Cloud-Landschaft ständig und rapide. Wie bleibt man auf dem aktuellen Stand? Wie gestaltet man eine ganzheitliche und effektive Strategie? Um Ihr Unternehmen erfolgreich schützen zu können, bedarf es einer umfassenden Cloud-Sicherheit.

Hier sehen Sie die wesentlichen Komponenten einer Cloud:

Daten in der Cloud | **Benutzer** in der Cloud | **Anwendungen** in der Cloud | **Konnektivität** in der Cloud | **Infrastruktur** in der Cloud | **Sicherheit** in der Cloud

Und genau darum geht es beim Thema Cloud-Sicherheit. Um Sicherheitslücken zu vermeiden und Benutzer und Daten zu schützen, müssen all diese Komponenten durch die Sicherheitsmaßnahmen abgedeckt sein. Dass es keine allgemeingültige Definition von Cloud-Sicherheit gibt, bedeutet nicht, dass es nicht den richtigen Weg in die Cloud gibt.

Wie sieht dieser also aus?

Unternehmen müssen die folgenden Maßnahmen ergreifen, um Ihre Cloud anzubinden und zu schützen:

- Zugriff auf Web-Inhalte und Cloud-Anwendungen für jeden Benutzer unabhängig von Standort oder Gerät schützen
- Sicherheitsstrategie für die Cloud unternehmensweit transparent gestalten und kontrollieren
- Daten schützen, die in die und aus der Cloud übermittelt werden
- Direkte Cloud-Konnektivität für Benutzer und Standorte ohne Backhaul-Netzwerk aktivieren
- Infrastruktur und Workflows optimieren
- Schutz vor komplexen Bedrohungen bieten, einschließlich Zero-Day-Exploits

So weit, so gut. Aber wie können diese Ziele erreicht werden? Viele Unternehmen haben möglicherweise bereits Produkte implementiert, die einige der genannten Voraussetzungen erfüllen oder setzen unterschiedliche Teams ein, die für bestimmte Bereiche der Cloud-Sicherheit verantwortlich sind. Es kann allerdings in keinem Unternehmen zielführend sein, die ohnehin ausgelasteten Sicherheitsteams mit Einzelprodukten zu überhäufen, die weder in eine Gesamtlösung integriert noch miteinander verknüpft sind. Anstelle zusammengewürfelter Produkte unterschiedlicher Hersteller sollte daher eine ganzheitliche Lösung angestrebt werden. Ganz ohne Abhängigkeiten geht es nicht – so bedarf es z. B. Transparenz, um die Kontrolle zu behalten oder der Migration von vor Ort installierten Web-Sicherheitslösungen in die Cloud, um netzwerkexterne Benutzer zu schützen. Im Optimalfall ist Cloud-Sicherheit eine kombinierte Lösung, die Daten, Internetzugriff, Cloud-Zugriff, Cloud-Daten und Konnektivität umfasst. Mit einer solchen Lösung kann Ihr Sicherheitsteam alle Probleme beheben und Sicherheitslücken eliminieren. Ob ein Lieferant oder drei – Unternehmen müssen sicherstellen, dass die Komponenten ihrer Lösung ihren Bedürfnissen entsprechen und aufeinander abgestimmt sind, um alle wichtigen Geschäftsanforderungen zu erfüllen.

Risiken bei der Cloud-Nutzung

Daten in die Cloud zu verlagern ist ein komplexes Unterfangen. Wenn Sie Bedenken haben, sind Sie damit nicht allein. Wie kann man Nutzungsrechte verwalten und die Kontrolle behalten? Wie können Bedrohungen weiterhin abgewehrt werden? Wie kann man die erforderliche Leistung weiterhin sicherstellen?

Wir geben Ihnen Antworten auf die häufigsten Fragen.

