LOGITECH SYNC

WHITEPAPER SULLA SICUREZZA E SULLA PRIVACY

logitech®

INTRODUZIONE

Logitech® Sync rende la gestione delle sale riunioni e dei dispositivi Logitech semplice e intuitiva. Sviluppata su un'architettura sicura basata su cloud, Sync aiuta a diffondere e gestire le videoconferenze su vasta scala. Questo whitepaper spiega come Logitech Sync gestisce la sicurezza e la privacy dei dati dei clienti, le release del firmware e lo sviluppo software.

Leader mondiale nello sviluppo di hardware, software e soluzioni per servizi, Logitech connette le persone con le esperienze digitali di loro interesse. Offriamo una gamma di strumenti di collaborazione semplici da usare. Inoltre, forniamo software semplici da utilizzare per aiutarti a monitorare, gestire e ricevere dati analitici relativi alle soluzioni di collaborazione video, consentendo ai team virtuali di collaborare in modo più efficiente.

Logitech Sync è parte integrante delle nostre soluzioni di collaborazione video. Sync è una piattaforma per la gestione di dispositivi basata su cloud che consente all'IT di gestire e monitorare i dispositivi per sale riunioni Logitech su vasta scala. Funziona insieme all'app Logitech Sync, che viene eseguita su un computer o un apparecchio video nella sala riunioni.

Sync elabora i dati e le informazioni raccolte dai dispositivi hardware e fornisce agli amministratori IT dati utilizzabili relativi a monitoraggio, gestione e dati analitici della sala. Gli utenti Sync accedono facilmente al portale web dedicato all'indirizzo sync.logitech.com per gestire i propri dispositivi Logitech.

Questo nuovo approccio al monitoraggio remoto e alla gestione dei dispositivi semplifica attività come l'aggiornamento del firmware e l'abilitazione delle funzionalità, mentre l'API e l'architettura orientata al futuro costituiscono una solida base per nuove evoluzioni e integrazioni.

Naturalmente, i leader IT sono particolarmente attenti alla sicurezza e alla privacy quando si tratta di gestione dei dati e aggiornamenti software. Per trattare in modo approfondito questo argomento, abbiamo creato il seguente whitepaper, che analizza la gestione dei dati personali e la distribuzione di release del firmware di Logitech Sync. Utilizziamo tali dati in modo coerente con i termini del servizio e l'informativa sulla privacy Logitech.

Nota: La versione più attuale di questo whitepaper è disponibile sul sito web Logitech.

GOVERNANCE SULLA SICUREZZA DI LOGITECH

I clienti possono essere sicuri del fatto che Logitech stabilisce e adotta processi volti ad assicurare la sicurezza delle informazioni, basati sulle best practice. Tutti i protocolli di sicurezza nell'ambito dello sviluppo software per la collaborazione video fanno riferimento alle norme NIST 800-53 e ISO/IEC 27001:2013. I nostri processi di sicurezza sono gestiti da diversi stakeholder, dai responsabili della gestione prodotto agli addetti alla relativa progettazione, che applicano questi standard di sicurezza come principi operativi chiave nel nostro Secure Software Development Lifecycle (SSDLC).

INTEGRAZIONE E DISTRIBUZIONE CONTINUE

Logitech adotta una pipeline consolidata di Integrazione e distribuzione continue (Continuous Integration and Delivery, CI/CD) che applica rigidi requisiti di progettazione per garantire la qualità del software prima di nuovi cambiamenti alla produzione. Il processo semplifica il controllo della qualità che include, ma non è limitato a, test funzionali, test di sicurezza, test di integrazione e approvazioni delle modifiche da parte di tutti gli stakeholder. Il nostro processo di distribuzione garantisce che la release del nuovo software sia implementata senza intoppi e senza compromettere la disponibilità del servizio.

