
MDSİBER
Güvenliğiniz Bizim İçin Önceliğimiz


MDSİBER
Güvenliğiniz Bizim İçin Önceliğimiz

HAKKIMIZDA

MD Siber Güvenlik Ltd. Şti. Siber Güvenlik konusunda yerel çözümler geliştirme ve yeni teknolojileri Türkiye'ye tanıştırma hedefiyle kurulmuştur. Amacımız ihtiyacınıza uygun teknolojik çözümleri yenilikçi bir anlayış ile hem kaliteli hem de uygun teknolojik çözümler haline getirmek ve siz değerli müşterilerimize sunmaktır. Hedefimiz sadece Türkiye pazarı değil tüm dünyaya satış yapabilecek yetkinlikte yazılım çözümleri geliştirmektir. MD Siber Güvenlik olarak biz öncelikle var olan bir teknolojiyi ülkemizin kaynaklarına katmak ve bunun üzerine geliştirmelere devam ederek daha hızlı bir şekilde Yerli ve Milli Siber güvenlik yazılımını ortaya çıkarmak hedefindeyiz.

MD Siber Güvenliğin sunduğu SIEM, DLP ve Firewall çözümleri, tehditleri verimli ve etkili şekilde önceliklendirmeniz, araştırmanız ve bunlara yanıt vermeniz için gereken sezgisel arayüzü, eyleme dökülebilir istihbaratı ve fabrika ayarlı entegrasyonları sağlar. MD Siber Güvenlik Ltd. Şti. olarak endüstriyel SIEM ürünüz Tarkan ile enerji sektörü alanındaki Türkiye'nin geleceği için milli bağımsız ürün çalışmalarımızı yazılım kadromuz ile geliştirmekteyiz. Birçok üniversite ile iş birliği yaptığımız çalışmalarımız devam ekmektedir. Update merkezimiz kurulacak olan Teknopark ofisimizden sağlayarak ülke içerisindeki veri kaynakları İstanbul lokasyonlu sunucularımızdan servis desteği sağlanacaktır.

TEŞEKKÜRLER..

+90 541 521 7979

www.**mdsiber**.com.tr

Bağcılar, Şanlıurfa Blv. Yanyolu
Buğdaycılar H-Office Plaza A/44
BAĞLAR/DİYARBAKIR

Tehdit ve Olay Yönetimi

SIEM

Tespit Edilemeyen Saldırıların Büyümesi

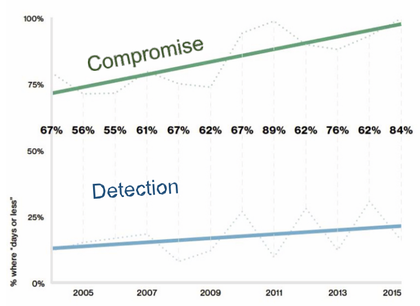
62% hedefine ulaşan siber saldırılar

10% kurbanlar tarafından tespit edilebilen sızmalar

3 Yıl Kurumsal sistemlerde tespit edilemeyen sızmaların ortalama süresi

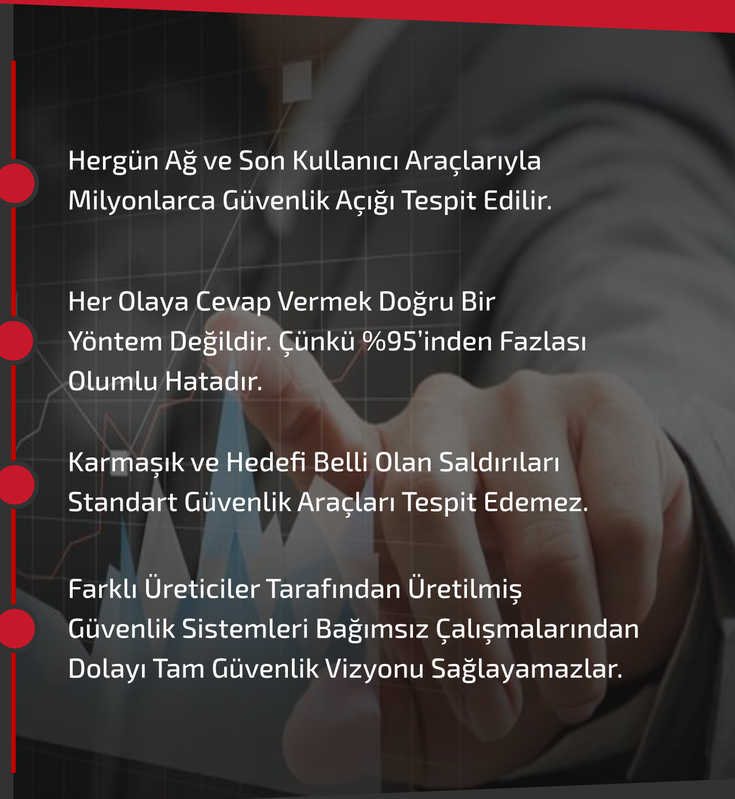
Uzlaşma
Vakaların %84'ünde bir günden az sürüyor

SızmalarTespit süreci
Vakaların %75'inde 1 haftadan fazla sürüyor

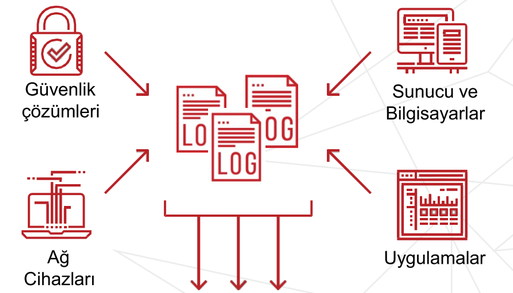


OLAY TESPİTİ NEDEN UZUN SÜRER?

- Hergün Ağ ve Son Kullanıcı Araçlarıyla Milyonlarca Güvenlik Açığı Tespit Edilir.
- Her Olaya Cevap Vermek Doğru Bir Yöntem Değildir. Çünkü %95'inden Fazlası Olumlu Hatadır.
- Karmaşık ve Hedefi Belli Olan Saldırıları Standart Güvenlik Araçları Tespit Edemez.
- Farklı Üreticiler Tarafından Üretilmiş Güvenlik Sistemleri Bağımsız Çalışmalarından Dolayı Tam Güvenlik Vizyonu Sağlayamazlar.



TEHDİTLERİN TESPİT SÜRECİ



SIEM
(Security Information and Event Management)

- **Log(Bilgi) Toplama**
- **Olay Korelasyonu**
- **Olay Tespiti**

- Veri Kaynaklarının Tanımlanarak Olay Raporlarının Toplanması.
- Kaynağa Bağlı Olarak Olay Türüne Öncelik Vermek.
- Birden Fazla Kaynaktan Gelen Veri Raporlarını Temel Alarak Olayları Tespit Etmek İçin Tanımlama Kurallarının Oluşturulması.
- İzleme Ekranlarının Belirlenmesi ve Zamanlanmış Raporların Tanımlanması.

IT ALTYAPISININ MODELLENMESİ

Otomatik olarak eksiksiz ve doğru bir IT altyapı modeli oluşturur

Modeli, varlıklar hakkındaki yeni verilerle sürekli olarak zenginleştirir.

IP ve MAC adresi ve diğer parametreler değiştirilmiş olsa bile IT varlıklarını otomatik olarak tanımlar.

