Next-Generation Firewall: gestione dei dati personali

Forcepoint

Sommario

Informazioni generali

Finalità del documento

Questo documento è stato redatto per illustrare con trasparenza il processo di gestione dei dati personali nei seguenti prodotti e servizi Forcepoint: Next-Generation Firewall (NGFW), Security Management Center (SMC), Endpoint Context Agent (ECA), User ID Service e VPN Client. L'obiettivo di questo documento è offrire ai team di valutazione della privacy e procurement le informazioni necessarie per prendere decisioni informate in merito ai succitati prodotti e servizi Forcepoint.

Regolamento Generale sulla Protezione dei Dati (RGPD)

I prodotti e servizi Forcepoint sono destinati a funzionare in conformità ai principi sulla privacy stabiliti nel Regolamento Generale sulla Protezione dei Dati (RGPD), ovvero il Regolamento (UE) 2016/679. Nel pieno rispetto dei principi dell'RGPD, i clienti Forcepoint sono considerati i soli titolari del trattamento dei dati. Forcepoint non è né titolare né responsabile del trattamento dei dati archiviati nei prodotti e servizi Forcepoint NGFW, SMC, ECA, User ID Service e VPN Client. Ulteriori informazioni sull'RGPD sono disponibili presso https://ec.europa.eu/info/law/law-topic/data-protection/reform_en.

Dati personali

In questo documento vale la definizione di "dati personali" di cui all'articolo 4.1 dell'RGPD, ovvero qualsiasi informazione riguardante una persona fisica identificata o identificabile (”interessato”); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Tutela dei dati personali

Forcepoint fa uso di tecniche standard del settore per proteggere i dati conservati nei prodotti Forcepoint, incluso i dati personali. Questo approccio alla sicurezza dei dati aiuta a garantire che i dati ad alto rischio siano inintelligibili a chiunque non sia autorizzato ad accedervi. I dettagli completi sui processi e la politica sulla privacy di Forcepoint sono disponibili all'indirizzo: https://www.forcepoint.com/forcepoint-privacy-hub.

Clausola esonerativa

Questo documento contiene informazioni su prodotti e/o servizi Forcepoint. Le informazioni appartengono a Forcepoint. Nonostante sia stato fatto ogni sforzo per garantire che i contenuti siano aggiornati e accurati, le informazioni sono fornite *nello status quo*, senza alcuna garanzia esplicita o implicita e sono soggette a modifiche senza preavviso.

Eventuali riferimenti a funzionalità o rilasci futuri hanno valore unicamente previsionale e non vincolante. Forcepoint non si assume responsabilità per l'utilizzo di tali informazioni.

Identità e politica

Set di dati	Quali dati personali vengono utilizzati?	Scopo	Stato dei dati	Archiviazione, flusso e protezione	Conservazione
Account di amministratore	Durante l'installazione di SMC, viene creato un account superuser. Questo account viene utilizzato per creare gli account di amministratore dopo l'installazione. Se i clienti decidono di utilizzare l'autenticazione dei certificati, un identificativo dell'interessato – ad esempio un indirizzo e-mail – viene usato per identificare gli amministratori.	Gli amministratori con livelli di accesso diversi possono svolgere delle attività in SMC in base ai ruoli a loro assegnati.	I dati non sono pseudonimizzati	I nomi utente e gli hash SHA-512 generati da SMC sono archiviati nel database di server di gestione che i clienti gestiscono nella loro installazione di rete locale / interna del prodotto oppure nel loro cloud tenant / nella loro soluzione esterna a Forcepoint.	Il cliente può cancellare manualmente gli account di amministratore.
Database utenti LDAP interno	Il database utenti LDAP all'interno di SMC contiene nomi utente e hash di password utente. Se viene utilizzata l'autenticazione dei certificati, per identificare gli utenti viene utilizzato un identificativo dell'interessato – ad esempio un indirizzo e-mail.	Gli account utente possono essere utilizzati per l'autenticazione e il controllo degli accessi alla rete.	I dati non sono pseudonimizzati	I nomi utente e gli hash AES delle password utente sono archiviati nel database utenti LDAP interno sul server di gestione. Possono essere replicati nei motori NGFW con una connessione protetta da TLS standard di settore. Il cliente può avere accesso ai dati utilizzando un account che consente l'accesso al sistema operativo.	Il cliente può cancellare manualmente gli account utente.

