QNAP ile IT/OT Güvenliğini Güçlendirin

Depolamadan Katmanlı Korumaya, Kesintisiz Operasyonlar Sağlayın

Adım adım IT/OT güvenliği, kararlı ve doğru

Modern işletmelerde, IT sistemleri ve OT (Operasyonel Teknoloji) ortamları artık birbirinden ayrılamaz durumdadır ve siber tehditler ofis ağlarından üretim sahalarına kadar uzanmaktadır. Birçok üretici için OT güvenliğini uygulamak genellikle bir kaynak sorunu değil, daha çok yöntem ve uygulama zorluğudur.

QNAP, işletmelerin siber güvenliği uygularken karşılaştıkları gerçek dünya zorluklarını anlar. Bu yüzden 'tek seferlik' bir yaklaşımı savunmuyor, bunun yerine depolamadan korumaya kadar görünür, yönetilebilir ve uygulanabilir bir güvenlik temeli oluşturmayı öneriyoruz. Bu da KOBİ'lerin IT/OT güvenliğine doğru her adımı kararlılıkla atmasını sağlar.

80%

oranında üretim firması güvenlik olaylarında bir artış yaşadı ya da

45%

'i bu tehditleri yönetmek için yeterli donanıma sahip olduğunu hissetti

60%

state that OT security complexity was top concern

Kaynak

https://www.telstrainternational.com/en/news-research/research/secure-manufacturing-the-challenges-of-IT-OT-convergence

https://www.paloaltonetworks.com/blog/network-security/state-of-ot-security-2024/

QNAP, depolama teknolojisini siber savunma gücüne dönüştürerek kurumların IT/OT güvenlik cephelerini koruma altına alır.

QNAP; depolama, ağ yönetimi, tehdit tespiti, çevrim dışı yedekleme ve uzaktan erişim gibi geniş bir yelpazede çözümler sunar.

NIST CSF ve IEC 62443 gibi önde gelen OT siber güvenlik standartlarıyla tam uyumlu çalışan QNAP çözümleri, kritik sektörlerin güvenliğini ve mevzuata uyumunu sağlar. Kurumların hem IT hem de OT ortamlarında şeffaf, dirençli ve felaket anında hızla kurtarılabilir bir güvenlik altyapısı kurmalarına olanak tanıyoruz.





Doğru Yol Haritasıyla Siber Güvenlik.

NIST CSF 2.0 ile Adım Adım IT/OT Savunması İnşası

- NIST Siber Güvenlik Çerçevesi (CSF); kurumlar, üreticiler ve kritik altyapı sağlayıcıları tarafından geniş kabul görmüştür. NIST CSF 2.0'ın 2024 güncellemesi, çerçevenin OT ortamlarındaki pratik uygulanabilirliğini daha da artırmaktadır.
- Altı temel işlev (Tanımla, Koru, Tespit Et, Müdahale Et, Kurtar, Yönet); kurumlara net bir siber güvenlik yol haritası sunar.
- Katmanlı savunma, varlık görünürlüğü, olaya müdahale ve kurtarma kabiliyetlerine odaklanan bu çerçeve, QNAP'ın çözüm mimarisiyle birebir örtüşmektedir.
- KOBİ'ler için NIST CSF, yalnızca bir standart değil, aynı zamanda aşamalı geçişi sağlayan pratik bir uygulama rehberidir.
- QNAP; NAS depolama birimlerini, ağ cihazlarını ve güvenlik uygulamalarını entegre edip NIST CSF 2.0'ı temel alarak kurumların sürdürülebilir ve uygulanabilir IT/OT siber savunma altyapıları kurmasını sağlar.

