Acronis

WHITEPAPER

Sechs kostspielige G Suite-Daten-bedrohungen und wie Sie diese beheben

Einfaches, effizientes und sicheres Cloud Backup für G Suite-Daten mit **Acronis**

JETZT TESTEN

EIN DROHENDES DATENVERLUST-DESASTER

Wenn Ihr Unternehmen auf G Suite angewiesen ist, sollten Sie eigentlich einen zuverlässigen Zugriff auf dessen Applikationen und Ihre Daten bei sehr hoher Verfügbarkeit erwarten können. Viele IT-Profis arbeiten jedoch unter einer gefährlichen Fehlannahme: dass Google bei G Suite auch eine vollwertige Data Protection und langfristige Datenaufbewahrung bietet.

Tatsächlich sind die in G Suite gespeicherten E-Mails, Anhänge, Kalenderereignisse, Kontakte und Dateien nicht vor gängigen und schweren Datenverlustproblemen geschützt – egal ob sich es um versehentliche Löschungen oder ausgeklügelte Malware-Angriffe handelt.

Für viele Unternehmen stellt die G Suite-Nutzung daher eine große Data Protection-Lücke dar – wie ein drohendes Unheil, das früher oder später zuschlagen wird. Dann ist es jedoch zu spät, um zu erkennen, dass Google nur begrenzte Funktionen zur Verfügung stellt, mit denen verlorene, zerstörte oder beschädigte G Suite-Daten wiederhergestellt werden können. Diese Funktionen sind außerdem weit entfernt von der üblichen Backup-Funktionalität oder Robustheit, mit der Unternehmen sonst ihre geschäftskritischen Applikationen schützen.

> Dieses Whitepaper beschreibt mehrere leicht übersehbare Einschränkungen der Data Protection-Fähigkeiten von Google – und zeigt auf, wie Sie diese Mängel beheben können, damit Sie den vielen Datenverlustproblemen, für die G Suite anfällig ist, schnell entgegentreten können.

DIE 6 GRÖSSTEN DATENSICHERHEITSBEDROHUNGEN FÜR IHR UNTERNEHMEN BEI DER NUTZUNG VON G SUITE

Google hat viel in die Hardware, Software, Netzwerke, Sicherheit und Betriebsabläufe seiner Datenzentren investiert, um eine hohe Performance und Verfügbarkeit für die G Suite zu gewährleisten. Die wesentlichen Ziele dabei sind eine grundlegende Resilienz der Infrastruktur, die Betriebskontinuität bei natürlichen Desastern (z.B. Überflutungen, Erdbeben, Wirbelstürme) sowie verlorene oder beschädigte G Suite-Daten in einem begrenzten, kurzen Zeitrahmen wiederherstellen zu können.

Das bedeutet, dass Google viele Betriebssstörungen der eigenen Cloud-Datenzentren (wie Stromausfälle, Hardware-Fehler, Netzwerkprobleme) schnell erkennen und beheben kann, um seine Service Level-Vereinbarungen in Hinblick auf Verfügbarkeit einzuhalten. Diese Maßnahmen schützen Ihre G Suite-Geschäftsdaten jedoch nicht vor vielen gängigen Datenverlustproblemen, wozu beispielsweise versehentliche oder vorsätzliche Datenlöschungen durch Mitarbeiter oder externe Angriffe auf die Integrität Ihrer Daten durch Malware-Angriffe (wie Ransomware) gehören. Hinzu kommt, dass viele IT-Administratoren relativ aggressive (d.h. zu kurze) Aufbewahrungsfristen für die Gmail-E-Mails festlegen. Das führt zu einer schnellen Löschung von Nachrichten – von denen man später aber vielleicht feststellt, dass man sie doch noch benötigt hätte. Leider ist dann aber auf Seiten von Google keine Wiederherstellung mehr möglich.

