KOTTO
BİLİŞİM A.Ş.

KURUMSAL TANITIM KİTAPÇIĞI

www.kottoas.com

KOTTO HAKKINDA

Kotto A.Ş., müşterilerine stratejik dış kaynak kullanımı, entegrasyon ve e-dönüşüm konularında çözüm ve servis sağlayan bir teknoloji şirketi olup, aynı zamanda kamu BT sektörünün en yeni bağımsız kuruluşudur.

Şirketimizi farklı kılan güvenilir yapımız, güçlü iş ortaklarımız, uzman kadrolarımız, son teknolojiyi uygulama yeteneğimiz ile müşteri ve sektör odaklı yaklaşımımızdır. 25 yılı aşkın sektör deneyimi barındıran şirketimiz müşterilerinin teknoloji ortağı olarak onlarla uzun dönemli ilişkiler kurmayı ve müşteri memnuniyetini en üst seviyede tutmayı ilke edinmiştir.

Bugün Kotto A.Ş. olarak Türkiye'nin en güncel bağımsız bilgi, iletişim ve yüksek teknoloji şirketiyiz. Aynı zamanda kamu sektöründe hem yerli hem milli sermayeli yatırımları tercih eden öncü firmayız. İştiraklerimiz ve stratejik ortaklıklarımız ile birlikte altyapı ve iş çözümlerini destekleyen çok sayıda uzman çalışan istihdam ediyor, imkânlar yaratıyor ve kapsayıcı faydalar sağlıyoruz.
Büyüme eğrimiz ve gelirlerimizin dağılımına bakıldığında Kotto A.Ş., kurulduğundan bu yana hızlı ama sağlıklı bir büyüme sergilemiş, 2016 yılından başlayarak kendi çözüm ve hizmetlerinin toplam gelirleri içindeki payı sürekli olarak büyümüştür.

Vizyonumuz

Sahip olduğu teknolojik altyapı, gelişmiş yetkinlikler ve uzman ekibi, kendi geliştirdiği ürün ve servisleriyle müşteriye özel esnek çözümler ve değer üreterek ulusal pazarlardaki faaliyetini sürekli genişleten öncü bir teknoloji şirketi olmaktır.

Misyonumuz

Bilgi teknolojilerinin fikirden uygulama ve uzun dönem yönetimine kadar her aşamasında müşterilerimizin, güvenilir ve profesyonel teknoloji ortağı olarak verimliliklerini artırmak, maliyet ve rekabet avantajı sağlamaktır.

Kalite Politikamız

Bilgisayar ve İletişim Teknolojileri alanında;

- Müşterilerimizin ihtiyaç ve beklentilerini, en uygun çözümler ile uçtan uca karşılamak,
- Geleceğe taşıyan uygulamalar ve çözümler sunarak işbirliği yaptığı kurumlara değer katmak
- Çalışan ve müşteri memnuniyetini arttırmak,
- Kalıcı müşteriler edinmek,

Şeklinde tanımlanmıştır ve şirketimiz kalite sisteminin temelini oluşturmaktadır.

Kurumsal Özel Tasarım Projelerin Hayat Bulduğu
ve
Hedeflerinizin Ötesine Geçtiğiniz Yerdesiniz.

Sunucu Sanallaştırma

Masaüstü Sanallaştırma

Veri Depolama Sanallaştırma

Ağ Sanallaştırma

Özel Bulut Veri Merkezi

Olağanüstü Durum Merkezi

Cihaz, Bilgi, Personel ve Erişim Yedekleme

Mobil Cihaz, Uygulama ve Erişim Yönetimi

Hassas Erişim ve Çok Faktörlü Yetkilendirme

Çevresel Güvenlik, Uzaktan Algılama ve Ölçme

Son Kullanıcı Gereksinimleri

Yüksek Teknoloji Temini

Sistem Entegrasyonları

Proje Yönetim Ofisi (PMO)

Yönetim Sistemleri Kuruluşu

İş Sürekliliği ve Acil Durum Yönetimi

KOTTO
BİLİŞİM A.Ş.

İş Çözümlerimiz

İş Çözümleri ürünleri müşteri beklentileri ve sektör ihtiyaçları doğrultusunda geliştirilmektedir. Müşterilere sunulan çözümler arasında, daha önce geliştirilmiş Kotto markalı hazır iş çözümlerinin yanı sıra, müşteri istekleri doğrultusunda kurumlara özel geliştirilen yazılım ve çözümler de bulunmaktadır.

Bu çözümlerin önemli bir kısmı farklı sektörlerde kullanılabilecek ortak çözümler iken, kalanı belirli sektörlere özel çözümler olarak geliştirilmiştir.
İş Çözümleri, müşteri ihtiyaçlarının ve iş süreçlerinin analizi doğrultusunda; danışmanlık, iş ihtiyaçlarının gerektirdiği bir yazılımın seçimi, yeni bir yazılımın geliştirilmesi, sistem ve çözümün tasarımı, kurulum, işletim ve bakım hizmetlerinin sağlanması konularındaki çalışmaları kapsamaktadır.

Teknoloji Çözümlerimiz

Kotto Bilişim; network, güvenlik, sistem çözümleri, alanlarındaki farklı uzmanlıkları ile müşteri ihtiyaçlarına yönelik danışmanlık, tasarım, test/demo, ürün sağlama ve kurulum hizmetlerini sunduğu anahtar teslim sistem entegrasyonu projelerinde yer alırken, müşterilerinde kalıcı olmayı amaçlayan, güvenilir, destek hizmetlerini de beraberinde sunmaktadır.

Temel İlke ve Değerlerimiz

Kotto ailesinin tüm bireyleri

- **GÜVENİLİRLİK,**
- **MÜŞTERİ MERKEZİYETÇİLİK,**
- **SONUÇ ODAKLILIK,**
- **TAKIM ÇALIŞMASI,**
- **SÜREKLİ GELİŞİM,**
- **YARATICILIK ve**
- **İLETİŞİM**

şeklinde tanımlanabilecek ilke ve değerlere sahip olarak kendisini sürekli geliştirmeye çalışır.

DivvyDrive Her Şeyi Saklayın, İstediğinizi Paylaşın

Kullanıcılarınızın elektronik ortamdaki tüm bilgi ve belgeleri artık tam koruma altında.