Standartlardan Uygulamaya

QNAP Çözümleri, NIST CSF 2.0'ın Temel İşlevlerini Birebir Karşılar

● Tüm Ürün Ailelerinde Desteklenir

● Yalnızca Belirli Ürün Modellerinde Desteklenir; Tüm Serilerde Bulunmaz

– Desteklenmiyor

İşlev Kategorisi"	Sorun Noktaları	Çözüm	NAS	QHora Router	ADRA Switch	QSW Managed Switch
Tanımla	Farklı IT/OT ortamı cihazlarında merkezi bir varlık envanterinin bulunmaması	Merkezi cihaz yönetimi	●	●	●	●
		Görselleştirilmiş envanter	●	●	●	●
		Bulut tabanlı izleme	●	●	–	●
Koru	Eski nesil kontrol sistemlerinin modern tehditlere karşı yetersiz kalması	Veri şifreleme	●	●	–	–
		Çok katmanlı erişim kontrolü	●	●	–	●
		Ağ segmentasyonu	●	●	●	●
Tespit Et	IT/OT ortamlarındaki anormallikler için gerçek zamanlı izleme eksikliği	Cihaz anormallik tespiti	●	●	●	●
		Oturum açma anormallik tespiti	●	●	●	●
		Ağ anormallik tespiti	●	●	●	●
Müdahale Et	Olay anında anlık bildirim/raporlama mekanizmasının olmaması	Anlık uyarılar	●	●	●	●
		Uzaktan erişim	●	●	●	●
		Bulut yönetimi	●	●	–	●
Kurtar	Otomatik yedekleme mekanizmasının olmaması; zorlu felaket kurtarma	Yedekleme mekanizmaları	●	●	–	●
		Veri bütünlüğü	●	–	–	–
		Felaket kurtarma	●	–	–	–

Depolamadan Ağ Altyapısına, QNAP, IT/OT Siber Güvenliğini Güçlendiriyor





NAS

IT/OT Ortamları İçin Kritik Depolama, Yedekleme ve Uygulama Entegrasyonu Platformu

- Yapay zekâ analizi, sanallaştırma, QuFirewall ve AMIZcloud yönetimini destekler
- Bazı modeller; zorlu ortam şartlarına uygun, endüstriyel standartlarda tasarıma (masaüstü, kabinet tipi, duvara monte, çift güç beslemesi) sahiptir

Kurumsal Sınıf QuTS hero NAS:

- Guvenilir dosya depolama ve yedekleme (anlık görüntüler/snapshots, değiştirilemez yedekler, WORM)
- Kesinti süresi riskini en aza indiren yüksek erişilebilirlik (HA) mimar



QHora Router'lar

IT/OT Etki Alanları Arası Ağ Güvenliği ve Bağlantı Koruması Sağlar

- İlke tabanlı / mikro segmentasyon yönlendirmesi, L3 - L7 güvenlik duvarı, DPI paket inceleme, IPS izinsiz giriş önleme
- Güvenli uçtan uca veri iletimi için Qbelt (DTLS + AES-256), WireGuard ve OpenVPN desteği
- WPA/WPA2/WPA3 Wi-Fi ile güvenli kablosuz erişim

QuWAN SD-WAN:

- Çoklu saha bağlantısı ve merkezi yönetim
- WAN optimizasyonu ve otomatik yedekli geçiş (failover) ile kararlı uzaktan bağlantılar



ADRA NDR Switch'ler

Kötü Amaçlı Trafiğe ve Anormal Davranışlara Karşı Gerçek Zamanlı IT/OT Ağ Koruması

- Yüzlerce cihazda yapay zekâ destekli anormallik tespiti; iç ve dış tehditlerin erkenden saptanması
- Hassas saldırı engelleme için gelişmiş trafik analiziyle otomatik olaya müdahale ve iyileştirme
- Yatay ilerlemeyi (lateral movement) önler, enfekte olmuş cihazları izole eder ve şüpheli etkinlikleri engeller
- SOC/SIEM entegrasyonu; NAS, PC, yazıcılar ve PoE cihazlarını koruyarak eksiksiz bir ağ savunması oluşturur



QSW Yönetilebilir Switch'ler

IT/OT Sistemleri İçin Uzak Mesafe, Yüksek Bant Genişliği ve Düşük Gecikmeli Omurga Bağlantısı Sunar

