SYMANTEC

VINCERE LA SFIDA DELLA SICUREZZA

breve resoconto tecnico

Il regolamento GDPR (General Data Protection Regulation) dell'Unione Europea sta per arrivare e imporrà alle aziende la compliance a nuovi obblighi di sicurezza e privacy. Ogni azienda che elabora dati personali di residenti nell'Unione Europea, incluse aziende non-UE, deve essere conforme a un unico set di regole che disciplinano acquisizione, archiviazione e protezione dei dati personali, tenendo conto dei diritti delle singole persone ad avere accesso ai propri dati, esaminarli e modificarli.

Questa panoramica consente di verificare quali aree non sono state ancora esaminate dall'azienda. Le soluzioni indicate non vanno considerate come garanzia di compliance al GDPR, ma come utili suggerimenti per migliorare la sicurezza dell'azienda in senso generale.

Cosa significa il GDPR per un'azienda e i suoi dirigenti:

- Le aziende hanno l'obbligo di segnalare entro 72 ore qualsiasi violazione dei dati personali.
- Il **Diritto all'oblio** dei singoli sarà ulteriormente tutelato.
- A molte aziende sarà richiesta la figura del **Data Protection Officer**.
- Agli utenti sarà garantito un maggiore **Diritto di accesso** ai dati personali.
- Saranno applicate regole più restrittive per la **profilazione dei consumatori** e l'uso del **consenso**.
- È possibile che le aziende siano tenute a informare le persone colpite da una violazione di dati.

La strategia di sicurezza unificata Symantec può aiutare a mantenere la compliance ai requisiti di sicurezza del GDPR grazie al principio del modello "Privacy by Design." Questa strategia integra componenti di protezione delle informazioni e protezione dalle minacce per tutelare i dati personali, ridurre le perdite di dati e arrestare gli accessi non autorizzati a dati e applicazioni.

I software e servizi di sicurezza Symantec sono disponibili sia on-site che in cloud con data center localizzati in tutto il mondo, molti dei quali in Europa. Sono scalabili e protetti in base ai massimi standard attuali come le norme ISO 2700x o SAS 70 tipo I e II. Symantec offre SLA leader di settore per la disponibilità e i tassi di rilevamento dei malware. Infine, per una privacy ancora più protetta, la crittografia e un livello di anonimato presente nella piattaforma di analisi con sicurezza unificata rendono sicuri i dati personali.

Cyber Security Services forniscono supporto alle aziende monitorando e rilevando le violazioni dei dati prima di quanto le grandi imprese o le PMI possano fare da sole. La tecnologia di Incident Response aiuta a prepararsi alle violazioni e fornisce le tecnologie e i processi integrati per reagire rapidamente e per ridurre i rischi potenziali di attacco. Tutti questi servizi e soluzioni sono supportati dalla Global Intelligence Network, una delle più grandi reti civili di intelligence informatica al mondo, che permette di prendere decisioni accurate su minacce note e sconosciute.

Symantec

PROTEZIONE DALLE MINACCE

Symantec Advanced Threat Protection

Le minacce avanzate persistenti sfruttano i sistemi endpoint per infiltrarsi nelle aziende da colpire, facendo leva su vulnerabilità, tecniche di ingegneria sociale, siti Web di phishing o una combinazione di questi elementi. Una volta all'interno dell'infrastruttura, attraversano la rete, rubano le credenziali e si connettono ai server C&C, con il fine di compromettere i sistemi critici e i dati sensibili, che spesso sono quelli disciplinati dal GDPR. L'utente può:

- Rilevare, dare priorità, investigare e rimediare alle minacce attraverso più punti di controllo da un'unica console
- Scoprire le minacce nascoste su endpoint, reti, e-mail e traffico Web
- Contenere e porre rimedio agli elementi di un attacco in pochi minuti, con un singolo clic
- Personalizzare il flusso di Incident Response con API pubbliche e integrazione SIEM di terze parti
- Prioritizzare gli elementi più importanti correlando gli eventi da tutti i punti di controllo protetti da Symantec, per una piena visibilità e una remediation rapida

Symantec Control Compliance Suite

Symantec Control Compliance Suite offre sicurezza commisurata al business e visibilità sul rischio per consentire ai clienti di allineare con efficacia le priorità tra sicurezza, operazioni IT e conformità al GDPR. Automatizza le valutazioni di routine e fornisce un quadro unificato dei controlli e delle vulnerabilità della sicurezza.