Dosyalarınız Güvende
Cihazlarınızın başına ne gelirse gelsin, DivvyDrive'da depolanan dosyalarınız güvendedir.

Veri Şifreleme
Dosyalarınız DivvyDrive'da özel kripto algoritmaları ile şifrelenerek saklanır.

Güçlü Arama
DivvyDrive dosyalarınıza daha hızlı erişmenizi sağlar. Anahtar kelimeyle içerik arayabilirsiniz.

Paylaşım
Dosyalarınızı istediğiniz kişilerle paylaşabilir ve düzenleyebilirsiniz.

Virüslere Karşı Koruma
DivvyDrive tüm verileri parçalayarak depoladığı için hiçbir virüs aktif hale gelemez.

7/24 Erişim
Verilerinize erişmek herhangi bir bilgisayardan DivvyDrive ile tüm verileriniz elinizin altında.

Kolay ve Güvenli Yedekleme

DivvyDrive, bulunduğunuz her yerde. Evinizde, iş yerinizde ve hareket halindeyken yanınızda. Siz neredeyseniz, dosyalarınız da tam orada. Harekete ve paylaşmaya hazır.

- Dosya Yükleme ve İndirme
- Şifreli Koruma
- SSL Sertifikası ile Bağlantı
- Sınırsız Bant Genişliği
- Güçlü ve Hızlı İçerik Araması
- Media Önizleme

YERLİ ÜRETİM

www.kottoas.com

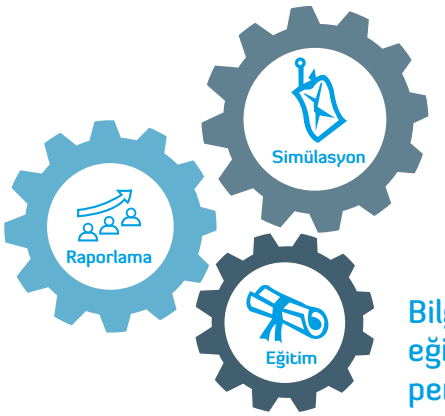
Olta.la ile Güvenliğiniz Kendi Elinizde

Olta.la, personel farkındalığını en üst düzeye çıkarmak için oltalama saldırılarını simüle etmenizi ve personelinizi bilgisayar başında eğitmenizi sağlar.

Personeliniz, Sizin Güvenliğiniz

Siber güvenlik tarihi boyunca, endüstri sürekli gelişen teknoloji altyapısından ve çevrelerden kaynaklanan tehditlere odaklandı. Yeni yatırımlara rağmen, yeni güvenlik olaylarının sayısı artmaya devam ediyor. Olta.la, makineler yerine siber güvenliğin en zayıf halkası olan insan savunmasını güçlendiriyor.

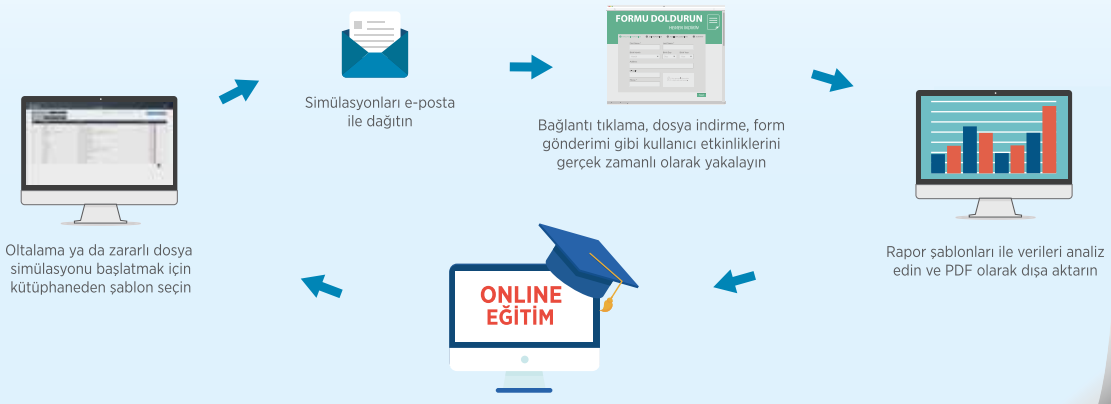
Oltalama ve Eğitim sonuçlarınızı grafiksel ve detaylı bir şekilde raporlayabilirsiniz.



Zengin ve güncel oltalama şablonları ile personelinizi oltalama saldırılarına karşı test edebilir

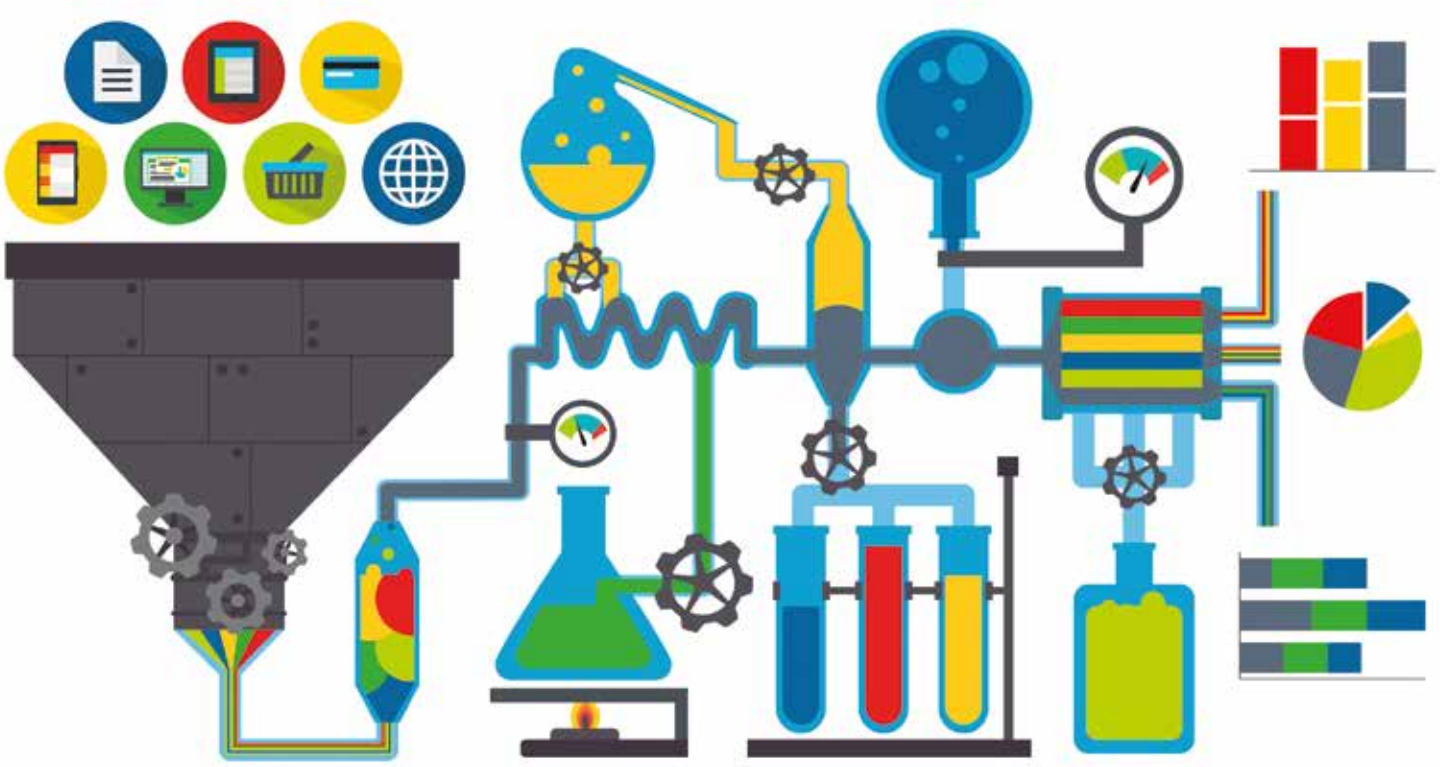
Bilgisayar başında eğitim alt yapısı ile personelinizi eğitebilir