Latenz

Für eine Reduzierung der Latenzzeit bedarf es einer guten Infrastruktur. Ein breiter Aktionsradius mit zahlreichen Kommunikationspunkten weltweit ist ausschlaggebend für geringe Latenzzeiten und andere produktivitätssteigernde Vorteile, wie z. B. die genaue Lokalisierung von Inhalten. Durch den Einsatz von **Tier-1-Netzwerken und Tier-4-Rechenzentren kann für verzögerungskritische Anwendungen eine große Reichweite und ein hohes Maß an Redundanz, Konnektivität und Qualität erzielt werden.**

Transparenz

Was nicht sichtbar ist, kann man nicht adäquat schützen. Und man muss sich über die Auswirkungen von Änderungen oder Richtlinien im Klaren sein, bevor man sie umsetzt. Die Kombination aus einem **in der Cloud bereitgestellten Web-Gateway** und einer **Firewall** ermöglicht eine konsistente Transparenz und Durchsetzung für alle Benutzer an allen Standorten, u. a. die Durchsetzung von Richtlinien und die Kontrolle von Schatten-IT. Mittels **CASB**-Funktion können Unternehmen nachvollziehen, was Benutzer mit genehmigten und nicht genehmigten Anwendungen in der Cloud treiben und somit Risiken erkennen und Benutzer und Daten schützen.

Compliance

Vertrauen Sie Zertifizierungen und nicht selbst auditierter und erklärter Compliance. Die folgenden Standards sind für Ihr Unternehmen wahrscheinlich relevant:

- **ISO 27018**: Schutz von personenbezogenen Daten (PII) in der Cloud
- **ISO 27001**: Multi-Site-Zertifizierung für Entwicklung, Qualitätssicherung, Installation und Support
- **CSA (Cloud Security Alliance)**: Software-Sicherheit und funktionsübergreifende Abläufe in Cloud-Umgebungen (basierend auf den Regularien der DSGVO)
- **SOC2 (Service Organization Control 2)**: nichtfinanzielle Kontrollen bezüglich Sicherheit, Verfügbarkeit, Verarbeitungsintegrität, Vertraulichkeit und Datenschutz; außerdem werden Details zu Rechenzentrumstests und operativer Effektivität untersucht.

Datenhoheit

Die Cloud verfügt zwar über keine konkreten Begrenzungen, ist jedoch nicht von gesetzlichen Regelungen hinsichtlich geographischer Grenzen ausgenommen. Digitale Daten unterliegen den Rechtsvorschriften des Ortes, an dem sie gespeichert sind. Zur bestmöglichen Einhaltung der örtlichen Gesetze und Richtlinien und aus Leistungsgründen sollten sich die **Cloud-Rechenzentren in denselben Regionen befinden wie Ihr Unternehmen**.

Datenverlust

Ein einheitlicher Ansatz verspricht den größtmöglichen Erfolg. Mit integrierten **Datenschutzlösungen** können Sie Ihre Sicherheitsmaßnahmen vor Ort erweitern und darüber hinaus Web-, E-Mail-, Endpunkt-, Netzwerk- und Cloud-Umgebungen einbeziehen. Nutzen Sie Ihre bestehenden Richtlinien, um Daten in der Cloud und während der Übertragung zu schützen.

BYOD

Heutzutage sind Mitarbeiter von einer Vielzahl genehmigter und nicht genehmigter Cloud-Anwendungen sowie verwalteter und nicht verwalteter Geräte abhängig. Für den Schutz von ortsunabhängigen bzw. Roaming-Benutzern reichen Abwehrmaßnahmen an den Netzwerkgrenzen und Endpunktschutz nicht aus. Anhand **detaillierter Sicherheitsrichtlinien** muss zwischen verwalteten und BYOD-Geräten unterschieden werden, damit Mitarbeiter ihre eigenen Geräte flexibel und ohne zusätzliches Risiko nutzen können. Durch **erweiterte Kontrollen** können mobile Benutzer geschützt werden, die ihre Geräte sowohl für geschäftliche als auch für private Zwecke nutzen.

„Wird schon gutgehen" ist der falsche Ansatz

Viele Unternehmen sind dermaßen damit beschäftigt, agiler und effizienter zu werden, dass ihre Einstellung in Bezug auf die Cloud häufig „Darum kümmern wir uns später" lautet. Aber nur das Abhaken eines Punkts auf der Liste kann bereits Abstriche für Sicherheit und Effizienz bedeuten. Eine reine URL-Filterung z. B. bedeutet noch keine Sicherheit – und genauso wenig ist eine rekursive DNS-Lösung ein Ersatz für ein Web-Gateway. Nutzt man nur einen Bestandteil einer Lösung, darf man keinen vollständigen Schutz erwarten. Vielmehr kann man bei einem solch minimalistischen Ansatz in Bezug auf die Sicherheit nur reaktiv und nicht proaktiv handeln. Sorgen Sie dafür, dass **Sicherheit und Netzwerk ineinandergreifen** und dass sie in die Planung zur digitalen Transformation in Ihrem Unternehmen einbezogen werden – nur so können sie Ihren Geschäftszielen förderlich sein und nur so können Sie eine permanente Aufholjagd vermeiden.

