Next-Generation Firewall – Umgang mit personenbezogenen Daten

Forcepoint

Inhaltsverzeichnis

Allgemeine Informationen

Zweck des Dokuments

Dieses Dokument dient der Transparenz und Erläuterung des Umgangs mit personenbezogenen Daten durch die folgenden Forcepoint-Produkte und -Dienstleistungen: Next-Generation Firewall (NGFW), Security Management Center (SMC), Endpoint Context Agent (ECA), User ID Service und VPN Client. Dieses Dokument zielt darauf ab, die notwendigen Informationen für Beschaffungs- und Datenschutzbeurteilungsteams bereitzustellen, sodass diese fundierte Entscheidungen im Hinblick auf die zuvor erwähnten Forcepoint-Produkte und -Dienstleistungen treffen können.

Datenschutz-Grundverordnung (DSGVO)

Die Ausführung von Forcepoint-Produkten und -Dienstleistungen ist so konzipiert, dass sie den Datenschutzgrundsätzen der Datenschutz-Grundverordnung (DSGVO), (EU-Verordnung 2016/679), entspricht. In Übereinstimmung mit den Grundsätzen der DSGVO werden die Kunden von Forcepoint als alleinige Datenverantwortliche betrachtet. Forcepoint ist weder der Datenverantwortliche noch der Datenverarbeiter in Bezug auf Kundendaten, die in den Forcepoint-Produkten und -Dienstleistungen NGFW, SMC, ECA, User ID Service und VPN Client gespeichert sind. Weitere Informationen zur DSGVO finden Sie unter https://ec.europa.eu/info/law/law-topic/data-protection/reform_en.

Personenbezogene Daten

Dieses Dokument wendet die Definition des Begriffs „personenbezogene Daten“ aus Artikel 4.1 der DSGVO an, der „personenbezogene Daten“ als alle Informationen über eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) definiert. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu anderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Schützen von personenbezogenen Daten

Forcepoint verwendet branchenübliche Techniken zum Schutz der in Forcepoint-Produkten gespeicherten Daten, einschließlich personenbezogener Daten. Dieser Ansatz zur Datensicherheit trägt dazu bei, dass die risikoreichen Daten für alle Personen, die nicht zugriffsberechtigt sind, unverständlich sind. Alle Details zu den Datenschutzrichtlinien und -prozessen von Forcepoint finden Sie unter: https://www.forcepoint.com/forcepoint-privacy-hub.

Haftungsausschluss

Dieses Dokument enthält Informationen zu Produkten und/oder Dienstleistungen von Forcepoint. Die Informationen sind Eigentum von Forcepoint. Obwohl alle Anstrengungen unternommen wurden, um sicherzustellen, dass der Inhalt aktuell und korrekt ist, werden die Informationen ohne jegliche Garantie oder Gewähr, weder ausdrücklich noch stillschweigend, *in dieser Form* zur Verfügung gestellt und können ohne vorherige Ankündigung geändert werden.

Alle Hinweise auf zukünftige Versionen oder Funktionen sind Prognosen und nicht als Verpflichtungen anzusehen. Forcepoint übernimmt keine Haftung für die Verwendung dieser Informationen.