Come gestire le richieste di accesso degli interessati (Subject Access Request, SAR)

SAR – Diritto di accesso	Il cliente designato come amministratore superuser SMC può accedere e gestire (aggiungere / modificare / eliminare) i dati degli account utente e amministratore nel database degli account utente SMC archiviato nella configurazione del server SMC.
SAR – Correzione / Rettifica	L'amministratore superuser SMC può accedere e gestire (aggiungere / modificare / eliminare) i dati degli account utente e amministratore nel database degli account utente SMC archiviato nella configurazione del server SMC.
SAR – Diritto all'oblio	L'amministratore superuser può eliminare i dati degli account utente e amministratore nel database degli account utente SMC archiviati nella configurazione del server SMC. Tutte le azioni degli amministratori SMC sono raccolte e archiviate in registri di audit che non possono essere né filtrati né eliminati in base all'account di uno specifico amministratore.
Localizzazione / archiviazione di dati	I dati degli account amministratore e utente di NGFW ed SMC sono archiviati sui server gestiti dal cliente.

Registrazione delle attività

Set di dati	Quali dati personali vengono utilizzati?	Scopo	Stato dei dati	Archiviazione, flusso e protezione	Conservazione
Archiviazione nei log server (include registri di accessi, ispezioni e allarmi e contatori di dati)	Per default, nei registri degli accessi non vengono registrati dati personali. I clienti possono comunque configurare i motori NGFW per registrare i dati sugli accessi, incluse informazioni su indirizzi IP, URL, nomi utente e applicazioni. I dati possono essere utilizzati per varie finalità, ad esempio la raccolta di dati statistici. Per dettagli, v. la TABELLA 1: Attributi dei dati personali per i registri degli accessi in SMC, Appendice A.	Monitorare il traffico di rete e creare dei report	I dati non sono pseudonimizzati	I registri degli accessi sono archiviati nei dischi dei log server in un formato di proprietà. I motori NGFW ricevono i dati attraverso una connessione protetta da TLS standard di settore. Quando è configurata l'integrazione con Elasticsearch, SMC può delegare l'indicizzazione dei registri SMC a un'istanza di database Elasticsearch locale gestita da un cliente. In questo modo il cliente può contare su query dei registri più veloci e report statistici trasparenti tramite l'interfaccia utente di SMC. Il cliente può avere accesso ai dati utilizzando un account che consenta l'accesso al sistema operativo NGFW.	Il cliente può rimuovere o archiviare i dati dei registri delle attività di monitoraggio degli accessi sia manualmente che automaticamente, utilizzando la funzionalità delle attività pianificate di SMC e/o SMC.
Registri di audit	I registri di audit includono i nomi degli account amministratore e gli indirizzi IP delle workstation client. Per dettagli, v. la TABELLA 2: Attributi dei dati personali per i registri di audit in SMC, Appendice A.	Monitorare le azioni degli amministratori	I dati non sono pseudonimizzati	I registri di audit sono archiviati nei dischi dei log server e dei server di gestione, in un formato di proprietà. I motori NGFW ricevono i dati attraverso una connessione protetta da TLS. Il cliente può avere accesso ai dati utilizzando un account che consente l'accesso al sistema operativo.	Il cliente può utilizzare SMC per rimuovere oppure archiviare i dati dei registri di audit sia manualmente, utilizzando SMC, e/o automaticamente con la funzionalità di attività pianificata di SMC.
Report pianificati	I report vengono utilizzati per la presentazione di statistiche a partire dai dati di registro; le statistiche possono includere dei dati personali, in base alla configurazione dei registri del cliente.	Creare report sugli eventi del traffico di rete e/o soddisfare le esigenze di reporting del cliente	I dati non sono pseudonimizzati	I report vengono archiviati nei dischi dei server di gestione, in un formato di proprietà. Il cliente può avere accesso ai dati utilizzando un account che consente l'accesso al sistema operativo oppure alle interfacce di gestione di SMC.	Il cliente può stabilire la data di scadenza dei report nei progetti dei report. Per default, i report scadono dopo 10 giorni.
Registri dei dump di debug ECA sugli endpoint Windows	I dati nei registri dei dump di debug ECA includono gli utenti attualmente registrati sull'endpoint e relativi domini, nonché alcune informazioni di base come il sistema operativo, il tipo di CPU, la memoria fisica totale e libera, lo spazio su disco totale e libero e le applicazioni installate.	Risolvere problemi di natura tecnica per i clienti.	I dati non sono pseudonimizzati	I clienti devono archiviare i registri dei dump di debug nella cartella di installazione ECA.	I dati dei registri dei dump di debug sono archiviati in file di 2 MB. Visto che la quantità massima di dati di registro archiviabili è 10 MB, il sistema può conservare fino a 5 file di 2 MB. Quando viene raggiunto il numero massimo di file di registro, il sistema elimina i più vecchi, per lasciare spazio ai file di dati di registro più recenti