TEST DELLA SICUREZZA DELLE APPLICAZIONI

Logitech effettua test della sicurezza mediante consulenti di sicurezza di terze parti per identificare le vulnerabilità. Il test statico della sicurezza delle applicazioni (SAST), il test dinamico della sicurezza delle applicazioni (DAST) e la valutazione della configurazione del servizio cloud sono allineati, senza alcuna limitazione, con i punti deboli comuni in termini di sicurezza, come evidenziato nell'Open Web Application Security Project (OWASP) e nella Common Weakness Enumeration (CWE) di MITRE. Qualora durante un test siano rilevate eventuali vulnerabilità, Logitech risolverà tutti i problemi di sicurezza come identificato dal fornitore. Sebbene la valutazione della sicurezza da terze parti sia effettuata sulle release principali, Logitech esegue anche SAST e DAST interne durante i cicli di sviluppo.

AUTORIZZAZIONE E AUTENTICAZIONE DELL'UTENTE

Quando gli utenti Sync accedono al portale web per gestire i propri dispositivi Logitech, il portale Sync usa meccanismi di accesso basati su token e ruoli per autenticarli e autorizzare l'ambito di accesso. Gli utenti visualizzano o modificano i dati in base al proprio ruolo assegnato nel sistema. Ciascun token di sicurezza è anche basato su sessione e valido per un certo periodo di tempo. Una volta scaduto il token, gli utenti devono aggiornare l'accesso inserendo nuovamente le proprie credenziali per garantire un sistema sicuro.

INTEGRAZIONI DEL PROTOCOLLO SINGLE SIGN-ON (SSO)

Il servizio di autenticazione del portale Logitech Sync supporta il protocollo Single Sign-On (SSO) e può essere integrato con provider di identità (IdP) SAML 2.0 come Azure Active Directory e Okta. Questi provider consentono al portale Sync di autenticare gli utenti usando le loro credenziali aziendali senza gestire credenziali separate per la piattaforma Sync.

DATI IN TRANSITO

Logitech Sync è costituito da due parti: l'applicazione desktop Sync che viene eseguita sull'hardware in sala e il portale Sync basato su cloud. Una volta installata e dopo aver eseguito l'autenticazione, l'applicazione Sync comunica direttamente con il portale Sync per consentire la gestione remota, le funzionalità di monitoraggio e vari dati analitici relativi all'uso e alle prestazioni della sala.

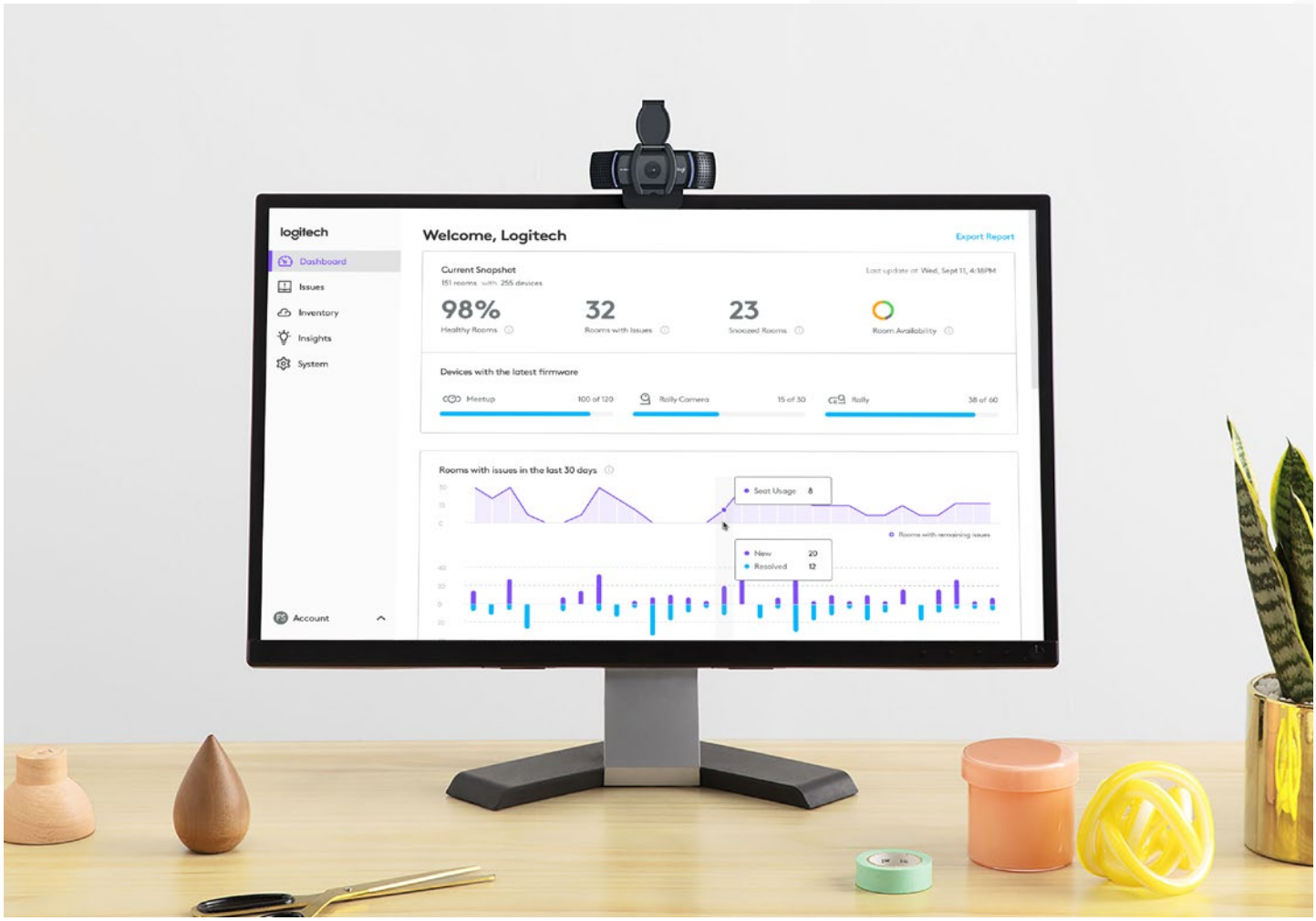
Tutte le comunicazioni[1] tra il portale Logitech Sync basato su cloud e l'applicazione Sync avvengono tramite protocolli di rete HTTPS e MQTT. Il traffico da entrambi i protocolli è autenticato e crittografato usando la versione 1.2 o versioni superiori del protocollo Transport Level Security (TLS) con il supporto di pacchetti di crittografia AES a 128/256 bit per garantire la riservatezza e l'integrità dei dati su internet.

