SOLUZIONE

Sectigo Orchestration Gateway per Sectigo Certificate Manage (SCM)

Quando complessità, scalabilità e sicurezza si scontrano

Oggi le aziende gestiscono ambienti ibridi e multi-cloud in cui la riduzione della durata dei certificati, la crescente complessità delle integrazioni e la frammentazione degli strumenti di automazione sono diventati rischi operativi primari. Spesso i team si affidano a connettori multipli, script instabili e documentazione disomogenea, creando errori di configurazione, punti ciechi e ostacoli alla scalabilità dell'automazione.

Al contempo, i volumi dei certificati stanno esplodendo con il consolidamento delle architetture Zero Trust e l'espansione dell'autenticazione machine-to-machine. Secondo il rapporto Sectigo **State of Crypto Agility Report 2025**, il 95% delle organizzazioni dipende ancora da processi manuali, evidenziando le crescenti difficoltà operative man mano che le identità digitali si diffondono tra cloud, dispositivi e carichi di lavoro.

L'evoluzione delle pressioni normative, i requisiti di agilità crittografica e la spinta verso una verifica continua amplificano questa urgenza. Con l'accelerazione dei cicli di rinnovo e la diversificazione degli ambienti, le aziende necessitano di un livello di orchestrazione unificato che garantisca fiducia, conformità e scalabilità tra diversi fornitori e modelli di deployment.

Presentazione di Sectigo Orchestration Gateway (SOG) per SCM

SOG è un livello di orchestrazione leggero progettato appositamente per funzionare con **Sectigo Certificate Manager (SCM)**, eseguendo le attività legate al ciclo di vita e al deployment dei certificati in ambienti complessi e multi-vendor.

Gestito da SCM, SOG funge da gateway sicuro tra SCM e i sistemi aziendali distribuiti, sostituendo script complessi e connettori legacy con una capacità di automazione scalabile e guidata dalle policy. Attualmente automatizza le operazioni sui certificati TLS in un'infrastruttura ampia e in continua espansione, grazie a un'architettura modulare predisposta per supportare ulteriori casi d'uso nel tempo.

Perché le aziende scelgono SCM con SOG:

- Automatizzano l'intero ciclo di vita dei certificati su server, CDN, WAF e sistemi di accesso.
- Individuano ogni certificato attraverso scansionamento combinato cloud e locale.
- Scalano le operazioni guidate dalle policy per gestire durate ridotte e agilità crittografica.
- Consolidano connettori, script e macchine virtuali nell'installazione di un unico gateway.
- Applicano una rigorosa igiene delle chiavi e il recupero delle credenziali just-in-time tramite integrazioni con PAM e vault.
- Accelerano il deployment su piattaforme moderne e multi-vendor.

In quanto componente di orchestrazione integrato all'interno di Sectigo Certificate Manager (SCM), il Sectigo Orchestration Gateway centralizza e semplifica l'automazione sostituendo script e integrazioni puntuali con una soluzione unica e leggera. Gestito tramite le policy di SCM, SOG automatizza le operazioni sul ciclo di vita dei certificati TLS su server, bilanciatori di carico, CDN, WAF e sistemi di accesso privilegiato supportati, consentendo al contempo il recupero sicuro e just-in-time delle credenziali con privilegi elevati. Estendendo l'automazione di SCM a server, infrastrutture e repository di credenziali, SOG permette ai team di scalare le operazioni di sicurezza senza aumentare la complessità gestionale.

Operazioni sui certificati semplificate e sicure

SOG centralizza l'automazione su più server, bilanciatori di carico e piattaforme cloud, sostituendo script frammentati e workflow manuali. Recupera dinamicamente le credenziali privilegiate da vault remoti in modalità just-in-time, evitando di memorizzare dati sensibili a livello locale.

Server supportati:

IIS, BIG-IP, Apache Tomcat, Cloudflare WAF, Apache HTTP Server Project, NGINX, Imperva WAF, NetScaler

... e altro ancora

Vault di credenziali supportati:

Delinea, CyberArk, HashiCorp Vault, BeyondTrust Pathfinder, Local Vaults

... e altro ancora

Per l'elenco aggiornato delle integrazioni supportate, consultare la pagina della documentazione tecnica.

Ingombro ridotto. Deployment rapido e prevedibile

Leggero e modulare, il gateway si installa rapidamente in ambienti Linux, Windows e Docker. La sua architettura flessibile integra nuove piattaforme e servizi senza richiedere modifiche strutturali, mentre il supporto per API REST consente un'integrazione fluida dei workflow e una rapida distribuzione su infrastrutture distribuite.

Automazione end-to-end su larga scala

L'individuazione, l'emissione, il rinnovo, il deployment e la revoca dei certificati TLS sono completamente automatizzati sui server, servizi cloud e piattaforme aziendali supportati da SOG. Gli aggiornamenti paralleli garantiscono che le operazioni mantengano il passo con la durata ridotta dei certificati e gli ambienti ad alto volume.