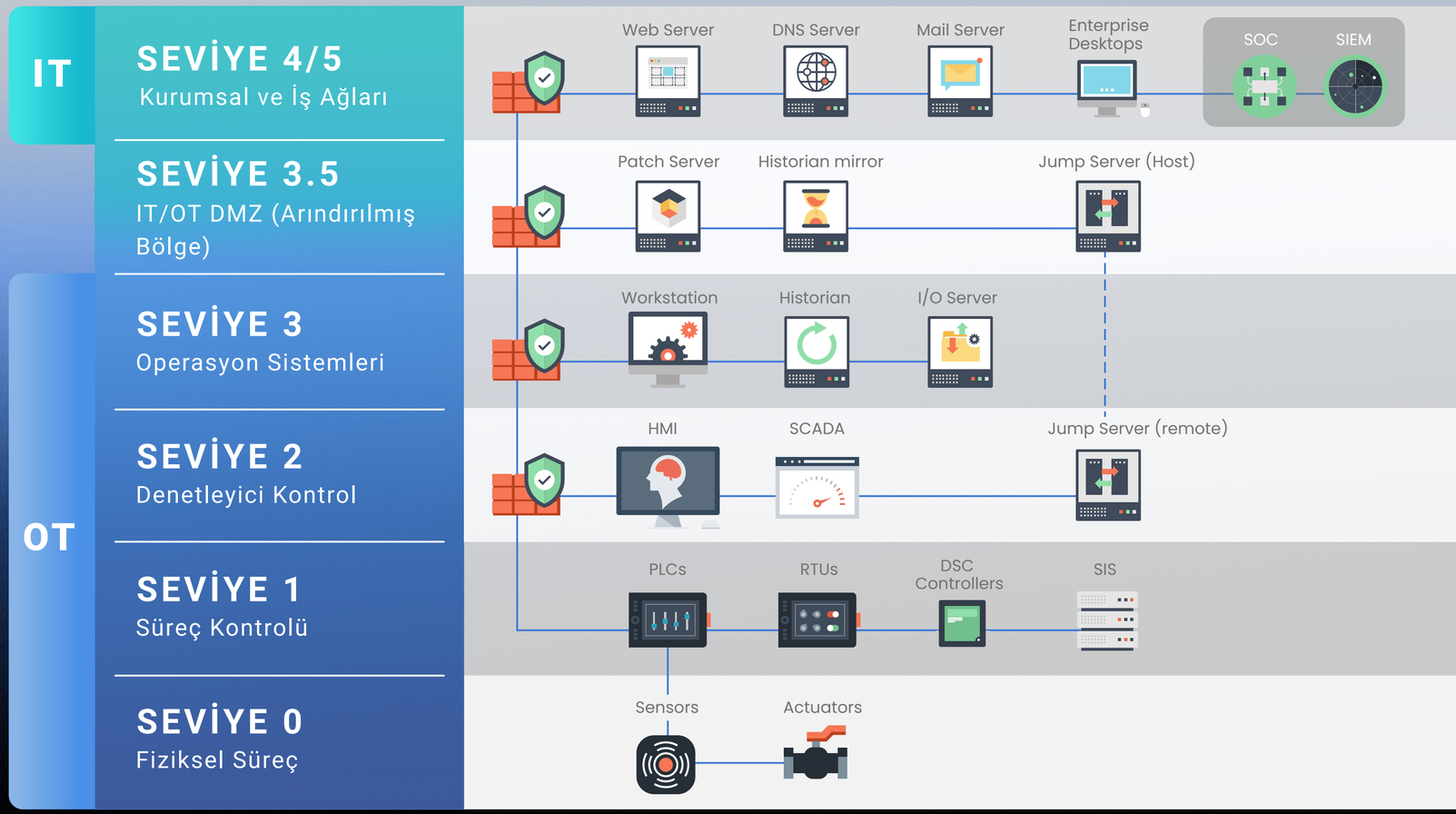
- Kurumsal çekirdek/uç (core/edge) ağlara uygun 2.5GbE / 10GbE / 25GbE / 100GbE fiber ve bakır bağlantı seçenekleri
- Farklı uygulamalar için trafiği optimize eden VLAN ve QoS yönetimi
- AMIZcloud merkezi izleme ve yönetim desteği
- Bazı modeller cihazlara güç sağlamak için PoE özelliğine sahiptir; zorlu ortam şartları için tasarlanmıştır

