Acronis


WHITE PAPER

# Sei minacce che mettono a rischio i dati di G Suite e come sconfiggerle

Il backup nel cloud per i dati di G Suite: semplice, efficiente e sicuro con **Acronis**

PROVA SUBITO

# G SUITE E LE POTENZIALI PERDITE DI DATI: UN PERICOLO INCOMBENTE

In azienda, G Suite consente l'accesso affidabile alle applicazioni e un'operatività dei servizi molto elevata. Molti professionisti IT tuttavia lavorano in un'ottica pericolosamente errata, ritenendo che Google offra una protezione dei dati di G Suite completa e la conservazione degli stessi a lungo termine.

In realtà e-mail, allegati, eventi in calendario, contatti e file condivisi archiviati in G Suite non sono protetti dalle cause più comuni e gravi di perdita dei dati, che vanno dalle semplici eliminazioni involontarie agli attacchi malware più complessi.

G Suite presenta importanti lacune nella protezione, con potenziali rischi incombenti. Le aziende potrebbero scoprire troppo tardi che Google fornisce solo funzionalità limitate per il ripristino dei dati di G Suite perduti, distrutti o danneggiati, e che non dispone né delle funzionalità né dell'affidabilità delle soluzioni di backup con le quali molte attività proteggono le proprie applicazioni critiche.

> Questo white paper spiega alcune delle limitazioni spesso non note delle capacità di protezione dei dati di Google e offre indicazioni su come porre rimedio a queste carenze per garantire un ripristino rapido nel caso in cui si concretizzino le potenziali perdite di dati a cui G Suite è soggetto.

# LE SEI PRINCIPALI MINACCE ALLA SICUREZZA DEI DATI CHE INCOMBONO SUGLI UTENTI DI G SUITE

Google ha investito in modo significativo in hardware, software, reti, sicurezza e operatività dei propri data center, per garantire a G Suite elevati livelli di prestazioni, accesso e disponibilità del servizio. Obiettivi prioritari di questi interventi sono la resilienza dell'infrastruttura, la capacità di tornare rapidamente operativi dopo una calamità naturale come un'inondazione o un terremoto e alcune modalità di ripristino limitate e a breve termine dei dati di G Suite danneggiati o perduti.

Ciò significa che Google è in grado di rilevare e correggere in tempi rapidi molti errori operativi, interruzioni, guasti hardware e problemi di rete che possono potenzialmente verificarsi nei data center cloud, per rispettare gli accordi sui livelli di servizio incentrati sui tempi di attività delle applicazioni. Queste misure tuttavia non proteggono l'azienda da molti dei rischi di perdita di dati di G Suite, quali la cancellazione accidentale o volontaria da parte di dipendenti o gli attacchi esterni all'integrità dei dati causati da ransomware e altri malware. Spesso, inoltre, gli amministratori IT impostano periodi di conservazione eccessivamente brevi per le e-mail di Gmail, con una conseguente eliminazione anticipata di messaggi che potrebbero rivelarsi necessari in un secondo momento, quando il ripristino con Google non sarà più possibile.

> Google è in grado di ripristinare la maggior parte delle origini dati di G Suite per un breve periodo dopo la loro eliminazione da parte di un utente o di un amministratore (l'impostazione predefinita è 25 giorni per i messaggi di Gmail e i file di Drive, 20 giorni per i profili utente). Può accadere che i dati presenti nell'archivio di un ex dipendente o un progetto fermo da tempo diventino nuovamente necessari, per poi rendersi conto che Microsoft non ne ha conservato alcuna copia che sia possibile recuperare.