In einer Cloud-basierten Welt zum Erfolg

Zu Beginn haben wir ausgeführt, dass Cloud-Sicherheit vom Menschen gesteuert wird. Daher muss sie sich auch am Menschen orientieren.

Seit der Cloud **bestimmt der Mensch die Grenzen.**

Da Benutzer, Partner und Kunden von überall auf der Welt auf die Daten Ihres Unternehmens zugreifen, reichen die bisherigen virtuellen Schutzmechanismen nicht mehr aus.

Veraltete, infrastrukturorientierte Sicherheitslösungen, die vertrauenswürdige Benutzer innerhalb und nicht vertrauenswürdige Benutzer außerhalb des Netzwerks gruppieren, sind nicht mehr zeitgemäß.

Ein Security Stack kann nicht auf vorgegebenem Vertrauen basieren.

Außerdem ist Ihr Security Stack kein nebensächlicher, sondern ein integraler Bestandteil Ihrer digitalen Transformation.

Beachten Sie die folgenden Grundsätze, um die Transformation voranzutreiben und zu schützen:

Gehen Sie Ihr eigenes Tempo
Rom wurde nicht an einem Tage erbaut. Auch Ihre Cloud-Migration wird nicht über Nacht geschehen. Die meisten Unternehmen agieren in hybriden IT-Umgebungen bzw. in Umgebungen mit mehreren Clouds – und daran wird sich auf absehbare Zeit auch nichts ändern. Ihr Web-Sicherheits-Gateway sollte über flexible Implementierungsoptionen verfügen, mit denen Sie die Migration jederzeit ganz nach Ihren Bedürfnissen gestalten können. So erfolgt die Migration nach Ihren eigenen Bedingungen und Ihre Sicherheit ist jederzeit und in allen Bereichen gewährleistet.

Erweitern Sie Ihre Grenzen
Schützen Sie Cloud, Netzwerk und Endpunkte dynamisch entsprechend Ihrer Geschäftsanforderungen. Eine konvergente Plattform mit modularen Sicherheitsfunktionen, für die nur wenig Hardware erforderlich ist, bietet weit verzweigten Unternehmen Erweiterungsmöglichkeiten und Agilität. Damit können sie von neuen Entwicklungen profitieren, „tote Winkel" vermeiden und standortübergreifende Verbindungen sicher und einfach verwalten.

Haben Sie alles im Blick
„Vertrauen ist gut, Kontrolle ist besser" sollte von nun an Ihr Motto sein. Schützen Sie die Daten Ihres Unternehmens, indem Sie fortlaufend kontrollieren, welche Benutzer über welche Geräte auf diese Daten zugreifen. So können Sie das „wer" und das „wie" nachvollziehen. Und wenn Sie über das „warum" Bescheid wissen, sind Sie nicht nur im Bilde, sondern können auch die richtigen Präventionsmaßnahmen definieren. Eine mehrschichtige Verhaltensanalyse hilft Ihnen, die Absichten zu verstehen.

Sind Sie bereit, Ihre Cloud-Sicherheit ab sofort skalierbar zu gestalten?

› In unserem E-Book Schutz für mobile Mitarbeiter unabhängig von Zeit und Ort erhalten Sie weitere Informationen.

Forcepoint

forcepoint.com/contact

Über Forcepoint

Forcepoint ist einer der weltweit führenden Anbieter von Cyber-Sicherheit im Bereich Anwender- und Datenschutz und hat es sich zur Aufgabe gemacht, Organisationen zu schützen und gleichzeitig die digitale Transformation und das Wachstum voranzutreiben. Die verhaltensbasierten Lösungen von Forcepoint passen sich in Echtzeit an das Nutzerverhalten an und ermöglichen Mitarbeitern einen sicheren Datenzugriff bei voller Produktivität. Forcepoint mit Sitz in Austin, Texas, schafft sichere, vertrauenswürdige Umgebungen für Tausende von Kunden weltweit.