> Google kann die meisten G Suite-Datenressourcen innerhalb eines gewissen, recht kurzen Zeitraums wiederherzustellen, nachdem diese von einem Benutzer oder Administrator gelöscht wurden. Die Standardeinstellungen sind 25 Tage für Gmail-Nachrichten und Google Drive-Dateien sowie 20 Tage für Benutzerprofile. Und vielleicht stellen Sie ja an einem Tag plötzlich fest, dass die Dateien eines länger ruhenden Projekts oder die E-Mails eines früheren Mitarbeiters wieder wichtig sind – nur um dann nach einer längeren Suche zu erkennen, dass Google keine Kopien dieser Daten gespeichert hat, welche Sie wiederherstellen könnten.

G SUITE-ADMINISTRATOREN MÜSSEN DATENBEDROHUNGEN IN SECHS SCHLÜSSELBEREICHEN HANDHABEN

1. Versehentliche Löschungen

DATENRISIKO: Bei ihrer täglichen Arbeit löschen IT-Administratoren und andere Mitarbeiter regelmäßig G Suite-Benutzerprofile, Gmail-E-Mails/-Anhänge, Kalenderereignisse, Kontakte und Google Drive-Dateien. Egal ob diese Löschungen versehentlich oder vorsätzlich passieren (und dann bedauert werden) – die meisten Anwender kennen die Situation, dass man plötzlich eine E-Mail benötigt, die erst gestern gelöscht wurde.

DIE SCHWACHSTELLE BEI GOOGLE: Solche alltäglichen Ressourcen-Löschungen werden regelmäßig über das gesamte Netzwerk repliziert. Aber je älter die jeweilige Ressource, desto größer wird natürlich das Problem: ältere Daten können bereits vollständig gelöscht („hard-deleted“) und damit nicht wiederherstellbar sein. Erst kürzlich erfolgte Löschungen von neueren Ressourcen sind etwas weniger problematisch, da Dateien/E-Mails, die nur einfach gelöscht wurden („soft-deleted“), oft noch aus dem Papierkorb bzw. dem Ordner 'Gelöschte Objekte' wiederherstellbar sind.

2. Bösartige Insider

DATENRISIKO: Es sind aber nicht nur die gängigen, zulässigen Löschungen, vor denen Ihre G Suite-Ressourcen geschützt werden müssen. Ein weiteres Risiko sind unzulässige Datenänderungen/-zerstörung – etwa durch verärgerte oder sogar kriminelle Mitarbeiter, Auftragnehmer oder Partner.

DIE SCHWACHSTELLE VON GOOGLE: Sieht man von erst kürzlich gelöschten Ressourcen einmal ab, werden G Suite-Daten in keiner Weise von Google gegen böswillige Änderungen/Zerstörungen durch solche Angreifer geschützt. Schließlich hat Google auch keine Möglichkeit zu wissen, was eine Bedrohung darstellt oder was nicht.

3. Cyber-Bedrohungen

DATENRISIKO: G Suite-Daten sind anfällig für Datenänderungen/-zerstörungen durch diverse Malware-Bedrohungen – insbesondere Ransomware, die Benutzerdaten verschlüsselt und für deren Freigabe ein Lösegeld verlangt. Solche Angriffe können durch Hacker, Cyber-Kriminelle oder feindliche staatliche Akteure erfolgen.

DIE SCHWACHSTELLE BEI GOOGLE: Google bietet kaum Schutz vor Angriffen durch Malware (wie Ransomware) und nur begrenzte Möglichkeiten, um veränderte/verschlüsselte Daten auf den Zustand zurückzusetzen, in dem diese kurz vor einem Malware-Angriff vorlagen.

4. Ausscheidende Mitarbeiter

DATENRISIKO: Unternehmen begehen häufig den Fehler, die G Suite-Konten von ausscheidenden oder entlassenen Mitarbeitern zu kündigen, ohne deren Daten zu sichern.

