Yeni Nesil Güvenlik Duvarı - Kişisel Verilerin Yönetimi

Forcepoint

İçindekiler

Genel Bilgiler

Belgenin Amacı

Bu belge, kişisel verilerin aşağıdaki Forcepoint ürün ve hizmetleriyle yönetimi konusunda şeffaflık ve açıklama sağlamak için tasarlanmıştır: Yeni Nesil Güvenlik Duvarı (NGFW), Güvenlik Yönetim Merkezi (SMC), Uç Nokta Bağlam Aracısı (ECA), Kullanıcı Kimliği Hizmeti ve VPN İstemcisi. Bu belge, tedarik ve gizlilik değerlendirme ekiplerinin yukarıda bahsedilen Forcepoint ürün ve hizmetleriyle ilgili bilgiye dayalı kararlar verebilmesi için gereken bilgileri sağlama amacını taşımaktadır.

Genel Veri Koruma Yönetmeliği (GDPR)

Forcepoint ürün ve hizmetleri, Genel Veri Koruma Yönetmeliğinde (GDPR) (Yönetmelik (EU) 2016/679) belirtilen gizlilik ilkelerine uyacak şekilde tasarlanmıştır. GDPR ilkelerine uygun şekilde, Forcepoint müşterileri yegane veri kontrolörleri olarak değerlendirilmektedir. Forcepoint; Forcepoint NGFW, SMC, ECA, Kullanıcı Kimliği Hizmeti ve VPN İstemcisi ürün ve hizmetlerinde depolanan müşteri verilerinin veri kontrolörü veya veri işleyicisi değildir. GDPR hakkında daha fazla bilgiye https://ec.europa.eu/info/law/law-topic/data-protection/reform_en adresinden erişebilirsiniz.

Kişisel Veriler

Bu belge, GDPR'nin 4.1 maddesinde bulunan ve "kişisel verileri", kimliği belli olan veya belirlenebilecek doğal bir kişiye ('Veri sahibi') ait tüm bilgiler olarak tanımlayan kişisel veri tanımını uygulamaktadır; kimliği belirlenebilecek gerçek kişiler, kimlikleri isim, kimlik numarası, konum verisi, çevrimiçi tanımlayıcı veya o kişinin fiziksel, fizyolojik, genetik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özel diğer faktörler dahil ancak bunlarla sınırlı olmamak üzere belli bir tanımlayıcı yoluyla doğrudan veya dolaylı olarak belirlenebilecek kişilerdir.

Kişisel Verilerin Korunması

Forcepoint, ürünlerinde bulunan ve kişisel verileri de içeren verileri korumak için endüstri standardı olan teknikleri kullanmaktadır. Veri güvenliği konusundaki bu yaklaşım, yüksek riskli verilerin erişim yetkisi olmayan kişilerce okunamamasını sağlamaktadır. Forcepoint'in gizlilik politikası ve süreçlerine ilişkin tüm ayrıntılar şu adreste bulunabilir: https://www.forcepoint.com/forcepoint-privacy-hub.

Sorumluluk Reddi:

Bu belge, Forcepoint ürün ve/veya hizmetlerine ilişkin bilgiler içermektedir. Bu bilgiler, Forcepoint'e aittir. İçeriğin güncel ve doğru olması için her türlü çaba gösterilmiş olsa da bilgiler açık veya zımni herhangi bir garanti verilmeden, *olduğu gibi* sunulmaktadır ve bildirimde bulunulmadan değiştirilebilir.

Gelecekteki sürümlere veya işlevlere ilişkin atıflar tahmin niteliğindedir ve taahhüt olarak değerlendirilmemelidir. Forcepoint, bu bilgilerin kullanımı konusunda hiçbir sorumluluk kabul etmez.

