Proofpoint CASB
Adaptive Zugangskontrollen

Zugriffs- und Datenmanagement zur Absicherung Ihrer Cloud-Anwendungen

HERAUSFORDERUNGEN

- Kompromittierte Cloud-Konten
- Riskante Zugriffe auf Cloud-Anwendungen
- Datenverlust- und Compliance-Risiken

WICHTIGE FUNKTIONEN

- Verhindert dank identitäts- und rollenbasierten Kontrollen nicht autorisierte Zugriffe
- Verringert Compliance-Risiken durch gerätebasierte Zugangs- und Datenkontrollen
- Schützt vertrauliche Dateien mit Echtzeitschutz vor Datenkompromittierung
- Schnelle Bereitstellung in der Cloud

PRODUKTE

- Proofpoint CASB
- Proofpoint SaaS Isolation

WARUM PROOFPOINT?

- Personenorientierte Sicherheitskontrollen (Very Attacked People™, privilegierte Nutzer sowie stärker durch Cyberangriffe gefährdete Anwender)
- Detaillierte Richtlinienkontrollen basierend auf Risiko, Kontext und Anwenderrolle
- Verwertbare Bedrohungsdaten (Reputation der IP-Adresse, riskante verdächtige Anmeldungen)
- Agentenlose und zuverlässige Lösung, die innerhalb von Stunden bereitgestellt wird

Heute ist es im geschäftlichen Alltag völlig normal, Cloud-Anwendungen zu nutzen und auch von außerhalb des Büros auf alle Systeme und Daten zugreifen zu können. Diese Tatsache ist auch Cyberkriminellen nicht verborgen geblieben. Nachdem herkömmliche Büroumgebungen und streng geregelte Arbeitstage neuen flexibleren und dynamischeren Abläufen gewichen sind, haben sich die Bedrohungen von der alten Netzwerkperipherie auf die Mitarbeitenden selbst verlagert sowie auf die von ihnen verwendeten Daten, Systeme und Ressourcen.

In dieser sich verändernden Umgebung sind sicherer Zugriff auf Cloud-Anwendungen, Verhinderung von Datenverlust sowie Einhaltung von Compliance-Vorschriften unabdingbar.

Wenn Anwender von Zuhause oder einem anderen Remote-Standort arbeiten, fehlt ihnen der Schutz des Unternehmensnetzwerks. Häufig arbeiten sie mit nicht verwalteten Geräten oder laden Dateien mit vertraulichen Daten auf ihre privaten Geräte herunter. Für Cyberbedrohungen wie Anmeldedaten-Kompromittierung sind das Einfallstore ins Unternehmen. Die Folge sind Kontoübernahmen, Datenverlust und verschiedenste Phishing-Angriffe wie Business Email Compromise (BEC).

Diese Risiken sind real und ziehen schwerwiegende Folgen nach sich. Zum Glück können Sie diese Bedrohungen mit Proofpoint CASB in den Griff bekommen. Unsere einfach implementierbare Lösung sichert schnell Microsoft 365 (Office 365), G Suite, Zoom, Box, Salesforce, Workday uvm. ab.

Die adaptiven Zugriffskontrollen von CASB erlauben Echtzeit-Sicherheitsmaßnahmen auf Grundlage von Risiko, Kontext und Rolle. Sie blockieren automatisch Zugriffsversuche von gefährlichen Standorten und Netzwerken oder Anmeldeversuche bekannter Bedrohungsakteure. Zudem wendet Proofpoint CASB die risikobasierten Kontrollen – darunter starke Authentifizierung, Richtlinienregeln für verwaltete Geräte und VPN-Durchsetzung – auf stark gefährdete und umfassend berechtigte Anwender an.

Im Gegensatz zu statischen Sicherheits- und Compliance-Kontrollen, die für jeden Anwender gleichermaßen gelten, sind die CASB-Zugangskontrollen adaptiv. Dadurch erhalten Sie die Möglichkeit, genau die richtigen Sicherheits- und Compliance-Kontrollen anzuwenden, ohne Anwender, die nur ein geringes Risiko aufweisen, unnötig zu belasten.

