

— 5651 LOG SAKLAMA VE DELİL PLATFORMU

LogHane

FortiGate loglarınızın noteri: mühürlü, damgalı, silinemez

LogHane, FortiGate loglarını toplar, her saati SHA-256 zinciriyle mühürler, günlük Merkle köküne RFC 3161 zaman damgası alır ve saklama süresi boyunca nesne kilitli arşivde tutar. Savcılık ya da mahkeme istediğinde, bağımsız doğrulayıcısıyla birlikte delil paketi tek tıkla hazırlanır.

ÖNE ÇIKANLAR

01

Kurcalanamaz arşiv

Saatlik hash zinciri, günlük Merkle kökü ve S3 Object Lock (COMPLIANCE): saklama bitmeden yönetici de silemez.

02

Hazır delil paketi

ZIP ya da CD/DVD'ye yazılabilir ISO; doğrulama raporu, teslim tutanağı ve internetsiz çalışan verify.py.

03

O IP'yi kim kullandı?

NAT, DHCP, misafir girişi, AD ve CGNAT port bloğunu birleştirip belirli bir anda IP'nin sahibini bulur.

04

Bulutta ya da kurum içinde

Marta Teknoloji bulutunda sunucusuz çalışır ya da kendi Linux sunucunuza tek betikle kurulur.

KİMLER İÇİN

Personeline ya da misafirine internet sunan şirketler, okullar ve kamu kurumları

Otel, kafe, AVM ve hastane gibi misafir Wi-Fi işletmeleri

Erişim, vekil ve yer sağlayıcılar

Çok şubeli yapıları ve müşterilerini tek panelden yöneten BT hizmet sağlayıcıları

Özellikler 90 ÖZELLİK

Aşağıdaki liste ürünün mevcut sürümünde çalışan özellikleri modül modül gösterir.

Log toplama ve cihaz yönetimi 10

- FortiGate loglarını 514/udp, 514/tcp ve TLS ile 6514/tcp (RFC 5425) üzerinden toplar
- İsteğe bağlı mTLS: cihaz kendi sertifikasıyla kimliğini aktarım katmanında da kanıtlar
- Cihazı IP'den değil seri numarasından tanır; NAT arkasındaki cihazlar karışmaz
- Yeni cihaz onay bekler; seri numarasını önceden tanımlarsanız doğrudan doğru kuruma düşer
- Panel, cihaza özel FortiGate syslog, filtre ve politika komutlarını hazır üretir
- Salt okunur REST API bağlantısı: DHCP kiralari, WAN IP, model, FortiOS sürümü ve config yedeği
- Cihaz listesinde syslog, API ve DHCP ajanı durumları rozetle; son görülme ve EPS takibi
- Windows Server ve ISC dhcpd/Kea için salt okunur DHCP ajanı; anahtar cihaz bazında üretilir
- Geçmiş FortiGate log dosyalarını içe aktarma: düz metin, .gz ya da .zip, dosya başına 512 MB'a kadar
- Tek ekrandan cihaz seçimi: bütün analiz ekranları seçilen cihaza daralır

5651 uyum ve mühürleme 12

- Yükümlülük profili: erişim/vekil sağlayıcı 365 gün, yer sağlayıcı ve toplu kullanım 730 gün saklama
- Profile göre zaman damgası zorunluluğu ve URL toplama kuralı otomatik belirlenir
- Her saat bir segment mühürlenir; SHA-256 özeti bir öncekine zincirlenir
- Günlük Merkle kökü RFC 3161 zaman damgası alır; yerleşik TSA ya da Kamu SM gibi bir ESHS
- TSA'ya ulaşılamazsa damga kuyruğa alınır ve alarm üretilir; sessizce atlanmaz
- Zincir 30 dakikada bir doğrulanır; kırık halka ve gölgeleme ayrı ayrı bildirilir
- Mühürlü arşiv S3 Object Lock COMPLIANCE kipinde; kilit her hedefte yazıp geri okunarak ölçülür
- Uyum Durumu ekranı: kontrol listesi, zincir ve damga durumu tek bakışta
- Süresi dolan kayıtlar parçaları ve tüm sürümleriyle imha edilir; imha tutanağı indirilir
- Saklama penceresi içinde arşivi olan kurumun silinmesi reddedilir ve denetim izine yazılır

- WAN IP değişikliği takibi, 15 günlük bildirim geri sayımı ve 'bildirildi' işaretleme
- URL kaydı varsayılan kapalı; açmak için hukuki gerekeç girilir, kapalıyken yalnızca alan adı saklanır

Delil paketi ve denetim 8

- Tarih aralığı seçerek delil paketi: ZIP ya da doğrudan CD/DVD'ye yazılabilir ISO 9660
- Pakette düz metin loglar, log formatı açıklaması (PDF), arşiv dosyaları, zaman damgaları ve manifest
- Doğrulama raporu ve teslim tutanağı şablonu PDF olarak pakete eklenir
- LogHane kurulu olmadan, internetsiz çalışan bağımsız doğrulayıcı; insan ya da makine okunur çıktı
- Doğrulama üç sonuç verir: geçerli, uyarılı geçerli, geçersiz; eksik segmentler ayrıca işaretlenir
- İndirme 5 dakika geçerli imzalı bağlantıyla yapılır; her indirme denetim izine yazılır
- Denetim İzi: kim neyi ne zaman sorguladı, kendi hash zincirinde
- KVKK ilgili kişi başvurusu ekranı ve denetim komisyonu özeti