- Automatizza la valutazione di sicurezza dei controlli e unifica i dati relativi alle prove per una visione completa sulla sicurezza, la compliance e la condizione di rischio dei clienti
- Architettura con deployment scalabile e flessibile
- È possibile personalizzare le valutazioni di sicurezza per supportare gli standard di sicurezza e per mantenersi allineati agli SLA delle operazioni IT e agli obiettivi prestazionali
- Programma di riduzione del rischio e di valutazione della sicurezza scalabile e sostenibile
- Supporta le capacità centrali di sicurezza offrendo un continuo monitoraggio e una piena sicurezza informatica

Come massimizzare gli investimenti esistenti

Iniziative per valorizzare gli investimenti esistenti in prodotti Symantec e di altri fornitori:

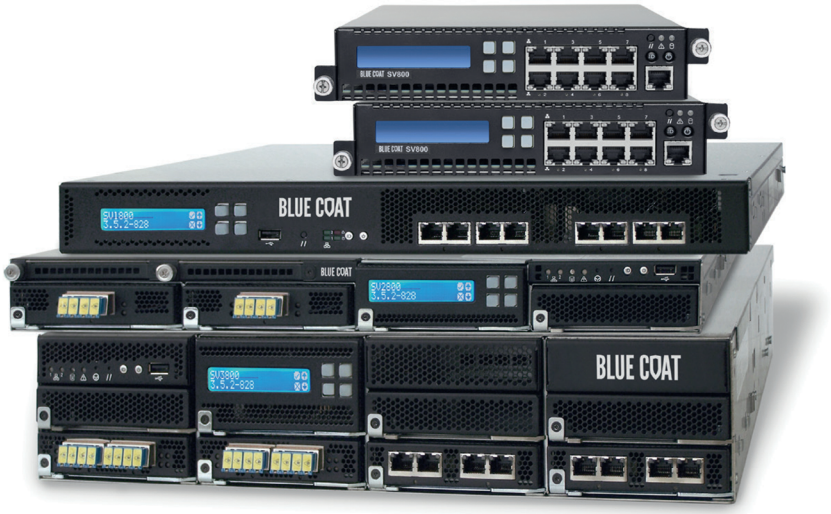
- Ottimizzare e personalizzare il flusso di Incident Response tramite API pubbliche e l'integrazione con Splunk e ServiceNow
- Aggiungere funzionalità EDR (Endpoint Detection and Response) senza richiedere la distribuzione di un nuovo agente sugli endpoint
- Aggiungere protezione avanzata a Symantec Email Security.cloud e ottenere una visibilità dettagliata sulle minacce
- Esportare dettagliate informazioni di intelligence sulla sicurezza verso sistemi di gestione delle informazioni e degli eventi di sicurezza (SIEM) di terze parti
- Monitorare Symantec Advanced Threat Protection utilizzando i Symantec Managed Security Services

PROTEZIONE DALLE MINACCE

Symantec SSL Visibility Appliance

Per proteggere nella massima misura possibile i dati personali da furti o compromissioni, è essenziale riuscire a rilevare intrusioni malevole o fughe di dati anche nel traffico cifrato con SSL o TLS. **Symantec SSL Visibility Appliance** è una soluzione dedicata di classe enterprise che l'utente può configurare per decifrare il traffico SSL/TLS in entrata e per rilevare minacce alla sicurezza o alla privacy senza rallentare le prestazioni.