Kimlik ve Politika

Veri Kümesi	Hangi Kişisel Veriler Kullanılıyor?	Amaç	Veri Durumu	Depolama, Akış ve Koruma	Saklama
Yönetici hesapları	SMC kurulurken, bir süper kullanıcı hesabı oluşturulur. Bu hesap, kurulumdan sonra yönetici hesaplarını oluşturmak için kullanılır. Müşterilerin sertifikalı kimlik doğrulama kullanmayı tercih etmeleri halinde, yöneticilerin kimliğini belirlemek için e-posta adresi gibi bir tanımlayıcı kullanılır.	Farklı erişim seviyelerine sahip olan yöneticiler, SMC'de kendilerine atanan yönetici rollerine göre farklı görevleri yerine getirebilir.	Veriler anonimleştirilmemektedir	Kullanıcı adları ve SMC tarafından yönetici şifreleri için oluşturulan SHA-512 komutları müşterilerin ürünün şirket içindeki/dahili ağ kurulumunda veya Forcepoint dışındaki kendi bulut çözümlerinde saklayacakları Yönetim Sunucusu veri tabanında saklanmaktadır.	Müşteri, yönetici hesaplarını manuel olarak silebilir.
Dahili LDAP kullanıcı veri tabanı	SMC'de bulunan dahili LDAP kullanıcı veri tabanı, kullanıcı adlarını ve kullanıcı şifrelerinin hash değerlerini içerir. Sertifikalı kimlik doğrulama kullanılıyorsa kullanıcıların kimliğini belirlemek için e-posta adresi gibi bir tanımlayıcı kullanılır.	Kullanıcı hesapları, kimlik doğrulama ve ağ erişimi kontrolü için kullanılabilir.	Veriler anonimleştirilmemektedir	Kullanıcı adları ve kullanıcı şifrelerinin AES komutları, Yönetim Sunucusunun dahili LDAP kullanıcı veri tabanında saklanır. Bu bilgiler, endüstri standardındaki TLS korumalı bir bağlantıyla NGFW Motorlarına kopyalanabilir. Müşteri, bu verilere, işletim sistemine erişim izni sağlayan bir hesabı kullanarak erişebilir.	Müşteri, kullanıcı hesaplarını manuel olarak silebilir.

Veri Sahibi Erişim Talepleri (SAR) Nasıl Yönetilir?

SAR - Erişim Hakkı	Müşteri tarafından atanan SMC süper kullanıcı yöneticisi, SMC sunucu yapılandırmasında depolanan SMC kullanıcı hesapları veritabanındaki yönetici ve kullanıcı hesabı verilerine erişebilir ve bunları yönetebilir (ekleme/değiştirme/silme yapabilir).
SAR - Düzeltme	SMC süper kullanıcı yöneticisi, SMC sunucu yapılandırmasında depolanan SMC kullanıcı hesapları veritabanındaki yönetici ve kullanıcı hesabı verilerine erişebilir ve bunları yönetebilir (ekleme/değiştirme/silme yapabilir).
SAR - Unutulma Hakkı	Süper kullanıcı yöneticisi, SMC sunucu yapılandırmasında depolanan SMC kullanıcı hesapları veritabanındaki yönetici ve kullanıcı hesabı verilerini silebilir. Tüm SMC yöneticilerinin eylemleri, belirli bir yönetici hesabına göre filtrelenip silinemeyen denetim kayıtlarında toplanır ve saklanır.
Veri Depolama/Yerelleştirme	NGFW ve SMC kullanıcı ve yönetici hesabı verileri, müşterinin yönetimli sunucularında saklanır.

