Kiteworks

Die 5 besten Methoden, mit Kiteworks® die Microsoft 365-Kommunikation mit Dritten zu schützen

Die jüngsten Angriffe auf Exchange haben viele IT-Sicherheitsteams dazu veranlasst, ihre Microsoft365 Cloud- und Microsoft On-Premises-Software neu zu bewerten. Dabei stellen sie häufig fest, dass der Schutz in der Cloud und vor Ort inkonsistent ist, was zusätzliche Herausforderungen bei der Prüfung und Kontrolle von Daten für die Kommunikation mit Dritten mit sich bringt. Viele Microsoft 365-Kontrollen wurden nicht für den Schutz der Kommunikation mit Dritten entwickelt, aber angesichts der zunehmenden Zahl von Angriffen erfordert diese Kommunikation spezielle Verteidigungsschichten. Das Kiteworks® Private Content Network (PCN) bietet fünf wesentliche Schutzebenen rund um Microsoft 365 Angebote wie E3, E5 und GCC. Kiteworks in Kombination mit E3 wird oft als kostengünstiger und sicherer angesehen als E5 und GCC allein.

1. Unveränderliches und umfassendes Microsoft 365 Auditing

IT-Sicherheitsteams, die eine Sicherheitslücke schließen oder ein Audit durchführen, stellen häufig fest, dass ihre Microsoft 365-Protokolldaten entweder verspätet, nicht vorhanden oder nicht verwertbar sind. Kiteworks bietet eine zentralisierte Echtzeit-Überwachung und Alarmfunktion für Dateiübertragungen von und zu Microsoft 365, Outlook, SharePoint, Teams und OneDrive. Während Microsoft 365 seine Protokollierung in Zeiten hoher Aktivität, z. B. bei Sicherheitsverletzungen, häufig drosselt, sorgt das umfassende Kiteworks-Protokoll dafür, dass jeder Eintrag erfasst, indiziert und über alle angeschlossenen Produkte hinweg vereinheitlicht wird. Kiteworks speichert seine unveränderlichen Audit-Logs in gehärteten Umgebungen außerhalb des Microsoft 365-Speichers für noch mehr Schutz.

2. Sichere und gesetzeskonforme OneDrive-Freigabe

Benutzer speichern ihre sensibelsten Dokumente in OneDrive und können sie mit der ganzen Welt teilen, wenn die externe Freigabe nicht deaktiviert ist. Administratoren können nicht genau bestimmen, wer auf welche OneDrive-Inhalte zugreifen kann, wenn Dritte sich indirekt authentifizieren, indem sie andere Microsoft-Kontodaten als die von Microsoft 365 verwenden. Kiteworks kann eine Schutzschicht um OneDrive-Inhalte legen und diese sicher mit externen Parteien teilen. IT-Sicherheitsteams können die volle Kontrolle über OneDrive behalten und die Compliance mit umfassenden Logging- und Reporting-Funktionen nachweisen.

3. Unbegrenzter und sicherer Austausch von Dateien

Benutzer gehen oft ein hohes Risiko ein, wenn sie große Inhalte an Dritte versenden, da Outlook eine relativ kleine Dateigrößenbeschränkung hat. Entweder versuchen sie, die Dateien auf unsichere Weise über OneDrive auszutauschen, oder sie greifen auf andere unsichere Kommunikationsformen zurück. Mit Kiteworks können Sie Dateien unbegrenzter Größe sicher und einfach in Outlook versenden.

4. Zero Trust Phish-sichere E-Mail

Endbenutzer werden trotz der Microsoft E-Mail-Filter Opfer von Phishing-E-Mails. Der Grund dafür ist einfach: Microsoft Outlook akzeptiert E-Mails von beliebigen E-Mail-Adressen. Kiteworks Secure E-Mail akzeptiert nur E-Mails von autorisierten Adressen, wodurch praktisch alle unsicheren Quellen ausgeschlossen werden.

5. Volle Datenkontrolle durch private Bereitstellung

Sensible Daten, die in Microsoft 365 gespeichert sind, können ohne Ihre Zustimmung verwendet und/oder per Vorladung angefordert werden, da sich Ihre Verschlüsselungsschlüssel in der öffentlichen Cloud-Umgebung von Microsoft befinden. Kontrollieren Sie den Zugriff, indem Sie Ihren eigenen Schlüssel (HYOK) in Ihrer Umgebung über Kiteworks Private Cloud, FedRAMP Private Cloud und lokale Bereitstellungsoptionen von Kiteworks halten. Selbst Vorschriften wie der U.S. Federal CLOUD Act können Kiteworks nicht zwingen, Ihre Daten freizugeben.