Kurumsal Sınıf L3 Switch'ler:

- Dahili MC-LAG HA (Yüksek Erişilebilirlik) ile 7/24 kesintisiz çalışma olanağı
- PTP IEEE ITU-T G.8273.3 Sınıf A <100ns zaman senkronizasyonu ile OT ve endüstriyel kontrolün hassasiyet gereksinimlerini karşılar

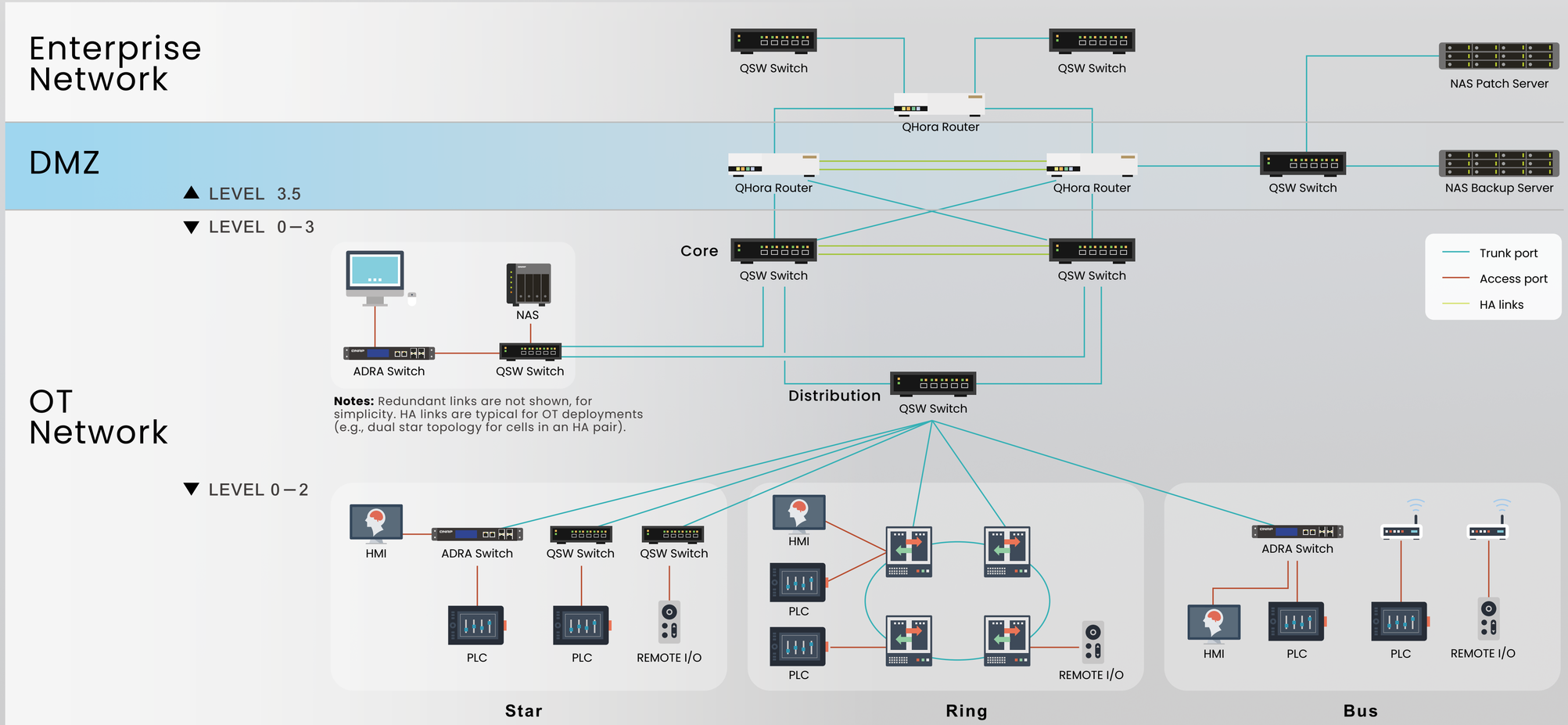
Purdue Modelini Esas Alarak – IT/OT İçin Kapsamlı Koruma

İşletmeler, katmanlı bir endüstriyel kontrol ağı mimarisi olarak uluslararası düzeyde kabul gören **Purdue Modelini*** benimseyebilir. IT ve OT arasındaki rolleri ve sınırları net bir şekilde belirleyen bu model; güçlü siber güvenlik savunmaları kurmak ve alanlar arası iş birliğini sağlamak için sağlam bir temel sunar.