IT altyapısının bütün modeli

Ağdaki Değişkenlere Karşı Koruma

Tehdit Algılama /Önleme

LOG TOPLAYICI VE TARAYICI

IT altyapısının bütün modeli

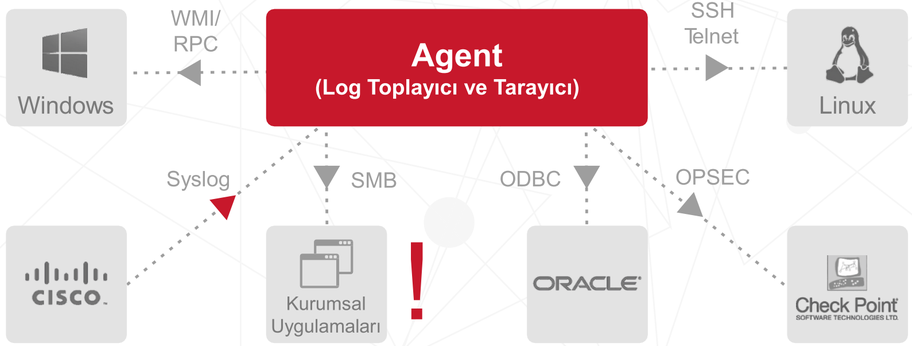
Çeşitli kaynaklardan gelen anlık verilerini toplar (Geleneksel SIEM'ler gibi)

Varlıklardan data toplar (Donanım, OS, Yazılım, Sistemsel Açıklar) beyaz ve kara kutu testi ile ağ taraması yapar (White Black Box Testing),

Özel geliştirilen uygulamalar dahil tüm kaynakları destekler

Ağdaki Değişkenlere Karşı Koruma

Tehdit Algılama /Önleme



ÇALIŞAN VERİ ANALİZİ

Şüpheli olayları algılar

Saldırıları erken aşamada tespit eder

Malware aktivitelerini algılar

Çalışanları İzleme

IT altyapısının bütün modeli

Ağdaki Değişkenlere Karşı Koruma

Tehdit Algılama /Önleme

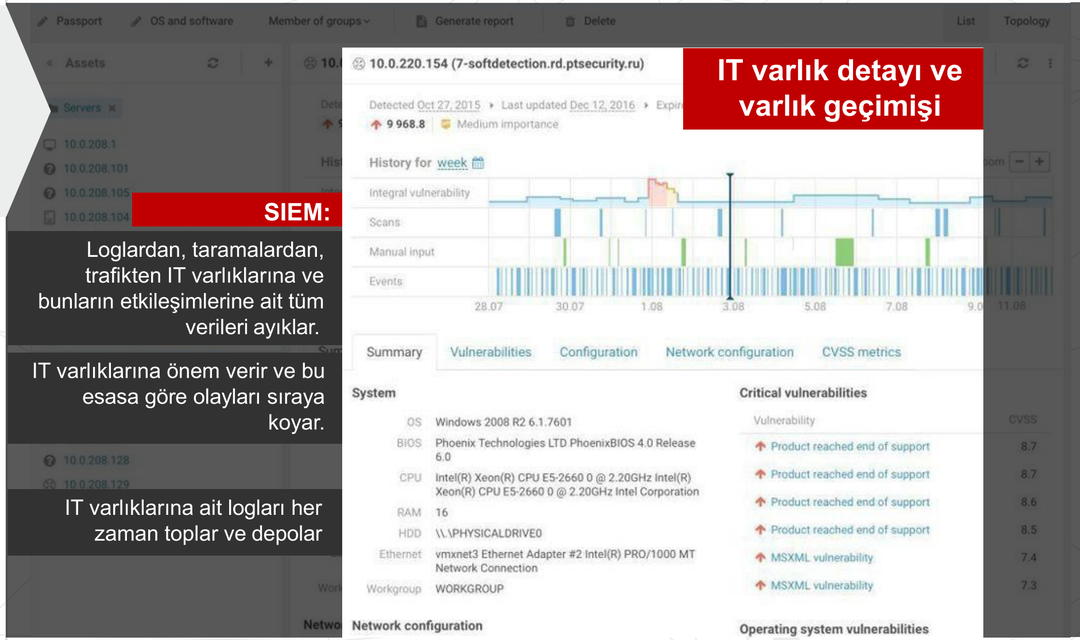
DOĞRU IT ALTYAPISININ OLUŞTURULMASI

IT VARLIKLARININ GRUPLANDIRILMASI

IT altyapısının bütün modeli

Ağdaki Değişkenlere Karşı Koruma

Tehdit Algılama /Önleme

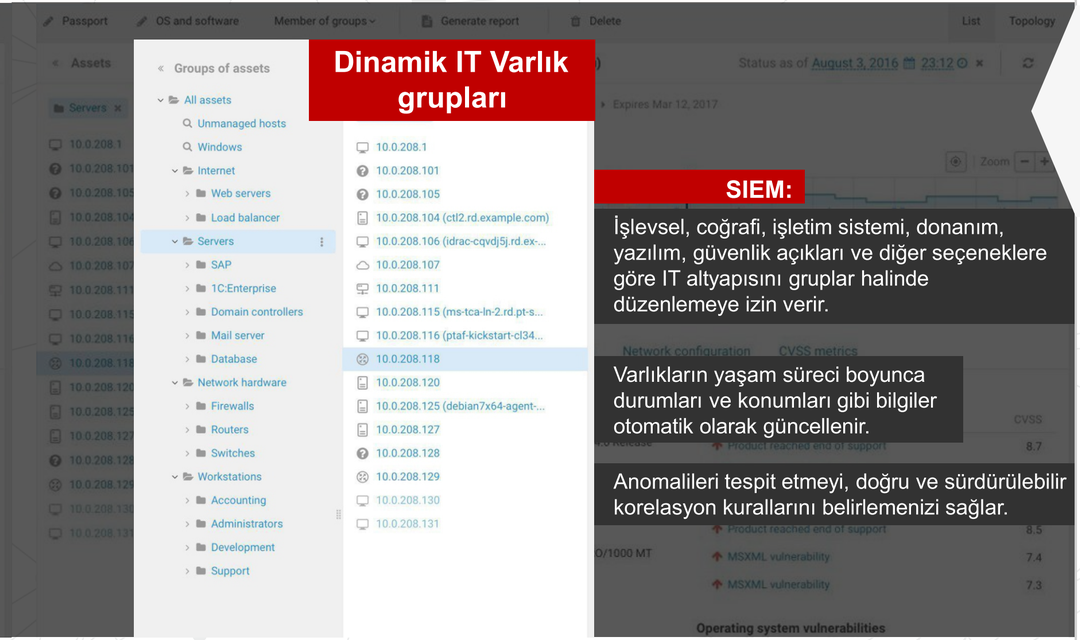


SIEM:

Loglardan, taramalardan, trafikten IT varlıklarına ve bunların etkileşimlerine ait tüm verileri ayıklar.

IT varlıklarına önem verir ve bu esasa göre olayları sıraya koyar.

IT varlıklarına ait logları her zaman toplar ve depolar



SIEM:

İşlevsel, coğrafi, işletim sistemi, donanım, yazılım, güvenlik açıkları ve diğer seçeneklere göre IT altyapısını gruplar halinde düzenlemeye izin verir.

Varlıkların yaşam süreci boyunca durumları ve konumları gibi bilgiler otomatik olarak güncellenir.

Anomalileri tespit etmeyi, doğru ve sürdürülebilir korelasyon kurallarını belirlemenizi sağlar.