DIE SCHWACHSTELLE BEI GOOGLE: Mit Ausnahme von erst kürzlich (in den letzten 20 Tagen) gekündigten G Suite-Konten kann Google die G Suite-Daten eines gelöschten Benutzers nicht wiederherstellen.

5. Lückenhafte Aufbewahrungsrichtlinien

DATENRISIKO: Geänderte oder falsch gestellte Prioritäten in den Data Protection-Richtlinien von G Suite können dazu führen, dass Daten dauerhaft gelöscht werden („hard-deleted"), obwohl diese vielleicht noch nützlich gewesen wären. Dies kann nur teilweise durch Überprüfung und Aktualisierung der Aufbewahrungsrichtlinien kompensiert werden.

DIE SCHWACHSTELLE BEI GOOGLE: G Suite-Kunden obliegt die Verwaltung der Aufbewahrungsrichtlinien. Wenn der Aufbewahrungszeitraum einer vorhandenen Richtlinie jedoch überschritten wurde und es daher zu dauerhaften Löschungen gekommen ist, hat auch Google keine Möglichkeiten mehr, derartig gelöschte Ressourcen wiederherzustellen.

6. Rechts- und Compliance-Probleme

DATENRISIKO: Compliance-Anforderungen (wie z.B. gesetzliche Aufbewahrungspflichten für Steuerunterlagen) und andere gesetzliche Auflagen können die Folgekosten von nicht abgesicherten Datenverlusten deutlich nach oben treiben. Nicht behebbare G Suite-Datenverluste können für Unternehmen schwerwiegende Folgen haben – wie etwa staatliche oder branchenspezifische Bußgelder, strafrechtliche Folgen (Schadensersatzforderungen oder andere rechtliche Konsequenzen, die sich z.B. aus der Nichterfüllung von E-Discovery-Anforderungen oder Nachweispflichten ergeben), Umsatz- und Aktienkursverluste, verlorenes Kundenvertrauen, Image-Schaden und ähnliches.

DIE SCHWACHSTELLE BEI GOOGLE: Bei all den bisher beschriebenen Risiken kann Google wenig tun, um Unternehmen, die G Suite verwenden, vor den vielfältigen rechtlichen und Compliance-bezogenen Konsequenzen zu schützen. Ein typisches Beispiel wäre beispielsweise ein Unternehmen, welches personenbezogene Daten von seinen europäischen Kunden in G Suite speichert. Wenn ein solches Unternehmen Opfer eines Ransomware-Angriffs wird, kann es Anfragen nach Kopien dieser Daten möglicherweise nicht mehr erfüllen – und würde dann gegen die GDPR-Anforderungen verstoßen.

FAZIT

Sobald Sie die Schwachstellen verstehen, die Google beim Schutz von G Suite-Daten unberücksichtigt gelassen hat, können Sie nach Data Protection-Lösungen suchen, die diese Lücken schließen. Wobei der Einsatz, um den es geht, bekanntermaßen hoch ist: nicht abgesicherte Datenverluste bei G Suite können karriere- bzw. unternehmensschädigend sein.

ACRONIS BACKUP BIETET EIN EINFACHES, EFFIZIENTES UND SICHERES CLOUD BACKUP FÜR G SUITE

ANWENDERFREUNDLICHES CLOUD-ZU-CLOUD-BACKUP FÜR G SUITE

Acronis Backup sichert G Suite-Daten mit einem agentenlosen Backup direkt aus den Google Datenzentren heraus in die weltweit verfügbaren Acronis Datenzentren. Der Acronis Backup Agent wird nicht lokal auf Ihren Systemen ausgeführt, sondern läuft in der sicheren Acronis Cloud. Dadurch werden die Konfigurations- und Wartungsprozesse optimiert und vereinfacht.

