

Eine sichere Patientenversorgung – heute und morgen

Schützen Sie Ihre wichtigen Daten
und Mitarbeiter jederzeit und überall



Herausforderungen

- › Zunahme der Telemedizin: Virtuelle Sprechstunden mit Patienten müssen geschützt werden.
- › Beobachtung von Patienten aus der Ferne: Sicherheitslücken im Telemonitoring könnten ausgenutzt werden.
- › Verstärkter Datenaustausch: Beim Zugriff auf und bei der Weitergabe von geschützten gesundheitsbezogenen Daten (PHI) und anderen sensiblen Daten muss die Sicherheit im Vordergrund stehen.

Unsere Lösung

Forcepoint Cloud Security Gateway

- › Vereint Web-, Daten- und Cloud-Sicherheit in einem einzigen, in der Cloud bereitgestellten und zentral verwalteten Dienst.
- › Schützt Remote-Mitarbeiter vor böswilligen Angriffen durch detaillierte Inhaltsuntersuchung, Cloud-Sandboxing und Remote Browser Isolation (als Add-on erhältlich).
- › Sichert den Zugriff der Mitarbeiter auf lokale medizinische und Patientendaten sowie geschäftskritische Cloud-Anwendungen von jedem Ort aus.
- › Bietet Kontrollen für BYOD, verwaltete Geräte sowie Echtzeit-Compliance.

Vorteile

- › Schützt die Nutzung von E-Mail-Clients, Internet und Cloud an Remote-Standorten.
- › Stoppt Malware, Viren und Phishing, unabhängig davon, wo Mitarbeiter arbeiten.
- › Bietet umfassende Web- und Datensicherheit mit einheitlichen Richtlinien für jeden Benutzer, unabhängig von dessen Arbeitsort.
- › Warnt vor risikoreichen Cloud-Anwendungen sowie Schatten-IT und sichert gleichzeitig den Cloud-Zugriff ab.

Die Pandemie hat die Digitalisierung im Gesundheitswesen beschleunigt. Sie hat Ihre Aufgaben verändert und verlangt von Ihren Mitarbeitern ein höheres Maß an Belastbarkeit, Tempo und Flexibilität als je zuvor. Um neuen Gesundheitsrisiken zu begegnen, externe Mitarbeiter zu organisieren und mit Drittanbietern zusammenzuarbeiten, brauchen Sie einen Schutz, auf den Sie sich verlassen können – heute und morgen.

[Forcepoint Cloud Security Gateway](#) bietet Ihnen den durchgängigen Schutz, den Sie benötigen, um sich auf die neue Normalität einzustellen.

Hat sich Ihre Cyber-Sicherheit durch die Gesundheitskrise verändert? Der Schutz von dezentralen und Remote-Mitarbeitern ist für Ihr Unternehmen möglicherweise nichts Neues. Gleichwohl hat die Flut von Cyber-Angriffen während der globalen Pandemie viele Gesundheitsorganisationen auf kritische Sicherheitslücken aufmerksam gemacht, denen ihre Mitarbeiter (sowohl innerhalb als auch außerhalb des Unternehmens) und die sensiblen Daten, mit denen sie arbeiten, ausgesetzt sind.

Dieses Bewusstsein hat die Verantwortlichen für Cyber-Sicherheit im Gesundheitswesen dazu veranlasst, ihren derzeitigen Schutz zu überdenken und sich einige kritische Fragen zu stellen:

- Wie können wir unsere Sicherheitslösung so skalieren, dass unsere medizinischen und Patientendaten überall geschützt sind?
- Wie können wir riskante Cloud-Anwendungen (sowohl genehmigte als auch nicht genehmigte) erkennen?
- Wie können wir die Cloud sicher nutzen, so dass Produktivität und Geschäftskontinuität gewährleistet sind, ohne Sicherheit und Compliance zu gefährden?
- Wie können wir eine Umgebung für die reibungslose Zusammenarbeit unserer dezentralen Mitarbeiter sicherstellen?

Die Antworten auf diese Fragen sind umso wichtiger, wenn Sie Ihr Unternehmen auf ein neues Geschäftsmodell umstellen.

Ihre Datensicherheit ebnet den Weg zu einer ergebnisorientierten Gesundheitsversorgung

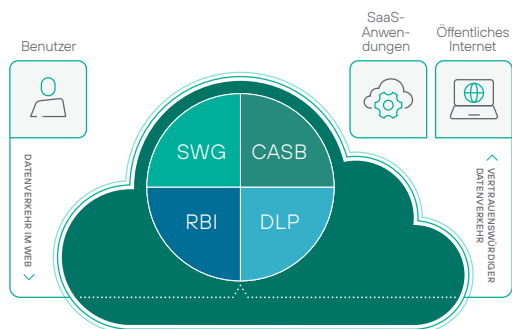
Je mehr Ihrer Mitarbeiter Internet, E-Mail und Cloud für ihre Arbeit nutzen, desto mehr Daten zirkulieren außerhalb Ihres Netzwerks. Die Absicherung dieser vergrößerten Angriffsfläche ist entscheidend – nicht nur heute, sondern auch, um Ihre Cyber-Sicherheit für eine ergebnisorientierte Gesundheitsversorgung vorzubereiten. Mit der Umstellung auf ein ergebnisorientiertes Vergütungsmodell werden Gesundheitseinrichtungen verstärkt fach- und disziplinübergreifend im gesamten Spektrum der Gesundheitsversorgung zusammenarbeiten.