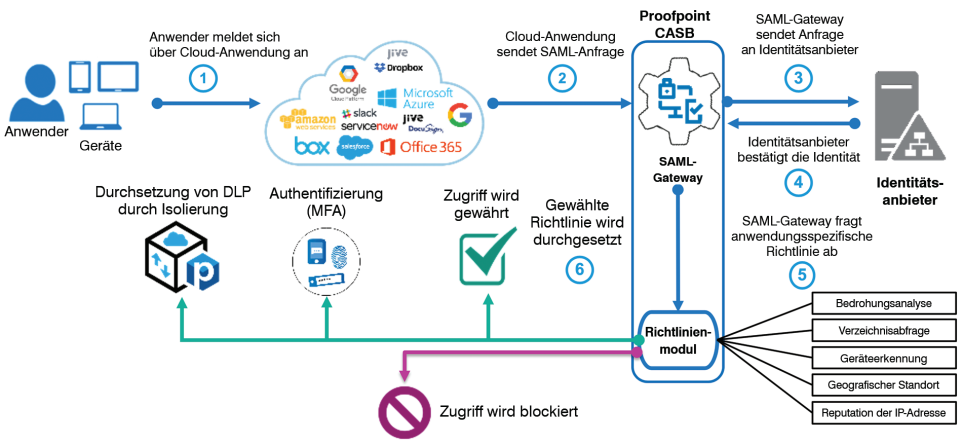

Abb. 1: Architektur für adaptive Zugangskontrollen.

SCHUTZ VOR CLOUD-BEDROHUNGEN

Die Anmeldedaten Ihrer Anwenderkonten sind der Schlüssel zu Ihrem Unternehmen. Wenn Cyberkriminelle diese Anmeldedaten Ihrer Cloud-Konten kompromittieren, können sie Angriffe von inner- und außerhalb Ihres Unternehmens starten.

Adaptive Zugangskontrollen nutzen Bedrohungsdaten zu bekannten Bedrohungsakteuren, um verdächtige Anmeldungen zu blockieren und Kontoübernahmen zu verhindern. Zudem greift das CASB auf Kontextdaten zurück und nutzt sie als zusätzliche Bestätigung einer Anwenderidentität sowie zur Verhinderung gefährlicher Zugriffe. Die Kontextdaten umfassen folgende Elemente:

- Anwenderstandort
- Gerät
- Netzwerk
- Anmeldezeitpunkt

Mithilfe dieser Risikoindikatoren können Sie Zugangsrichtlinien definieren, die verhindern, dass Angreifer Zugriff auf Ihre Unternehmensanwendungen erhalten.

Häufig verwendete Richtlinien

Cloud-basierte Bedrohungen werden mit folgenden häufig verwendeten CASB-Richtlinien abgewehrt:

Blockierung besonders verdächtiger Anmeldeversuche

Wenn Proofpoint die Signatur eines Angreifers bereits kennt, können Sie solche besonders verdächtigen Anmeldeversuche mithilfe der adaptiven CASB-Zugangskontrollen blockieren. Proofpoint verfolgt verdächtige Anmeldeversuche über Dutzende Millionen Konten hinweg und verfügt über unerreichte Kenntnisse von Cloud-Bedrohungen. Sie können beispielsweise den Zugriff auf Ihre besonders gefährdeten Anwenderkonten blockieren, sobald CASB eine verdächtige Anmeldung entdeckt.

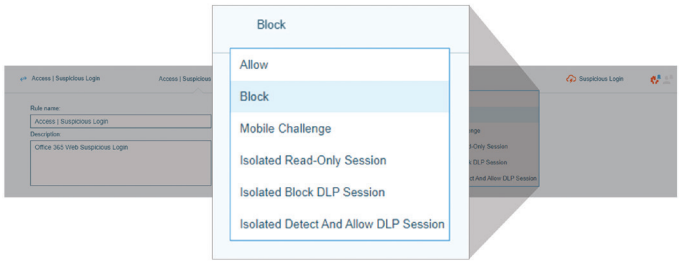

Abb. 2: Beispiel für eine CASB-Regel zur Blockierung verdächtiger Anmeldeversuche.

Blockierung des Zugriffs aus riskanten Ländern und Netzwerken

Sie können eine Blockierungsliste der Länder erstellen, in denen Ihr Unternehmen keine Niederlassung unterhält, die aber Quelle häufiger Angriffe sind. Ebenso haben Sie aber auch die Möglichkeit, anhand der von Proofpoint bereitgestellten IP-Adressen-Reputation Zugriffe aus häufig von Angreifern verwendeten riskanten Netzwerken wie Tor, Proxys und VPNs (Virtual Private Networks) zu blockieren oder Multifaktor-Authentifizierung zu erzwingen.