## LE SEI POTENZIALI MINACCE INFORMATICHE DI CUI DEVONO OCCUPARSI GLI AMMINISTRATORI DI G SUITE

# 1. Eliminazione involontaria

**DATI A RISCHIO:** durante le attività di routine, gli amministratori IT e i dipendenti eliminano profili utente di G Suite, e-mail e allegati di Gmail, eventi del calendario, contatti e file di Google Drive. Può trattarsi di cancellazioni accidentali oppure intenzionali, che potrebbero poi rivelarsi errate: chi non ha avuto all'improvviso bisogno di quell'e-mail eliminata proprio ieri?

**PUNTO DEBOLE DI GOOGLE:** queste attività quotidiane di eliminazione delle risorse vengono replicate su tutta la rete. L'età della risorsa aggrava il problema: i dati più obsoleti potrebbero essere stati eliminati definitivamente ed essere ormai irrecuperabili. La cancellazione delle risorse più recenti può implicare meno problemi, poiché file e e-mail eliminati temporaneamente sono ancora recuperabili, nel breve termine, dal Cestino o dalla cartella Elementi ripristinabili.

# 2. Minacce interne all'azienda

**DATI A RISCHIO:** oltre che dalle cancellazioni di routine e involontarie, le risorse di G Suite devono essere protette da modifiche o eliminazioni intenzionali e dannose perpetrate da dipendenti, appaltatori o partner insoddisfatti o animati da intenti criminali.

**PUNTO DEBOLE DI GOOGLE:** ad eccezione delle eliminazioni di risorse relativamente recenti, Google non offre protezione contro le modifiche o le cancellazioni volontarie dei dati di G Suite determinate da persone interne all'azienda. Del resto, il sistema non ha modo di sapere se qualcosa costituisce una minaccia oppure no.

# 3. Minacce informatiche

**DATI A RISCHIO:** i dati di G Suite sono vulnerabili ad attività di modifica o distruzione causate da varie minacce malware, in primo luogo dal ransomware, che crittografa i dati degli utenti e li tiene in ostaggio fino al pagamento di un riscatto in denaro. Questo tipo di attacco è in genere perpetrato da hacker, criminali informatici o altri aggressori istituzionali.

**PUNTO DEBOLE DI GOOGLE:** Google offre una protezione davvero limitata contro gli attacchi malware come il ransomware, e capacità minime di ripristinare i file alterati o crittografati allo stato precedente all'attacco.

# 4. Dipendenti in uscita dall'azienda

**DATI A RISCHIO:** in azienda è frequente l'errore di chiudere gli account G Suite di dipendenti con i quali la collaborazione è stata interrotta senza salvarne i dati.

**PUNTO DEBOLE DI GOOGLE:** ad eccezione delle eliminazioni recenti (ultimi 20 giorni) di account di G Suite, Google non è in grado di ripristinare i dati di G Suite di un utente il cui profilo è stato eliminato.

# 5. Lacune dei criteri di conservazione

**DATI A RISCHIO:** la modifica o il mancato allineamento delle priorità dei criteri di conservazione dei dati di G Suite possono determinare l'eliminazione definitiva dei dati quando potrebbero essere ancora utili. L'evento può essere parzialmente limitato solo con la revisione e l'aggiornamento periodico dei criteri di conservazione.

**PUNTO DEBOLE DI GOOGLE:** agli utenti di G Suite spetta l'onere di gestire i criteri di conservazione dei dati, ma se per qualsiasi ragione la cancellazione definitiva è determinata dalla scadenza di un criterio esistente, Google non offre alcuna possibilità di ripristinare la risorsa eliminata.

# 6. Questioni legali e di conformità

**DATI A RISCHIO:** i costi aziendali correlati alle perdite di dati non protetti elencate fin qui sono aggravati dai requisiti di conformità normativa, ad esempio l'obbligo di archiviazione dei documenti fiscali per un periodo specifico. Una perdita irrecuperabile dei dati di G Suite può esporre l'attività a sanzioni specifiche di settore, amministrative o penali, ad esempio azioni legali per danni o perdite causate dal mancato rispetto dei requisiti in materia di e-discovery o prove, perdite di profitto e azionarie, perdita della fiducia dei clienti e danni alla reputazione del marchio.