Sicurezza rafforzata ad ogni livello

Ogni certificato è associato a una chiave unica, eliminando chiavi condivise o archiviate centralmente che aumentano i rischi. Le chiavi sono gestite localmente o tramite integrazioni PAM e vault, e la rotazione automatizzata sui server garantisce un'igiene crittografica costante. La scansione continua individua i certificati non gestiti negli ambienti cloud, riducendo la superficie di attacco e garantendo la conformità.

Visibilità completa in ogni ambiente

L'individuazione locale e cloud lavorano insieme per tracciare i certificati nei sistemi interni ed esterni. Il tracciamento on-demand 24/7 elimina i punti ciechi e mantiene un inventario affidabile su server, piattaforme e servizi cloud, supportando l'applicazione delle policy e la gestione proattiva dei rischi.

Pronto per il futuro e adattabile

SOG è progettato per l'agilità crittografica, supportando la transizione degli algoritmi, la preparazione alla crittografia post-quantistica e gli standard emergenti su tutti i server, piattaforme e protocolli supportati. Che si tratti di modernizzare web server legacy o di scalare carichi di lavoro in container, le policy di orchestrazione si applicano in modo uniforme senza dover riprogettare le integrazioni.

Efficienza operativa con ritorno misurabile

Con SOG, le integrazioni native e l'automazione semplificano il deployment e le attività quotidiane. Il consolidamento delle macchine virtuali di integrazione in un unico gateway riduce l'impronta infrastrutturale, i costi di manutenzione e i punti di errore, accelerando il ROI. I team eliminano il lavoro ripetitivo, riducono le escalation e scalano le operazioni sui certificati senza aumentare i costi digestione.

Casi d'uso comuni di SOG all'interno di SCM

Automatizzare il TLS in ambienti ibridi

Individuare, emettere, installare, rinnovare e revocare certificati SSL/TLS su server, bilanciatori di carico e piattaforme cloud senza interventi manuali.

Gestire cicli di vita dei certificati accelerati

Gestire la riduzione delle scadenze e gli aggiornamenti crittografici tramite un'automazione guidata dalle policy, allineando le operazioni ai moderni requisiti di sicurezza.

Workflow semplificato uno-a-molti

Eseguire azioni basate su policy sui certificati TLS attraverso più server tramite un unico gateway centralizzato, eliminando le attività ridondanti.

Aumentare l'efficienza operativa

Semplificare i deployment ad alto volume, ridurre le attività ripetitive e sostituire script frammentati con un'automazione centralizzata.

Visibilità totale sui certificati tramite SCM

Supportare SCM nella scansione di certificati interni ed esterni per mantenere un inventario completo su server, dispositivi ed endpoint cloud.

Individuare i certificati su tutti i sistemi

Combinare l'individuazione cloud e locale per eliminare i punti ciechi e garantire una conformità continua.

Ridurre la superficie d'attacco delle credenziali privilegiate

Recuperare le credenziali just-in-time tramite integrazioni PAM, evitando l'archiviazione locale e limitando l'esposizione.

Conformità e preparazione alle audit

Centralizzare le policy, automatizzare la gestione dei certificati e mantenere controlli di audit uniformi.

Ridurre la dispersione dell'infrastruttura

Sostituire le VM dedicate e le configurazioni in alta affidabilità con un unico gateway, riducendo i costi di gestione e i punti di errore.

Supporto multi-server e multi-piattaforma

Eseguire il deployment su IIS, Apache, Tomcat, F5, NGINX, Netscaler, Cloudflare e Imperva tramite gateway locali o remoti.

Informazioni su Sectigo

Sectigo è un provider leader nella gestione del ciclo di vita dei certificati (CLM), che aiuta le aziende a proteggere le identità umane e delle macchine riducendo i rischi nascosti della fiducia digitale moderna. Con la crescita dei volumi di certificati e la riduzione della loro durata, i certificati non gestiti diventano causa di disservizi, sanzioni di conformità e problemi operativi. Sectigo utilizza l'Automazione Orchestrata per offrire Semplificazione su Larga Scala attraverso la sua piattaforma CLM nativa in cloud, unendo visibilità, controllo e gestione del ciclo di vita in ambienti complessi. Con oltre 700.000 clienti, tra cui il 65% delle aziende Fortune 500, Sectigo è una delle autorità di certificazione più grandi e storiche, con oltre 20 anni di esperienza nel garantire la fiducia digitale.

La soluzione globale per la gestione dei certificati di Sectigo consente alle aziende di automatizzare, proteggere e ottimizzare la propria infrastruttura digitale in modo semplice. Semplificando le operazioni complesse sui certificati, rafforzando i protocolli di sicurezza e supportando i requisiti di conformità, le organizzazioni possono proteggere i propri ambienti ibridi in sicurezza e ottimizzare i workflow IT.

Contattaci oggi stesso per una demo personalizzata o scrivi a sales@sectigo.com per scoprire come Sectigo può trasformare la tua strategia di gestione dei certificati.