Olta.la nasıl çalışır?



www.kottoas.com

YERLİ ÜRETİM



atarlabs

ATAR (Automated Threat Analysis and Response), tek bir siber güvenlik çözümüyle farklı ürünler kullanan kurumların da etkili sonuçlar elde etmesini sağlayan bir SOC ve siber güvenlik ROBOTU çözümü.

ATAR siber güvenlik robotumuz siber saldırıların hızına ve hacmine yetişemeyen kurumlara destek olan bir çözüm. ATAR savunma robotu, ona öğretilen saldırı reflekslerini otomatik olarak işletiyor. Böylece ATAR bir güvenlik operasyon merkezi içerisinde sık tekrarlanan işlemleri bir insana uzmana gerek kalmadan işletebiliyor. Toplam alarm işleme yükünün %30-40'lık bölümü otomatik olarak (robotla) karşılanırken, ATAR'ın sağladığı vaka inceleme ve yanıtlama imkanları operasyon merkezi uzmanlarının 15-20 kat daha hızlı analiz ve çözümleme yapmasına imkan sağlıyor.

TEKRARLANAN İŞLEM OTOMASYONU

- Senaryo odaklı otomasyon
- Karmaşık mantık bileşen desteği
- 90+ Platform için Bağlantı Desteği
- Tam veya Yarım Otomatikleştirme

ANALİST VERİMİNİ ARTIRMA

- Bütünleşik inceleme arayüzü
- İşbölümcü çalışma ortamı
- Tek tıklamayla delil topla ve işle
- Delil saklama / arşivleme

GÜVENLİK OPERASYON MERKEZİ

- SOC işlemlerinden ölçüm toplama
- Servis seviyesi anlaşma ölçümü
- İşyükü izleme
- Raporlama ve Tablolama
- İş/İşlem tasarrufu

YERLİ ÜRETİM

LimRAD
AUTH PLATFORM

Mobil Cihaz Yönetimi (MDM, Mobile Device Management) bir kısaltma olup, işletmelerin varlık ve taşınabilir bilgi güvenliği için kullandığı en güncel teknolojidir. MDM, dağıtım, güvenceye alma, izleme ve entegrasyon işlemlerinin yapıldığı idari alandır ve işletmelere temel olarak, iş yerlerindeki mobil aygıtların (akıllı telefon, tablet vb.) merkezden ve uzaktan yönetimine dair hizmetler sunar. Aşağıdaki işlev sayesinde, kullanıcıların çalışmalarını kesintiye uğratmadan, kablosuz bağlantı yoluyla mobil cihazlar hızlı ve etkin bir şekilde yönetilebilir ve uzak destek verilebilir.

Güvenlik Yönetimi:

Mobil cihazın çalınması veya kaybedilmesi halinde, güvenlik önlemi olarak tüm kurumsal veriler uzaktan kaldırılabilir ve silinebilir.

Politika Yönetimi:

Kurumsal verileri (kamerayı kapatmak, ekran görüntüsü aldırmamak, ekran kilidi ve parola kilidini zorunlu kılmak, bir hesaptan başka hesaba e-posta yönlendirmesini engellemek vb. yoluyla) güvence altına almak amacıyla işletmelere yönelik bilgi güvenliği kısıtlamaları mobil cihazlara otomatik olarak dağıtır.

Yazılım Dağıtımı:

İşletmelerin, uyguladıkları bilgi güvenliği politikasını esas alarak, kurulum için gerekli uygulamaları mobil cihazlara dağıtmasına olanak sağlar ve tekil kurulum yapma zorluğundan kurtarır.

Envanter Yönetimi:

Cihazdaki yazılım ve donanım verilerini düzenli olarak toplar ve kullanıcıların uygulamaları nasıl kullandıklarını izler.

LimRAD Auth Platform herhangi bir açık kaynak kod kullanılmadan yeniden kodlanmış geliştirilmiştir. Her bir modülü yeniden endüstri standartlarına göre yorumlanarak hazırlanmıştır. Lisanslama adedine göre ölçeklenebilir multithreading mimarisi sayesinde donanım kaynak kullanımını kendisi belirler. Erişimin yapıldığı erişim cihazı, zaman, cihaz türü, lokasyon, kullanıcı adı gibi bilgiler ile doğrulama sırasında kullanıcılar ayrıştırılabilir ve buna göre yetkilendirme yapılabilir. Çoklu donanım üreticisi desteği sayesinde (Multi-Vendor) donanım marka bağımlılıklarınızı ortadan kaldırır. Endüstri standardı çalışan tüm üreticiler ile birlikte çalışabilir. Çalışırken arttırılabilir kapasite özelliği sayesinde tek bir sanal cihaz (Virtual Appliance) üzerinde 1.000.000 cihaza kadar eş zamanlı yönetim yapılabilir.