Identität und Richtlinie

Datensatz	Welche personenbezogenen Daten werden verwendet?	Zweck	Datenstatus	Speicherung, Datenfluss und Schutz	Speicherung
Administratorkonten	Ein Superuser-Konto wird während der Installation des SMC erstellt. Dieses Konto wird verwendet, um nach der Installation Administratorkonten zu erstellen. Wenn sich Kunden für die Zertifikatsauthentifizierung entscheiden, wird eine Antragsteller-ID, wie z. B. eine E-Mail-Adresse, zur Identifizierung der Administratoren verwendet.	Administratoren, für die unterschiedliche Zugriffsebenen vorliegen, können Aufgaben im SMC je nach den ihnen zugewiesenen Administratorrollen durchführen.	Die Daten werden nicht pseudonymisiert.	Benutzernamen und vom SMC generierte SHA-512-Hashes der Administratorkennwörter werden in der Verwaltungsserver-Datenbank gespeichert, die die Kunden entweder in ihrer lokalen/internen Netzwerkinstallation des Produkts oder in ihrem eigenen Cloud-Mandanten oder ihrer Lösung außerhalb von Forcepoint ablegen.	Der Kunde kann Administratorkonten manuell löschen.
Interne LDAP-Benutzerdatenbank	Die interne LDAP-Benutzerdatenbank im SMC enthält Benutzernamen und Hashes der Benutzerkennwörter. Wenn die Zertifikatsauthentifizierung eingesetzt wird, wird eine Antragsteller-ID, wie z. B. eine E-Mail-Adresse, zur Identifizierung der Benutzer verwendet.	Benutzerkonten können für die Authentifizierung und die Netzwerkzugriffskontrolle verwendet werden.	Die Daten werden nicht pseudonymisiert.	Die Benutzernamen und AES-Hashes der Benutzerkennwörter werden in der internen LDAP-Benutzerdatenbank auf dem Verwaltungsserver gespeichert. Sie können für die NGFW-Engines über eine TLS-geschützte Verbindung gemäß Industriestandard repliziert werden. Der Kunde kann über ein Konto, das den Zugriff auf das Betriebssystem zulässt, auf die Daten zugreifen.	Der Kunde kann Benutzerkonten manuell löschen.

Verwalten eines Auskunftsersuchens (Subject Access Request, SAR)

SAR – Recht auf Zugriff	Der vom Kunden zugewiesene SMC-Superuser-Administrator kann auf die Daten der Administrator- und Benutzerkonten in der SMC-Benutzerdatenbank (die in der SMC-Serverkonfiguration gespeichert ist) zugreifen und sie verwalten (hinzufügen/ändern/löschen).
SAR – Korrektur/Verbesserung	Der SMC-Superuser-Administrator kann auf die Administrator- und Benutzerkontodaten in der SMC-Benutzerkontendatenbank (die in der SMC-Serverkonfiguration gespeichert ist) zugreifen und sie verwalten (hinzufügen/ändern/löschen).
SAR – Recht auf Vergessenwerden	Der Superuser-Administrator kann die Administrator- und Benutzerkontodaten in der SMC-Benutzerkontendatenbank, die in der SMC-Serverkonfiguration gespeichert ist, löschen. Alle Aktionen des SMC-Administrators werden erfasst und in Prüfprotokollen gespeichert, die nicht basierend auf einem bestimmten Administratorkonto gefiltert oder gelöscht werden können.
Datenspeicherung/Lokalisierung	NGFW- und SMC-Benutzer- und Administratorkontendaten werden auf den vom Kunden verwalteten Servern gespeichert.

Aktivitätsprotokollierung

Datensatz	Welche personenbezogenen Daten werden verwendet?	Zweck	Datenstatus	Speicherung, Datenfluss und Schutz	Speicherung