HOCHGRANULARES RECOVERY FÜR G SUITE

Acronis Backup bietet eine Reihe von erweiterten Wiederherstellungsfunktionen, die es einfach machen, eine Vielzahl von G Suite-Elemente schnell wiederherzustellen. Mit diesen hochgranularen Wiederherstellungsfunktionen können Sie benötigte Dateien direkt aus einem Backup herunterladen, eine ganz bestimmte Dokumentversion wiederherstellen (also nicht nur die aktuellste) oder beliebige Datenelemente an ihrem ursprünglichen oder einem neuen Speicherort wiederherstellen.

ERWEITERTE SUCHFUNKTIONEN

Mit einer einfachen, komfortablen Suchfunktion können gewünschte Daten schnell gefunden werden – beispielsweise bestimmte E-Mails eines ehemaligen Mitarbeiters oder ein älteres Dokument, welches zur Lösung rechtlicher Probleme benötigt wird. Bei Gmail können die Postfächer nach E-Mail-Metadaten (wie Betreff, Empfänger, Absender, Dateiname oder Datum von Anhängen) durchsucht werden oder eine Volltextsuche verwendet werden, um bestimmte Daten in den eigentlichen E-Mail-Inhalten zu finden. Bei Google Drive, den Kontakten und Kalendern können Kunden nach Metadaten (wie Dateinamen) suchen.

EINDEUTIGE BLOCKCHAIN-BASIERTE BEGLAUBIGUNG VON GOOGLE DRIVE-DATEN

Unternehmen, die Ihre Google Drive-Daten mit Acronis Backup sichern, können vom integrierten Acronis Notary Service profitieren, der mithilfe der Blockchain-Technologie sicherstellen kann, dass die Backups von Google Drive nicht manipuliert wurden. Die Integrität Ihrer Google Drive-Backups nachweisen zu können, ist besonders nützlich für juristische Dokumente, Verträge, Mediendateien, Überwachungskameraaufnahmen, Krankenunterlagen, Miet-/Pacht-/Leihverträge etc.