YERLİ ÜRETİM

volthread®

WebLogic Akıllı Kontrol ve İzleme Panosu

Volthread ürünleri hali hazırda kullandığınız APM (Application Performance Monitoring) yapınıza, veritabanı yapınıza ve diğer benzer dış sistemlere kolayca entegre olarak sistemin bir parçası haline gelir.

Tamamı microservis mimarisi ile tasarlanmıştır. Yerleşik uygulama sunucusu üzerinde koşan uygulamalar, yerleşik veritabanı ile desteklenmektedir.

Bu mimari ile hiçbir ek/yan kurulum olmaksızın dakikalar içerisinde ayağa kalkarak kullanılmaya başlanabilir.

Bir arıza yada yavaşlık anında, sorunlu servisin sorumluları entegre olunan sistemlerden sorgulanarak HTML e-posta ve SMS ile bilgilendirilir. Benzer şekilde sorunun çözülmesi durumunda ilgili kişi ve birimler tekrar HTML e-posta ve SMS ile bilgilendirilir ve bu sayede tepki ve sorun çözme süreleri dakikalar seviyesine geriler.

Oluşturulan tüm bildirimler saklanarak, uygulama arayüzü üzerinden geçmişe yönelik sorgulama ve raporlama imkanı sunar.

Sistem tarafından izlenen tüm servislerin, son yirmidört saatlik verileri izleme panolarına (dashboard) ve saklama sınırı kullanıcı tarafından belirlenen raporlama sistemine aktarılır.

Panolar ile tüm servisler anlık olarak izlenirken, raporlama sistemi ile günlük, haftalık, aylık, üç aylık ve yıllık performansları raporlanarak sorgulanabilir.

WLSDM:
Tam Uyumlu WL İzleme ve Teşhis

WL-OPC:
WLSDM Operasyon Merkezi

VOI:
Volthread Outbound Inspector
Web Servis İzleme

JSL:
Java Server Loader

SMReporter:
Rapor Görselleştirme Aracı

Java4Admin:
Java Admin Öğretimi

YERLİ ÜRETİM

BiSoft
Bilirsen Yönetirsin

vispeahen

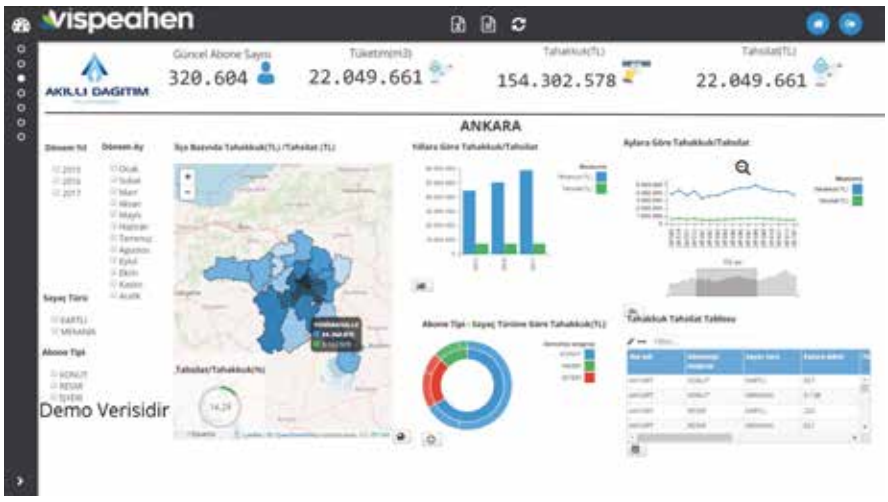
Big Data Visualization Tool

Büyük Veri Görselleştirme Aracı

Açık mimari (open architecture) yapısındadır.
Görseller plug in'ler şeklinde eklenebilmektedir.
Big Data Entegrasyonu yapılabilmektedir.
Farklı veri kaynaklarını aynı modelde görselleştirebilmesine olanak sağlamaktadır.
Dağıtık mimaride çalışabilmektedir.
Yüksek yük altında çalışabilmektedir.
Web tabanlı modelleme yapılabilmektedir.