Etkinlik Kayıtları

Veri Kümesi	Hangi Kişisel Veriler Kullanılıyor?	Amaç	Veri Durumu	Depolama, Akış ve Koruma	Saklama
Kayıt sunucusunda depolama (Erişim, inceleme ve uyarı kayıtları ve sayaç verilerini içerir)	Varsayılan olarak, erişim kayıtlarında kişisel veriler kaydedilmez. Ancak, müşteriler IP adresi, URL, kullanıcı adı ve uygulamalar hakkında bilgi içeren erişim verilerini kaydedecek şekilde NGFW Motorlarını yapılandırabilir. Bu veriler, istatistik toplamak gibi çeşitli amaçlarla kullanılabilir. Ayrıntılar için bkz. TABLO 1: SMC'deki Erişim Kayıtlarına ilişkin Kişisel Veri Özellikleri, Ek A.	Ağ trafiğini takip etmek ve raporlar oluşturmak için	Veriler anonimleştirilmektedir	Erişim kayıtları, Kayıt Sunucusu disklerinde, özel bir formatta saklanmaktadır. Veriler, endüstri standardındaki TLS korumalı bir bağlantıyla NGFW Motorlarından alınır. Elasticsearch entegrasyonu yapılandırıldığında, SMC; SMC kayıtlarının endekslenmesine ilişkin yetkiyi, müşteri tarafından yönetilen yerel bir ElasticSearch veri tabanı örneğine devredebilir. Bu, müşterinin kayıtlar içinde daha hızlı sorgular yapmasına ve SMC kullanıcı arayüzünden şeffaf istatistik raporlar almasına imkan sağlar. Müşteri, bu verilere, NGFW işletim sistemine erişim izni veren bir hesabı kullanarak erişebilir.	Müşteri, SMC ve/veya SMC programlanmış görev işlevini kullanarak takip faaliyetlerine ilişkin kayıt verilerini manuel veya otomatik olarak silebilir veya arşivleyebilir.
Denetleme günlükleri	Denetleme günlükleri, yönetici hesap adlarını ve istemci iş istasyonlarının IP adreslerini içerir. Ayrıntılar için bkz. TABLO 2: SMC'deki Denetleme Günlüklerine ilişkin Kişisel Veri Özellikleri, Ek A.	Yönetici eylemlerini denetlemek için	Veriler anonimleştirilmektedir	Denetleme günlükleri, Yönetim Sunucusu ve Kayıt Sunucusu disklerinde, özel bir formatta saklanmaktadır. Veriler, TLS korumalı bir bağlantıyla NGFW Motorlarından alınır. Müşteri, bu verilere, işletim sistemine erişim izni sağlayan bir hesabı kullanarak erişebilir.	Müşteri, SMC ve/veya SMC programlanmış görev işlevini kullanarak denetleme günlüğü verilerini manuel veya otomatik olarak silebilir veya arşivleyebilir.
Programlanmış raporlar	Raporlar, kayıt verilerinden alınan ve müşterinin kayıt yapılandırmasına bağlı olarak kişisel verileri içerebilen istatistiklerin sunulması için kullanılır.	Ağ trafiği olayları hakkında raporlar oluşturmak ve/veya müşterinin raporlama ihtiyaçlarını karşılamak için	Veriler anonimleştirilmektedir	Raporlar, Yönetim Sunucusu disklerinde, özel bir formatta saklanmaktadır. Müşteri, bu verilere, işletim sistemine veya SMC'nin yönetim arayüzlerine erişim izni sağlayan bir hesabı kullanarak erişebilir.	Müşteri, rapor tasarımlarında raporların son kullanılma tarihini tanımlayabilir. Varsayılan son kullanılma tarihi 10 gündür.
Windows uç noktalarında ECA hata ayıklama döküm kayıtları	ECA hata ayıklama döküm kayıtlarında bulunan veriler, o anda uç noktada oturum açmış olan kullanıcıların ve alan adlarının yanı sıra, işletim sistemi, CPU türü, boş ve toplam fiziksel bellek, boş ve toplam disk alanı ve kurulu uygulamalar gibi bazı temel bilgileri içerir.	Müşteriler adına teknik sorunların çözülmesi için.	Veriler anonimleştirilmektedir	Müşteriler, hata ayıklama döküm kayıtlarını ECA kurulum klasörü altında saklamalıdır.	Hata ayıklama döküm kayıtları, 2 MB boyutundaki dosyalarda saklanır. Saklanabilecek maksimum kayıt verisi miktarı 10 MB olduğundan, sistem 5 adede kadar 2 MB'lik dosyayı saklayabilir. Maksimum kayıt dosyası sayısına erişildiğinde, sistem en eski dosyayı silerek, yeni kayıt veri dosyaları için yer açar

Veri Sahibi Erişim Talepleri (SAR) Nasıl Yönetilir?