- **Visibilità e controllo:** offre la visibilità indispensabile sulle applicazioni cifrate in entrata e in uscita dall'infrastruttura aziendale
- **Rafforza il livello attuale di sicurezza:** si integra con le attuali soluzioni DLP, IPS, NGFW, sandbox e forensi per individuare malware e fughe di dati nascoste nel traffico cifrato dell'azienda
- **Ottimizza la condizione di sicurezza:** offre crittografia ad alta sicurezza per mantenere robusta la condizione di sicurezza aziendale
- **Prestazioni e risparmi sui costi:** permette di togliere i processi SSL/TLS/HTTP dall'infrastruttura attuale evitando upgrade degli hardware non necessari
- **Compliance ottimale al GDPR:** decrittografia selettiva del traffico in base alle specifiche policy aziendali, per mantenere la privacy e rispettare le normative locali sulla privacy e le regole sulla protezione dei dati specifiche dell'azienda



La famiglia dei dispositivi Symantec SSL Visibility

È importante sapere che...

...SSL Visibility Appliance supporta un ampio ecosistema di soluzioni di partner, fra cui IPS, DLP, NGFW, antimalware/sandbox, analisi e certificati di sicurezza e sistemi di gestione.

Queste soluzioni compatibili sono la base dell'Encrypted Traffic Management (ETM)-Ready Partner Program di Symantec. L'integrazione di SSL Visibility Appliance con queste efficaci tecnologie di sicurezza di terze parti offre una soluzione completa per la gestione del traffico crittografato adatta a grandi e piccole aziende.

Ulteriori informazioni sull'esclusivo Encrypted Traffic Management (ETM)-Ready Partner Program di Symantec sono disponibili all'indirizzo:

www.symantec.com/it/it

PROTEZIONE DELLE INFORMAZIONI

Symantec Cloud Access Security Broker (CASB)

Basata sull'efficace **piattaforma Symantec CloudSOC™**, Symantec CASB consente di elaborare i dati disciplinati dal GDPR in applicazioni e servizi cloud mantenendo sicurezza e conformità. La soluzione offre visibilità sullo shadow IT, governance sui dati nelle applicazioni in cloud e protezione dei dati dalle minacce mirate agli account sul cloud.

- Permette di scoprire e analizzare l'uso di applicazioni cloud all'interno dell'azienda e di prevenire in modo proattivo la perdita o il furto di dati disciplinati dal GDPR
- Utilizza un controllo granulare in linea, analisi comportamentale e crittografia dei file per mantenere la sicurezza dei dati sensibili e disciplinati dal GDPR
- Protegge gli account sul cloud, controlla le attività degli utenti e governa i dati sensibili sugli account nel cloud tramite integrazione diretta di API con le applicazioni cloud
- Consente di crittografare o gestire tramite token i dati per garantire la compliance con le normative locali sui dati e altri regimi di compliance

Symantec Data Loss Prevention

In che modo vengono gestiti e protetti nei moderni ambienti dell'azienda i dati disciplinati dal GDPR? E come dovrebbe essere una strategia di protezione dei dati completa e funzionale, alla luce dei parametri di sicurezza sempre più limitati, della crescita degli attacchi mirati e dell'evolvere di abitudini e aspettative degli utenti? **Symantec Data Loss Prevention (DLP)** risponde a queste domande con un approccio completo verso la protezione delle informazioni che tiene conto delle attuali realtà del cloud e della centralità dei dispositivi mobili.

- Esegue un monitoraggio sul modo in cui vengono utilizzati i dati
- Protegge i dati da fughe o furti
- Scopre in quale sistema sono conservati i dati: cloud, mobile, rete, endpoint e storage
- Utilizza un'unica console basata sul Web per definire le policy sulla perdita di dati, esaminare e rimediare agli incidenti e svolgere il lavoro amministrativo

Estendere Symantec DLP al cloud

Sfruttare la soluzione integrata Symantec e Blue Coat

- Rilevamento dei dati sensibili sulle applicazioni in cloud: visibilità e controllo diretti su tutti i tipi di contenuti in oltre sessanta applicazioni cloud, come Google Apps, Office 365, Box, Dropbox o Salesforce
- Riutilizzo di policy e workflow di DLP: per sfruttare le policy e i workflow DLP attuali per le applicazioni in cloud senza dover riscrivere set di regole specifiche
- Prestazioni DLP su cloud ottimizzate: per eseguire il rilevamento DLP come servizio anziché in locale e migliorare l'efficienza operativa
- Gestione DLP da un'unica console: policy e workflow DLP per applicazioni cloud, endpoint, reti e data center si possono controllare da un'unica console

PROTEZIONE DELLE INFORMAZIONI

Symantec Endpoint Encryption

I requisiti di normative come il GDPR hanno trasformato la crittografia in una necessità. Per proteggere i dati dei clienti, alle aziende serve una soluzione di crittografia verificabile tramite auditing come **Symantec Endpoint Encryption**.