Protokollserverspeicherung (Zugriffs-, Prüfungs- und Warnungsprotokolle sowie Indikatordaten)	Standardmäßig werden keine personenbezogenen Daten in Zugriffsprotokollen erfasst. Kunden können jedoch NGFW-Engines so konfigurieren, dass Zugriffsdaten protokolliert werden, die Informationen zu IP-Adressen, URLs, Benutzerdaten und Anwendungen enthalten können. Die Daten können für verschiedene Zwecke, z. B. für das Erfassen von Statistiken, verwendet werden. Weitere Informationen finden Sie in TABELLE 1: „Attribute von personenbezogenen Daten für Zugriffsprotokolle im SMC“ in Anhang A.	Überwachen von Netzwerkverkehr und Erstellen von Berichten.	Die Daten werden nicht pseudonymisiert.	Zugriffsprotokolle werden auf den Protokollserver-Datenträgern im proprietären Format gespeichert. Die Daten werden von NGFW-Engines über eine TLS-geschützte Verbindung gemäß Industriestandard empfangen. Wenn die Integration mit Elasticsearch konfiguriert wird, kann das SMC die Indexierung von SMC-Protokollen an eine vom Kunden verwaltete lokale Elasticsearch-Datenbankinstanz delegieren. So kann der Kunde von schnelleren Protokollabfragen und transparenten statistischen Berichten über die SMC-Benutzeroberfläche profitieren. Der Kunde kann auf die Daten mit Hilfe eines Kontos zugreifen, das den Zugriff auf das NGFW-Betriebssystem ermöglicht.	Der Kunde kann die Daten desAktivitätenprotokolls für die Zugriffsüberwachung manuell oder automatisch mit dem SMC und/oder mit der SMC-Funktion für geplante Aufgaben entfernen oder archivieren.
Prüfprotokolle	Prüfprotokolle beinhalten Administratorkontonamen und die IP-Adressen der Client-Workstations. Weitere Informationen finden Sie in TABELLE 2: „Attribute von personenbezogenen Daten für Prüfprotokolle im SMC“ in Anhang A.	Prüfen von Administratoraktivitäten.	Die Daten werden nicht pseudonymisiert.	Prüfprotokolle werden auf den Verwaltungsserver- und Protokollserver-Datenträgern im proprietären Format gespeichert. Die Daten werden von NGFW-Engines über eine TLS-geschützte Verbindung empfangen. Der Kunde kann über ein Konto, das den Zugriff auf das Betriebssystem zulässt, auf die Daten zugreifen.	Der Kunde kann die Daten des Prüfprotokolls manuell mit dem SMC und/oder automatisch mit der SMC-Funktion für geplante Aufgaben entfernen oder archivieren.
Geplante Berichte	Berichte werden verwendet, um Statistiken aus Protokolldaten darzustellen, die je nach der Protokollkonfiguration des Kunden personenbezogene Daten enthalten können.	Erstellen von Berichten zu Ereignissen des Netzwerkverkehrs und/oder zur Erfüllung der Anforderungen der Kunden an die Berichterstellung.	Die Daten werden nicht pseudonymisiert.	Die Berichte werden auf den Verwaltungsserver-Datenträgern im proprietären Format gespeichert. Der Kunde kann über ein Konto, das den Zugriff auf das Betriebssystem oder auf die Verwaltungsoberfläche des SMC zulässt, auf die Daten zugreifen.	Der Kunde kann das Ablaufdatum für den Bericht im Berichtdesign festlegen. Die standardmäßige Ablauffrist für Berichte beträgt zehn Tage.

ECA-Debug-Dump-Protokolle auf Windows-Endpunkten	Die Daten in den ECA-Debug-Dump-Protokollen umfassen die Benutzer, die aktuell am Endpunkt angemeldet sind, und ihre Domänen. Ferner einige grundlegende Informationen wie Betriebssystem, CPU-Typ, freier und physischer Speicher insgesamt, freier und Festplattenspeicher insgesamt und installierte Anwendungen.	Lösen von technischen Problemen für die Kunden.	Die Daten werden nicht pseudonymisiert.	Die Kunden sollten die Debug-Dump-Protokolle im Ordner der ECA-Installation speichern.	Die Debug-Dump-Protokolle werden in Dateien mit 2 MB gespeichert. Die maximale Größe der Protokolldaten, die gespeichert werden können, beträgt 10 MB. Das System kann bis zu fünf Dateien mit 2 MB speichern. Wenn die maximale Anzahl der Protokolldateien erreicht wird, wird die älteste Datei vom System aussortiert, um Platz für aktuellere Protokolldatendateien zu schaffen.