Come gestire le richieste di accesso degli interessati (Subject Access Request, SAR)

SAR – Diritto di accesso	Gli amministratori di NGFW possono avere accesso e gestire il registro SMC e riportare i dati tramite l'API di gestione SMC.
SAR – Correzione / Rettifica	Per motivi di sicurezza e monitoraggio, NGFW ed SMC sono studiati per prevenire qualsiasi alterazione (correzione / rettifica) ai dati dei registri archiviati.
SAR – Diritto all'oblio	L'amministratore superuser di NGFW ed SMC può filtrare e cancellare dei registri selezionati in base a uno specifico dato identificativo dell'utente (ad es. nome utente, ID account utente). Tutte le azioni degli amministratori SMC sono raccolte e archiviate in registri di audit che non possono essere né filtrati né eliminati in base all'account di uno specifico amministratore.
Localizzazione / archiviazione di dati	Il cliente NGFW sceglie e gestisce la posizione dei propri server di dati e dell'installazione di NGFW ed SMC.

Moduli aggiuntivi

Set di dati	Quali dati personali vengono utilizzati?	Scopo	Stato dei dati	Archiviazione, flusso e protezione	Conservazione
Advanced Malware Detection (AMD)	AMD riceve dal prodotto NGFW i file, che devono essere analizzati per rilevare eventuali malware. Quando riceve i file, AMD li analizza per determinare se contengono malware. I file caricati per essere analizzati da AMD possono contenere dei dati personali. L'amministratore del cliente è in grado di configurare i tipi di file inoltrati ad AMD.	Capire se l'intero file inoltrato presenta un rischio di malware.	I risultati dei file vengono anonimizzati per generare un hash SHA-1 del file inoltrato e associare i risultati dell'analisi con l'hash del file. Completata l'analisi, il file e i suoi eventuali contenuti vengono immediatamente cancellati.	Advanced Malware Detection archivia il risultato dell'analisi dei malware collegandolo all'hash del file generato da AMD. Il file inoltrato viene cancellato non appena l'analisi viene completata. L'analisi può richiedere da 10 secondi a 5 minuti, in base alle dimensioni e al tipo del file analizzato. Il file viene inoltrato ad AMD mediante un canale con crittografia TLS standard dell'industria. La funzionalità di analisi di AMD è esternalizzata. L'analisi avviene in due data center che si trovano a Los Angeles, Stati Uniti, e ad Amsterdam, Paesi Bassi. I clienti selezionano il data center da utilizzare oppure scelgono l'opzione automatica che imposta il data center geograficamente più vicino all'indirizzo IP pubblico di NGFW che sta avanzando la richiesta al resolver DNS.	Advanced Malware Detection non conserva il file inoltrato. AMD conserva, invece, a tempo indeterminato i risultati dell'analisi di un file. Se durante l'analisi viene rilevato un malware, il codice del malware (artefatto malware) viene conservato per un tempo indeterminato.