Dinamik Görseller

Otonom Veritabanları İle Çalışma

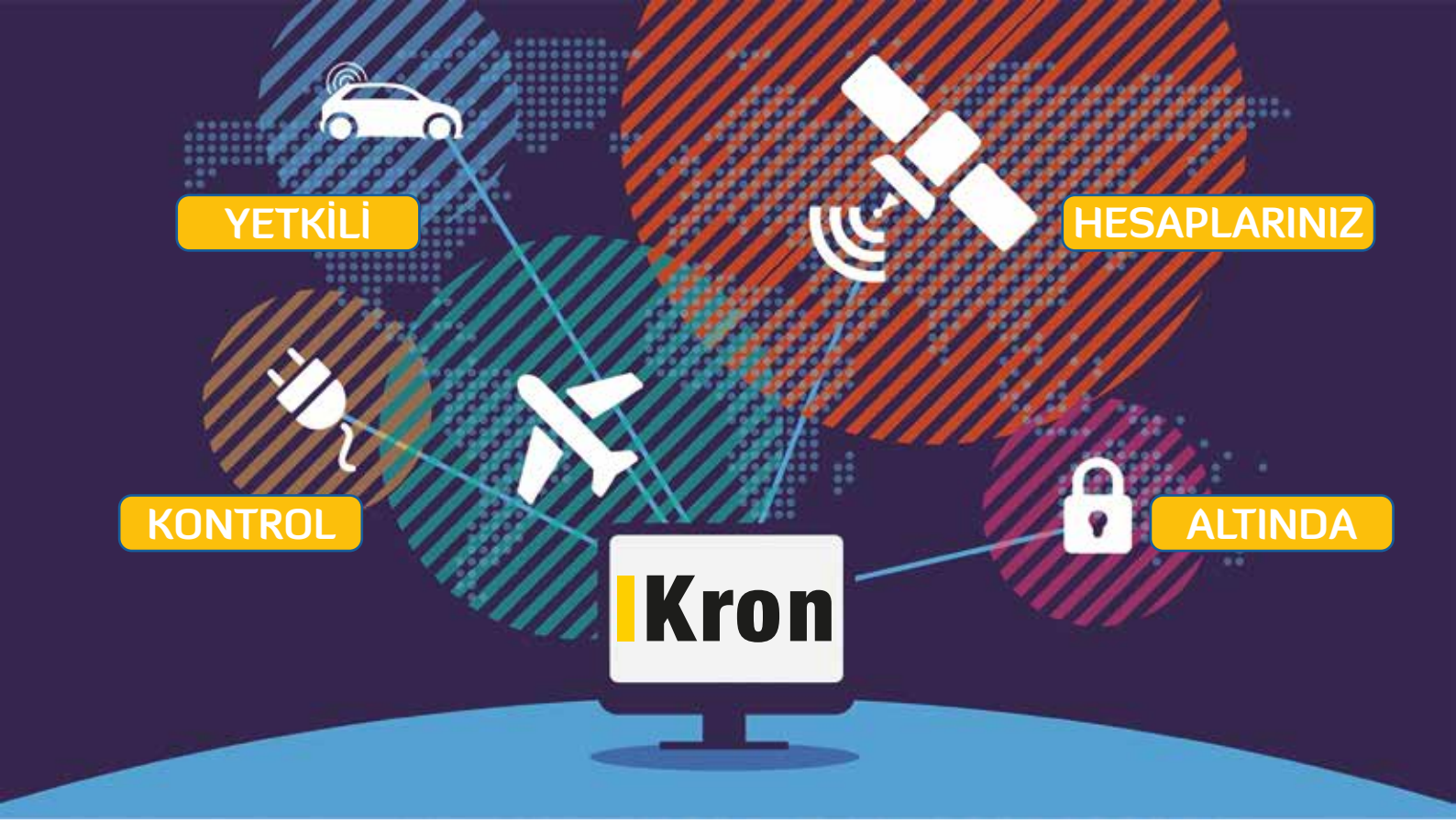


Cografi Raporlama

Ağ Bazlı Güvenlik

Resim dosyalarının metadataları üstünde sorgulama yapılarak raporlama imkanı sağlamaktadır.

YERLİ ÜRETİM



Geniş Ürün Gamı

Single Connect, kurumsal organizasyonların iç ve dış siber güvenlik tehditlerine karşı Kron tarafından geliştirilmiş kullanıma hazır geniş kapsamlı modüllere sahip yetkili hesap erişim güvenliği platformudur. Single Connect, bilişim altyapı sistemlerindeki tüm yetkili erişimleri yönetir ve veri güvenliğini sağlar.

Yetkili Oturum Yönetimi

Tüm yetkili kullanıcı işlemlerini ve oturumlarını denetim altına alır.

Merkezi Parola Yönetimi

Yetkili hesap parolalarının güvenliğini sağlar ve kullanımlarını kayıt altına alır.

Çok Faktörlü Kimlik Doğrulama

Tüm erişimlerde parola yanında ikinci bir kimlik doğrulama katmanı sağlar.

Benzersiz Özellikler

Single Connect, ayrıcalıklı ve yetkili erişim yönetimi alanında, sahip olduğu modüler yapısı ve ajansız mimarisi sayesinde çok kısa sürede devreye alınır. Gelişmiş oturum yönetimi sayesinde kötü niyetli aktiviteleri gerçekleşmeden gerçek zamanlı olarak tespit eder, önler ve kayıt altına alır.

Veritabanı Erişim Yönetimi

Veri tabanı yöneticilerinin hassas ve kritik verilere doğrudan erişimlerini yetkilendirir ve kayıt altına alır

Dinamik Veri Maskeleme

Hassas ve gizli verilerinize erişimi kaynak veriyi değiştirmeden maskeleyerek verilerin güvenliğini sağlar

TACACS+ / RADIUS

Ağ altyapınızdaki cihazlar için TACACS+ / RADIUS protokolü üzerinden merkezi kimlik doğrulama ve yetkilendirme servisi sunar

Regülasyon Uyumu

Single Connect™ finans, enerji , sağlık, telekomünikasyon gibi regülasyonlarla düzenlenen sektörlerde yetkili hesap yönetimi alanında uyumluluğu sağlamak için gerekli kritik güvenlik araçlarını merkezi olarak sunar. ISO 27001, ISO 31000:2009, KVKK, PCI DSS, EPDK, SOX, HIPAA, GDPR gibi regülasyonlara tam uyumluluk ve denetim süreçlerinde destek sağlar.

YERLİ ÜRETİM

Cyber X-Ray Nedir?

Roksit Cyber X-Ray, DNS trafiğini araştırır, analiz eder ve kategori sınıflandırması yapar. DNS trafiğinin analizine bağlı olarak "Kötü Amaçlı Yazılım – C&C Botnet – Fidye Yazılımı – Kimlik Avı vb." gibi zararlı ağ trafiğini algılar ve engeller. Böylece etkili bir koruma sağlar.

Secure DNS

Roksit DNS güvenlik duvarı, kullanıcıların DNS trafiğini analiz ederek web güvenliği ve uygulama kontrolü sağlayan etkili/gelişmiş Bulut Tabanlı bir Siber Güvenlik Hizmetidir. Gelişmiş ve esnek raporlama özelliği sayesinde ağ yöneticilerine gerekli aksiyonları alabilmeleri için anlamlı bilgiler sunar.

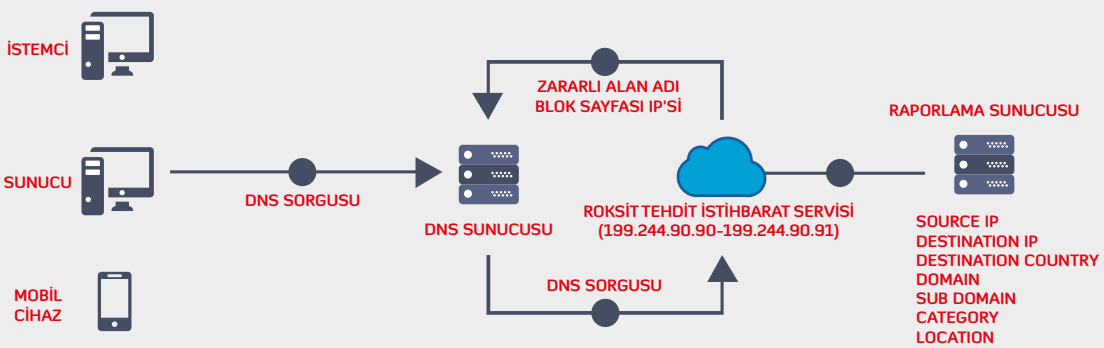
DNS & Threat Visibility

DNS and Threat Visibility çözümü, kurum DNS sunucu loglarını inceleyerek, sunucu / kullanıcıların herhangi bir port ya da protokol üzerinden yapmış oldukları trafik için gelişmiş ve analiz edilmiş DNS görünürlüğü sağlar. DNS isteklerini, Roksit İstihbarat Servisi aracılığı ile kontrol edip zararlı trafiği tespit eder.