SAR - Erişim Hakkı	NGFW yöneticileri, SMC kayıt ve rapor verilerine SMC Yönetimi Arayüzünden erişebilir ve bu verileri yönetebilir.
SAR - Düzeltme	NGFW ve SMC, güvenlik ve denetim amacıyla saklanan kayıt verilerinin düzenlenmesini (düzeltme) engelleyecek şekilde tasarlanmıştır.
SAR - Unutulma Hakkı	NGFW ve SMC süper kullanıcı yöneticisi, belirli bir kullanıcı kimliğine göre (ör. kullanıcı adı, kullanıcı hesap kimliği) seçilen kayıtları filtreleyebilir ve silebilir. Tüm SMC yöneticilerinin eylemleri, belirli bir yönetici hesabına göre filtrelenip silinemeyen denetim kayıtlarında toplanır ve saklanır.
Veri Depolama/Yerelleştirme	NGFW müşterisi, NGFW ve SMC kurulumlarının ve veri sunucularının konumunu seçer ve yönetir.

Ek Modüller

Veri Kümesi	Hangi Kişisel Veriler Kullanılıyor?	Amaç	Veri Durumu	Depolama, Akış ve Koruma	Saklama
Gelişmiş Kötü Amaçlı Yazılım Tespiti (AMD)	AMD, kötü amaçlı yazılım analizinden geçirilecek dosyaları NGFW ürününden alır. AMD, dosyayı aldıktan sonra, kötü amaçlı yazılım içerip içermediğini belirlemek için dosyanın analizini yapar. AMD tarafından analiz edilmek için yüklenen dosyalar, kişisel veri içerebilir. Müşteri yöneticisi, hangi dosya türlerinin AMD'ye gönderileceğini belirleyebilmektedir.	Gönderilen dosyanın tamamının kötü amaçlı yazılım riski içerip içermediğini anlamak için.	Dosyaların sonuçları, gönderilen dosyanın bir SHA-1 sağlama komutu oluşturularak ve analiz sonucu sağlama dosyasıyla ilişkilendirilerek anonim hale getirilir. Analiz tamamlandığında, dosya ve tüm içeriği derhal silinir.	Gelişmiş Kötü Amaçlı Yazılım Tespiti çözümü, kötü amaçlı yazılım analizinin, AMD tarafından oluşturulan sağlama dosyasına bağlanan sonucunu depolar. Analiz tamamlandığında, gönderilen dosya derhal silinir. Analiz, analiz edilen dosyanın boyutuna ve türüne bağlı olarak 10 saniye ile 5 dakika arasında sürebilir. Dosya, AMD'ye endüstri standardındaki bir TLS şifreli kanal üzerinden gönderilir. AMD'nin analiz özellikleri dış kaynaktan temin edilmektedir. Analiz, Los Angeles/ABD ve Amsterdam/Hollanda olmak üzere iki veri merkezinde gerçekleşmektedir. Müşteriler, kullanacakları veri merkezini seçebilir veya "Otomatik" seçeneğini kullanarak DNS çözümleyici talebinde bulunan halka açık NGFW IP adresine coğrafi olarak en yakın veri merkezinin kullanılmasını sağlayabilir.	Gelişmiş Kötü Amaçlı Yazılım Tespiti çözümü, gönderilen dosyayı saklamaz. AMD, dosyaların analiz sonuçlarını süresiz olarak saklar. Ayrıca, analiz sırasında kötü amaçlı bir kod tespit edilirse bu kötü amaçlı kod (kötü amaçlı olgu) da süresiz olarak saklanır.
Kullanıcı Kimliği Hizmeti	Kullanıcı ve IP adresi çiftleri. Ayrıntılar için bkz. TABLO 3: Forcepoint Kullanıcı Kimliği Hizmetine ilişkin Kişisel Veri Özellikleri, Ek A.	Kullanıcı IP adresleri ve kullanıcı grupları arasındaki ilişkileri çözmek için.	Veriler anonimleştirilmemektedir	Veriler, dahili veri tabanında açık bir metin dosyasında saklanır. Müşteriler, istedikleri bir şifreleme sistemiyle veri tabanını şifreleme seçeneğine sahiptir. Veri tabanı; kullanıcı adı, e-posta adresi, grup üyelikleri ve mevcut IP adresi gibi kullanıcıya özel Active Directory özelliklerinden oluşan bir alt kümeyi içerir. Bu verilere erişim için işletim sistemine erişim izni veren bir hesap gereklidir. UID Hizmetinin API'si ağdan bu veriler için kimliği doğrulanmamış sorgular yapılmasına izin verir. İşletim sisteminin güvenlik duvarı, ağdan API'ye erişimi kontrol etmek için kullanılabilir.	Kullanıcı ve IP adresi çiftlerine ilişkin veriler, 6 saat boyunca saklanır. Müşteri, verileri silmek için Forcepoint Kullanıcı Kimliği Hizmetini kaldırabilir.
Windows için VPN İstemcisi	VPN'de kimlik doğrulama yöntemi olarak e-posta adreslerini içeren bir sertifika kullanılıyorsa VPN İstemcisi kayıt verileri kullanıcıların e-posta adreslerini içerir.	NGFW üzerinden müşterilerin VPN kullanımları kaydedilir ve ayrıca müşterilerin teknik sorunlarını çözmek için de kullanılabilir.	Veriler anonimleştirilmemektedir	VPN İstemcisi kayıt verileri, VPN İstemcisi veri klasörünün altındaki düz metin dosyalarında saklanır (varsayılan olarak, C:\ProgramData\Forcepoint\Stonesoft VPN Client\log veya C:\ProgramData\Forcepoint\VPN Client\log).	Yeni kayıt verileri oluşturulduğunda, VPN İstemcisi kayıt verisi dosyalarında bulunan verilerin otomatik olarak üzerine yazılır. Verileri silmek için Windows VPN İstemcisini kaldırın, ardından manuel olarak dosyaları VPN İstemcisi veri klasöründen silin.