PERSONENORIENTIERTE ZUGRIFFE

Zur Einhaltung von Sicherheits- und Compliance-Vorschriften müssen Unternehmen den Zugriff auf zugelassene Anwendungen und Unternehmensdaten für alle Anwender absichern. Dazu gehören lokal oder remote verbundene Mitarbeiter sowie Auftragnehmer, Partner und Lieferanten. Die Tatsache, dass die Cloud universelle Zugriffe erlaubt, bedeutet jedoch nicht, dass Sie diese Möglichkeit zulassen müssen. Unternehmen müssen Richtlinienpakete erstellen können, die auf die spezifische Benutzerrolle und -berechtigungen sowie den Sicherheitsstatus der Anwendung und ihre Daten zugeschnitten sind. Mitarbeiter sind die neue Peripherie, und für ihre Absicherung ist eine durchdachte Benutzerführung erforderlich. Mit Proofpoint können Sie adaptive Zugangskontrollen für Anwender/Gruppen anwenden, die als Very Attacked People™ (VAPs) gelten oder Zugriffsberechtigungen für wertvolle Daten, Systeme und Ressourcen besitzen.

Was ist ein VAP?

Ebenso wie jeder Mensch einzigartig ist, sind auch sein Wert für die Cyberangreifer und Risiko für den Arbeitgeber individuell.

Menschen haben ihre ganz eigenen digitalen Gewohnheiten und Schwachstellen. Sie werden von Angreifern mit unterschiedlichen Mitteln und wechselnder Intensität ins Visier genommen. Und jeder Mensch hat seine ganz eigenen beruflichen Kontakte und privilegierten Zugriff auf Daten, Systeme und Ressourcen.

Diese drei Risikofaktoren – Anfälligkeit, Angriffe und Berechtigungen – bestimmen sein Gesamtrisiko.

V: Vulnerability (Anfälligkeit). Mitarbeiter nutzen möglicherweise nicht verwaltete Geräte oder nicht vertrauenswürdige Netzwerke ohne VPNs oder Zero-Trust-Netzwerkzugriffskontrollen. Sie können dazu neigen, Phishing-E-Mails zu öffnen oder auf dubiose Links zu klicken.

A: Attack (Angriff). Mitarbeiter werden massiv mit Cyberattacken angegriffen. Das kann bedeuten, dass sie sehr häufig, sehr gezielt und auf besonders perfide Weise oder von äußerst erfolgreichen Angreifern attackiert werden.

P: Privilege (Berechtigungen). Mitarbeiter haben Zugriff auf wertvolle Daten, Systeme und Ressourcen. Manchmal sind die Berechtigungen nicht offensichtlich. Eine Assistentin hat möglicherweise keinen Zugriff auf wertvolle Unternehmensdaten, doch sie kann die E-Mails, Kontakte und Kalendereinträge aller Mitglieder der Chefetage abrufen, was bei BEC-Angriffen nützlich ist.

VAPs sind Personen, die aufgrund einer Kombination dieser Faktoren ein erhöhtes überdurchschnittliches Risiko darstellen.

Nicht alle Personen sind VIPs. Aber jeder kann ein VAP – eine besonders häufig angegriffene Person – sein.

Häufig verwendete Richtlinien

Mit diesen CASB-Richtlinien wird häufig der Zugriff entsprechend der individuellen Schwachstellen von Anwendern, ihres Angriffsprofils und ihrer Berechtigungen verwaltet.

Durchsetzung von MFA für VAPs

Sie können die Sicherheit besonders gefährdeter Anwender verbessern. Wenn bestimmte Anwender beispielsweise von den personenorientierten Proofpoint-Bedrohungsdaten als VAPs identifiziert werden, können Sie deren Zugriff auf vertrauliche Anwendungen blockieren oder ihn besonders absichern.