DATI NON IN TRANSITO

I dati del cliente nel servizio backend di Sync sono protetti usando la crittografia standard più solida AES a 256 bit all'interno del database. Inoltre, le chiavi di crittografia sono ulteriormente crittografate e gestite a livello centrale dai servizi di dati AWS per salvaguardare le informazioni dei clienti da eventuali violazioni.

DISPONIBILITÀ DEL SERVIZIO E RIPRISTINO IN CASO DI EMERGENZA

Per garantire un servizio 24 ore su 24, 7 giorni su 7, Logitech Sync è progettato con un'architettura e un'infrastruttura software a tolleranza di errore per un servizio sempre disponibile. Per ottenere una disponibilità elevata, le risorse di elaborazione sono altamente scalabili e il carico è ben distribuito. I dati attuali si trovano su server nella costa occidentale degli Stati Uniti e sono costantemente sottoposti a backup nel data center. In caso di emergenza, Logitech Sync può ripristinarsi in qualsiasi momento e in qualsiasi regione senza alcuna interruzione del servizio nell'arco degli ultimi 35 giorni.



RACCOLTA E PRIVACY DEI DATI

L'informativa sulla privacy e sulla sicurezza descrive i tipi di dati raccolti da Logitech, l'utilizzo di tali dati e le modalità per la protezione delle informazioni personali raccolte mediante i nostri prodotti, servizi, app e software. Logitech è un gruppo di aziende che opera sotto il controllo dell'azienda principale, Logitech International S.A. L'azienda Logitech che controlla i dati degli utenti varia a seconda della relazione dell'utente con Logitech (cliente, partner, fornitore o qualsiasi altra relazione commerciale rilevante). Non acquisiamo o archiviamo suoni, video o immagini statiche da una sala riunione su cloud. Nel grafico 1.1 di seguito, offriamo un elenco completo dei dati che raccogliamo e del loro utilizzo.