*Katmanlı endüstriyel kontrol ağları için yaygın olarak kullanılan ve ISA/IEC 62443 ile NIST 800-82 standartlarında geniş kabul gören bir çerçeve.

QNAP, IT/OT Yakınsama Katmanı Siber Güvenliğini Koruma Altına Alır



Page. 12

Adım Adım IT/OT Güvenliği Page. 2

NIST CSF 2.0 Temeliyle Başlangıç Page. 4

QNAP'ın Kapsamlı Depolama ve Ağ Çözümleri Page. 6

Purdue Modelini Esas Almak Page. 11

IT/OT Yakınsama Katmanının Emniyete Alınması Page. 12

Breaking Down the Five Core Functions of NIST CSF 2.0 Page. 13

NIST CSF 2.0'ın Beş Temel İşlevinin İncelenmesi Uygulanabilir Bir IT/OT Siber Güvenlik Savunması İnşa Etmek



Tanımla

Varlık görünürlüğünden kullanıcı farkındalığına: IT/OT güvenliğinin temellerini inşa etmek

Siber güvenlikte ilk adım 'sahip olduğunuz şeyleri bilmektir.' Ancak pratikte birçok kurum; parçalanmış varlık yönetimi, dağınık hesaplar ve karmaşık bağlantı yapıları gibi zorluklarla karşılaşır. QNAP; kişiler, cihazlar, ağlar ve veriler genelinde tanımlama ve erişim yönetimi sağlayarak kuruluşların etkili bir risk kontrol temeli kurmasına yardımcı olur.



Merkezi Varlık Envanteri ve Cihaz Yönetimi

- **QuWAN Orchestrator:** SD-WAN bulut orkestrasyon sistemi; IP adresi, model ve cihaz durumu dahil olmak üzere QNAP cihazlarına sahip kurumsal ağ segmentlerinin otomatik olarak tanımlanmasını ve merkezi olarak yönetilmesini sağlar.
- **ADRA NDR Switch Cihaz Envanteri:** Paket analizi yoluyla; MAC adresi, IP adresi, anasistem adı (hostname) ve durum bilgileri de dahil olmak üzere ağa bağlı cihazları otomatik olarak tanımlar.

Felaket Kurtarma Kabiliyeti:

- Anlık Görüntüler (Snapshots) sayesinde sistemler hızla normal durumuna döndürülebilir; böylece kesinti süreleri en aza indirilir, insan hatası veya kötü amaçlı saldırılardan kaynaklanan riskler azaltılır.

Kapsamlı Veri Yedekleme ve Kurtarma Çözümleri:

- QNAP; veri kaybı riskini en aza indirmek ve operasyonel sürekliliği sağlamak için Windows PC'leri, sunucuları, SaaS bulut verilerini ve sanal makineleri (VM) kapsayan çok yönlü yedekleme çözümleri sunar.

Koru

Çok katmanlı savunma mekanizmaları: sistemler, veriler ve ağlar için kapsamlı koruma

OT ortamlarında, modern saldırılara karşı koymak için tek bir savunma önlemine güvenmek artık yeterli değildir. QNAP; sistemlerden verilere, iç ağlardan ağ yönetimine kadar çok katmanlı koruma mekanizmaları sunarak altyapı dayanıklılığını artırır ve kesintisiz üretim ile operasyon sağlar.



NAS Sistem Koruması:

Yetkisiz erişimi ve kötü amaçlı işlemleri önlemek için Çok Faktörlü Kimlik Doğrulamayı (MFA) ve dahili güvenlik duvarını destekleyerek NAS kararlılığını ve kullanılabilirliğini güvence altına alır.