IT altyapısının bütün modeli

Ağdaki Değişkenlere Karşı Koruma

Tehdit Algılama /Önleme

IT altyapısının bütün modeli

Ağdaki Değişkenlere Karşı Koruma

Tehdit Algılama /Önleme

Geleneksel SIEM

LOG1

Olaylar

TCP Ports
Donanım Yazılım Konfigrasyon

Varlık bilgileri

Korelasyon Kuralları

Muhafız SIEM altyapısını tamamını görüntüler,

IT varlıkları ve Loglar yerine dinamik gruplara dayalı korelasyon kuralları oluşturmanızı sağlar,

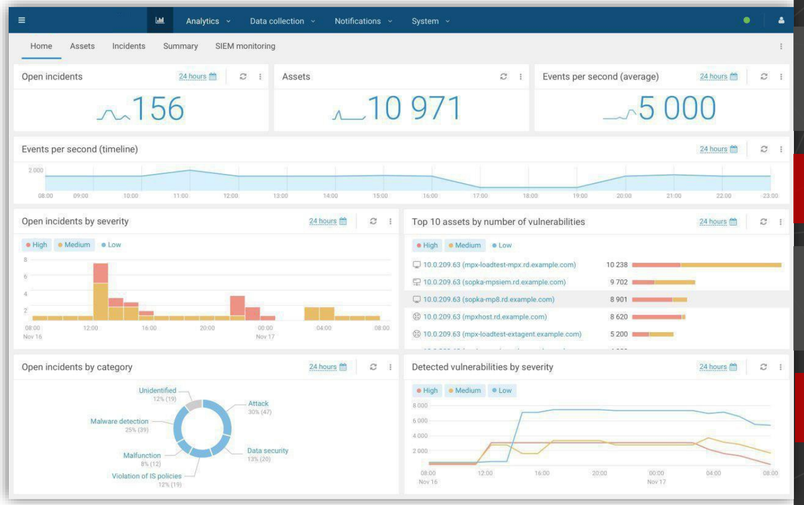
Korelasyon kuralları ağda yeni cihazlar göründüğünde veya ağ yapılandırması değiştirildikten sonra bile çalışmaya devam eder.

IT altyapısının bütün modeli

Ağdaki Değişkenlere Karşı Koruma

Tehdit Algılama /Önleme

SANALLAŞTIRMA VE RAPORLAMA



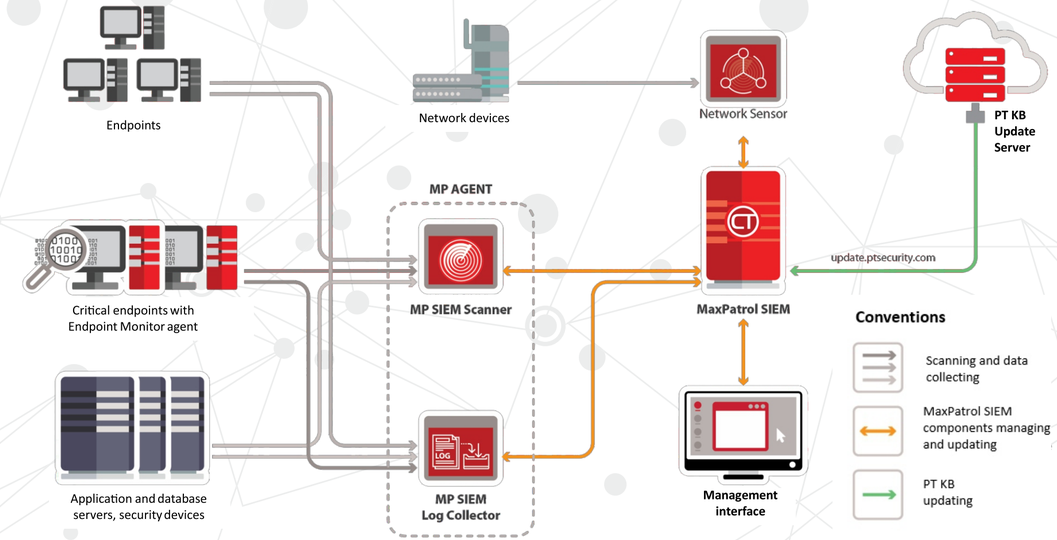
Yapılandırılabilir Dashboard ve Widget'lar

Detaylı Dashboards

Talep Üzerine / Planlı Raporlama

Otomatik rapor teslimi

SİSTEM MİMARİSİ



DLP

VERİ KAYBI ÖNLEME

NEDEN DLP?

DLP, sızıntıların meydana gelebileceği uç nokta kanallarındaki veri akışlarının hem bağlamının hem de içeriğinin farkında olarak veri koruma ve denetim politikalarını uygular.

ayrı içerik bulma özellikleri, kurumsal bilgisayarlarda, ağ paylaşımlarında ve depolama sistemlerinde depolanan verilerin sızmasını önlemeye yardımcı olur.

ayrıca, veri sızıntısının önlenmesini çeşitli oturum tabanlı, akışlı ve yerel sanal makinelere ve masaüstü ve uygulama sanallaştırma mimarilerini kullanan BYOD cihazlarına genişleten Sanal DLP sunar.

DLP, minimum maliyetle maksimum sızıntı önleme için korumalı uç nokta bilgisayarlarında hem bağlamsal hem de içerik tabanlı kontroller sağlar. Çok katmanlı denetim ve yakalama motoru, her müşterinin hassas olarak tanımladığı verilerin kaçmamasını sağlamak için hem "kullanımda veri" hem de "hareket halinde veri" senaryolarında bir dizi veri sızıntısı yolu üzerinde ayrıntılı kontrol sağlar.

içerik analizi ve filtreleme, çıkarılabilir medya, Tak ve Kullan aygıtları, yazıcılar, e-posta, web, Skype ve IM oturumlarının yanı sıra diğer ağ iletişimleriyle uç nokta veri alışverişlerine uygulanabilir. Buna ek olarak, içerik farkındalığı, DeviceLock'un ağ paylaşımlarında, depolama sistemlerinde ve Windows uç nokta bilgisayarlarında bulunan verileri incelemek için Discovery modülüyle birlikte sağladığı kritik bir DLP işlevi olan "boşta kalan veriler" sızıntılarını önlemek için temeldir

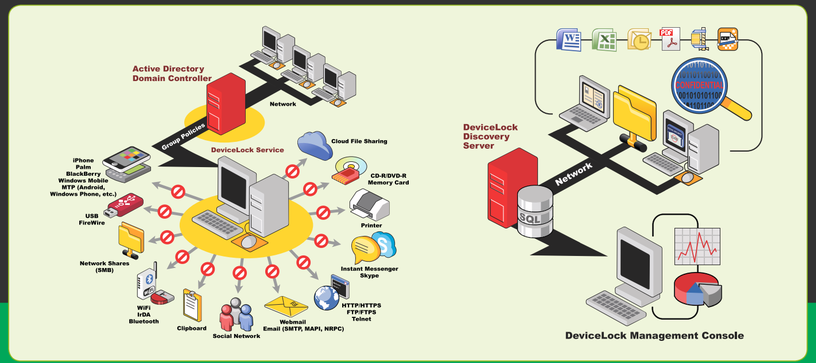
ile güvenlik yöneticileri, kurumsal bilgisayarlara bağlı ortamlara veya ağ protokolleri aracılığıyla veri aktarma, alma ve depolama ile ilgili erişim haklarını iş işleviyle tam olarak eşleştirebilir. Ortaya çıkan güvenli bilgi işlem ortamı, tüm meşru kullanıcı işlemlerinin engellenmeden ilerlemesine olanak tanır, önceden belirlenmiş sınırlar dışında işlem gerçekleştirme amaçlı yanlışlıkla veya kasıtlı denemeleri engeller.

Veri korumasını uç noktalardan yalnızca "kullanımda veri" ve "hareket halinde veri" ötesine genişleten Discovery, şirketteki Windows sunucuları, diğer ağdan erişilebilen veri depoları ve Windows uç nokta çevre birimlerindeki dosya içeriğini otomatik olarak tarayabilir ve inceleyebilir "Veri engelli" depolama politikası ihlallerini tespit eder ve giderir.