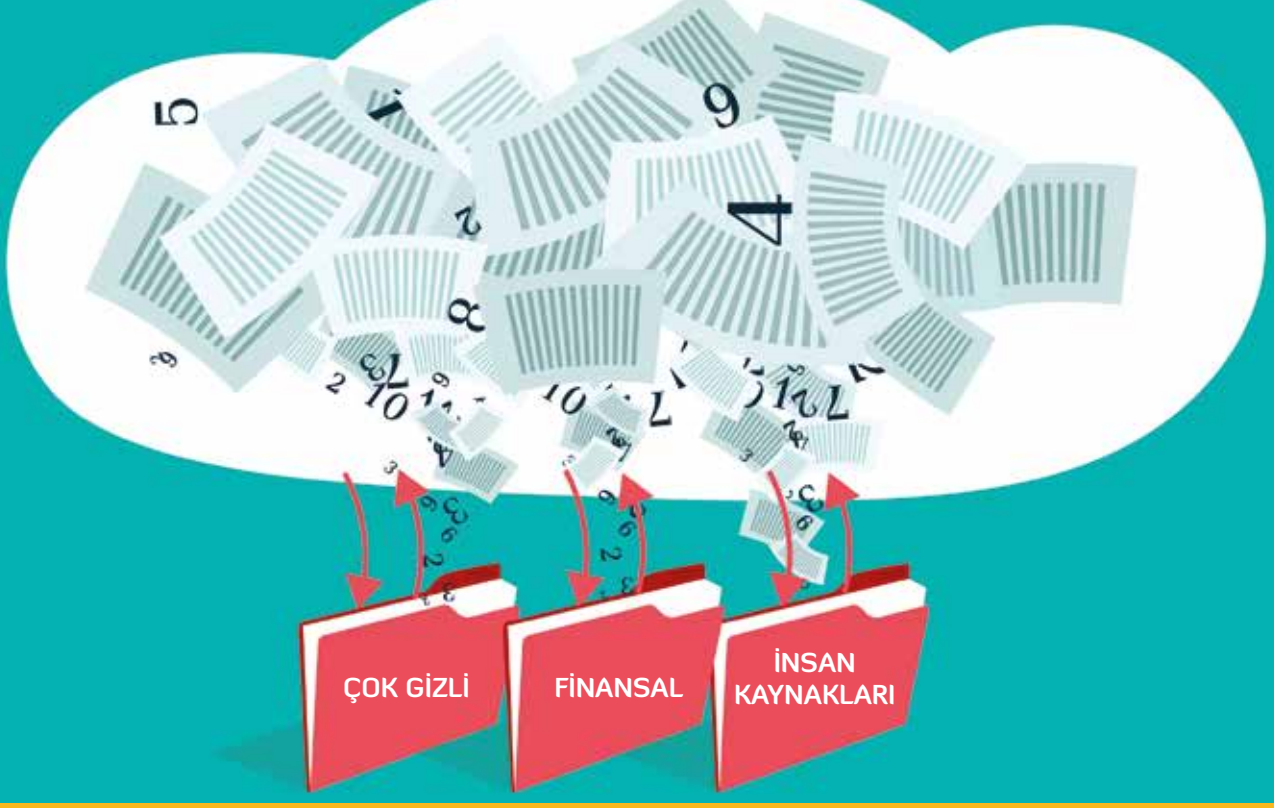
Threat Hunter

Roksit Threat Hunter, istemci ya da sunucularda; zararlı trağı, hangi uygulama, hangi proses ya da hangi dosyanın bu zararlı trağı oluşturduğunu tespit eden ve raporlayan, ajansız bir çözümdür. Threat Hunter ürünün çalışması için istemci, sunucu ya da ağ seviyesinde herhangi bir değişiklik yapılmasına gerek yoktur.

SecureDNS



YERLİ ÜRETİM



TÜM KURUMLARA ÖZEL KVKK UYUMLULUK DESTEĞİ

TITUS, kuruluşunuzun KVKK ile uyumunu nasıl sağlar?

TITUS, mevcut verilerinizi, bu verilerin ne kadar hassas olduklarını ve güvenlik biriminiz tarafından bunların nasıl kontrol edilmesi gerektiğini belirleyerek, veri koruma ve gizlilik programınızın etkililiğini güçlendirir. Sektör ve analist araştırmaları, verilerinizin belirlenmesi ve sınıflandırılmasının KVKK uyumunun en temel adımları olduğunu göstermiştir. TITUS, kişisel verilerin belirlenmesi, sınıflandırılması ve güvenliğinin sağlanması konusunda çalışanlarınızı ve politikalarınızı bu doğrultuda harekete geçirecek bir çözüm sunar.

TITUS

Mevcut Datayı Tespit Etme
- İçerik
- Dosya Adı
- Dosya Lokasyonu
- Dosya Öznitelikleri

Metadata ile Sınıflandırma
- Sınıflandır
- Sınıflandırma Öner

Hassas Veri Koruma
- RMS Şablonu Uygula
- Dosyayı Kopyala/Taşı/Sil
- Dosyayı İşaretle

Dosya Analizi
- Dosya Erişim İzinleri
- Dosya Sahipleri
- Sınıf

TITUS, hassas verilerinizi keşif/belirleme, sınıflandırma ve etiketlemede, güvenlik politikalarına dayalı bir yapı oluşturmanızı sağlar.

TITUS 12'den fazla KVKK maddesinin gereksinimlerini destekleyerek KVKK uyumlu hale gelmenize yardımcı olurken iş hedeflerinizi de yerine getirir. Esnek politika mekanizması ile çalışan en güçlü ve birlikte çalışabilir veri koruma çözümü sayesinde TITUS, çalışanlarınızı, süreci ve teknolojiyi destekler.