Veri Güvenliği ve Değiştirilemez:

AES-256 şifreleme ve değiştirilemez depolama (WORM, Object Lock) ile veri bütünlüğünü korur. Airgap+ izole yedeklerle birleştiğinde, fidye yazılımlarına karşı koruma sağlar ve yedekleme cihazlarının uzun süre ağa maruz kalmasını önler.

İç Tehdit İzolasyonu:

ADRA NDR, kötü amaçlı OT ağ trafiğini hızla tespit edip filtreler; yatay ilerlemeyi (lateral movement) ve kötü amaçlı yazılım yayılımını izleyerek saldırganların yayılmasını veya hassas verileri sızdırmasını etkili bir şekilde engeller.

Ağ Segmentasyonu ve Erişim Kontrolü:

QNAP switch'ler; üretim, izleme ve yönetim ağlarını segmentlere ayırmak için VLAN ve ACL kullanarak alanlar arası riskleri azaltır ve güvenli izolasyonu artırır.

Tespit Et

Ağ trafiğini ve kullanıcı davranışlarını analiz etmek için izleme sistemleri kurun

Anormal OT ağ trafiği ve davranışları için gerçek zamanlı izlemenin bulunmaması, tehditlerin varlığını sürdürmesine ve daha büyük hasarlara yol açmasına neden olur. QNAP; anormallikleri hızla tespit etmek, müdahale sürelerini kısaltmak, üretim ve operasyon güvenliğini sağlamak amacıyla sistem, ağ ve trafik davranışlarının kapsamlı ve gerçek zamanlı izlenmesini sağlar.

Sistem ve Operasyonel Durum İzleme:

NAS; yetkisiz erişimleri, anormal oturum açma işlemlerini ve şüpheli eylemleri hızla belirlemek için sistem durumunu, dosya etkinliklerini ve erişim günlüklerini (log) sürekli izler. AMIZcloud merkezi yönetimi ve QuWAN orkestrasyonu sayesinde yöneticiler, tüm QNAP cihazlarının operasyonel durumları ve riskleri üzerinde tam görünürlük elde eder.

Kötü Amaçlı Yazılım Tespiti ve Temizleme:

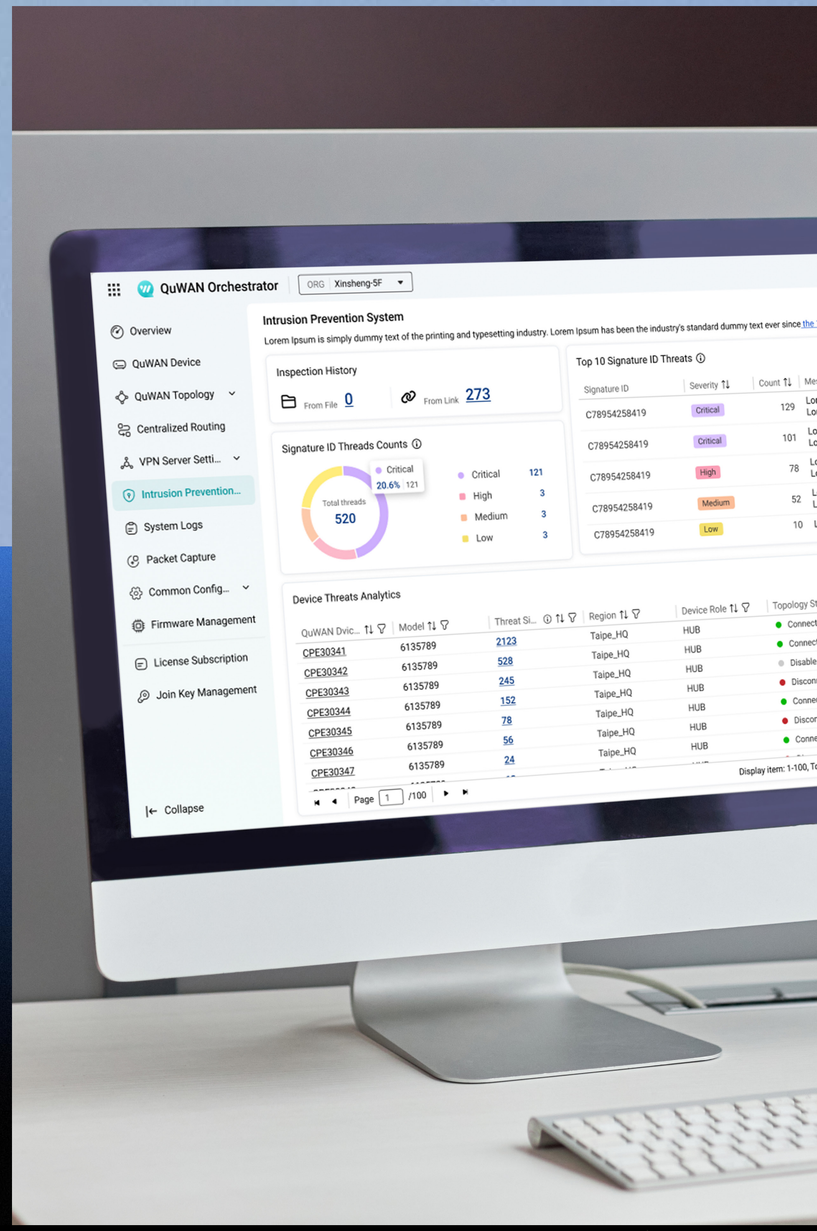
Kötü amaçlı yazılımları tespit etmek ve ortadan kaldırmak için NAS üzerinde planlı antivirüs taramaları gerçekleştirin. QNAP'ın düzenli olarak güncellenen virüs tanımları güncel koruma sağlar. Ayrıca ADRA NDR Trap, proaktif savunma için erken aşamada kötü amaçlı yazılım tespiti ve uyarılar sunar.