**PUNTO DEBOLE DI GOOGLE:** considerati tutti i rischi associati alla perdita dei dati fin qui elencati, è poco quel che Google può fare per proteggere le organizzazioni che hanno adottato G Suite contro i numerosi rischi legali e di conformità a cui sono esposte. Dopo un attacco ransomware, ad esempio, un'azienda che archivia i dati personali dei propri clienti UE in G Suite potrebbe non essere più in grado di inviare le copie di tali dati su richiesta, violando quindi i requisiti del regolamento GDPR.

## COSA FARE?

Dopo aver compreso i tanti punti deboli nella capacità di Google di proteggere i dati di G Suite, è bene iniziare a individuare soluzioni di protezione in grado di colmare queste carenze. È chiaro come la posta in gioco sia alta: l'incapacità di evitare una perdita di dati può causare perdite finanziarie importanti.

# BACKUP IN CLOUD FACILE, EFFICIENTE E SICURO PER G SUITE

## INTUITIVO BACKUP DI G SUITE CLOUD-TO-CLOUD

Acronis Backup protegge i dati di G Suite con un backup diretto e senza agente dai data center Google alla rete globale di data center Acronis. L'agente di Acronis Backup è eseguito nel cloud protetto Acronis e non in locale, nella sede dell'utente, per ottimizzare e semplificare le procedure di configurazione e manutenzione.

## RIPRISTINO ALTAMENTE GRANULARE PER G SUITE

Le numerose funzionalità avanzate di Acronis Backup semplificano il ripristino rapido di numerosi elementi di G Suite. Queste funzionalità di ripristino altamente granulari consentono di scaricare i file richiesti direttamente dal backup, di scaricare qualsiasi versione dei documenti, non solo la più recente, e di ripristinare qualsiasi elemento dati nella posizione originale o su una nuova destinazione.

## AVANZATE CAPACITÀ DI RICERCA

Grazie a intuitive e pratiche funzionalità di ricerca, è possibile individuare con rapidità i dati richiesti, ad esempio l'e-mail di un ex dipendente o un documento necessario per risolvere questioni legali. Per Gmail, gli utenti possono eseguire una ricerca per metadati nelle caselle postali, inserendo oggetto dell'e-mail, destinatario, mittente, nome e data del file allegato, oppure utilizzare la ricerca a tutto testo per trovare i dati nel corpo dell'e-mail. Per Drive, Contatti e Calendario, è possibile eseguire una ricerca per metadati, ad esempio i nomi dei file.

## AUTENTICAZIONE BLOCKCHAIN ESCLUSIVA PER I DATI DI GOOGLE DRIVE

Le aziende che eseguono il backup dei dati di Google Drive con Acronis Backup possono sfruttare il servizio Acronis Notary integrato, che utilizza la tecnologia blockchain per verificare che tali backup non siano stati manomessi. La possibilità di attestare l'integrità dei backup di Google Drive è utile soprattutto per documenti legali, contratti, file multimediali, riprese di videocamere di sorveglianza, referti medici, contratti di noleggio o leasing, contratti di finanziamento.