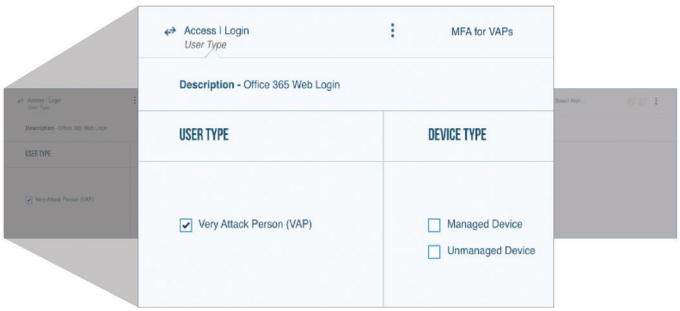

Abb. 3: Beispiel einer CASB-Richtlinie, die kontrolliert, mit welchen Geräten VAPs auf Microsoft 365 im Web zugreifen können.

Durchsetzung von VPN-Zugriffen (virtuelles privates Netzwerk) für privilegierte Anwender vertraulicher Anwendungen

Sie können den Zugriff auf vertrauliche Anwendungen für alle privilegierten Anwender blockieren, die kein Unternehmens-VPN oder Zero-Trust-Netzwerkzugriffskontrollen wie Proofpoint Meta nutzen. Sie haben die Möglichkeit, IP-Adressbereiche für Ihr Unternehmensnetzwerk und VPN zu definieren.

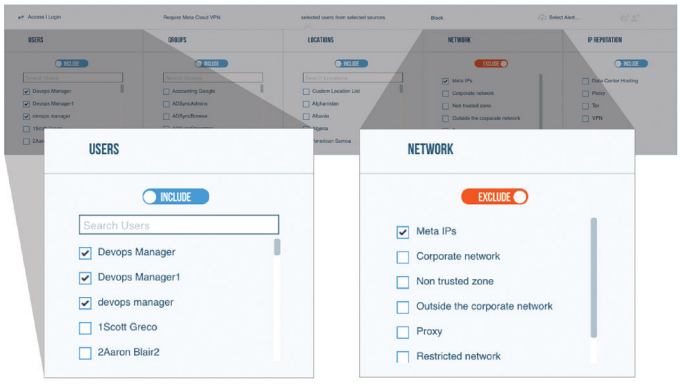

Abb. 4: Beispiel von CASB-Regeln, die für Administratoren und andere privilegierte Anwender die Nutzung von VPN oder Zero-Trust-Netzwerkzugriffskontrollen für Remote-Zugriff vorschreiben.

GERÄTEBASIERTE KONTROLLEN FÜR ECHTZEITSCHUTZ VOR DATENDIEBSTAHL

Eines der größten Risiken nicht verwalteter Geräte ist deren unzureichende Sicherheit. Wenn ein Mitarbeiter mit einem nicht verwalteten Gerät über ein unsicheres Netzwerk auf Unternehmensdaten zugreift, wächst das Risiko eines Datenlecks geradezu explosionsartig. Die Informationen können von anderen Personen außerhalb des Unternehmens leicht abgerufen und weitergeleitet werden, wenn für die Anwendungen zum Zugriff, Teilen oder Speichern der Daten keine Kontrollmaßnahmen eingerichtet wurden.

Mit CASB-fähigen adaptiven Zugangskontrollen können Ihre Mitarbeiter an jedem Ort und mit jedem Gerät sicher auf Cloud-Anwendungen zugreifen. CASB:

- Erkennt Gerätezertifikate
- Ermöglicht die Erstellung von Datensicherheitsrichtlinien für Geräte
- Erzwingt Echtzeitkontrollen durch Integration von Proofpoint SaaS Isolation

Sie können Anwendern die Nutzung einer Anwendung in einem sicheren isolierten Browser im schreibgeschützten Modus erlauben oder das Hoch- bzw. Herunterladen von Dateien bei DLP-Verstößen verhindern.

Mitarbeiter fast aller Unternehmen verschieben wertvolle Inhalte routinemäßig in die Cloud, einschließlich Mitarbeiter- und Kundendaten, Quellcode sowie Formeln. Die Erkennung und Verhinderung von Datenkompromittierungen und Compliance-Verstößen ist unverzichtbar. Erstens benötigen Sie risikobewusste Datensicherheit, die Echtzeit-Scans zur Datenverlustprävention (DLP) bietet. Zudem müssen Sie verhindern können, dass vertrauliche Inhalte in die Cloud hoch- oder auf private Geräte heruntergeladen werden.

Häufig verwendete Richtlinien

Mit diesen CASB-Richtlinien werden typischerweise Geräte abgesichert.