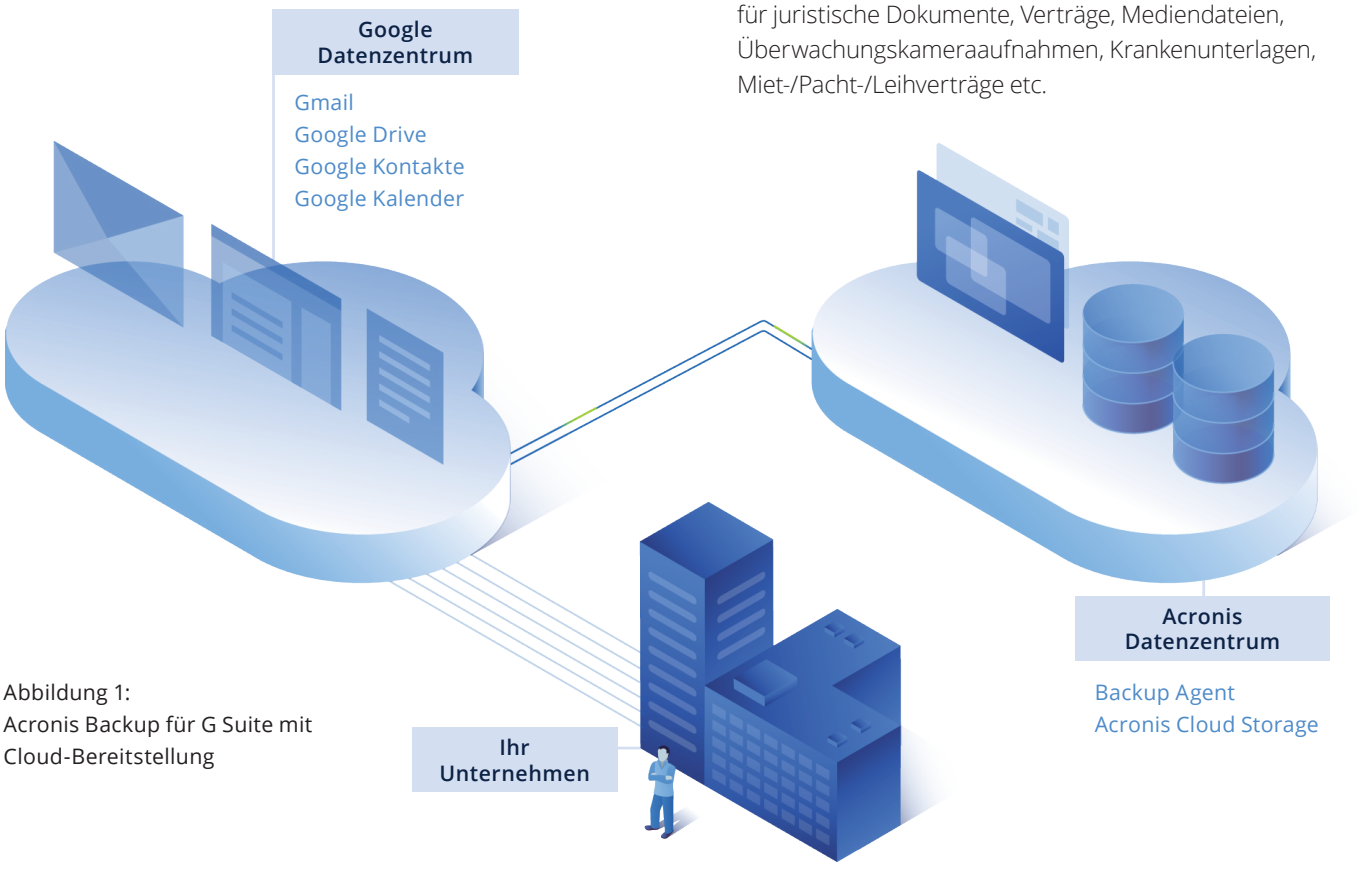

Abbildung 1:
Acronis Backup für G Suite mit Cloud-Bereitstellung

HOHE DATENVERTRAULICHKEIT

Acronis Backup sorgt durch mehrstufige Verschlüsselungen für die Vertraulichkeit Ihrer Daten: die Netzwerkübertragungen werden per TLS verschlüsselt, der Storage des Datenzentrums durch hochwertige Laufwerksverschlüsselungen geschützt und die Backups durch eine archivspezifische AES-256-Verschlüsselung abgesichert.

AUTOMATISCHE ERKENNUNG NEUER G SUITE-BENUTZER UND TEAM DRIVES

Sobald ein erster Gruppen-Backup-Plan für eine G Suite-Umgebung konfiguriert und aktiviert wurde, muss sich Ihr IT-Team nicht mehr darum kümmern, den Plan jedes Mal anzupassen, wenn ein neuer G Suite-Benutzer oder ein neues Team Drive hinzugefügt wird. Acronis Backup kann neu hinzugekommene Benutzer und Laufwerke automatisch erkennen und diese dem Backup-Plan selbst hinzufügen.

UNTERSTÜTZUNG FÜR DIE MULTI-FAKTOR-AUTHENTIFIZIERUNG VON GOOGLE

Acronis unterstützt die mehrstufige Authentifizierungstechnik MFA (Multi-Factor Authentication) von Google, um zusätzliche Authentifizierungsmaßnahmen wie vertrauenswürdige Geräte oder Fingerabdrücke einsetzen zu können. Ohne MFA ist eine Verifizierung nur per Kennwort möglich.

LEISTUNGSSTARKE BERICHTS- UND STATUSÜBERWACHUNGSFUNKTIONEN

Acronis verfügt über erweiterte Fähigkeiten zur Berichtserstellung und Backup-Statusüberwachung, damit Ihr IT-Team noch schneller und effizienter auf Probleme reagieren kann. Das Acronis Management Portal enthält kompakte, leicht verständliche Widgets, die Backup- und Wiederherstellungsstatistiken, Berichte, allgemeine Benachrichtigungen und Alarmmeldungen über kritische Ereignisse anzeigen.