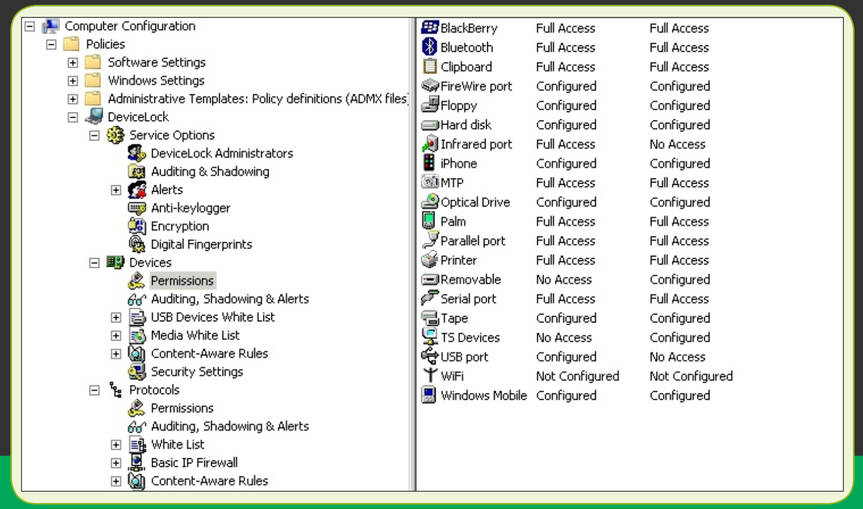
güvenlik yöneticilerinin tanıdık Microsoft Windows Active Directory® Grup İlkesi Nesneleri'ni (GPO'lar) ve ek bileşen DeviceLock konsollarını kullanmasına olanak tanıyan DLP yönetimine doğrudan bir yaklaşım sağlar. Active Directory'deki bu merkezi olarak tanımlanan DLP ilkeleri, fiziksel ve sanal Windows uç noktalarında ve Apple OS X bilgisayarlarda sürekli uygulama için dağıtılmış aracılara otomatik olarak aktarılır.

En savunmasız uç nokta veri kanalları için içerik filtreleme ile tamamlanan ayrıntılı bağlamsal kontrolleriyle DeviceLock DLP, basit ihmal veya kötü niyetli amaç nedeniyle çalışanların bilgisayarlarından sızan hassas bilgilerin riskini önemli ölçüde azaltır. DeviceLock DLP, veri koruma politikası şablonlarını içeren ve HIPAA, SarbanesOxley ve PCI DSS gibi yasal zorunlulukların yanı sıra kurumsal bilgi işleme kurallarına uyumu destekleyen bir güvenlik platformudur.

- AD Grup İlkesi Entegrasyonu
- **Cihaz Beyaz Listesi**
- Güvenli Politika İstisnaları
- **Ağ İletişim Denetimi**
- İçerik Filtreleme
- **Yerleşik OCR**
- **İçerik Bulma - Pano Kontrolü**
- BYOD Cihazları için Sanal DLP
- **Dış Müdahale Koruması**
- Mobil Cihaz Yerel Senkronizasyon Kontrolü
- **Yazdırma Güvenliği**
- Çevrimdışı Uç Nokta Güvenliği



- **Tak ve Kullan Aygıtları Bildirme**
- Grafiksel Raporlama
- **Veri Arama**
- Denetim Günlüğü
- **Ajan İzleme**
- Veri Gölgeleme



denetim özelliği, belirtilen cihaz türleri, bağlantı noktaları için kullanıcı ve dosya etkinliğini izleryönetilen bir bilgisayarda protokoller. Denetlenebilir olayları kullanıcı / gruba, gün / saate göre doğru olarak filtreleyebilirdosya türü, bağlantı noktası / aygıt türü / protokolü, okuma / yazma ve başarı / başarısızlık olaylarına göre sıralanabilir ve dize tabanlı ölçütlere göre filtrelenebilir.

veri gölgeleme işlevi, harici depolama aygıtlarına kopyalanan, seri, paralel ve ağ bağlantı noktalarından (NetworkLock eklentisiyle) yazdırılan veya aktarılan tüm verileri yansıtacak şekilde ayarlanabilir. servis toplama aracıları tarafından otomatik olarak toplandıktan sonra CD / DVD / BD yazıcılar tarafından üretilen ISO görüntülerini orijinal ayrılmış dosyalara bölebilir. Adli inceleme için dosyaların tam bir kopyası güvenli bir paylaşıma kaydedilebilir.

servis ajanları, uzak Windows bilgisayarları gerçek zamanlı olarak uç nokta aracısı durumunu (çalışıyor ya da çalışmıyor), sürümü, politika tutarlılığını ve bütünlüğünü kontrol ederek izleyebilir. Detaylı bilgi İzleme günlüğüne yazılır.

PnP Raporu, yöneticilerin ve denetçilerin şu anda ve geçmişte ağdaki seçili Windows bilgisayarlara bağlı olan USB, FireWire ve PCMCIA aygıtlarını görüntüleyen bir rapor oluşturmalarına olanak tanır. Bu rapor ayrıca, DeviceLock erişim ilkelerine belirli cihaz modelleri veya benzersiz cihazlar eklemek için ilk adım olarak USB beyaz listesinin verimli bir şekilde toplanmasına izin verir.

tarafından toplanan denetim günlüğü ve gölge dosyası verilerinin analizine dayalı olarak HTML, PDF veya RTF formatında grafik "hazır" raporlar oluşturabilir. Bu raporlar, oluşturulduğunda bir veri güvenliği yönetim listesine veya uyumluluk görevlilerine otomatik olarak e-postayla gönderilebilir.

Ayrı olarak lisanslanan modülü, merkezi olarak toplanan denetim günlüğü ve gölge dosyası verilerinin endekslenmesini ve kapsamlı tam metin aramasına izin vererek adli yeteneklerini geliştirir. bilgi bulmanın daha hızlı, daha kesin ve daha kullanışlı olmasını sağlayarak emek-yoğun bilgi güvenliği uyum denetimi, olay araştırmaları ve adli analiz süreçlerine yardımcı olur.

VPN

Virtual Private Network

Kanal Koruması, kamu ağları ve özel veri alışverişi kanalları üzerinden iletişimde veri güvenliği sorunlarını karşılamak için tasarlanmış bir ürün grubudur.

Avantajları

FIPS 140-2 ve BSI gibi dünyaca tanınan standartlara uygun olarak geliştirilen ViPNet Kanal Koruma ürünleri, anytopolojinin ağ nesneleri (istemciden istemciye, sunucudan sunucuya, istemciden sunucuya, istemci sunucu grubu vb.) Arasında güvenli bağlantılar kurmanıza olanak tanır. iletişim kanalının fiziksel türüne, fiziksel ağ topolojilerine ve bağlantı türüne (sabit veya mobil) bakılmaksızın.

ViPNet teknolojisi avantajları, bilgi güvenliği araçlarını herhangi bir topolojinin kurumsal ağlarına entegre etmenize ve fiziksel katmanda herhangi bir değişiklik yapmadan kurumsal ağınızdaki erişim kontrol politikalarını uygulamanıza olanak tanır.

ViPNet teknolojisi, özelliklerini etkilemeden farklı ağ hizmetlerinin trafiğini kapsüllemek için hem dinamik hem de statik ağ / bağlantı noktası adres çevirisi (NAT / PAT) ile çalışmanıza olanak tanır.

Noktadan noktaya ağ iletişimi özelliği ile ViPNet teknolojisi, trafik işleme yükünü merkeze kaydırmadan iletişim kanallarını korur, böylece tüm merkezi yönetim avantajlarını sağlar.

ViPNet ürün grubu olgunlaşmış ve uygulama ve sahip olma maliyetlerini en aza indirmeye yöneliktir. Bu sayede, istemci ve sunucu ayarlarını değiştirmeden güvenli bağlantılar ve iletişim kurmanın yaygın senaryolarını uygulayabilirsiniz.