- Durante la fase di crittografia iniziale, Symantec Endpoint Encryption esegue la cifratura di ogni drive, settore per settore, garantendo che nessun file rimanga privo di crittografia
- Gli utenti devono digitare la password una sola volta, la tecnologia SSO li fa quindi navigare oltre la schermata principale senza dover digitare nuovamente la password
- Le varie opzioni per il recovery consentono di trovare il giusto mix fra recupero dei dati self-service e supporto tecnico
- Gli utenti possono accedere alle loro unità USB, unità disco rigido esterne e supporti CD/DVD/Blu-ray su qualunque sistema Windows o Mac

Symantec VIP

Symantec VIP è un diffuso servizio di autenticazione forte, basato su cloud e facile da usare che offre accesso sicuro ai dati e alle applicazioni disciplinati dal GDPR in ogni momento e luogo e con tutti i dispositivi.

- Servizio sicuro, affidabile e scalabile che assicura l'autenticazione senza necessità di hardware dedicato on-site
- Crea un singolo punto di accesso per proteggere le applicazioni sul cloud e on-site
- Blocca i tentativi di accesso a rischio senza modificare le modalità di accesso degli utenti legittimi
- Elimina la necessità di utilizzare password abilitando altre credenziali, come impronte biometriche, accesso di prossimità senza usare le mani e verifica push con un tocco o uno sfioramento
- Supporta token hardware e software gratuiti o credenziali OTP mobili

Panoramica del prodotto: Symantec Encryption

- Symantec Endpoint Encryption: dotata di tecnologia di crittografia PGP, assicura una crittografia robusta di dischi e supporti rimovibili con una gestione di classe enterprise, report pronti per l'uso e varie opzioni di recupero dati
- Symantec Email Encryption: Symantec Gateway Email Encryption protegge le comunicazioni in uscita e Symantec Desktop Email Encryption offre crittografia e decrittografia complete sulle comunicazioni interne
- Symantec File Share Encryption: protegge i dati sensibili dall'esposizione accidentale o malevola dei file quando questi si moltiplicano e transitano, esegue inoltre la crittografia di file e cartelle sui file server e sui drive di rete
- Symantec SSL Suite for Enterprise: aiuta a generare fiducia presso utenti online e clienti, rendendo sicuri i siti web e i dati in transito con una robusta infrastruttura di convalida

CYBER SECURITY SERVICES

Symantec Incident Response

Quando si verifica un attacco sui dati disciplinati dal GDPR, i team di Incident Response devono urgentemente contrastare e respingere avversari molto preparati, rispettando nel contempo le esigenze degli stakeholder. Attività disgiunte di tipo manuale mettono a dura prova le capacità del team di sicurezza, che può riuscire o meno a rimediare all'incidente. Per reagire con successo a un incidente occorre eseguire in modo sempre uniforme un piano ben orchestrato, misurabile, ripetibile e ottimizzato.

Symantec Cyber Security Services: la tecnologia di Incident Response fornisce i Readiness Services, fra cui Incident Response Plan Assessments, Tabletop Exercises e Advanced Threat Hunting per aiutare le aziende a creare e ottimizzare piani di Incident Response e trasformarli in programmi proattivi.