HOCHSICHERE ACRONIS CLOUD

Acronis sichert G Suite-Daten direkt in die Acronis Cloud – ein globales Netzwerk aus Datenzentren, das über ein umfassendes Informationssicherheits- und Compliance-Programm abgesichert ist, welches administrative, physische und technische Zugangskontrollen auf der Basis laufender Risikobewertungen umfasst.

Unsere Richtlinien und Prozesse zur Informationssicherheit basieren auf allgemein anerkannten internationalen Sicherheitsstandards – wie NIST (National Institute of Standards and Technology) oder ISO 27001 – und berücksichtigen die Anforderungen entsprechender lokaler Regulierungsrahmen – wie die Datenschutz-Grundverordnung der Europäischen Union (EU-DSGVO, GDPR) oder dem US-Standard für Krankenversicherungsdaten (Health Insurance Portability and Accountability Act, HIPAA). Zu den Sicherheitsfunktionen der Acronis Cloud gehören:

- **Unternehmensweite Zugriffskontrollen** – basierend auf eindeutigen Benutzer-IDs, starken Kennwörtern, sicheren Authentifizierungsprotokollen (LDAP, Kerberos, SSH-Zertifikate), Zwei-Faktor-Authentifizierungen und dem Einsatz von Web Application Firewalls (WAF)
- **Mehrschichtige, zonenbasierte Datensicherheit** – die durch Echtzeit-Datenverschlüsselung bei Datenübertragung/-speicherung, sichere Datenübertragung über HTTPS (TLS), unternehmensweite AES-256-Verschlüsselung von Kundendaten und mit der Acronis CloudRAID-Technologie für maximale Datenverfügbarkeit sorgt
- **Konsequente, hohe physische Sicherheit** – mit Kontrolle der Zutrittsberechtigungen durch biometrische Handgeometrie-Scans, kontaktlose Schlüsselkarten, Videoüberwachung (90-Tage-Archivierung) und permanent (24x7x365) anwesende Sicherheitsmitarbeiter
- **Hochverfügbare, redundante Datenzentrumsinfrastruktur** – geschützt durch USVs und Notstrom-Dieselgeneratoren, redundant ausgelegte Klima-, Netzwerk- und USV-Systeme, Temperatur- und Feuchtigkeitsüberwachung, spezielle Feuerdetektoren (VESDA Air Sampling Technologie) und Dualzonen-Preaction-Trocken-Sprinkleranlagen.

ACRONIS SICHERT IHRE KOMPLETTE G SUITE-UMGEBUNG (WIE AUCH ALLE ANDEREN DATEN)

Acronis Backup ist eine umfassende **Data Protection-Lösung für Ihre komplette IT-Umgebung** – egal wo Ihre Daten liegen, ob auf lokalen Systemen oder in Private Clouds / Public Clouds.

Das beinhaltet auch eine **breite Palette von Plattformen und Applikationen** (inkl. physischer, virtueller und Cloud-Umgebungen) sowie Server, auf denen gängige andere Betriebssysteme und Hypervisoren laufen, eine Vielzahl gängiger Applikationen, Datenbanken und Desktop-Betriebssysteme (inkl. MacOS) sowie Mobilgerätesysteme (wie iOS und Android).

Eine einzige Data Protection-Plattform für Ihre komplette IT-Umgebung beseitigt die sonst üblichen Inkompatibilitäten zwischen reinen On-Premise-Lösungen und reinen Cloud-Backup-Lösungen. Sie senkt außerdem die Lizenzierungs-, Schulungs- und Integrationskosten. Abbildung 2. zeigt die 20+ Plattformen, die **Acronis Backup sichern kann.**

Darüber hinaus ist die Benutzerführung von Acronis Backup so einfach, dass es auch von weniger spezialisierten IT-Mitarbeitern verwendet werden kann. Sie können daher neue Data Protection-Mitarbeiter schneller einlernen und Kosten für Implementierung, Wartung und täglichen Betrieb einsparen.