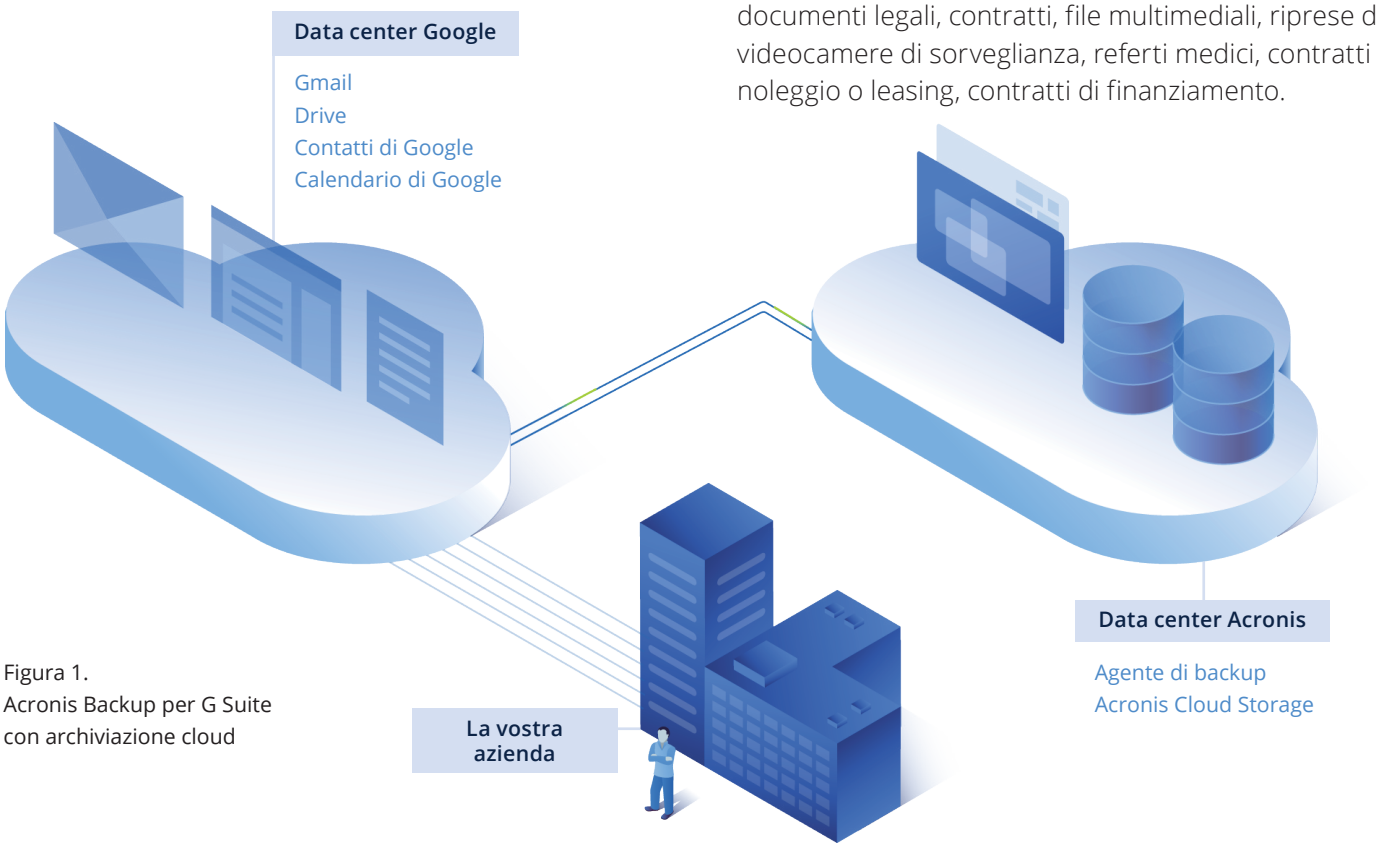


Figura 1.
Acronis Backup per G Suite con archiviazione cloud

## PRIVACY AVANZATA

Acronis Backup protegge i dati da occhi indiscreti con la crittografia del backup su più livelli (rafforzata mediante trasferimenti dei dati sulla rete con crittografia TLS), l'archiviazione in data center con crittografia avanzata del disco e la crittografia AES-256 di ogni singolo archivio.

## RILEVAMENTO AUTOMATICO DI NUOVI UTENTI E DRIVE DEI TEAM DI G SUITE

Dopo aver configurato il piano di backup di gruppo iniziale e averlo abilitato per uno specifico ambiente di G Suite, il personale IT non dovrà modificarlo ogni volta che viene aggiunto un nuovo utente di G Suite o Drive del team. Infatti, Acronis Backup individua automaticamente l'elemento aggiunto e lo include nel piano di backup, aggiornandolo.

