CHECK POINT™

Infinity Threat Exposure Management

Bu Gizlilik Veri Sayfası, Check Point'in Infinity Threat Exposure çözümünün kişisel verileri nasıl işlediğini açıklamaktadır.

Infinity Threat Exposure Management Hakkında

Check Point'in Infinity Threat Exposure çözümü, Proaktif Maruziyet Yönetimi (PEM) sunar. Kurum içi ve bulut ortamlarında tüm güvenlik yığını genelinde riskleri proaktif olarak tespit eder, önceliklendirir ve giderir.

Mevcut güvenlik çözümlerinizle verimli bir şekilde entegre olarak operasyonel siloları ortadan kaldırabilir, maruziyetler üzerinde birleşik görünürlük elde edebilir ve kesintisiz iş operasyonlarını sürdürürken güvenlik açıklarını ve yanlış yapılandırmaları proaktif olarak ele alabilirsiniz.

Check Point Geçerli Veri Koruma Düzenlemelerine Nasıl Uyum Sağlar?

1.Security. Son onlarca yıldır yapay zekâ destekli, bulut üzerinden sunulan bir siber güvenlik platformunun önde gelen sağlayıcılarından biri olarak, müşterilerimizin bilgilerini korumak amacıyla sıkı güvenlik önlemlerinin uygulanmasının öneminin farkındayız. Daha fazla bilgi için Information Security Measures Policy sayfamızı ziyaret edebilirsiniz.

2.Privacy by Design. Tasarımda gizlilik ilkesine göre faaliyet göstermekteyiz. Bu, ürün ve hizmetlerimizin tüm yaşam döngüsü boyunca kişisel verilerin ve gizliliğin korunmasına öncelik verdiğimiz anlamına gelir. Kişisel verileri azami özenle ele alırız. Gizliliğe olan bağlılığımız; politikalarımıza, prosedürlerimize ve iş yapış biçimimize yansımaktadır. Daha fazla bilgi için Privacy Policy ve Trust Point sayfalarımızı ziyaret edebilirsiniz.

3.Disaster Recovery. Felaket kurtarma ve iş sürekliliği için kapsamlı planlar ve prosedürler bulundurmaktayız.

4.Transfers. Check Point kuruluşları arasında kişisel veri aktarımını düzenlemek amacıyla Check Point, farklı Check Point kuruluşları arasındaki veri aktarımını kapsayan şirketler arası sözleşmeleri benimsemiştir. Bunlar arasında AB Standart Sözleşme Maddeleri ve AB Standart Sözleşme Maddelerine ilişkin Birleşik Krallık Uluslararası Veri Aktarım Ek'i bulunmaktadır. Check Point'in ABD'deki bağlı kuruluşu olan Check Point Software Technologies, Inc. (ve bağlı şirketleri), AB-ABD Veri Gizliliği Çerçevesi, AB-ABD Veri Gizliliği Çerçevesi'nin Birleşik Krallık Uzantısı ve İsviçre-ABD Veri Gizliliği Çerçevesi (DPF) kapsamında uyumluluğunu kendi kendine sertifikalandırmıştır.

Infinity Threat Exposure Management Hangi Tür Kişisel Verileri İşler?

Infinity Threat Exposure aşağıdaki bilgileri işler:

• Kuruluş yöneticilerinin ve platform kullanıcılarının (müşteri tarafından tanımlandığı şekilde) iletişim bilgileri; örneğin kurumsal e-posta adresi.

Infinity Threat Exposure, hizmetin sağlanmasının bir parçası olarak ve kişisel veri niteliği taşıdığı ölçüde aşağıdaki bilgileri de işleyebilir:

• Müşteri tarafından yapılandırılan güvenlik kontrollerinde yer alan bilgiler; örneğin IP adresleri, kullanıcı adları, profiller veya DNS bilgileri — bu veri unsurlarının tanımlanabilir bir bireyle ilişkili olması durumunda.

• Tespit edilen bir zafiyet veya tehditle ilişkilendirildiğinde ana makinenin IP adresi.

• Zafiyet içeren örneğin adı; söz konusu adın kişisel veri içermesi durumunda (müşteri yapılandırmasına bağlı olarak).

Infinity Threat Exposure Management Kişisel Verileri Neden İşler?

Infinity Threat Exposure, aşağıdaki yeteneklerini desteklemek amacıyla kişisel verileri işler:

• **Çok üreticili ortamlarda güvenlik risklerini sürekli olarak tespit etmek** ve gidermek; buna güvenlik duvarları, uç noktalar, WAF'lar ve bulut platformları dâhildir.

• Uzlaşma göstergelerini (IoC'ler) tespit edip doğrulayarak ve güvenlik yığını genelinde korumalar uygulayarak **gerçek zamanlı tehdit istihbaratını** hayata geçirmek.

• Her müşterinin ortamına uygun, güvenli ve bağlama duyarlı **otomatik iyileştirme sağlamak.**

Bu işleme faaliyetleri, Infinity Threat Exposure çözümünün entegre sistemler genelinde proaktif, kesintisiz güvenlik kapsaması ve sanal yama (virtual patching) sağlayabilmesi için gereklidir.

Kişisel verileri hangi amaçlarla işlediğimiz hakkında daha fazla bilgi için lütfen Privacy Policy sayfamızı ziyaret edin.

Sıklık Nedir?

Şirket içi (on-premises) bir dağıtım olarak, veri paylaşımının etkinleştirildiği durumlarda ve abonelik süresi boyunca, kişisel veriler müşterinin takdirine bağlı olarak Infinity Threat Exposure ile paylaşılır.

Saklama Süreleri Nelerdir?

Veri Türü	Saklama Süresi
Yöneticilerin iletişim bilgileri	Abonelik süresi
Tespit edilen bir zafiyet veya tehditle ilişkilendirilebilecek kişisel veriler	14 gün

Kişisel Veriler Nerede Saklanır?

Kişisel verilerin paylaşıldığı durumlarda, bu veriler Amerika Birleşik Devletleri'ndeki sunucularda saklanabilir.

Alt Veri İşleyenler

Check Point, ürün ve hizmetlerinin sağlanması kapsamında üçüncü taraf Alt Veri İşleyenlerle çalışmaktadır. Alt Veri İşleyenlerin listesine Sub-Processors Page üzerinden ulaşabilirsiniz.

Gizlilik Seçenekleri

Müşterilerimizin veri ve gizlilik tercihlerini belirleyebilmesini sağlamak amacıyla aşağıdaki araçları sunuyoruz:

- Müşterinin tercihine göre kullanıcıların belirli verilere erişiminin kısıtlanması.
- Müşterinin tercihine göre Check Point'e tanılama raporlamasının devre dışı bırakılması.

Kişisel verilere yetkili erişim

Müşteri Erişimi

Verilere erişim, müşterinin sistem yöneticisi tarafından kontrol edilir ve müşteri tarafından yönetilir.

Check Point Erişimi

- Şirket içi (on-premises) dağıtımlarda Check Point'in müşteri verilerine erişimi bulunmaz.
- Veri paylaşımının müşteri tarafından etkinleştirildiği durumlarda, bu verilere erişim yalnızca yetkili temsilcilerle sınırlıdır ve sadece kendilerine verilen görevleri yerine getirmek için gerekli olduğu ölçüde sağlanır.