Kimlik çözümleme ve rehber 8

- 'O anda bu IP'yi kim kullanıyordu?': NAT, DHCP, hotspot ve AD oturumlarıyla korelasyon
- CGNAT'ta kaynak port girilerek port bloğundan tekil abone bulunur; tekil değilse uyarı verilir
- Sorgu, sorulan ana en yakın kayıtları döndürür ve sınır aşılırsa bunu açıkça bildirir
- Kimlik kapsamı: trafiğin ne kadarında kimlik var ve hangi kaynaktan geliyor
- IP başına birleşik kimlik haritası; çelişkili eşleşmeler gizlenmez, işaretlenir
- FortiGate FSSO etki alanı oturumlarından IP ↔ kullanıcı eşleşmesi
- Rehber: statik IP'li sunucu, yazıcı, kamera için etiket; CSV içe ve dışa aktarma
- Active Directory rehber eşitlemesi: ad soyad, birim, unvan, e-posta, telefon (varsayılan 6 saatte bir)

Misafir interneti (Hotspot) 9

- Mobil uyumlu captive portal; FortiGate harici captive portal ile otomatik geri yönlendirme
- Giriş yöntemleri: SMS kodu, T.C. kimlik no, pasaport no, oda no + soyadı, LDAP/AD hesabı
- SMS kodu varsayılan 6 hane, 180 saniye geçerli; portal profilinden ayarlanır
- Hazır SMS sağlayıcıları: NetGSM, Verimor, İleti Merkezi, Vatan SMS ve özel HTTP; test düğmesi
- Kimlik numarası açık saklanmaz, kuruma özel tuzlu özet tutulur
- MAC ya da telefon numarasıyla beyaz/kara liste; toplu ekleme ve silme
- Oturum kayıtları: kimlik ↔ IP ↔ MAC ↔ zaman; numaralar maskeli, oturum tek tek ya da toplu sonlandırılır
- Versiyonlu KVKK aydınlatma metni; hangi misafirin hangi sürümü gördüğü kaydedilir
- Yerleşik RADIUS sunucusu 1812/1813 (RFC 2865/2866): Ubiquiti, Mikrotik, Aruba gibi erişim noktaları için

Log arama ve trafik analizi 12

- Genel Bakış: KPI'lar, EPS grafiği, trafik ve tehdit özeti, cihaz sağlığı, uyum durumu
- Log Gezgini: otomatik tamamlamalı sorgu çubuğu, facet filtreleri, histogramda aralık seçme
- Arama sonuçlarını CSV olarak dışa aktarma
- Canlı Akış: loglar anlık filtreyle ekrana akar
- Kullanıcılar: trafik, oturum, süre; MAC↔IP eşleşmesi, ziyaret edilen siteler ve uygulamalar, zaman çizelgesi
- Web ve Uygulamalar: kategori, site ve uygulama kırılımı; her satırdan 'kimler girdi' detayı
- Bant genişliği FortiGate delta sayaçlarından hesaplanır; uzun oturumlar trafiği şişirmez
- VPN Erişimi: SSL ve IPsec oturumları, başarısız girişler, uzak IP ve tünel tipleri
- Ülke Analizi: hedef ve kaynak ülke kırılımı, 'bu ülkeye kimler erişti' detayı
- DNS Analizi: alan adı sorguları, engellenenler ve şüpheli desenler
- Güvenlik: önem dağılımı, en sık saldırılar, tehdit ve engellenen trafik
- Kişisel veri gösteren her görüntüleme (kullanıcı ayrıntısı, kimlik sorgusu) denetim izine yazılır

Risk, danışman ve tehdit istihbaratı 10

- Saatlik sapma: her saat önceki günlerin aynı saatiyle ortanca/MAD ölçüsüyle kıyaslanır
- Yatay hareket, ısrarcı engellenen kaynaklar ve mesai dışı dışarı çıkış tespiti
- Kripto madencilik göstergeleri, kimlik doğrulama hataları ve ilişkilendirilmiş olaylar
- Her bulgu masum açıklamasıyla birlikte gösterilir; yön (içeriden/dışarıdan) ayrılır
- Saldırı yüzeyi ve kural denetimi: dışarıdan kabul edilen trafik, loglaması kapalı kurallar
- Kural denetimi bulguları için FortiGate düzeltme komut betiği indirilir
- Kural danışmanı izinleri gözlenen trafikle kıyaslar, gözlem penceresini belirtir, daraltma önerir
- Öneriyi kabul/ret, etki önizlemesi ve ayrı yazma yetkisiyle onaylanınca cihaza uygulama
- Tehdit listeleriyle eşleşme: AdGuard, EasyList, HaGeZi, hostsVN beslemeleri; 6 saatte bir eşitleme
- Listeler kategori bazında FortiGate dış kaynak (external resource) olarak yayımlanır; jeton yenilenebilir

