**BASIN BÜLTENİ**

**Fortinet, CES 2018’de geleceğin akıllı arabaları için entegre güvenlik ve koruma çözümleri sundu**

**Renesas ile işbirliğine giren Fortinet, akıllı arabaların güvenliğini sağlamak için son teknoloji siber güvenlik çözümleri sunuyor. Bu çözümlerin kapsamına güç aktarım mekanizmaları ve motorlar, telematik ve bilgi-eğlence sistemleri de dahil.**

Kapsamlı, entegre ve otomatik siber güvenlik çözümlerinde dünya lideri [Fortinet](http://www.fortinet.com) (NASDAQ: FTNT), 9-12 Ocak tarihleri arasında Las Vegas’ta düzenlenen CES 2018’de, akıllı arabalara yönelik olarak geliştirdiği ileri düzey siber güvenlik yeteneklerini sergiledi. Fortinet’in çözümleri, Renesas İleri Düzey ve Otonom Test Hattı ve Geleceğe Hazır Çözümler portföyü içinde yer aldı.

Renesas Electronics işbirliği ile geliştirilen siber güvenlik prototipi, Fortinet FortiOS güvenlik işlemleri sisteminin, Renesas’ın R-Car H3 çip-üzeri-sistemi ile entegre olarak; araçtaki ağ alanlarını, bulut tabanlı hizmetleri ve uygulamaları nasıl koruduğunu gösteriyor. Fortinet ve Renesas, CES’te internet ağına bağlı bir prototip arabada saldırı önleme sistemi (IPS) ihlali ve DDoS (Dağıtık Hizmet Dışı Bırakma Saldırıları) gibi deney amaçlı siber ihlaller gerçekleştirerek, saldırganların otomobil veya uygulamaları ele geçirmelerini önleyip, otomatik ve entegre güvenlik çözümünün ne kadar etkin olduğunu gösterdiler.

**Fortinet’in kurucusu ve teknolojiden sorumlu başkanı Michael Xie**, “En yeni teknolojik inovasyonlardan biri olan akıllı ulaşım araçları, otomotiv sektöründe taşları yerinden oynatacaktır. Geleceğin arabalarında 3B haritalama, sensör verileri işleme, akıllı cihaz entegrasyonu, bulut tabanlı hizmet, ileri düzey LAN/CAN ağları ve kendi kendine sürüş gibi özellikler, muazzam siber riskleri de beraberinde getiriyor. İçerik ve uygulamalara erişebilmek için arabalarla Nesnelerin İnterneti cihazlarının birbirine bağlanması ise saldırı yüzeyinin daha da büyük olacağı anlamına geliyor. Akıllı arabalarda emniyet ve tüketici güveni için entegre güvenlik sağlanması şart. Üreticiler, gerçek zamanlı tehdit istihbaratı olan araçlar geliştirmeye ve arabaların karmaşık mimarilerini koruyacak stratejik segmentasyonlar yapmaya başladıkça, Fortinet de buna paralel olarak, ağ güvenliğindeki küresel liderliğini, otomotiv sektörünü de içine alacak şekilde genişletiyor. Renesas ile işbirliği yaparak, otomotiv sektörünün evrilen bilgi-işlem ortamının gerektirdiği benzersiz çözümleri CES’te sergilemekten heyecan duyuyoruz” diyor.

**Akıllı taşıt teknolojisi ve güvenlik sisteminin temeli : Otomatik Güvenlik**

2016 yılında akıllı araba sayısı 37 milyon iken 2025 yılına gelindiğinde bu rakamın 300 milyona çıkacağı tahmin ediliyor. Buna bağlı olarak, akıllı araba teçhizatı ve destek hizmetleri gelirlerinin yılda 250 milyar doları geçmesi bekleniyor.[[1]](#endnote-1) Akıllı araba pazarını etkileyen kilit unsurların başında kendi kendine sürüş özelliğine duyulan talebin artması, veriye dayalı karar verme uygulamaları ve bağlanabilirlik çözümleri (akıllı telefon özellikleri, istendiğinde müzik, internet bağlantısı ve bilgi-eğlence uygulamaları) geliyor.

Akıllı arabalarda internet erişimi ve kablosuz yerel ağ (LAN) gibi özellikler bulunur. Bu özellikler sürücünün, hem aracın içinde hem de dışındayken internet bağlantısını diğer cihazlarla paylaşabilmesine de izin verir. Otomobil üreticilerinin uygun bir siber koruma sağlamaları ve tüketici güvenini koruyabilmeleri için, teknolojiyi tasarlarken ve hizmete alırken en büyük önceliği güvenliğe vermeleri gerekiyor. Güvenlik sistemlerinin iletişim standartlarını, cihazları ve ağları kapsaması gerekir. Ayrıca, aracın dışına da uzanabilmeli, yol ve trafik kontrol sistemleri gibi ulaşım ekosistemini de içine alarak görünürlük, karşılıklı etkileşim ve kontrol sağlamalıdır.