ViPNet ürünleri, mobil iletişim ve endüstriyel otomasyon taleplerini karşılamak için, uygulama katmanında ve operasyonel senaryolarda ödün vermeden yeterli düzeyde koruma sağlayan yaratıcı bir şekilde geliştirilmiştir.

GÜVENLİK AĞ GEÇİDİ

ViPNet Coordinator HW Güvenlik ağ geçidi, güvenlik duvarı, VPN sunucusu

ViPNet Coordinator VA
Güvenlik ağ geçidi, güvenlik duvarı, bulut sanallaştırma platformları için VPN sunucusu

ViPNet Coordinator HW-RPi
Güvenlik duvarlı kompakt VPN Güvenlik Ağ Geçidi

ViPNet Coordinator IG
Güvenlik ağ geçidi, güvenlik duvarı, endüstriyel sistemler için VPN sunucusu

ViPNet xFirewall
Güvenlik ağ geçidi ve yeni nesil güvenlik duvarı

ViPNet Coordinator Software
Güvenlik ağ geçidi, güvenlik duvarı, Windows için VPN sunucusu

and Linux

YÖNETİM VE MÜŞTERİ BİLEŞENLERİ

ViPNet NSMS ViPNet ağını yapılandırır ve yönetir

ViPNet Policy Manager
Güvenlik duvarı güvenlik politikalarını merkezi olarak yönetir

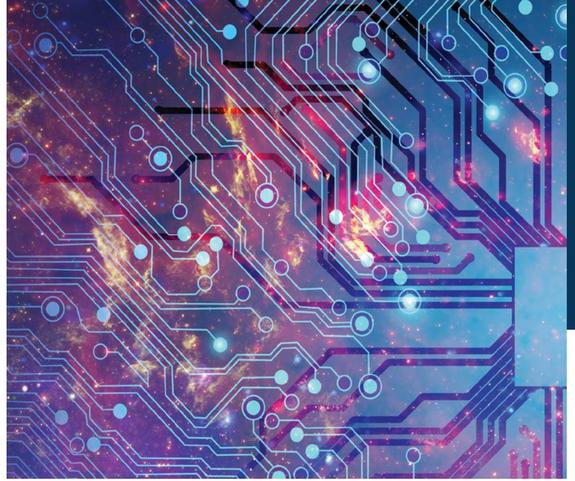
ViPNet Client
VPN istemcisi ve kişisel güvenlik duvarı

kuruluşlar arasında korumalı iletişim kanalları kurmak için bir güvenlik geçididir.

Benzersiz entegre özellikleri (kriptografik veri koruması, güvenlik duvarı, entegre ağ hizmetleri) nedeniyle, ViPNet Koordinatörü HW, genel ağlar üzerinden veri aktarımı yaparken kurumsal ağları kaynaklara yetkisiz erişime karşı korumak için çok yönlü bir çözüm oluşturur.

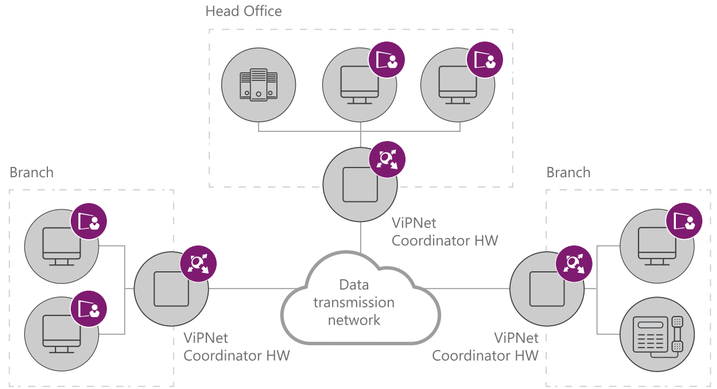
AVANTAJLARI

1. Tek bir cihazda ağ katmanı (L3) ve veri bağlantı katmanı (L2OverIP) VPN
2. Yük devretme kümesi
3. Merkezi ve uzaktan yönetim (SSH, WebUI)
4. Gözetimsiz kullanım 7/24
5. Modern, çok hizmetli veri ağlarının desteklenmesi ve aşağıdakilerle tam uyumluluk:
   - DHCP, WINS ve DNS hizmetleri
   - Dinamik adres çevirisi (NAT, PAT)
   - Multimedya protokolleri
   - (SIP, H323, SCCP ve diğerleri)



- Bir kuruluşun şubeleri arasında güvenli iletişim (siteden siteye ve çoklu siteden siteye)
- Veri merkezleri arasındaki omurga bağlantılarını koruma
- Kablosuz ağ koruması
- Uzak ve mobil kullanıcılar için kurumsal ağa korumalı erişim
- Çok hizmetli ağların korunması (IP telefonu dahil) ve video konferans)
- Yerel ağlarda farklı veri erişimi, yerel ağları bölme (örneğin, bir DMZ oluşturma)
- Diğer kuruluşların ViPNet ağlarıyla iletişim kurmak

KULLANIM VAKALARI



ÖZELLİKLERİ

VPN

Ağ katmanı VPN ağ geçidi (L3 VPN)

Veri bağlantı katmanı VPN ağ geçidi (L2OverIP VPN)

IP adres sunucusu

VPN yönlendirici

Trafiğin UDP ve TCP'ye kapsüllenmesi nedeniyle trafik maskeleme

NETWORK FUNCTIONS

Statik yönlendirme

Dinamik yönlendirme

VLAN (dot1q) desteği

Kanal bağlantısı (EtherChannel, LACP)

Trafik sınıflandırması ve önceliklendirme (QoS, ToS, DiffServ)

FIREWALL

Durum bilgisi olan güvenlik duvarı

Şifrelenmemiş ve şifrelenmiş IP trafiği için ayrı trafik filtreleme kuralları

NAT / PAT

Anti-sızdırma

Proxy sunucusu ve antivirüs

INTEGRATED SERVICES

Dns sunucusu

NTP sunucusu

DHCP Sunucusu

DHCP Geçişi

UPS desteği

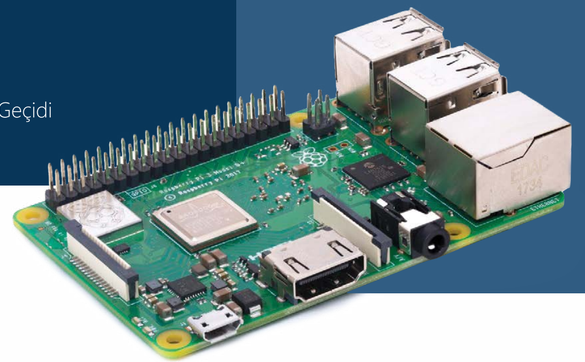
Yük devretme kümesi

Coordinator VA

Koordinatörü bir sanallaştırma platformuna dağıtmak için oluşturulan sanallaştırılmış yazılım çözümü

- Koordinatör VA sanal cihazı, bir sanallaştırma platformuna dağıtım için çok yönlü bir güvenlik ağ geçididir. Dinamik bulut ortamlarındaki sanallaştırılmış veri merkezlerine güvenli erişim sağlayarak ağ saldırılarına ve yetkisiz erişime karşı koruma sağlar. Sanal cihaz, mevcut bir altyapıya sorunsuz bir şekilde entegre edilebilir ve en iğrenç işlevsellik, kullanılabilirlik, güvenilirlik ve hataya dayanıklılık gereksinimlerini karşılar.
- Koordinatör VA, Koordinatör HW donanım cihazının sanal cihaz versiyonudur. Sanal bir ana bilgisayarda bir hipervizör içinde çalışır.
- Güvenlik seçeneklerini yapılandırmak için Koordinatör VA Web Erişimi.