Yeni Nesil Güvenlik Duvarıyla birlikte kullanılabilen veya entegre edilebilen aşağıdaki ürünler, kişisel verileri yerel olarak saklamamaktadır:

- Forcepoint Android VPN İstemcisi
- Forcepoint Mac VPN İstemcisi

Veri Sahibi Erişim Talepleri (SAR) Nasıl Yönetilir?

SAR - Erişim Hakkı	AMD: NGFW müşterileri, korumalı alan kayıtlarına müşteri AMD portalı hesabından ve dosya filtreleme kayıtlarında bulunan “Tarama raporu” bağlantılarından erişebilir. AMD’ye özel ek veri koruma ve raporlama ayrıntıları için Forcepoint AMD ürün destek belgelerine bakılmalıdır. Kullanıcı Kimliği hizmeti: Forcepoint Kullanıcı Kimliği (FUID) hizmetinde bulunan kullanıcı verileri, doğrudan NGFW müşterisi tarafından yapılandırılan Microsoft Active Directory’den (AD) içe aktarılır. FUID kullanıcı verilerine erişmek ve bu verileri yönetmek (ekleme/değiştirme/silme) için NGFW – FUID yönetici hesabı ve müşterinin Microsoft AD yönetim araçları kullanılır.
SAR - Düzeltme	FUID, doğrudan müşterinin Microsoft Active Directory (AD) sisteminden içe aktarılan kullanıcı verilerini Microsoft AD’de göründükleri şekilde saklar. Kullanıcı verilerindeki düzeltmeler, Microsoft AD’de yapılmalı ve veriler tekrar FUID’ye aktarılmalıdır.
SAR - Unutulma Hakkı	FUID hizmetlerinin kaldırılması, tüm kullanıcı verilerinin otomatik olarak silinmesini sağlar.
Veri Depolama/Yerelleştirme	NGFW müşterisi, FUID kurulumunun ve veri sunucusunun konumunu seçer ve yönetir.