Çevre Ağ Tehdit Tespiti:

QHora router'lar; Saldırı Önleme Sistemi (IPS) ve derin paket inceleme (DPI) sunarak kötü amaçlı trafiği tespit edip engeller ve OT ile IT ağlarının çevre güvenliğini güçlendirir.

İç Ağ Davranış Analizi:

ADRA NDR; OT trafiğinin ve iç davranışların derinlemesine analizini yapar, tehditlerin yatayda yayılmasını önlemek için şüpheli etkinlikleri sürekli izler ve otomatik olarak işaretler.



Müdahale Et

Tehditleri etkili bir şekilde durdurmak için gerçek zamanlı uyarılar, sınırlandırma ve uzaktan sistem güncellemeleri

OT ortamlarında, bir güvenlik olayındaki herhangi bir gecikme veya hatalı müdahale, üretim hattında aksamalara veya güvenlik kazalarına yol açabilir. QNAP, tehditleri yayılmadan önce durdurmak için anlık bildirimler ve hızlı sınırlandırma olanağı sunar.

Gerçek Zamanlı Olay Bildirimleri:

Notification Center (Bildirim Merkezi) ile anormal olaylar eş zamanlı olarak birden fazla kanala (e-posta, SMS, syslog ve webhook'lar dahil) iletilerek güvenlik ekiplerinin ve saha personelinin anında bilgilendirilmesi sağlanır.

Hızlı Tehdit Sınırlandırması:

Bir güvenlik olayı meydana geldiğinde, ADRA NDR Switch'ler kötü amaçlı trafiğin yayılmasını durdurmak için tehdit kaynağını hızla doğrular ve virüs bulaşmış cihazları izole eder. Bu sayede diğer OT sistemlerinin çalışmaya devam etmesi sağlanır ve genel etki azaltılır.

Uzaktan Cihaz Güncellemeleri:

AMIZcloud ve QuWAN SD-WAN kullanan yöneticiler; QNAP cihazlarını uzaktan yönetebilir, kapatma, yeniden başlatma ve sistem güncellemeleri gibi işlemleri gerçekleştirebilir. Bu da yama dağıtımını hızlandırır, güvenlik açıklarını zamanında kapatır ve insan hatası riskini azaltır.

Kötü Amaçlı Yazılım Temizleme:

Planlı kötü amaçlı yazılım temizleme işlemleri, enfekte olmuş süreçlerin anında sonlandırılmasını sağlayarak sistemlere ve verilere daha fazla zarar verilmesini önler."