Güvenlik duvarlı kompakt VPN Güvenlik Ağ Geçidi



Koordinatör HW-RPi, bir Raspberry Pi platformunda çalışanlar için akıllı, uygun fiyatlı, güvenli bir şifreleme çözümüdür. Tek kartlı bilgisayar, yenilikçi iş bileşenine sahip olmalı. Infotecs'in Raspberry 3 model B çözümü, Linux tabanlı bir işletim sistemi ve bir Koordinatörden oluşuyor. Raspberry Pi ile birlikte görüntü bir donanım cihazı oluşturur. Kredi kartı boyutundaki mini bilgisayar, teknolojisine dayalı bir güvenlik duvarı ile tamamen işlevsel bir VPN ağ geçidi görevi görür.

ÖZELLİKLERİ

• Koordinatör HW-RPi, sunucuda veya istemci tarafında kullanılan çok çeşitli hizmetler sunar.

• VPN ağ geçidi: şifrelenmiş siteden siteye ve istemciden siteye bağlantılar.

• Katman 3 Durumsal Denetim Güvenlik Duvarı: genel trafiği ve VPN trafiğini IP adresine, VPN kimliğine ve TCP / UDP bağlantı noktasına göre filtreler.

• VPN yönlendirici: Şifrelenmiş trafik, IP paketlerinin şifrelenmemiş bölümünde belirtilen ve yanlışlamaya karşı korunan ana bilgisayar tanımlayıcılarına göre yönlendirilir. Yönlendirme, trafiğin güvenli dinamik yönlendirmesi için tasarlanmış özel bir protokol üzerinden gerçekleştirilir. Yönlendirme ile birlikte, şifreli trafik için ağ adresi çevirisi (NAT) gerçekleştirilir. Bir koordinatör tarafından alınan tüm ileri şifreli paketler, kaynak IP adresi olarak koordinatörün IP adresine sahip diğer ana bilgisayarlara gönderilir.

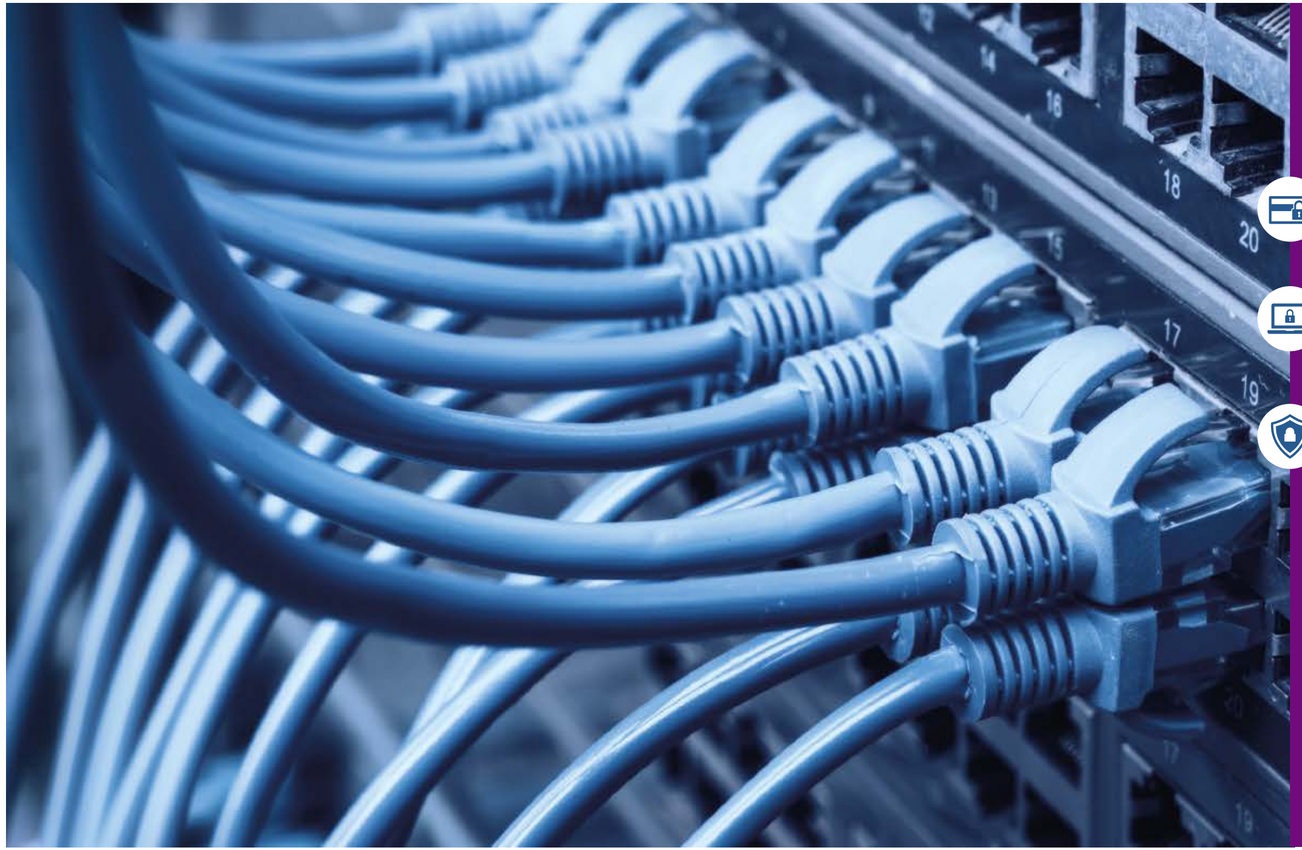
KULLANIM VAKALARI

ViPNet Teknolojisi, Raspberry Pi ile birlikte birçok uygulama alanı ve özellikle Nesnelerin İnterneti (IoT) için etkili ve umut verici bir çözümdür.
Uzaktan izleme sistemleri ve endüstriyel kontrol sistemleri için hem harici hem de dahili saldırılara karşı makul bir maliyetle son derece güvenli koruma sağlar.
Yaygın örnekler çözümü kullanmak, ağ bilgisayar kontrollü nakit sistemlerini korumak, VoIP, yazıcılar, bina altyapısı veya IP video kameraları korumaktır. ViPNet Koordinatör HW-RPi ile konum veya cihaz / sistem başına maliyetleri azaltabilirsiniz.

xFirewall

Yeni Nesil Güvenlik Duvarı

xFirewall, ağınıza erişimi kısıtlamaktan daha fazlasını yapan bir cihazdır. Uygulama algılama, izinsiz giriş önleme, web filtreleme ve kötü amaçlı yazılım koruması dahil bir güvenlik duvarını entegre eder. “Kullanıcı”, “Uygulamalar” profilleri ve ağ erişim kontrolüne dayalı ayrıntılı güvenlik politikaları sağlar.



Avantajları

Ayrıntılı güvenlik politikası “Kullanıcı” - “Uygulama” - “İzin Ver / Engelle” kavramlarına dayalı

İşyerinde kişisel cihazların güvenli kullanımı, şirketin güvenlik politikalarına tam olarak uyulmasını sağlar - BYOD (Kendi Cihazınızı Getirin)

2.000'den fazla uygulama protokolünün ve uygulamasının algılanması ve engellenmesi: oyunlar, sosyal ağlar, Torrent vb.