Akıllı arabalar, tek bir sistem içinde birçok farklı güvenlik çözümü gerektirir ve bu nedenle tehditlerin otomatik olarak kuşatılıp yok edilmesini sağlamak için güç aktarım mekanizmaları ve motorlar, telematik ve bilgi-eğlence sistemleri gibi kilit işlev alanlarının stratejik segmentasyonunu da yapabilmelidir. Bir diğer kilit gereklilik ise Fortinet’in FortiGuard Labs ürünü gibi gerçek zamanlı tehdit güncelleme sistemidir. FortiGuard Labs, en son açıkları ve tehdit bilgilerini araca iletip etkin ve otomatik koruma sağlıyor. Bu hizmet ayrıca, güvenlik yamalarını ve güncellemelerini zamanında almak ve olayları paylaşıp ilişkilendirmek için tekrar bir bulut ağına bağlanmayı da içeriyor.

**Fortinet ve Renesas akıllı araba ağlarının güvenliğini nasıl sağladıklarını gösteriyor**

Fortinet ve Renesas bir güvenlik çözüm prototipi için işbirliğine girerek günümüzdeki akıllı araba mimarisindeki siber güvenlik risklerine odaklandılar. En son siber ihlaller, giderek karmaşıklaşan araç ağları için entegre bir güvenliğe acilen ihtiyaç duyulduğunu gösteriyor. Örnek olarak 2015’teki Jeep Cherokee korsan saldırısını verebiliriz; olayda bir korsan grubu kablosuz ağdan araca girmiş ve hayati işlevleri elektronik olarak kontrolleri altına almıştı. Tesla S Model korsan saldırısı olarak geçen diğer bir örnekte ise aracın CAN (kontrol alan ağı) veri yoluna saldırarak aracın frenlerine, kapı kilitlerine ve bilgisayar paneline 12 mil uzaktan müdahale etmişlerdi.

CES’de Fortinet ve Renesas, R-Car H3 SoC üzerinde Fortinet Security Fabric teknolojisinin nasıl çalıştığını ve araçta güvenlik politikası yönetimi oluşturarak, güç aktarım mekanizmaları ve motorların, LTE modül, araçtan-araca iletişimi kablosuz erişim noktası, motor kontrol modülü gibi araçtaki iletişim alanlarının otomatik şifrelenmesini sağlıyor. Renesas R-Car H3’te bulunan çip-üzeri-güvenlik işlevlerinden destek alan Fortinet, alanlar arasındaki iletişimi emniyetli hale getiriyor, belli alanlar arasındaki erişimi kısıtlayarak potansiyel siber tehditleri en aza indirip kontrol altına alıyor. Deney amaçlı IPS ve DDoS siber saldırıları kullanılarak yapılan gösterilerde FortiOs’un, genel bir bulut hizmetinden araç-içi eğlence sistemine iletilen verileri otomatik olarak nasıl koruduğuna tanık olunabiliyor.

Reenesas, otomotiv sistemlerden sorumlu başkan yardımcısı *Amrit Vivekanand,* “Tedarik zincirinin her halkasından otomotiv mühendisleri, geliştirme döngülerini hızlandıracak ve pazara giriş hızını artıracak kapsamlı çözümler için Renesas’a güveniyor. Renesas da bu amaçla yani yarının akıllı arabalarında gereken entegre koruma seviyesini sağlamayı amaçlayan son teknoloji siber çözümleri tasarlaması için Fortinet ile çözüm ortağı oldu. Ağ güvenliğinde lider uzmanlığıyla, geleceğin otomotiv ağı güvenlik sistemlerinin ihtiyaç duyduğu benzersiz talep ve altyapı gerekliliklerine çözüm bulunmasında güvenilir bir danışman olan Fortinet’e inancımız tamdır” diyor.

Fortinet/Renesas örnek sergisi hakkında daha ayrıntılı bilgi ve Renesas İleri Düzey ve Otonom Test Hattı ve Geleceğe Hazır Çözümler portföyünü görmek için <http://renesasatces.com> adresi ziyaret edilebiliyor.

**İlgili Kişi**

Eray Çoşan Akkuş

Marjinal Porter Novelli

0533 927 23 97

erayc@marjinal.com.tr

**Fortinet hakkında**

Fortinet (NASDAQ: FTNT) dünya genelinde büyük ölçekli şirketlere, servis sağlayıcılarına ve kamu kurumlarına güvenlik sunar. Fortinet, her geçen gün artan sanal saldırılara karşı müşterilerine akıllı ve sorunsuz koruma sağlar, sınırların ortadan kalktığı ağların artan performans ihtiyaçlarını karşılar. Ağlardaki uygulamaların, bulut sistemlerinin ve mobil cihazların karşılaştığı en kritik güvenlik sorunlarına karşı performanstan ödün vermeden güvenlik sunan tek çözüm sadece Fortinet’in Security Fabric mimarisidir. Fortinet global çapta sevkiyatı yapılan en güvenilir çözümler alanında dünyanın bir numarasıdır ve dünya genelinde 330 binden fazla müşteri ticari faaliyetlerini korumak için Fortinet’e güvenmektedir. Daha fazla bilgi için: http://www.fortinet.com, Fortinet Blog sayfası veya FortiGuard Labs.

1. [ON World Connected Car Markets Repo](https://www.onworld.com/connectedcar/), Nisan 2017

 [↑](#endnote-ref-1)