Schreibgeschützter Zugriff für nicht verwaltete Geräte in nicht vertrauenswürdigen Netzwerken

Mitarbeiter greifen mit ihren privaten Geräten auf Unternehmensdaten in sanktionierten Anwendungen wie Microsoft 365, Salesforce, Atlassian usw. zu, was zu neuen Risiken für Ihre Unternehmensdaten führt.

Wenn Daten mit einem privaten Gerät heruntergeladen oder synchronisiert werden, fließen die Informationen in einen ungesicherten Bereich ab. Falls das Gerät gestohlen wird, sind die Daten verloren.

Wenn also Unternehmen ihren Anwendern Zugriff auf Collaboration-Tools von jedem Gerät gestatten, sollten sie Daten-Downloads ausschließlich auf verwaltete Geräte beschränken. Mit CASB können Sie leicht eine Richtlinie erstellen, die nicht verwaltete Geräte in eine sichere isolierte Browser-Sitzung umleitet, in der das Hoch- oder Herunterladen von Dateien nicht möglich ist.

Blockieren von DLP-Verstößen für nicht verwaltete Geräte selbst im Unternehmensnetzwerk oder ähnlichen Umgebungen

Hinter mehr als der Hälfte der Datenschutzverletzungen stehen schädliche oder kriminelle Angriffe. Wenn sich der Anwender im Unternehmensnetzwerk oder einem VPN befindet, ist das Risiko eines externen Cyberangriffs geringer. In diesem Fall können Sie Downloads nicht vertraulicher Dateien auf nicht verwaltete Geräte tendenziell zulassen, sollten dabei aber die Übertragung vertraulicher Dateien sperren.

Mit CASB können Sie eine Richtlinie erstellen, die Anwender in eine isolierte Sitzung umleitet und unternehmenseigene DLP-Richtlinien auf alle Dateiübertragungen anwendet. Sobald ein DLP-Verstoß entdeckt wird, wird die Übertragung blockiert.

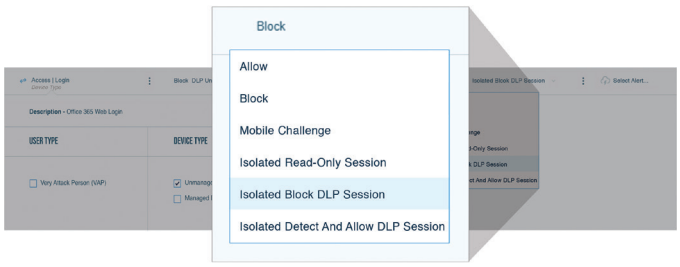

Abb. 5: Beispiel für eine CASB-Regel zur Blockierung von Downloads vertraulicher Inhalte auf nicht verwalteten Geräten.

SCHNELLE BEREITSTELLUNG IN DER CLOUD

Die adaptiven CASB-Zugriffskontrollen leiten Ihre Anmeldungen bei Cloud-Anwendungen an unser SAML-Gateway weiter. Dieses Gateway kontrolliert die föderierte Authentifizierung zwischen jedem Serviceanbieter und dem Identitätsanbieter und wird bei diesem inline implementiert.

Dadurch wird für alle Anwendungen das SAML-Gateway als Identitätsanbieter angezeigt. Für den eigentlichen autorisierenden Identitätsanbieter (der das Anwenderverzeichnis und die Anwenderlebenszyklen verwaltet) wird das SAML-Gateway hingegen als Serviceanbieter angezeigt.

Die Provisionierung der Anwender und andere Identitäts-verwaltungsfunktionen werden von der Identitäts- und Zugriffsverwaltungslösung übernommen. Auf Grundlage der Regelmodul-Bewertung unterstützt das SAML-Gateway verschiedene Zugangskontrollaktionen, beispielsweise MFA, Sitzungsschutz und Echtzeit-DLP.