Verwalten eines Auskunftsersuchens (Subject Access Request, SAR)

SAR – Recht auf Zugriff	NGFW-Administratoren können auf das SMC-Protokoll zugreifen und die Daten über die SMC Management-API in einen Bericht aufnehmen.
SAR – Korrektur/Verbesserung	NGFW und das SMC sind so konzipiert, dass das Bearbeiten (Korrektur/Verbesserung) der gespeicherten Protokolldaten für Sicherheits- und Prüfzwecke verhindert wird.
SAR – Recht auf Vergessenwerden	Der NGFW und SMC-Superuser-Administrator kann ausgewählte Protokolle basierend auf einer bestimmten Benutzer-ID (z. B. Benutzername, Benutzerkonto-ID) filtern und löschen. Alle Aktionen des SMC-Administrators werden erfasst und in Prüfprotokollen gespeichert, die nicht basierend auf einem bestimmten Administratorkonto gefiltert oder gelöscht werden können.
Datenspeicherung/Lokalisierung	Der NGFW-Kunde wählt und verwaltet den Speicherort der NGFW- und SMC-Installation und der Datenserver.

Add-On-Module

Datensatz	Welche personenbezogenen Daten werden verwendet?	Zweck	Datenstatus	Speicherung, Datenfluss und Schutz	Speicherung

Advanced Malware Detection (AMD)	Die AMD empfängt Dateien, die auf Malware analysiert werden, vom NGFW-Produkt. Nach dem Empfang der Datei führt die AMD eine Analyse durch, um festzulegen, ob Malware in der Datei enthalten ist. Die Dateien, die für die AMD-Analyse hochgeladen werden, können möglicherweise personenbezogene Daten enthalten. Der Administrator des Kunden kann festlegen, welche Dateitypen an die AMD gesendet werden.	Verstehen, ob die gesendete Datei ein Risiko für Malware beinhaltet.	Die Ergebnisse der Dateien werden durch das Generieren eines SHA-1-Hashes für die gesendete Datei und das Verknüpfen des Ergebnisses der Analyse mit dem Datei-Hash anonymisiert. Nach der Analyse werden die Datei und alle Inhalte sofort gelöscht.	Die Advanced Malware Detection speichert das Ergebnis der Malware-Analyse, das an die von der AMD generierten Datei-Hashes gebunden ist. Die gesendete Datei wird sofort nach der Analyse gelöscht. Die Analyse kann zwischen 10 Sekunden und 5 Minuten dauern, je nach Größe und Typ der zu analysierenden Datei. Die Datei wird über einen TLS-verschlüsselten Kanal gemäß Industriestandard an die AMD gesendet. Die Analysekapazität der AMD wird ausgelagert. Die Analyse wird in zwei Rechenzentren durchgeführt, die sich in Los Angeles (USA) und Amsterdam (Niederlande) befinden. Die Kunden können das verwendete Rechenzentrum auswählen oder die Option für die automatische Festlegung wählen, sodass das geografisch nächstgelegene Rechenzentrum für die öffentliche NGFW-IP-Adresse konfiguriert wird, die die DNS-Auflösungsanforderung stellt.	Die Advanced Malware Detection speichert die gesendete Datei nicht. Die AMD speichert die Analyseergebnisse einer Datei auf unbestimmte Zeit. Ferner wird der in der Analyse gefundene Malware-Code (Malware-Artefakt) auf unbestimmte Zeit gespeichert.
User ID Service	Benutzer und IP-Adressen werden gekoppelt. Weitere Informationen finden Sie in TABELLE 3: „Attribute von personenbezogenen Daten für den Forcepoint User ID Service“ in Anhang A.	Auflösen von Verknüpfungen zwischen IP-Adressen und Benutzergruppen.	Die Daten werden nicht pseudonymisiert.	Die Daten werden in Klartext in einer internen Datenbank gespeichert. Kunden haben die Option, die Datenbank mit einem Schlüssel ihrer Wahl zu verschlüsseln. Die Datenbank enthält einen Teil der benutzerspezifischen Active Directory-Attribute, wie Benutzername, E-Mail-Adresse, Gruppenmitgliedschaften und die aktuelle IP-Adresse. Für den Zugriff auf die Daten ist ein Konto erforderlich, das den Zugriff auf das Betriebssystem zulässt. Die UID Service-API ermöglicht nicht authentifizierte Abfragen dieser Daten aus dem Netzwerk. Die Firewall des Betriebssystems kann verwendet werden, um den Netzwerkzugriff auf die API zu kontrollieren.	Die Daten des Benutzer- und IP-Adresspaares werden sechs Stunden lang gespeichert. Zum Entfernen der Daten kann der Kunde den Forcepoint User ID Service deinstallieren.
VPN Client für Windows	Die VPN Client-Protokolldaten enthalten die E-Mail-Adressen der Benutzer, wenn ein Zertifikat, das die E-Mail-Adressen enthält, als Authentifizierungsmethode in VPNs verwendet wird.	Protokolliert die VPN-Verwendung des Kunden durch NGFW und kann daher verwendet werden, um technische Probleme für die Kunden zu lösen.	Die Daten werden nicht pseudonymisiert.	Die VPN Client-Protokolldaten werden als Nur-Text-Dateien im Ordner der VPN Client-Daten gespeichert (standardmäßig C:\ProgramData\Forcepoint\Stonesoft VPN Client\log oder C:\ProgramData\Forcepoint\VPN Client\log).	Die Daten aus den Protokolldatendateien des VPN Clients werden automatisch überschrieben, wenn neue Protokolldaten erstellt werden. Zum Entfernen der Daten deinstallieren Sie den VPN Client für Windows und entfernen die Dateien manuell aus dem Ordner für die VPN Client-Daten.

