LÖSUNGSPROFIL

# Forcepoint + Kiteworks

## Eine gemeinsame Lösung für die umfassende Reduzierung inhaltsbezogener Risiken

Ein von Kiteworks unterstütztes Private Content Network (PCN) und Zero Trust Content Disarm and Reconstruction (CDR) von Forcepoint bilden die erste integrierte Lösung, die Zero Trust auf die Inhaltsebene bringt. Dies bietet ein Höchstmaß an Schutz vor dem Abfließen sensibler Informationen in die falschen Hände und vor Bedrohungen innerhalb von Inhalten, wie z. B. Malware, die in die Umgebung eines Unternehmens eingeschleust wird.

**Eine integrierte Lösung. Weltweit führende Technologie. Entwickelt speziell für Umgebungen mit hohem Bedrohungs- und Risikopotenzial.**

### Die massenhafte Verbreitung von Inhalten und die Fragmentierung der Kommunikationssysteme für Inhalte haben eine neue Risikolücke geschaffen, die Unternehmen angehen müssen.

Wir alle haben schon einmal das Sprichwort “Content is King” gehört, doch im Bereich der Cybersicherheit können schädliche oder korrumpierte Inhalte zum bösen König werden, wenn diese nicht als potenzielle Bedrohung eingestuft werden. Inhalte haben zwei wesentliche Schwachstellen:

- **Schwachstelle #1**—Die sensible Natur der Informationen in den Inhalten. Nicht alle Inhalte sind für die Öffentlichkeit bestimmt; viele davon sind reguliert, kontrolliert, klassifiziert und unterliegen bestimmten Einschränkungen. Wenn solche Inhalte in die Hände krimineller Akteure gelangen, stellt dies ein erhebliches Cyber- und finanzielles Risiko für das Unternehmen dar, das diese Inhalte sendet, empfängt oder speichert.
- **Schwachstelle #2**—Nicht vertrauenswürdige externe Parteien und die in deren Inhalten eingeschleuste Malware. Wenn der Inhalt freigesetzt wird, kann diese Malware in die Geräte, Netzwerke und Systeme eindringen, auf denen sensible Daten gespeichert sind, und dem Zielunternehmen Schaden zufügen, indem Lösegeld für die Daten verlangt wird, diese beschädigt und zerstört werden, oder sogar öffentlich zugänglich gemacht werden, was zu einer Kaskade von Schäden für Kunden, ordnungsrechtlichen Maßnahmen, Gerichtsverfahren und Reputationsverlusten führt.

Beide inhaltsbezogenen Schwachstellen stellen unabhängig voneinander bereits ein erhebliches Risiko dar. Doch wenn sie kombiniert werden, droht einem Unternehmen, das sich dagegen nicht schützt, katastrophaler Schaden.

### Zero-Trust Prinzipien auf der Inhaltsebene sorgen für ein Höchstmaß an Risikominderung

Zum Glück haben Kiteworks und Forcepoint gemeinsam eine zentrale, integrierte Lösung entwickelt, die diese Risikolücke schließt: ein von Kiteworks unterstütztes Private Content Network (PCN) , das inhaltsdefiniertes Zero Trust bietet und mit dem Zero Trust CDR von Forcepoint zusammenarbeitet. Diese Lösung bringt Zero Trust auf die Inhaltsebene und reduziert das Risiko wie folgt:

- **Alle Entitäten sind grundsätzlich nicht vertrauenswürdig, einschließlich der Inhalte selbst** — Nach dem Zero-Trust-Prinzip sind Entitäten nicht nur Benutzer, sondern auch Inhalte. Diese Inhalte können sowohl bekannte als auch unbekannte Bedrohungen enthalten. Mit Forcepoint Zero Trust CDR wird die Philosophie "vertraue niemandem" auf "vertraue keinem Inhalt" ausgeweitet und sichergestellt, dass alle unstrukturierten Daten (aka Inhalte) als gefährlich eingestuft werden. Es extrahiert die gültigen Geschäftsinformationen aus eingehenden Dateien, überprüft die extrahierten Informationen anhand der korrekten Strukturen für den Dateityp und erstellt dann neue, voll funktionsfähige Dateien, um nur die sicheren Informationen nahezu in Echtzeit an ihr Ziel zu übertragen.
- **Least Privilege-Zugriff auf Inhalte** — Bei der Zugriffskontrolle geht es nicht nur um den Zugriff auf Anwendungen. Für eine echte Risikominderung muss dieses Prinzip über die Anwendung hinaus auf die Inhalte übertragen werden: Welcher Inhalt hat welche Risikostufe, basierend auf seiner Sensibilität, in Kombination mit der Frage, wer sendet, empfängt, betrachtet, verändert oder speichert, von wo aus und wohin. Das Kiteworks PCN stellt sicher, dass für jede einzelne Inhaltsklasse und jeden Kontext die geringsten Berechtigungen gewährt werden.
- **Umfassende, permanente Überwachung** — Sie können nicht überwachen, was Sie nicht kontrollieren bzw. nicht sehen können. Mit einem von Kiteworks unterstützten PCN werden alle Kommunikationskanäle in einem System konsolidiert, so dass die Kontrollen vereinheitlicht und die Audit-Logs zentralisiert werden, was Ihnen die nach den Zero-Trust-Prinzipien erforderliche Überwachung ermöglicht. Mit dem Zero Trust CDR von Forcepoint können Sie außerdem sicherstellen, dass Sie nur sichere Inhalte zulassen und somit überwachen können, was sich "unter der Haube" eines jeden Inhalts-Assets befindet.

## Sichere und gesetzeskonforme Datenflüsse sorgen für Sicherheit bei der Kommunikation von Inhalten

Um Zero Trust CDR zu ermöglichen, muss eine Lösungsarchitektur zwei Arten von sicheren, gesetzeskonformen Datenflüssen bieten. Erstens müssen nicht vertrauenswürdige Inhaltsdateien an den CDR-Server geliefert werden, und zweitens muss der daraus resultierende bereinigte Inhalt an das vorgesehene Ziel geliefert werden. Kiteworks fügt diese Schritte nahtlos in die Kommunikationsabläufe für Inhalte ein.

- **Verarbeitung nicht vertrauenswürdiger Inhalte durch Zero Trust CDR**—Als Kanal für die Kommunikation externer Inhalte stellt die Kiteworks-Plattform eingehende, nicht vertrauenswürdige Inhaltsdateien unter Quarantäne, um ihre Verwendung im Unternehmen zu verhindern, und sendet sie sofort an das CDR zur Verarbeitung.
- **Bereitstellung bereinigter Inhalte an ihren Zielorten**—Wenn die nahezu in Echtzeit ablaufende CDR-Verarbeitung abgeschlossen ist, ersetzt Kiteworks die unter Quarantäne gestellte Inhaltsdatei durch die bereinigte Version und ermöglicht es den Benutzern so, sie sicher herunterzuladen, in anderen Repositories zu speichern oder per E-Mail zu versenden oder sie automatisiert über SFTP, Managed File Transfer (MFT) und andere Methoden zu übertragen. Natürlich kann Kiteworks die unter Quarantäne gestellte Originalversion auch für eine weitere Analyse speichern.

Die heutige Herausforderung im Bereich der Sicherheitsrisiken besteht nicht nur im Schutz und der Kontrolle von Geräten, Anwendungen und Netzwerken, sondern auch der Daten selbst. Es geht darum, wie Sie Ihr Unternehmen vor Compliance- und finanziellen Risiken aufgrund von Schwachstellen in den vorhandenen Inhalten schützen können. Glücklicherweise haben Kiteworks und Forcepoint dieses Risiko erkannt und bieten ihren Kunden diese branchenweit erste integrierte Lösung, die Zero Trust dort ansetzt, wo es am dringendsten benötigt wird: auf der Inhaltsebene.

**Erfahren Sie mehr über Zero-Trust-Lösungen auf der Inhaltsebene mit einem Klick auf [kiteworks.com/de/kontakt/](kiteworks.com/de/kontakt/).**

Kiteworks