User ID Service	Coppie utente e indirizzo IP. Per dettagli, v. la TABELLA 3: Attributi di dati personali per lo User ID Service di Forcepoint, Appendice A.	Risolvere le associazioni tra gli indirizzi IP degli utenti e i gruppi di utenti.	I dati non sono pseudonimizzati	I dati vengono archiviati in chiaro in un database interno. I clienti hanno la possibilità di crittografare il database con una soluzione di crittografia a loro scelta. Il database contiene un sottogruppo di attributi Active Directory specifici dell'utente, ad esempio nome utente, indirizzo e-mail, membership di un gruppo e l'indirizzo IP corrente. L'accesso ai dati richiede un account che consente l'accesso al sistema operativo. L'API del servizio UID consente di eseguire delle query non autenticate su questi dati, provenienti dalla rete. Il firewall del sistema operativo può essere utilizzato per controllare l'accesso della rete all'API.	I dati indirizzo IP e utente associati restano memorizzati per 6 ore. Per cancellarli, il cliente può disinstallare User ID Service di Forcepoint.
VPN Client per Windows	I dati dei registri di VPN Client contengono gli indirizzi e-mail degli utenti se nelle VPN viene utilizzato come metodo di autenticazione un certificato che contiene gli indirizzi e-mail.	Registrare l'utilizzo delle VPN da parte del cliente tramite NGFW; utilizzabile anche per risolvere dei problemi tecnici per i clienti.	I dati non sono pseudonimizzati	I dati dei registri del VPN Client vengono memorizzati in formato di testo semplice nella cartella dati del VPN Client (per default, C:\ProgramData\Forcepoint\Stonesoft VPN Client\log o C:\ProgramData\Forcepoint\VPN Client\log).	I dati presenti nei file di dati di registro del VPN Client vengono automaticamente sovrascritti quando vengono creati nuovi dati di registro. Per cancellare i dati, disinstallare il VPN Client per Windows e poi rimuovere manualmente i file dalla cartella dati del VPN Client.

I seguenti prodotti, integrabili o utilizzabili con Next-Generation Firewall, non memorizzano localmente alcun dato personale:

- Forcepoint VPN Client per Android

- Forcepoint VPN Client per Mac

Come gestire le richieste di accesso degli interessati (Subject Access Request, SAR)

SAR – Diritto di accesso	AMD: i clienti di NGFW possono accedere ai report della loro sandbox dall'account del portale AMD dei clienti; lo “Scan report” si collega ai registri per filtrare i file. È consigliabile consultare i documenti di supporto del prodotto Forcepoint AMD per migliorare la protezione dei dati specifici AMD e ottenere report più dettagliati. Servizio User ID: i dati utente nel servizio Forcepoint User ID (FUID) vengono importati dal servizio Microsoft Active Directory (AD) configurato dal cliente NGFW. I dati dell'utente FUID sono accessibili e gestibili (accessibili / modificabili / cancellabili) tramite l'account dell'amministratore di NGFW – FUID e gli strumenti di gestione Microsoft AD del cliente.
SAR – Correzione / Rettifica	In FUID sono memorizzati i dati importati direttamente dal sistema Microsoft Active Directory (AD) del cliente, così come appaiono in Microsoft AD. Eventuali rettifiche ai dati utente vanno eseguite in Microsoft AD e reimportate in FUID.
SAR – Diritto all'oblio	La disinstallazione dei servizi FUID comporta la cancellazione automatica di tutti i dati utente.
Localizzazione / archiviazione di dati	Il cliente NGFW sceglie e gestisce la posizione del proprio server di dati e della propria installazione di FUID.