## SUPPORTO PER L'AUTENTICAZIONE A PIÙ FATTORI DI GOOGLE

Acronis supporta l'autenticazione a più fattori (MFA) di Google, abilitando l'uso di misure di autenticazione quali dispositivi attendibili o impronte digitali. Senza MFA, per la verifica è richiesta solo la password.

## FUNZIONALITÀ AVANZATE DI MONITORAGGIO DELLO STATO E DI CREAZIONE DI REPORT

Acronis offre capacità avanzate di monitoraggio dello stato del backup e di creazione di report che contribuiscono ad aumentare l'efficienza e la reattività dei team IT. Sul portale di gestione Acronis sono disponibili widget compatti e di facile impiego che presentano tutte le statistiche di backup e ripristino, oltre a report, notifiche e avvisi di eventi critici.

## LA SICUREZZA AFFIDABILE DI ACRONIS CLOUD

Acronis esegue il backup dei dati di G Suite direttamente in Acronis Cloud, una rete globale di data center protetti con un programma completo di sicurezza delle informazioni e di gestione della conformità, con controlli amministrativi, fisici e tecnici basati sulla valutazione continua del rischio.

Le policy e i processi per la sicurezza delle informazioni Acronis si basano su standard riconosciuti a livello internazionale come ISO 27001 e NIST (National Institute of Standards and Technology) e tengono in considerazione i requisiti dei quadri normativi locali correlati, come il GDPR (Regolamento generale sulla protezione dei dati) dell'Unione Europea e lo statunitense HIPAA (Health Insurance Portability and Accountability Act). Le funzionalità di sicurezza di Acronis Cloud prevedono:

- **Controllo degli accessi enterprise** basato su ID utente univoci e password complesse, protocolli di autenticazione sicura (LDAP, Kerberos, certificati SSH), autenticazione a due fattori e web application firewall.
- **Sicurezza dei dati multi-layer, basata su zone** e rafforzata da crittografia dei dati in tempo reale in transito e a riposo, trasferimento dei dati sicuro su HTTPS (TLS), crittografia AES-256 dei dati utente di livello enterprise, tecnologia RAID di Acronis Cloud per la massima disponibilità dei dati.
- **Sicurezza fisica garantita da alte grate** , accesso controllato da scansioni biometriche della geometria della mano e da schede di prossimità, videosorveglianza con 90 giorni di archiviazione e personale di sicurezza disponibile 24x7x365.
- **Data center ridondanti ad alta disponibilità** protetti a livello di infrastruttura con gruppi di continuità e generatori diesel di riserva, HVAC, reti e UPS ridondanti, campionamento dell'aria VESDA, sistemi antincendio sprinkler bizonali, a secco e a preazione (con tubazioni a secco), monitoraggio continuo della temperatura e dell'umidità.

# PROTEZIONE DELL'INTERO AMBIENTE G SUITE (E NON SOLO)

Acronis Backup è un'**unica soluzione di protezione dei dati per l'intero ambiente IT**, ovunque si trovino i carichi di lavoro: in locale oppure, in hosting in cloud pubblici o privati.

La protezione si estende a un'**ampia gamma di piattaforme** e applicazioni, compresi ambienti fisici, virtuali e cloud, server che eseguono i principali sistemi operativi e hypervisor, numerosi database e applicazioni, sistemi operativi desktop come macOS e sistemi operativi mobile come iOS e Android.

Un'unica piattaforma per la protezione dei dati per l'intero ambiente IT elimina l'incompatibilità reciproca delle soluzioni di backup predisposte solo per il locale o solo per il cloud, e contribuisce altresì a ridurre i costi di licenza, formazione e integrazione. Nella Figura 2 sono elencate le oltre 20 piattaforme protette da **Acronis Backup**.