İster uyumluluk yolculuğunun başında olun, isterseniz mevcut veri güvenliği yatırımlarınızı etkili kullanmaya yönelik bir çözüm arayışında olun, TITUS her iki iş ve uyumluluk hedefinizi de gerçekleştirmenize yardımcı olacaktır.

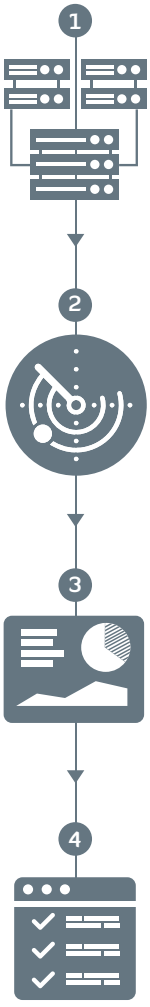
PICUS

Her geçen gün kurumların en büyük tehdidi haline gelen siber saldırılar için yerli girişimci Picus harekete geçti. Kurumların siber güvenlik açıklarını test eden ürünümüz, bu alanda ihracata başlayan ilk çözüm.

Picus ile birçok kurumun uzun sürede tespit edebildiği güvenlik açıklarını, çok daha kısa sürede ortaya çıkarmaya yardımcı oluyoruz.

Sürekli güvenlik denetimi yaklaşımını geliştirerek, şirketlerin sahip olduğu teknolojiyle kurumların bu tehditlere ne ölçüde hazır olduklarını ve ellerindeki mevcut güvenlik yatırımıyla bu saldırılardan korunmak için yapmaları gerekenleri raporluyoruz.

Saldırganlar tarafından kullanılan 2 bin 400'den fazla atak tekniğine Picus Security Labs tarafından her ay 200 farklı tehdidin eklendiği ve testlerin günlük olarak sürekli yapılabildiği bir yapı, kurumların siber saldırılara hazırlık seviyesinin arttırılmasını sağlıyor.



Yükle ve Yaygınlaştır

Yazılım seti birkaç saat içinde kurulabilir ve hemen çalışmaya başlayarak kritik sonuçlar üretir.

İlk Durum Değerlendirmesi

Güvenlik açıklarını ve zafiyetleri tespit ederek gerçek zamanlı eylemler için rehberlik eder.

Ölçüm ve Görselleştirme

Elde edilen sonuçları gerçek zamanlı olarak raporlar, tablolar ve objektif kıyaslamalar yapmaya olanak tanır.

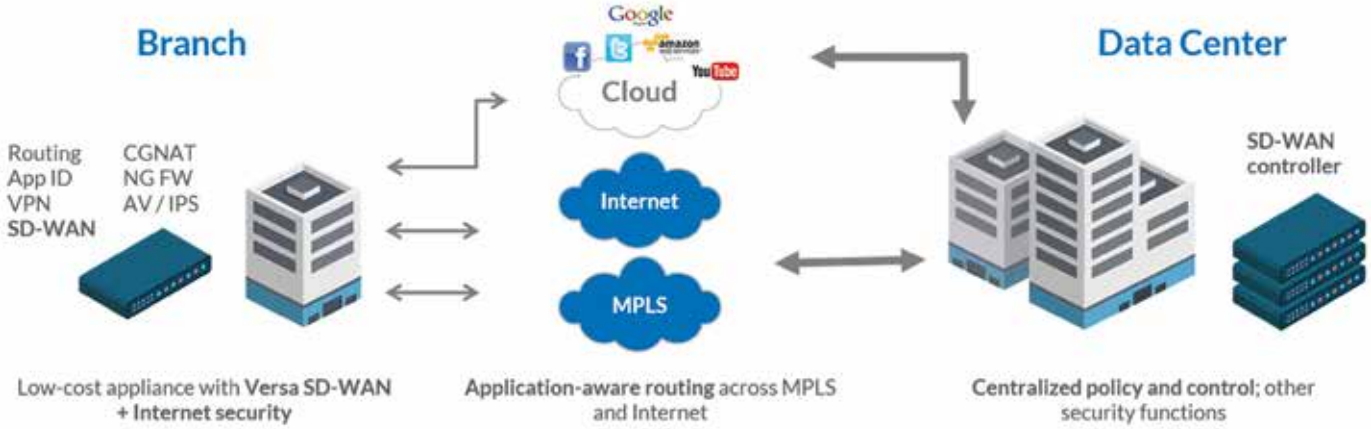
Yatıştırma ve Hafifletme

Ürün ve üreticiye özel tespit edilmiş olan zafiyetlere yönelik iyileştirme önerileri ve acil eylem planları hazırlar.

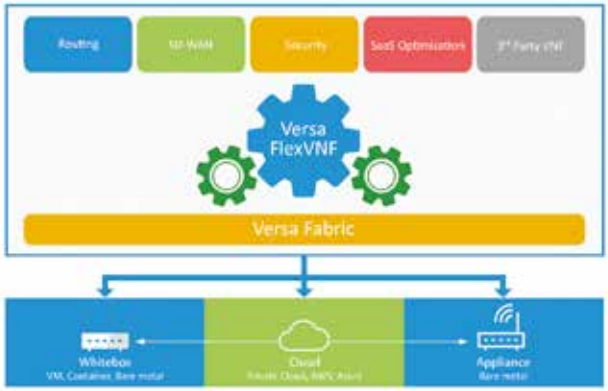
YERLİ ÜRETİM

Yazılım Tanımlı Geniş Alan Ağı Çözümleri (SD-WAN)

Versa, WAN/şube networkünü basitleştirip güvence altına alarak uçtan-uca bir çözüm sunan yazılım tanımlı geniş alan ağı çözümleri (SD-WAN) sunmaktadır. Versa'nın tamamen yazılıma dayanan Cloud IP Platformu, çevik ve güvenli kurumsal networkler oluşturma yeteneği, yüksek verim ile yönetilen servis için sadeleştirme, yalınlaştırma ve uygulayıcılar için geniş bir set sunar.



Network endüstrisi uzmanları tarafından kurulan Versa Networks; SD-WAN, SD-Güvenlik ve SD-Şube pazarında yenilikçi bakış açısı getiren bir tedarikçidir. Versa, WAN/şube networkünü basitleştirip ve güvence altına alarak uçtan-uca bir çözüm sunan yazılım tanımlı network üreticileri arasında benzersiz bir yapıya sahiptir.