Appendice A

Terminologia

Termine	Spiegazione
Next-Generation Firewall (NGFW)	La soluzione Next-Generation Firewall include i motori Next-Generation Firewall, i componenti del server SMC e i componenti dell'interfaccia utente SMC.
Security Management Center (SMC)	SMC è il componente di gestione della soluzione Next-Generation Firewall. SMC gestisce e controlla gli altri componenti del sistema.
Server di gestione	Il server di gestione costituisce l'elemento centrale dell'amministrazione del sistema.
Log Server	I log server archiviano i registri sul traffico. Questi registri possono essere gestiti e organizzati in report. I log server, inoltre, correlano gli eventi, monitorano lo stato dei motori NGFW, mostrano statistiche in tempo reale e inoltrano i registri ai dispositivi di terze parti.
Motori Next-Generation Firewall (Motori NGFW)	I motori Next-Generation Firewall ispezionano il traffico. Vengono utilizzati per configurare il controllo degli accessi alle risorse e per monitorare le azioni di utenti e amministratori. I motori Next-Generation Firewall nel ruolo Firewall / VPN possono essere utilizzati anche come gateway VPN.
Advanced Malware Detection (AMD)	Forcepoint AMD rileva le minacce avanzate analizzando il comportamento dei file. I motori NGFW possono essere configurati per l'invio dei file ad AMD, a scopo di analisi.
Endpoint Context Agent (ECA)	L'ECA raccoglie informazioni su applicazioni e utenti per ogni connessione sui client endpoint Windows. L'ECA è integrabile con Forcepoint NGFW per ricevere informazioni su applicazioni e utenti riguardo ai client endpoint Windows che si collegano tramite un motore NGFW gestito da SMC. Le informazioni sono utilizzabili come criteri per il controllo e il monitoraggio degli accessi e per creare dei report.
Servizio Forcepoint User ID (FUID)	Il servizio Forcepoint User ID raccoglie informazioni su utenti, gruppi e indirizzi IP dai server Windows Active Directory (AD) e dai Microsoft Exchange Server. Il servizio Forcepoint User ID può essere integrato con Forcepoint NGFW e le informazioni fornite dal servizio Forcepoint User ID possono essere utilizzate per monitorare gli utenti e configurare il controllo degli accessi.

Attributi di dati personali

TABELLA 1: Attributi dei dati personali per i registri degli accessi in SMC

I dati personali di questo dataset non possono essere anonimizzati per assicurare la conformità alle migliori prassi di sicurezza che vietano di disattivare gli audit trail degli incidenti di ispezione e degli accessi alla rete; la raccolta delle informazioni in questi registri è, in ogni caso, facoltativa.

Attributo	Requisiti
Indirizzo IP	Opzionale
Nome di accesso utente e dominio	Opzionale

TABELLA 2: Attributi dei dati personali per i registri di audit in SMC

Per non impedire il corretto funzionamento della policy di sicurezza i dati personali di questo dataset non possono essere anonimizzati. I registri di audit non possono essere disabilitati. Possono, però, essere deselezionati tramite le attività pianificate di gestione dei registri in SMC oppure rimuovendo dal disco i dati dei registri di audit.

Attributo	Requisiti
Nome di accesso amministratore	Obbligatorio
Indirizzo IP del client amministratore	Obbligatorio

TABELLA 3: Attributi dei dati personali per il servizio User ID

I dati personali di questo dataset sono specchiati dall'ambiente Microsoft Active Directory configurato e vengono rimossi automaticamente quando vengono rimossi da AD. I dati personali di questo dataset non possono essere anonimizzati per assicurare la conformità alle migliori prassi di sicurezza che impediscono di abbinare gli utenti nella policy degli accessi alla rete. La disinstallazione del server FUID elimina anche tutti i dati presenti nella cache dell'installazione di FUID.

Attributo
Nome di accesso utente e dominio
Membership dei gruppi AD utenti
Indirizzo IP utente (come visto da AD Domain Controller)
Indirizzo e-mail utente