Kurtar

Felaket kurtarma ve veri bütünlüğü yedekleme mimarilerini hayata geçirin

OT ortamlarının temel amacı 'kesintisiz üretimdir.' QNAP, normal operasyonların en kısa sürede geri yüklenmesini sağlamak için hızlı felaket kurtarmaya ve veri bütünlüğünü korumaya odaklanır.



Yüksek Erişilebilirlikli Yedekleme Mimarisi (Sunucular ve Ağlar):

NAS HA (Aktif/Pasif Yüksek Erişilebilirlik) ve switch MC-LAG sayesinde sistemler, kesintiler sırasında otomatik olarak yedek ekipmana geçiş yapar (failover); böylece iş sürekliliği sağlanır ve OT kontrol sistemi kesintileri önlenir.

Felaket Kurtarma Kabiliyeti:

Anlık Görüntüler (Snapshots) sayesinde sistemler hızla normal durumuna döndürülebilir; böylece kesinti süreleri en aza indirilir, insan hatası veya kötü amaçlı saldırılardan kaynaklanan riskler azaltılır.

Yüksek Erişilebilirlikli Yedekleme Mimarisi (Çoklu Saha):

QuWAN destekli QHora router'lar, OT ortamlarında çoklu saha WAN yedeklemesi sağlar. Sahalar arası yedekli geçiş (failover), otomatik olarak alternatif düğümlere ve rotalara yönlendirilir. Çift WAN (Dual-WAN) yapısı, kesintisiz uzaktan/bulut hizmetleri için yerelden buluta sorunsuz bağlantı yedeklemesi sunar.

Kapsamlı Veri Yedekleme ve Kurtarma Çözümleri:

QNAP; veri kaybı riskini en aza indirmek ve operasyonel sürekliliği sağlamak için Windows PC'leri, sunucuları, SaaS bulut verilerini ve sanal makineleri (VM) kapsayan çok yönlü yedekleme çözümleri sunar.

Siber güvenlik tek bir hamlede tamamlanmak zorunda değildir — ancak mutlaka başlatılmalıdır.

QNAP çözümleriyle; depolamadan siber güvenliğe kadar eksiksiz koruma sağlayarak IT/OT güvenlik dönüşümünü güvenle yönetin ve esnek, dayanıklı iş operasyonları güvence altına alın.

Cihazlardan erişim kontrolüne kadar kurumsal varlıklar ve kullanıcı davranışları üzerinde tam görünürlük elde edin.

Kurulumdan tehdit azaltmaya (mitigation) kadar güvenlik savunmalarını ve operasyonel verimliliği etkili bir şekilde entegre edin.

Önlemeden kurtarmaya kadar operasyonel istikrarı kapsamlı bir şekilde koruma altına alın.

Daha Fazla Bilgi Edinin



QNAP, mevcut altyapınızla başlayarak IT/OT güvenliğine doğru ilk adımı atmanıza yardımcı olur.

Hangi çözümlerin ortamınıza en uygun olduğunu öğrenmek mi istiyorsunuz? Kurulum tavsiyesine veya teknik danışmanlığa mı ihtiyacınız var?

İletişime Geçin

QNAP Systems, Inc.
New Taipei City
Email: sales@qnap.com
Tel: +886 2 2641 2000

QNAP Inc. (USA)
Pomona CA
Email: usasales@qnap.com
Tel: +1-909-595-2782

QNAP Inc. (Canada)
Markham, Ontario
Email: canadasales@qnap.com
Tel: +1-905-947-1000

QNAP GmbH (Germany)
Willich
Email: desales@qnap.com
Tel: +49-2154-88428-0

QNAP SRL (Italy)
Roma
Email: eusales@qnap.com
Tel: +39-(0)687-738456

QNAP UK Limited
Swindon
Email: uksales@qnap.com
Tel: +44-(0)333-344-2522

QNAP Türkiye
İstanbul
Email: ismaildogan@qnap.com
Tel: +90 533 377 98 84

QNAP Japan
Tokyo
Email: jpsales@qnap.com
Tel: +81-3-5901-9735