Inoltre, la soluzione è dotata di un'intuitiva interfaccia utente che ne consente l'impiego immediato anche agli utenti non esperti senza richiedere attività di formazione, con un risparmio netto sui costi di implementazione, manutenzione ed esercizio.

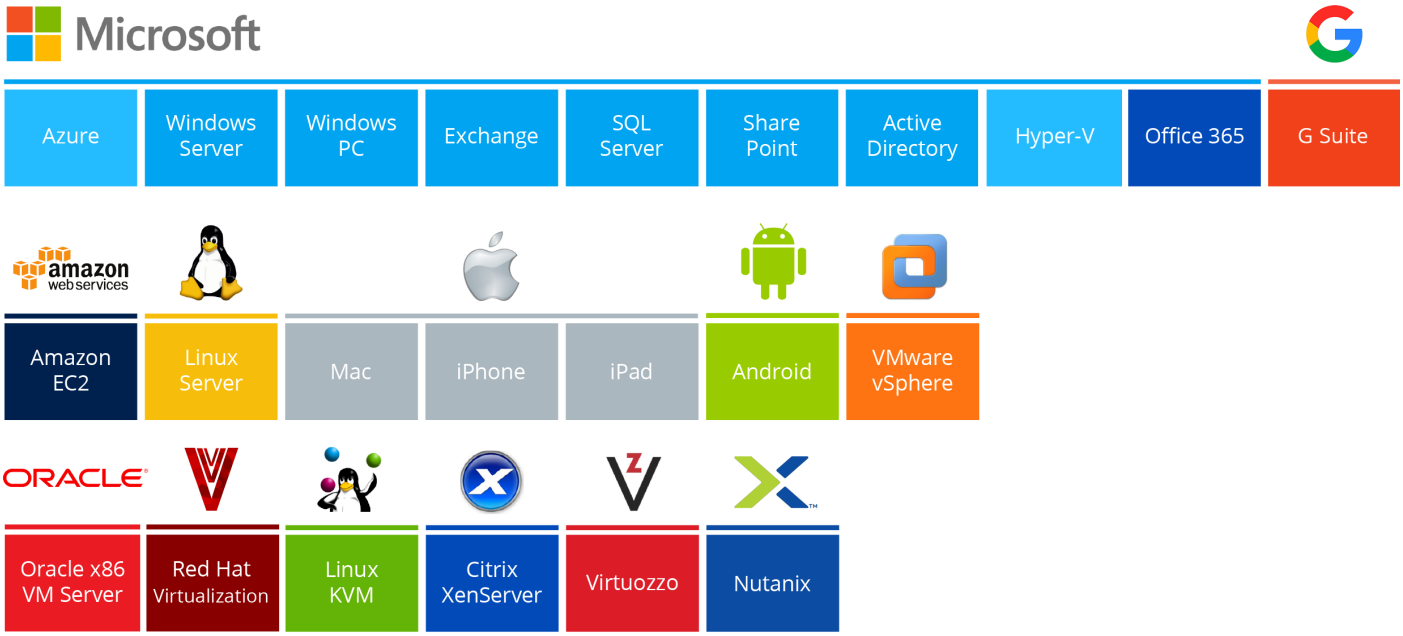


Figura 2. Piattaforme protette da Acronis Backup

## CONCLUSIONI

Se la vostra azienda ha adottato G Suite, dovrebbe completare la limitata capacità di protezione dei dati di Google con Acronis Backup, il backup più affidabile e intuitivo per le imprese di ogni dimensione.

Per saperne di più su **come Acronis Backup può significativamente migliorare,** semplificare e rendere più economica la protezione dei dati di G Suite, richiedete una versione di prova gratuita valida 30 giorni qui, oppure trovate un rivenditore Acronis qui.

Acronis

Per saperne di più, visitare
**www.acronis.com**