Die folgenden Produkte, die in Next-Generation Firewall integriert oder damit verwendet werden, speichern keine personenbezogenen Daten lokal:

- Forcepoint VPN Client für Android
- Forcepoint VPN Client für Mac

Verwalten eines Auskunftsersuchens (Subject Access Request, SAR)

SAR – Recht auf Zugriff	AMD: NGFW-Kunden können auf Ihre Sandbox-Berichte vom AMD-Portalkonto des Kunden und von den Verknüpfungen zum Scannen der Berichte in den Dateifilterprotokollen aus zugreifen. Informationen über den zusätzlichen AMD-spezifischen Datenschutz und Berichterstellungsdetails sind in den Produktunterstützungsdokumenten von Forcepoint AMD enthalten. User ID Service: Die Benutzerdaten im Forcepoint User ID (FUID) Service werden direkt aus dem Microsoft Active Directory (AD) importiert, das vom NGFW-Kunden konfiguriert wurde. Die FUID-Benutzerdaten können über das FUID-Administratorkonto von NGFW und die Microsoft AD-Verwaltungstools des Kunden verwendet und verwaltet (geöffnet/geändert/gelöscht) werden.
SAR – Korrektur/Verbesserung	FUID umfasst die Benutzerdaten, die direkt aus dem Microsoft Active Directory- (AD-)System importiert wurden, so wie sie in Microsoft AD vorliegen. Korrekturen an Benutzerdaten müssen in Microsoft AD durchgeführt und erneut in FUID importiert werden.
SAR – Recht auf Vergessenwerden	Durch die Deinstallation von FUID Service werden automatisch alle Benutzerdaten gelöscht.
Datenspeicherung/Lokalisierung	Der NGFW-Kunde wählt und verwaltet den Speicherort der FUID-Installation und des Datenservers.