EK A

Terminoloji

Terim	Açıklama
Yeni Nesil Güvenlik Duvarı (NGFW)	Yeni Nesil Güvenlik Duvarı çözümü, Yeni Nesil Güvenlik Duvarı Motorlarını, SMC sunucu bileşenlerini ve SMC kullanıcı arayüzü bileşenlerini içerir.
Güvenlik Yönetimi Merkezi (SMC)	SMC, Yeni Nesil Güvenlik Duvarı çözümünün yönetim bileşenidir. SMC, sistemdeki diğer bileşenleri yönetir ve kontrol eder.
Yönetim Sunucusu	Yönetim Sunucusu, sistem yönetiminin merkezi bileşenidir.
Günlük Sunucusu	Günlük Sunucuları, yönetilip rapor haline getirilebilen trafik kayıtlarını saklar. Günlük Sunucuları ayrıca olaylar arasındaki ilişkileri tanımlar, NGFW Motorlarının durumunu takip eder, gerçek zamanlı istatistikleri görüntüler ve günlükleri üçüncü taraf cihazlara aktarır.
Yeni Nesil Güvenlik Duvarı Motorları (NGFW Motorları)	Yeni Nesil Güvenlik Duvarı Motorları, trafiği denetler. Kaynaklara erişim kontrolünün yapılandırılması ve kullanıcı ve yönetici eylemlerinin takip edilmesi için kullanılırlar. Güvenlik Duvarı/VPN rolündeki Yeni Nesil Güvenlik Duvarı Motorları, ayrıca VPN ağ geçidi olarak da kullanılabilir.
Gelişmiş Kötü Amaçlı Yazılım Tespiti (AMD)	Forcepoint AMD, dosyaların davranışlarını analiz ederek gelişmiş tehditleri tespit eder. NGFW Motorları, dosyaları analiz için AMD'ye gönderecek şekilde yapılandırılabilir.
Uç Nokta Bağlam Aracısı (ECA)	ECA, Windows uç nokta istemcileri için bağlantı başına kullanıcı ve uygulama bilgilerini toplar. SMC tarafından yönetilen bir NGFW Motoru aracılığıyla bağlanan Windows uç nokta istemcilerine ilişkin kullanıcı ve uygulama bilgilerini almak için ECA'yı Forcepoint NGFW ile entegre edebilirsiniz. Bu bilgileri, erişim kontrolü ve takip için kriter olarak ve rapor oluşturmak amacıyla kullanabilirsiniz.
Forcepoint Kullanıcı Kimliği Hizmeti (FUID)	Forcepoint Kullanıcı Kimliği Hizmeti, Windows Active Directory (AD) ve Microsoft Exchange Sunucularından kullanıcılar, gruplar ve IP adreslerine ilişkin bilgileri toplar. Forcepoint Kullanıcı Kimliği Hizmetini Forcepoint NGFW ile entegre edebilir ve Forcepoint Kullanıcı Kimliği Hizmetinin sağladığı bilgileri kullanıcıları takip etmek ve erişim kontrolünü yapılandırmak için kullanabilirsiniz.

Kişisel Veri Özellikleri

TABLO 1: SMC'deki Erişim Kayıtlarına ilişkin Kişisel Veri Özellikleri

Ağ erişimi bilgilerinin alınmasını ve olay denetim yollarının incelenmesini imkansız hale getirerek en iyi güvenlik uygulamalarına engel olacağından, bu veri kümesindeki kişisel veriler anonimleştirilemez, ancak bu kayıtların toplanması isteğe bağlıdır.

Özellik	Gereksinim
IP adresi	İsteğe bağlı
Kullanıcı oturum açma adı ve etki alanı	İsteğe bağlı

TABLO 2: SMC'deki Denetleme Günlüklerine ilişkin Kişisel Veri Özellikleri

Güvenlik politikasının doğru işlemesini önleyeceğinden, bu veri kümesindeki kişisel veriler anonimleştirilemez. Denetleme günlükleri devre dışı bırakılamaz; ancak SMC programlı kayıt yönetimi görevleri kullanılarak veya diskteki kayıt verileri silinerek ortadan kaldırılabilirler.

Özellik	Gereksinim
Yönetici oturum açma adı	Zorunlu
Yönetici istemci IP adresi	Zorunlu

TABLO 3: Kullanıcı Kimliği Hizmetine ilişkin Kişisel Veri Özellikleri

Bu veri kümesindeki kişisel veriler, yapılandırılan Microsoft Active Directory ortamından kopyalanır ve AD'den kaldırıldığı anda otomatik olarak silinir. Ağ erişimi politikasında kullanıcıların eşleştirilmesini önleyerek en iyi güvenlik uygulamalarına engel olacağından, bu veri kümesindeki kişisel veriler anonimleştirilemez. FUID sunucusunun kaldırılması, FUID kurulumunda ön belleğe alınan tüm verilerin de silinmesini sağlayacaktır.

Özellik
Kullanıcı oturum açma adı ve etki alanı
Kullanıcı AD grubu üyelikleri
Kullanıcı IP adresi (AD Domain Controller tarafından görüldüğü şekliyle)
Kullanıcı e-posta adresi