Verglichen mit Forward- und Reverse-Proxy-Ansätzen bietet unser SAML-Gateway erhebliche Architekturvorteile für Echtzeit-Kontenkontrolle und DLP. Hier seien einige Beispiele genannt:

- **Funktioniert auf jedem Gerät:** Sie können den Anwendungszugriff für alle Anwender inner- und außerhalb des Unternehmensnetzwerks auf beruflich sowie auf privat genutzten Geräten absichern.
- **Funktioniert mit jeder genehmigten Anwendung:** Das SAML-Gateway kann jede von der IT-Abteilung genehmigte Cloud-Anwendung unterstützen, die SAML 2.0 beherrscht und über einen Identitätsanbieter föderiert wird.
- **Benötigt keinen Endgeräteagenten:** Da das SAML-Gateway als Identitätsanbieter agiert und den Anmeldevorgang untersucht, erfordert es keinen Agenten auf dem Endgerät zum Umleiten des Datenverkehrs. Da Sie den Lebenszyklus von Anwendergeräten nicht verwalten müssen, verkürzt das Ihre Amortisierungszeit.
- **Richtlinienbasiert:** Adaptive Zugriffskontrollen bieten anpassbare Abläufe für Bedrohungsschutz, DLP und Anwendungskontrollen, sodass Sie das richtige Gleichgewicht zwischen Risiko und Vertrauen erreichen.
- **Zuverlässig und skalierbar:** Das SAML-Gateway nutzt keine Techniken zur Untersuchung des Netzwerkverkehrs wie URL-Veränderung oder SSL-Sitzungsbeendigung. Die Beschränkung auf die Untersuchung des Anmeldevorgangs erlaubt geringere Latenzen. Zudem besteht kein Risiko von Störungen bei der Cloud-Anwendung oder nicht abgedeckten Funktionen.
- **Anwender-Datenschutz:** Im Gegensatz zu anderen Inline-Lösungen untersucht das SAML-Gateway weder alle Daten, noch hat es Einblick in Anmeldeinformationen. Wenn der Anwender zum Schutz vor Datenkompromittierung in die Browser-Isolierung umgeleitet wird, werden nur Datei-übertragungen untersucht. Daten werden nur dann gespeichert, wenn es zu einem Richtlinienverstoß kommt, sodass der Daten-schutz für die Anwender und das Unternehmen gewährleistet ist.

Da Proofpoint CASB agentenlos und Cloud-basiert funktioniert, kann die Lösung schnell und ohne zusätzliche Hardware-Installation implementiert werden. Die meisten Unternehmen können die Funktionen für Cloud- und Datenzugriffskontrollen mithilfe von Proofpoint Professional Services innerhalb weniger Stunden implementieren.

PRODUKTE

Proofpoint Cloud App Security Broker (CASB)

Proofpoint CASB unterstützt Sie beim Schutz von Cloud-Anwendungen wie Microsoft 365, Google G Suite und Box, um nur einige zu nennen. Wir schützen Sie vor Konten-kompromittierung, versehentlicher Datenweitergabe und Compliance-Risiken in der Cloud. Unsere Lösung stellt adaptive Kontrollen bereit, die den Zugriff auf Ihre Cloud-Anwendungen absichern. CASB bietet Ihnen folgende Vorteile:

- Personenorientierter Überblick über Bedrohungen
- Funktionen für automatisierte Reaktionen
- Umfassende Datensicherheit mit DLP
- Governance für Cloud- und Drittanbieter-Anwendungen

Unsere agentenlose Architektur ermöglicht eine bislang unerreichte Amortisierungszeit und kann Richtlinien in Echtzeit durchsetzen. Dank unserer leistungsstarken Analysen können Sie Ihren Anwendern und Drittanbieter-Add-on-Anwendungen die Zugangsberechtigungen zuweisen, die den für Sie relevanten Risikofaktoren entsprechen.

Proofpoint SaaS Isolation

SaaS Isolation ist ein optionales Add-on für Proofpoint CASB, das den Anwenderzugriff auf Cloud-Anwendungen und -Daten durch Isolierung von Browser-Sitzungen in einem geschützten Container absichert. Mit dieser einzigartigen Lösung wird die Sicherheit von Datei-Uploads und -Downloads bei riskanten Anwendern und Verhaltensweisen gewährleistet. Die Lösung wendet in Echtzeit Cloud-DLP-Richtlinien auf Dateiübertragungen an und verhindert so den Diebstahl oder Verlust vertraulicher Daten. Proofpoint SaaS Isolation behebt die Sicherheits-, Produktivitäts- und Datenschutzprobleme, die durch hochriskante Cloud-Nutzung entstehen. Mithilfe unserer agentenlosen Architektur unterstützt die Lösung alle von der IT-Abteilung genehmigten Anwendungen. Sie lässt sich einfach bereitstellen, verwalten und unterstützen.