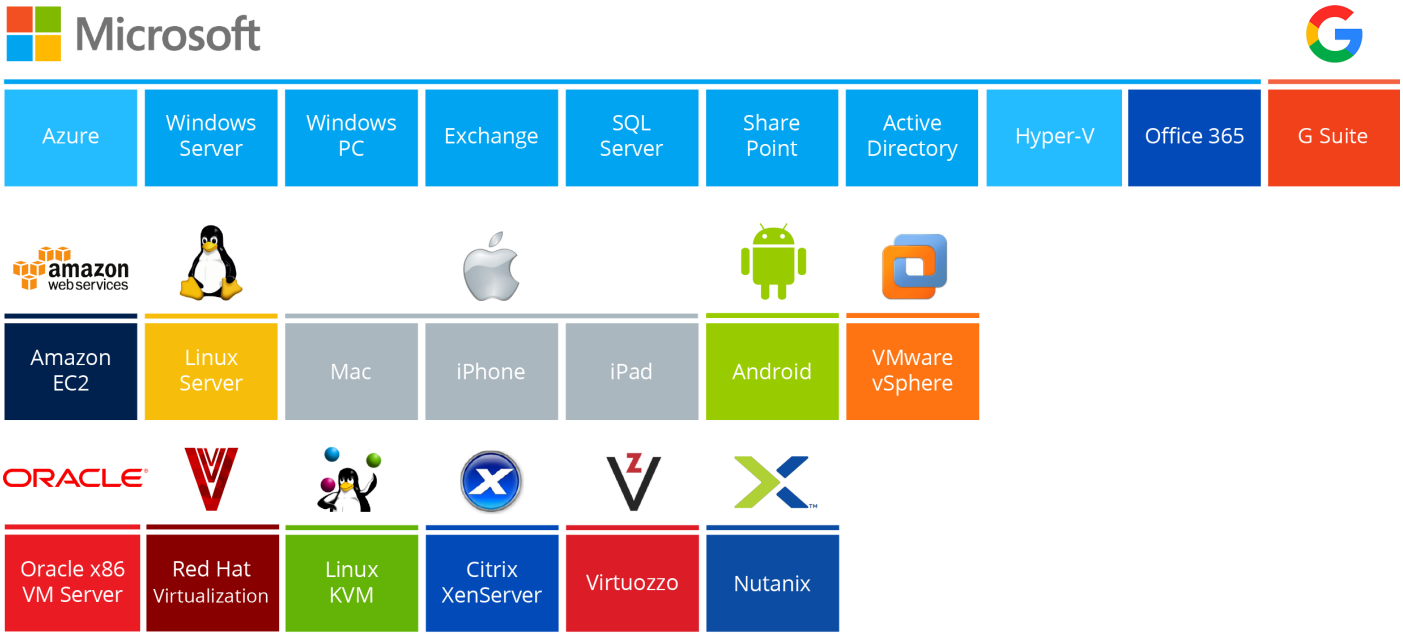

Abbildung 2. Plattformen, die Acronis Backup sichern kann

ZUSAMMENFASSUNG

Wenn Ihr Unternehmen auf G Suite setzt, müssen Sie die begrenzten Data Protection-Fähigkeiten von Google durch Acronis Backup erweitern – der zuverlässigsten und anwenderfreundlichsten Backup-Lösung für Unternehmen aller Größen.

Erfahren Sie mehr darüber, **wie Acronis Backup die Kosten für die Sicherung Ihrer G Suite-Daten erheblich verbessern**, vereinfachen und verringern kann. Sie können zudem eine kostenlose 30-tägige Testversion anfordern oder hier nach einem Acronis Fachhändler suchen.

Acronis

Weitere Informationen erhalten Sie unter **www.acronis.com**