Anhang A

Terminologie

Begriff	Erläuterung
Next-Generation Firewall (NGFW)	Die Lösung von Next-Generation Firewall umfasst Next-Generation Firewall-Engines, SMC-Serverkomponenten und Komponenten der SMC-Benutzeroberfläche.
Security Management Center (SMC)	Das SMC ist die Verwaltungskomponente der Lösung von Next-Generation Firewall. Das SMC verwaltet und kontrolliert die anderen Komponenten im System.
Verwaltungsserver	Der Verwaltungsserver ist die zentrale Komponente für die Systemverwaltung.
Protokollserver	Auf den Protokollservern werden Datenverkehrsprotokolle gespeichert, die verwaltet und in Berichten zusammengefasst werden können. Protokollserver korrelieren außerdem Ereignisse, überwachen den Status der NGFW-Engines, zeigen Statistiken in Echtzeit und leiten Protokolle an Geräte von Drittanbietern weiter.
Next-Generation Firewall-Engines (NGFW-Engines)	Next-Generation Firewall-Engines untersuchen den Datenverkehr. Sie werden verwendet, um die Zugriffskontrolle für Ressourcen zu konfigurieren und die Benutzer- und Administratoraktivitäten zu überwachen. Next-Generation Firewall-Engines in der Firewall-/VPN-Rolle können auch als VPN-Gateways verwendet werden.
Advanced Malware Detection (AMD)	Forcepoint AMD entdeckt komplexe Bedrohungen durch die Analyse des Dateiverhaltens. NGFW-Engines können so konfiguriert werden, dass Dateien zur Analyse an die AMD gesendet werden.
Endpoint Context Agent (ECA)	ECA erfasst Benutzer- und Anwendungsinformationen pro Verbindung über Windows-Endpunkt-Clients. Sie können ECA in Forcepoint NGFW integrieren, um Benutzer- und Anwendungsinformationen über Windows-Endpunkt-Clients zu erhalten, die über eine vom SMC verwaltete NGFW-Engine verbunden sind. Sie können diese Informationen als Kriterien für die Zugriffskontrolle und Überwachung sowie für die Erstellung von Berichten verwenden.
Forcepoint User ID Service (FUID)	Der Forcepoint User ID Service erfasst Informationen über Benutzer, Gruppen und IP-Adressen von Windows Active Directory-(AD-)Servern und Microsoft Exchange-Servern. Sie können den Forcepoint User ID Service in Forcepoint NGFW integrieren, und die Informationen, die der Forcepoint User ID Service bietet, für die Überwachung von Benutzern und die Konfiguration der Zugriffskontrolle verwenden.

Attribute von personenbezogenen Daten

TABELLE 1: Attribute von personenbezogenen Daten für Zugriffsprotokolle im SMC

Personenbezogene Daten in diesem Datensatz können nicht anonymisiert werden. Dies würde gegen bewährte Sicherheitspraktiken verstoßen, da die Prüfprotokolle für Netzwerkzugriffe und Inspektionsvorfälle deaktiviert werden. Das Erfassen dieser Protokolle ist jedoch optional.

Attribut	Anforderung
IP-Adresse	Optional
Benutzeranmeldename und Domäne	Optional

TABELLE 2: Attribute von personenbezogenen Daten für Prüfprotokolle im SMC

Personenbezogene Daten in diesem Datensatz können nicht anonymisiert werden, da dies die ordnungsgemäße Durchsetzung der Sicherheitsrichtlinie verhindern würde. Prüfprotokolle können nicht deaktiviert werden. Sie können jedoch über die SMC-Funktion für geplante Protokollverwaltungsaufgaben oder durch Entfernen von der Festplatte gelöscht werden.

Attribut	Anforderung
Admin-Anmeldename	Obligatorisch
Admin-Client-IP-Adresse	Obligatorisch

TABELLE 3: Attribute von personenbezogenen Daten für den User ID Service

Personenbezogene Daten in diesem Datensatz werden von der konfigurierten Microsoft Active Directory-Umgebung gespiegelt und automatisch entfernt, wenn sie aus dem AD entfernt werden. Personenbezogene Daten in diesem Datensatz können nicht anonymisiert werden. Dies würde gegen bewährte Sicherheitspraktiken verstoßen, da das Zuordnen von Benutzern in der Netzwerkzugriffsrichtlinie verhindert wird. Durch die Deinstallation des FUID-Servers werden auch alle gespeicherten Daten in der FUID-Installation entfernt.

Attribut
Benutzeranmeldename und Domäne
AD-Gruppenmitgliedschaften der Benutzer
Benutzer-IP-Adresse (aus der Perspektive des AD-Domänencontrollers)
E-Mail-Adresse des Benutzers