Azalan İnternet trafik maliyetleri

Minimize edilmiş saldırı yüzeyi

xFirewall, İzinsiz Girişi Önleme Kurallarına (IPS kuralları) dayalı olarak imza ve sezgisel yöntemleri kullanarak trafiği analiz eder. Aşağıdaki tehdit türlerini otomatik olarak algılar ve ortadan kaldırır:

- Ağ hizmetlerine yönelik saldırılar
- Korunan ağ nesnelerinin yazılım güvenlik açıklarından yararlanma girişimleri
- Anormal trafik
- Virüsler

ÖZELLİKLERİ

xFirewall

UYGULAMA-KATMAN GÜVENLİK DUVARI (DPI, DERİ PAKET İNCELEME)

Tespit eder ve engeller Aşağıdakileri içeren 2.000 uygulama protokolü:

- Oyunlar
- Sosyal ağlar
- Anlık mesaj servisleri
- Video konferans
- P2P hizmetleri, Torrent
- Dosya barındırma
- Tünel açma, VPN
- Uzaktan kumanda
- Endüstriyel protokoller

FIREWALL

- Durum bilgisi olan güvenlik duvarı
- Ağ adresleri çevirisi (NAT / PAT) Kimlik sahtekarlığına karşı koruma

AĞ ÖZELLİKLERİ

- İyi geliştirilmiş statik yönlendirme
- Dinamik yönlendirme
- VLAN (dot1q) desteği
- Kanal Birleştirme (LACP, EtherChannel)
- QoS, ToS, DiffServ desteği

DİREKTÖRLER İLE ENTEGRASYON

- Microsoft AD
- LDAP dizinine sahip Sabit Portal

PROXY SUNUCU

- HTTP ve FTP desteği
- Dosyanın MIME türüne ve HTTP istek yöntemine göre trafik kontrolü ve filtreleme
- ICAP üzerinden üçüncü taraf antivirüs ile trafik taraması

DPI (DERİN PAKET DENETİMİ)

DPI, kullanıcıların uygulama trafiğini tanımlamak için farklı teknikler kullanır: bağlantı noktaları ve protokollere, imza yöntemine, sezgisel yönteme dayalı. Bu yöntemlerle, ürünler şifreli veya maskelenmiş trafiği olan uygulamaları bile algılayabilir.

ENTEGRE SERVİSLER

- Dns sunucusu
- NTP sunucusu
- DHCP Sunucusu
- DHCP Geçişi

YÜKSEK KULLANILABİLİRLİK VE KÜMELEME

- Yük devretme kümesi
- UPS desteği

ÖZELLİKLERİ

- Bu ürünle, herhangi bir TCP / IP ağını kullanarak dünyanın herhangi bir yerinden kurumsal bilgi sistemlerinin kaynaklarına eşit erişim sağlayabilirsiniz.

- Trafik şifreleme ve filtreleme özellikleri nedeniyle ürün gerçek zamanlı olarak TCP / IP ağlarında ses trafiğini, video iletişimini, VoIP bağlantılarını, posta alışverişini ve diğer hizmetleri koruyabilir.

- Ürünün arkasındaki ViPNet teknolojisi, coğrafi olarak dağıtılmış bilgi sistemlerini tek bir kontrol merkezi aracılığıyla çalıştırmanıza ve şifreleme anahtarlarını ve yazılımı güvenli bir kanal üzerinden dağıtmanıza olanak tanır.

- Ürün mimarisi, farklı kurumsal ağ segmentlerinin kaynaklarıyla eş zamanlı çalışmayı sağlayabilir.

- VPN istemcisi: simetrik 256 bit anahtarlı AES algoritması kullanarak IP paketlerinin noktadan noktaya şifreleme ve MAC koruması

- Kişisel güvenlik duvarı

Client

Şifrelenmemiş kanallar üzerinden aktarılan bilgileri mobil cihazlardan ve masaüstü bilgisayarlardan koruyan bir istemci yazılımı

KULLANIM VAKALARI

1 Şifreli kanallar üzerinden şirket kaynaklarına ve hizmetlerine uzak istemci-site ve istemci-istemci bağlantılarını güvenli hale getirin. İstemciden istemciye (noktadan noktaya) bağlantı modu, yalnızca genel iletişim kanalları üzerinden veri alışverişinde değil, aynı zamanda İstemcisi bir şirket ağında kullanıldığında da koruma sağlar, böylece gizli bilgileri iç davetsiz misafirlere karşı da korur .

2 Koruma senaryolarına ek olarak, mevcut korumalı ağınıza güvenli kurumsal posta ve güvenli mesajlaşma gibi isteğe bağlı güvenli iletişim araçları ekleyebilirsiniz.

3 İstemci sanal bir cihaz olarak işlev görebilir ve böylece ViPNet koruma araçlarını VDI ortamlarında kullanmanızı sağlar.

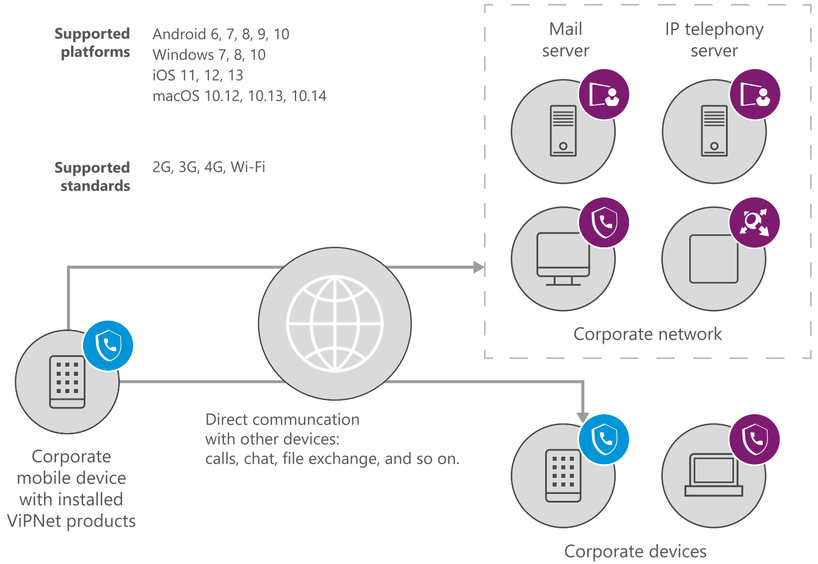
4 ViPNet İstemcisi, mevcut postalarınızı, belge alışverişinizi ve video konferans sistemlerinizi korumak için bir kaplama güvenlik aracı olarak kullanılabilir. Uygulama yazılımınızı değiştirmeden.

5 ViPNet İstemcisi ile, cihazınıza doğrudan İnternet erişimini engelleyebilirsiniz, böylece İnternet'e yalnızca proxy sunucuları, DLP sistemleri ve içerik filtreleme sistemleri gibi bir dizi güvenlik aracı kullanan kurumsal trafik temizleme bölgesi üzerinden erişebilir. Bu yaklaşım, çok düzeyli aygıt koruması sağlar ve güvenli çevre çevresini fiziksel olarak terk eden aygıtlara bile kurumsal veri güvenliği önlemleri uygular.

Kullanım Kılıfları, Mobil ve Masaüstü Koruması

Supported platforms
Android 6, 7, 8, 9, 10
Windows 7, 8, 10
iOS 11, 12, 13
macOS 10.12, 10.13, 10.14

Supported standards
2G, 3G, 4G, Wi-Fi



SCADA

Süreç kontrol sistemlerinin
bilgisayar saldırılarına karşı
geniş kapsamlı korunması

Global Deneyim, Her Şeyin Olabileceğini Gösteriyor!

Kontrollü alandaki Wi-Fi erişiminin tamamen yasaklanmasına rağmen, hidrolik bir tesiste yanlışlıkla bir kablosuz ağ keşfedildi

Bir süreç kontrol sistemi mühendisi barajın merkezine bir erişim noktası kurdu, aktüatörleri ona bağladı ve kontrol odasından çıkmadan onlardan bilgi aldı.

Uzmanlardan elektrik trafo merkezinin işlem ve kontrol sistemindeki garip kesintileri araştırması istendi, ve uzaktan teknik destek sağlayan şirket birincil şüpheliydi. Soruşturma şirketin suçlu olmadığını ortaya çıkarmasına rağmen, ünitenin ağa bağlanma şeklinin ciddi bilgi güvenliği ihlallerine yol açtığı tespit edildi: doğrudan İnternete bağlanmış ve TeamViewer aracılığıyla destek sağlanmıştır.