Raporlar ve uyarılar 6

- 7 hazır rapor: Bant Genişliği, Kullanıcı Etkinlik, Web Kullanım, Güvenlik, Oturum, İzleme ve Sistem, 5651 Uyum
- Rapor oluşturucu: 11 hazır bölümden sıra ve satır sayısı sizde olan özel rapor
- Tüm raporlar PDF, XLSX ve CSV; günlük, haftalık ya da aylık zamanlama ve e-postayla gönderim
- Hazır uyarılar: log akışı kesintisi, damga kuyrukta, saat kayması, WAN IP değişikliği, disk baskısı
- Ek uyarılar: içerik filtresi devre dışı, engellemeden yalnızca izleyen IPS
- Bildirim kanalları: e-posta, webhook, syslog; kanal başına önem eşiği ve test gönderimi

Yönetim, güvenlik ve kurulum 15

- Çok kurumlu yapı: her kurumun verisi ayrı; bir kullanıcı birden fazla kuruma üye olabilir
- Roller: süperadmin, kurum yöneticisi, analist, denetçi (salt okunur + delil), izleyici
- TOTP iki adımlı doğrulama, tek kullanımlık kurtarma kodları; yönetici 2FA sıfırlayabilir
- Modüller kurum bazında açılıp kapatılır: risk, danışman, kara liste, DNS, hotspot, AD, rapor oluşturucu
- Kurulum sihirbazı: parola değişimi, kurum adı, yükümlülük profili, ilk cihaz, zaman damgası tercihi

- Depolama hedefleri: IDrive e2, AWS S3, Azure Blob, Google Cloud, Wasabi, Backblaze B2, MinIO, Cloudflare R2
- Her kurum ayrı depolama hedefine atanır; geçmiş, hedefte doğrulanarak taşınır
- Sistem sağlığı, veri akış hattı, veri kalitesi ve kapasite planlama ekranları
- Günlük otomatik yapılandırma yedeği (30 gün) ve arayüzden indirme
- Felaketten dönüş: seçilen aralık mühürlü arşivden analiz katmanına yeniden kurulur
- Bulut: kuruma özel cihaz sertifikası (PKCS#12) panelden üretilir; log TLS 6514 ile gelir
- Bulut paketleri: Tek (1 cihaz), Şube (3), Kurumsal (5), Zincir/MSP (10); modüller pakete göre
- Kurum içi: tek betikle Debian 12/13 ya da Ubuntu 22.04+ (amd64/arm64), güçlü sırlar ve TLS otomatik
- Üretim kipinde zayıf sırla açılmaz; HSTS ve CSP başlıkları, iç adreslere istek engeli
- Türkçe ve İngilizce arayüz

Teknik özellikler

Desteklenen cihaz	FortiGate (FortiOS 7.x; 6.x zaman damgası biçimi)
Log alımı	Syslog 514/udp, 514/tcp; TLS 6514 (RFC 5425), mTLS seçenekli
Cihaz verisi	Salt okunur FortiGate REST API: DHCP kiralari, WAN IP, config yedeği
Bütünlük	SHA-256 hash zinciri, günlük Merkle kökü, RFC 3161 zaman damgası
Arşiv	S3 Object Lock (COMPLIANCE); kilit yazılıp geri okunarak ölçülür
Depolama hedefleri	IDrive e2, AWS S3, Azure Blob, Google Cloud, Wasabi, Backblaze B2, MinIO
Sorgu ve arşiv	Son 30 gün hızlı sorgu, sonrası soğuk katman; ara tampon sayesinde bakımda log kaybı yok
Kimlik doğrulama	Parola + TOTP; misafirler için SMS, LDAP/AD, RADIUS (RFC 2865/2866)
Kurulum	Bulut ya da kurum içi; Debian 12/13, Ubuntu 22.04+ için tek kurulum betiği
Yedekleme	Günlük yapılandırma yedeği (30 gün); analiz verisi arşivden yeniden kurulur

KURULUM VE TESLİM Marta Teknoloji'nin işlettiği bulutta (FortiGate, kuruma özel sertifikayla TLS 6514 üzerinden bağlanır) ya da kurum içi Linux sunucuda tek kurulum betiğiyle.

Demo ve fiyat teklifi için

Ürünü kendi ortamınızda görmek, kapsamı ve fiyatı konuşmak için bize ulaşın.

TELEFON +90 850 441 3 441
E-POSTA bilgi@martateknoloji.com.tr
WEB martateknoloji.com.tr
ADRES Mersin Üniversitesi Teknopark İdari
Binası 35C/B5, Yenişehir, Mersin
Mersin · İzmir · Londra

© 2026 Marta Teknoloji A.Ş. — Bu broşürdeki bilgiler bilgilendirme amaçlıdır; özellik kapsamı sürüme ve kurulumu göre değişebilir.