Was bedeutet das für die Zukunft Ihrer Einrichtung? Höchstwahrscheinlich werden Sie Informationen mit mehr Ärzten und Mitarbeitern außerhalb Ihres Unternehmens austauschen, Datenanalysen implementieren und klare Verantwortlichkeiten für die Koordination der Versorgung festlegen. Ihr oberstes Ziel ist es, Kosten und Wiederaufnahmen zu reduzieren und gleichzeitig die Qualität der Gesundheitsversorgung zu verbessern.

Auch wenn die ergebnisorientierte Gesundheitsversorgung noch kein definiertes Ziel für Ihre Einrichtung ist, können Sie schon heute vorbereitende Schritte ergreifen. Beginnen Sie damit, die Sicherheit Ihrer Remote-Mitarbeiter zu verbessern, einschließlich des Datenaustauschs und der digitalen Zusammenarbeit, die bereits jetzt per E-Mail, Internet und Cloud stattfinden.

Überlegen Sie anschließend, was Sie aus der jüngsten Gesundheitskrise in Sachen Sicherheit gelernt haben – und was eventuell noch offen ist. Wie wollen Sie Ihren Schutz skalieren, damit Ihre Einrichtung auf künftige Krisensituationen vorbereitet ist?

Forcepoint Cloud Security Gateway



CSG vereint Web-, Cloud- und Datensicherheit in einem einzigen, konvergierten Dienst, der für die Cloud konzipiert ist und zentral verwaltet wird. Das Lösungspaket umfasst Secure Web Gateway (SWG), Cloud Access Security Broker (CASB) und Data Loss Prevention in einer einzigen SKU.

Ebenfalls verfügbar: Forcepoint Private Access für echten Zero-Trust-Zugriff auf private Anwendungen ohne die Komplexität, Engpässe und Risiken von VPNs.

Ihre Mitarbeiter sind die neue Sicherheitsgrenze

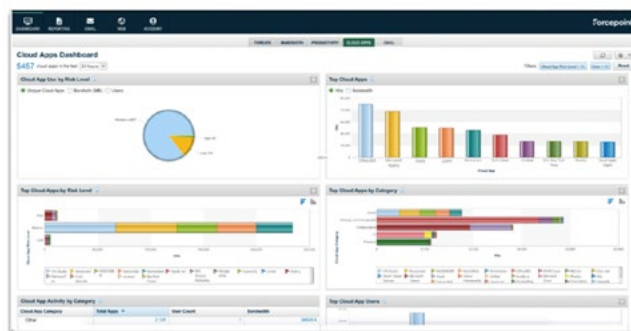
Der Arbeitsort Ihrer Mitarbeiter – innerhalb oder außerhalb Ihrer Einrichtungen – definiert Ihre neue Sicherheitsgrenze. In Notfall- oder Krisensituationen müssen sie mitunter anders auf Daten zugreifen und diese bereitstellen, als es in Ihrem Standardprotokoll vorgesehen ist. Möglicherweise arbeiten sie auch mit Fachärzten außerhalb Ihres Netzwerks zusammen.

Forcepoint Cloud Security Gateway liefert flexiblen und skalierbaren Schutz, der sich an die neuen Gegebenheiten in Ihrer Einrichtung anpassen lässt. CSG sichert den Zugriff Ihrer Mitarbeiter auf öffentliche Anwendungen im Internet und in der Cloud, unabhängig von ihrem Arbeitsort. Außerdem schützt CSG Ihre kritischen Daten und Ihr geistiges Eigentum durch eine vereinfachte Verwaltung der Sicherheitsrichtlinien zu geringeren Kosten.

Flexibler Schutz für aktuelle und zukünftige Bedrohungen

Mit Forcepoint Cloud Security Gateway profitieren Sie von folgenden Vorteilen:

- Sie gewinnen Einblicke in die gesamte Angriffskette durch detaillierte Inhaltsuntersuchung, Cloud-Sandboxing und Remote Browser Isolation (als Add-on erhältlich).
- Sie erkennen auffälliges und riskantes Nutzerverhalten in der Cloud, um böswillige Benutzer zu stoppen und Mitarbeiteraktivitäten zu unterbinden, die nicht den Best Practices entsprechen.
- Sie verringern das Risiko, dass Ihre Remote-Mitarbeiter geschützte gesundheitsbezogene Daten und andere sensible Daten unbefugten Personen zugänglich machen und damit gegen behördliche Auflagen und/oder bundesweite, landesweite und örtliche Vorschriften verstoßen.
- Sie erkennen eine möglicherweise unangemessene Ausweitung von Rechten und implementieren eine standortbezogene Zugriffs- und Aktivitätsüberwachung, um legitime Remote-Mitarbeiter von Cyber-Kriminellen zu unterscheiden.
- Sie schützen Ihre eigenen Prozesse, Methoden und Verfahren vor einem schleichenden Datenverlust sowie vor großflächigem Datendiebstahl.



Forcepoint Cloud Security Gateway ist die einzige zu 100 % für die Cloud konzipierte und zentral verwaltete Sicherheitsplattform für Benutzer und Daten.



Stellen Sie Ihre Mitarbeiter in den Mittelpunkt Ihrer Cyber-Sicherheit

Sie fragen sich, was Cloud Security Gateway für Ihre Einrichtung leisten kann? Unsere Experten für Cloud-Sicherheit beraten Sie gerne. Erleben Sie live, wie unser konvergierter Sicherheitsdienst:

- die Anzahl der Lieferanten und Einzelprodukte reduziert
- den operativen Aufwand und die damit verbundenen Kosten senkt
- einheitliche Web-Sicherheit und einheitliche Richtlinien für jeden Benutzer an jedem Ort bereitstellt
- Schatten-IT erkennt und den Cloud-Zugriff im gesamten Unternehmen schützt.

+ Fordern Sie jetzt eine Demo von CSG an!

forcepoint.com/contact