PCS seviyeleri ve tehditlerin şeması

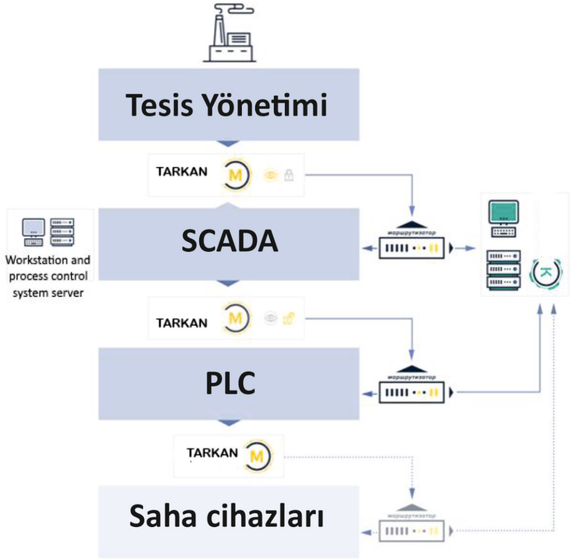
SEVİYELER	TEHDİTLER
Proje Yönetimi MES ve ERP	İnternet üzerinden saldırı Sosyal mühendislik Ürün Seçim Kriterleri ve Test/Demo Prosedürü (APT) Belirsiz cihazların kullanımı
SCADA Toplama, İşleme Bilgi Görüntüleme ve Arşivleme	Korumasız bağlantı ile uzaktan destek iç çalışanlar harici teknik destek
PLC Aktüatörlere sensörlerden ve üst seviye komutlardan gelen verilere dayanarak komutlar verir	MES seviyesinden saldırılar Kötü amaçlı yazılımın dağıtılması (flash bellek vb.) Belirsiz cihazların kullanımı
	PLC güvenlik açıkları PLC yönetim yazılımına geçin Endüstriyel protokol komutlarının izinsiz kullanımı Düzenli çalışmalar için gerekli olmayan açık limanların kullanılması Belirsiz cihazların kullanımı
Saha Cihazları Sensörler ve Aktüatörler	Endüstriyel protokol komutlarının izinsiz kullanımı Belirsiz cihazların kullanımı Cihazların güvenlik açıkları (güç dağıtımı ve elektrik ölçümü için belirgin)

Bu Saldırılar Neden Mümkün?

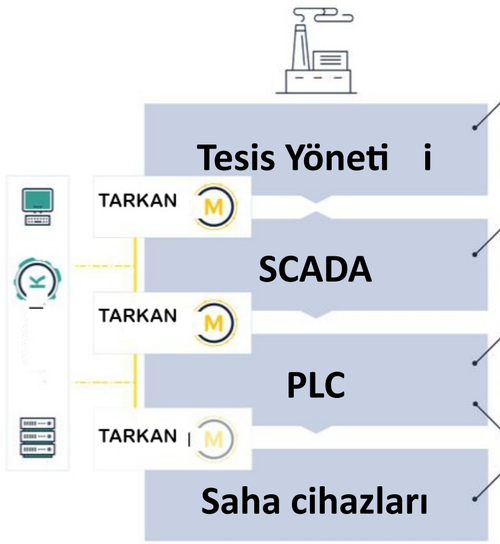
- İşlem kontrol sistemlerinin eski kalması ve yeni tehditlere karşı savunmasız olması
- Çalışanların zayıf bilgisayar becerileri
- Çoğu işletmede, en çok bilinen güvenlik açıkları hesaba katılmaz
- Kurumsal güvenlik politikası dahilinde iç standartların ve düzenlemelerin olmaması
- Özel protokollerin açıklamaları açık kaynaklar (open source) ile belirlenir ve yayınlanırsa saldırganlar tarafından erişilebilir
- Yasal gerekliliklerin yanı sıra endüstri standartlarına resmi uyum

Temel İlkeler

- **İKİ MODDA ÇALIŞMA**
  - İzleme modunda
  - Aktif saldırı engelleme modunda
- **IEC60870-5-104, OPC UA, OPC DA gibi Modbus da dahil olmak üzere endüstriyel protokollere göre filtreleme**
- **Kanal, ağ, ulaşım ve uygulama seviyelerinden bilgi işlenmesi**
- **Kuruluşun tüm üretim ağına ölçeklenebilirlik: kullanıcı, herhangi bir sayıda Tarkan-M cihazını bağlayabilir**
- **Herhangi bir SIEM sistemiyle Syslog üzerinden bilgi alışverişi**
- **Tüm olaylar Tarkan-K'nın tek arayüzü üzerinden uygun grafiksel raporlar halinde analiz edilip kullanılabilir.**



İzinsiz Giriş Algılama Özelliği İle Çok İşlevli Endüstriyel Duvar



Endüstriyel protokoller yoluyla kötü amaçlı trafiğe filtre uygulama, internet saldırılarına karşı koruma

- SCADA seviyesindeki saldırıları tesis yönetim seviyesinden önlemek
- Uzaktan destek kanalının korunması (hem iç çalışanlar hem de dış yardımlar)
- SCADA düzeyinde yazılım listesine göre gerekli engellemeler

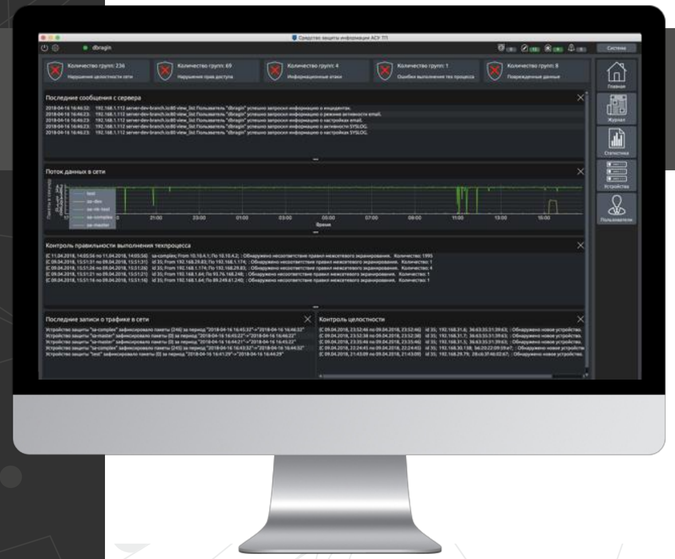
- PLC'yi yeniden yönlendirmeyi amaçlayan komutları algılama
- Genel işler için gerekmeyen PLC seviyesindeki açık portlardan gelen saldırıların önlenmesi

- PLC ve saha cihazlarında yetkisiz endüstriyel protokol komutları kullanımına karşı koruma
- Açık veri tabanlarındaki verilere ve kendi uzman merkez veri tabanımıza dayalı olarak PLC ve saha cihazlarının güvenlik açıklarının kullanılmasına karşı koruma

Ağdaki kayıtlı olmayan cihazların tüm PCS seviyelerinde tespiti

Temel İlkeler

Tüm sistem bileşenlerinden toplanan bilgilere hızlı erişim için kullanışlı arayüz



- Farklı kullanıcı grupları tarafından ihtiyaç duyulan bilgilere erişim
- Bilgi güvenliği çalışanları, BT uzmanları, otomatik kontrol sistemleri uzmanları
- Özel kullanıcı görevleri için gerekli widget'larla özelleştirilebilir konsol
- Syslog aracılığıyla olayları dışa aktarma
- Excel'de rapor yükleme, PDF
- SCADA'ya olay yükleme