Versa, Sequoia, Mayfield, Artis Ventures ve Verizon Ventures firmalarının önde gelen yatırımcıları tarafından desteklenmektedir.
Çeşitli branşlarda Gartner, IDC ve NSS tarafından derecelendirilmiştir.

Dünyada kabul görmüş test yaşam döngüsü metodoloji araçları

TESTINIUM

Testinium, Türk arge mühendisleri tarafından geliştirilmiş %100 Yerli ve Millli bir üründür. Temel olarak web ve mobil platformlarda Selenium ve Appium betiklerini koşturarak testlerinizin planlanması, raporlanması ve yönetimini sağlamaktadır.
Testinium Cloud platformu üzerinde 200' den fazla gerçek cihaz ve sim kart bulunan bir mobil cihaz platformu sunulmaktadır. Cloud tabanlı dakika bazlı kullanım sayesinde testlerinizi bu gerçek cihazlar üzerinde koşturabilirsiniz. Testinium cloud tabanlı kullanım dışında bilgi güvenliği gerekçesi ile iç kurulum desteği ile de sunulmaktadır.

Testinium aşağıdaki özelleştirmeleri sağlamaktadır.

- Test planlama
- Cihaz seçimi
- Ekran çözünürlüğü seçimi
- Bant genişliği seçimi
- İşletim sistemi seçimi
- Zamanlama seçimi
- Detaylı raporlama
- Jenkins ve Bamboo gibi sistemlerle entegrasyon
- Jira entegrasyonu
- HP ALM entegrasyonu

LOADIUM

Loadium, Türk arge mühendisleri tarafından geliştirilmiş %100 Yerli ve Millli bir üründür. Amacı yoğun yükte ve dağıtık sistemlerden gerçek kullanıcı davranışlarına yakın talep çıkmak ve anlık olarak raporlamaktır. Standart ürünlerden en önemli farkı talep sayısını geniş bir ağdan yapılan taleplerin gerçek taleplere en yakın sonuçları elde etmesi ve milyonlarca taleplik yüklere çılabilme yeteneğidir.
Loadium Cloud sayesinde istemci sayısı oranında fiyatlama yaklaşımı ile düşük maliyetlerde yüklerin çıkması sağlanabilir.

Loadium aşağıdaki özelleştirmeleri sağlamaktadır.

- Test planlama
- Anlık raporlama
- JMeter ve Gatling desteği
- Test koşumunda talep sayısı belirleme
- Test koşumu İstemci sayısı belirleme
- Bant genişliği seçimi
- APM (Application Performance Monitoring)
- Test koşumu sonrası detaylı loglar
- Detaylı raporlama
- Jenkins ve Bamboo gibi sistemlerle entegrasyon

JUnit git Gatling New Relic dynatrace JMeter AppDynamics

YERLİ ÜRETİM

Harddisk ve Manyetik Medya İmha Çözümleri, Degausserlar

Savunma ve güvenlik endüstrisinde faaliyet gösteren İngiltere menşeili firma, 30 yılı aşkın tecrübesiyle her türlü manyetik ortama uygun, piyasadaki en kapsamlı güvenli veri imha çözümlerini tasarlamakta, üretmekte ve satmaktadır.

DataGone

VSSP DataGone MANYETİK İZLERİ BOZMA (DEGAUSS) CİHAZI

VSSP DataGone, 3.5", 2.5" & 1.8" IDE/SATA Sabit Sürücüleri, ile DLT,2,3,4,5,6 & SDLT, LTO1,2,3,4,5,6,7 & 8; 3480/3490/3490e, 3590, 9840 & T9940 & T10000 tape; Ultrium & Redwood SD-3 tape & cartridges; Mammoth 1 & 2, 8mm, AIT1 & 2,M2 tape; DDS 1, 2, 3, 4 & 5, DD-2 kasetlere Degauss işlemi uygulayarak kullanılmayacak hale getirmektedir.

VSSP DataGone, yaklaşık 10000 Gauss manyetik kuvvetle ortalama 8 saniye içerisinde sabit sürücüleri kullanılmaz hale getirmektedir.
Ortalama İmha Bilgisi: Saatte 200 adet sabit disk veya kaset imha edebilmektedir

konneka
Bilgi ve İletişim Teknolojileri

TOTAL APPLICATION DELIVERY PLATFORM® (TADP)

Yük Dengeleme Platformu ve Web Uygulama Güvenlik Duvarı

Yük Dengeleyici ve Web Uygulama Güvenlik Duvarı (WAF) Geliştirilmesi Projesi kapsamında TADP markası altında Türkiye'nin ilk ve tek yerli "Yük Dengeleme ve WAF" cihazları geliştirilmiştir.

Yüksek Performans

Layer3 ve Layer7 ile farklı protokollerde (HTTP,DNS,SMTP,IMAP,POP3 vb.) Load-Balancing desteği.

Kullanıcı Dostu Arayüz

Uçtan uca tüm cihazları yönetmek için merkezi olarak lokal veya bulut üzerinden çalışan güvenli yönetim arabirimi.

Bulut Desteği

Bulut uyumluluğu için geliştirilmiş API desteği.

Gelişmiş WAF Seçenekleri

Pozitif ve Negatif WAF ile etkin koruma, öğrenme ve imza tabanlı güvenlik.

Paralel Çalışabilme Yeteneği

Yüksek trafik yoğunluğu ve yedeklilik senaryoları için ekstra kablolamaya ihtiyaç duymadan çalışan stacking mimarisi.

Tamamen yerli üretim olan TADP, sahip olduğu paralel çalışabilme teknolojisi ile diğer tüm yük dengeleyici veya uygulama dağıtıcı platformlarından ilerideidir. TADP hali hazırda tamamlanmış olup, resmi olarak satışları gerçekleştirilmektedir. Proje kapsamında yerli bir üretici bulunmamaktadır.

YERLİ ÜRETİM

GLOBAL ÇÖZÜM ORTAKLARIMIZ

Dijital Dönüşüm İş Ortağınız

KOTTO
BİLİŞİM A.Ş.

KOTTO BİLİŞİM

Plenty Plaza No: 17 Cevizlidere - Çankaya / ANKARA

Tel: +90 312 472 30 30

info@kottoas.com