Fonte della raccolta dei dati	Tipo di dati raccolti	Scopo della raccolta dei dati	Archivio dati
Portale Sync (registrazione e creazione dell'account)	• Indirizzo e-mail • Password • Nome • Cognome • Nome organizzazione	Autenticazione dell'utente e creazione dell'account per singoli utenti.	AWS
Informazioni aggiuntive specificate dall'utente per il portale Sync	• Nome stanza • Numero posti • Nome gruppo	Identificazione e raggruppamento delle sale in Sync. Il numero dei posti è usato per calcolare l'uso dei posti in combinazione con i metadati relativi all'occupazione della sala.	AWS
L'app Sync (installata sul dispositivo o PC della sala riunioni, come Logitech Rally Bar)	• Nome dispositivo • ID dispositivo univoco • Versione firmware dispositivo • Numero di serie dispositivo • Versione dell'app Sync • Tipo di sistema operativo del computer • Versione del sistema operativo del computer • Indirizzo IP/MAC • Metadati sulle specifiche del computer • Occupazione della sala riunioni (solo metadati)	Le informazioni sono usate per fornire funzionalità analitiche, di monitoraggio e di gestione attraverso il portale Sync.	AWS

ACCESSO AI DATI DEL CLIENTE E AL SERVIZIO

Logitech stipula contratti con le piattaforme AWS per ospitare i servizi software e i dati utente. Le piattaforme AWS adottano rigidi orientamenti operativi, strati di protezione e attività di monitoraggio per garantire che i data center siano accessibili soltanto a dipendenti autorizzati.

Presso Logitech, l'accesso al database del cliente e alle impostazioni di servizio sono limitati a un gruppo ristretto di soggetti autorizzati responsabili della manutenzione e dell'assistenza del servizio.

CONSERVAZIONE ED ELIMINAZIONE DEI DATI

Una volta che un cliente si registra su Logitech Sync, tutti i dati dell'utente e dei dispositivi regolarmente raccolti sono archiviati nel servizio finché il cliente non decide di interrompere il servizio. Per farlo, i clienti devono inoltrare la propria richiesta completando un modulo online disponibile sul sito support.logitech.com/response-center. A questo punto, Logitech procederà con il processo di eliminazione dei dati. Una volta che l'account viene contrassegnato come "eliminato", tutti i dati del cliente, tranne i registri dei prodotti, saranno immediatamente eliminati in modo permanente.

RISPOSTA A PROBLEMI DI SICUREZZA

Logitech si impegna a fornire prodotti e servizi sicuri ai propri clienti e accoglie di buon grado eventuali report di ricercatori indipendenti, organizzazioni del settore, fornitori, clienti e altre fonti interessate alla sicurezza. Logitech definisce una vulnerabilità in termini di sicurezza come un punto debole imprevisto individuato in un determinato prodotto, che potrebbe consentire a un soggetto malintenzionato di compromettere l'integrità, la disponibilità o la riservatezza di un prodotto, un software o un servizio.

Logitech Security implementa varie metriche per monitorare la latenza del traffico, le soglie e i tassi di errore per attività sospette. Effettua anche regolarmente test di sicurezza da parte di fornitori terzi sulle release principali per garantire che il prodotto sia totalmente sicuro. Eventuali vulnerabilità sono individuate e risolte di conseguenza.

Se l'utente dovesse riscontrare un problema, il team di prodotto in collaborazione con Logitech Security analizza prontamente le anomalie segnalate e le presunte violazioni della sicurezza a livello aziendale. È possibile segnalare un problema di sicurezza a Logitech Security usando la nostra pagina relativa alla Descrizione delle vulnerabilità o la pagina del programma bug bounty.

logitech

Contatta il rivenditore o contattaci su www.logitech.com/vcsales

Logitech Americas
7700 Gateway Blvd.
Newark, CA 94560 USA

Logitech Europe S.A.
EPFL - Quartier de l'Innovation
Daniel Borel Innovation Center
CH - 1015 Losanna

Logitech Asia Pacific Ltd.
Tel: 852-2821-5900
Fax: 852-2520-2230

[1] Nel 2021 sarà rilasciato un aggiornamento del firmware per Logitech Meetup, Rally, Rally Cam, Tap e Swytch per configurare la crittografia completa per questi nuovi dispositivi.

Data di pubblicazione: giugno 2021