- Il Symantec Incident Response è un team globale di esperti, collaudato e attivo da tempo, che ha il supporto della Global Intelligence Network e dei Cyber Security Services di Symantec
- I nostri Emergency Response Services forniscono supporto investigativo da remoto e/o on-site quando richiesto. Ciò permette alle aziende prive di soluzioni deterrenti di attenuare l'impatto degli incidenti e ripristinare la normale operatività
- Il nostro Incident Response Retainer Service è un servizio con abbonamento annuale basato sulla valutazione on-site. Il servizio consente di risolvere rapidamente incidenti, evitare che ricapitino e tenere informati i dirigenti aziendali

Symantec Cyber Insurance

I vantaggi dell'assicurazione informatica e della sicurezza in un'unica offerta

Symantec collabora con importanti compagnie assicurative per sviluppare offerte di prodotti e pacchetti su misura, destinati ai nostri comuni clienti, per migliorare la loro affidabilità in termini di sicurezza e disponibilità finanziaria tramite il Symantec Cyber Insurance Partner Program. Questo consente ai clienti di ridurre il rischio associato agli attacchi informatici e recuperare più rapidamente il costo degli eventi informatici.

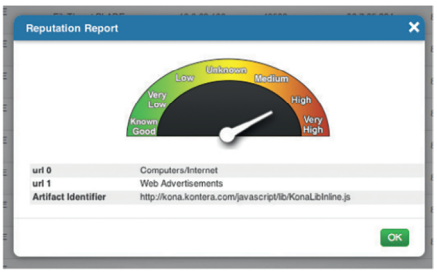
Symantec Cyber Security Services: Incident Response

CYBER SECURITY SERVICES

Symantec Security Analytics

Gli attacchi sofisticati e mirati possono causare pericolose violazioni di dati. La conformità al GDPR non è l'unica ragione per cui le aziende hanno necessità di scoprire, non appena possibile, in che modo si è potuta verificare una violazione e come collaborare con le forze di polizia e con le autorità del settore giudiziario e amministrativo per conservare le prove della violazione. Occorre sapere: quando, come e da chi è stata causata una violazione e se vi sono aree attaccate ancora compromesse.

Symantec Security Analytics combina visibilità sulla sicurezza su tutta la rete, Network Forensics avanzata, rilevamento di anomalie e ispezione di contenuti in tempo reale per tutte le attività di rete, offrendo al team di sicurezza gli strumenti per combattere gli attacchi avanzati che puntano ai dati aziendali disciplinati dal GDPR.



Analisi delle minacce in tempo reale

- Rispetto di normative e limitazioni sulla privacy dei dati specifiche dell'azienda, scansione dei protocolli attinenti e utilizzo di sistemi sandbox e di servizi di intelligence innovativi per individuare malware conosciuti e assicurare un punteggio della reputazione accurato alle soluzioni NGFW, IPS, SIEM e di sandbox
- Acquisizione di pacchetti avanzata per indicizzare, classificare e arricchire tutti i dati sul traffico di rete in base alla più recente intelligence sulle minacce e agli avvisi in tempo reale, identificando proattivamente file e URL malevoli e indicatori di compromissione
- Tempo di risoluzione inferiore ed efficaci capacità di Network Forensics per gli incidenti relativi alla sicurezza, tramite esplorazione della root-cause, ricostruzione di file, servizi di reputazione integrati e Data Enrichment
- La Security Analytics si integra perfettamente con le principali soluzioni di Endpoint Detection and Response (EDR) e supporta l'analisi del protocollo SCADA per una visione completa di qualunque attività malevola nella rete; ciò non è, allo stato attuale, attinente al GDPR, ma offre benefici ai clienti di settore che desiderano proteggere l'ambiente di produzione

Panoramica del prodotto

I componenti chiave dell'architettura Symantec Security Analytics includono:

- Security Analytics Software: opzione flessibile per ottenere alte prestazioni con un TCO e spese di capitale inferiori
- Security Analytics Appliances: dispositivi pronti per l'uso con acquisizione, classificazione e indicizzazione di tutta la rete
- Security Analytics Virtual Appliance: l'opzione perfetta per uffici remoti o filiali
- Security Analytics Central Manager: offre la visione aggregata di 200 sensori per l'analisi della sicurezza
- Security Analytics Storage Modules: moduli di capacità storage, come lo storage direct-attached o SAN

www.symantec.com/it/it

Symantec Italia (Milano), Via San Bovio 3, 20090 San Felice di Segrate (MI), tel: +39 02 36013200