Forcepoint

Çözüm Özeti

Hastalara Sunduğunuz Bakım Hizmetlerini Her Adımda Koruyun

Nerede olursa olsun kritik verilerinizi ve çalışanlarınızı sürekli olarak koruyun

Zorluklar

- Tele tıptaki büyüme: Hastalara yapılan sanal ziyaretler koruma altına alınmalıdır.
- Uzaktan hasta takibi: RPM'deki güvenlik açıkları suistimal edilebilir.
- Artan veri paylaşımı: PHI ve diğer hassas verilere erişim ve bu verilerin paylaşımı güvenli bir şekilde yapılmalıdır.

Çözümümüz

Forcepoint Cloud Security Gateway

- Web, veri ve bulut güvenliğini bulut tabanlı ve merkezi olarak yönetilen bir hizmette sunar.
- Derin içerik denetimi, cloud sandboxing ve remote browser isolation (eklenti olarak sunulmaktadır) özellikleriyle uzaktan çalışanları kötü amaçlı saldırılardan korur.
- Çalışanların şirket içi hasta verilerine ve tıbbi verilere ve bulutta bulunan iş açısından kritik uygulamalara her yerden güvenle erişmesini sağlar.
- BYOD, yönetilen cihazlar ve gerçek zamanlı uyum için kontroller sağlar.

Faydaları

- Web, e-posta ve bulutun uzaktan kullanımını güvence altına alır.
- Çalışanlarınızın bulundukları her yerde kötü amaçlı yazılımları, virüsleri ve kimlik avı saldırılarını durdurur.
- Her kullanıcı için her yerde aynı politikalarla eksiksiz web ve veri koruması sağlar.
- Güvenli bulut erişimi sağlarken, riskli bulut uygulamalarını ve Gölge BT uygulamalarını tespit eder.

Pandemi, dijital sağlık uygulamalarını hızlandırdı. Hizmetlerinizi yeniden şekillendirerek, çalışanlarınızı her zamankinden daha güçlü, daha hızlı ve esnek olmaya zorladı. Yeni sağlık riskleriyle mücadele ederken, uzaktan çalışanları yönetirken ve üçüncü taraf tedarikçilerle çalışırken, yalnızca bugün değil, yarın da güvenebileceğiniz bir korumaya ihtiyacınız var.

Forcepoint Cloud Security Gateway, yeni normale geçiş yaparken uyum sağlayabilmeniz için gereken sürekli korumayı sağlar.

Sağlık krizi, siber güvenliğinizi değiştirdi mi? Uzaktan ve dağınık bir şekilde çalışanları korumak, kurumunuz için yeni bir durum olmayabilir. Ancak, küresel pandemi süresince siber saldırılarda görülen büyük artış, pek çok sağlık kurumunu, personelleri (hem tesis içinde hem de uzaktan çalışan) ve kullandıkları hassas verileri tehdit eden kritik güvenlik açıklarına karşı hassas hale getirdi.

Bu farkındalık, sağlık sektöründeki siber güvenlik liderlerinin kendilerine kritik sorular sorarak mevcut korumalarını tekrar gözden geçirmelerine neden oldu:

→ Her nerede olurlarsa olsunlar hasta verilerini ve tıbbi verileri korumak için güvenliğimizi nasıl ölçeklendirebiliriz?

→ Riskli bulut uygulamalarını (onaylı ve onaysız uygulamalar) nasıl belirleyebiliriz?

→ Güvenlik ve uyumdan taviz vermeden verim ve iş sürekliliğini sağlamak için bulutu nasıl güvenli bir şekilde nasıl benimseyebiliriz?

→ Dağınık çalışanlarımız için nasıl iş birliğine dayalı bir ortam sağlayabiliriz?

Kurumunuz farklı bir iş modeline geçiş yaparken, bu soruların yanıtları daha da önemli bir hal alıyor.

Veri güvenliğiniz, değer tabanlı sağlık hizmetlerine giden yolu açabilir

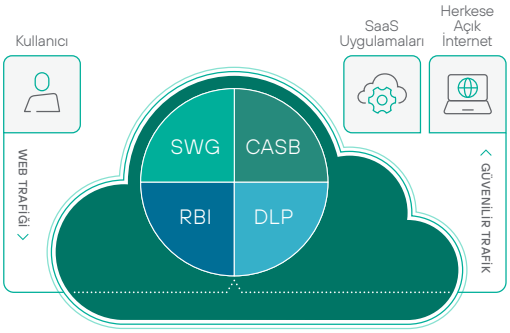
Çalışanlarınızın daha fazlası işleri için web, e-posta ve bulutu kullandıkça, daha fazla veri ağınızın dışına çıkar. Bu genişleyen saldırı yüzeyinin güvenlik altına alınması yalnızca bugün için değil, aynı zamanda siber güvenlik yaklaşımınızı değer tabanlı sağlık hizmetlerine hazırlamak açısından da kritik önem taşır. Sağlık kurumları, sonuç bazlı ödeme modeline geçiş yaptıkça, sağlık sektöründeki uzmanlık alanları ve disiplinler arasındaki iş birliği de artacaktır.

Bu, kurumunuzun geleceği açısından ne anlama geliyor? Muhtemelen şirketinizin dışındaki daha fazla klinisyen ve personelle bilgi paylaşımı yapacak, veri analizi uygulamaları gerçekleştirecek ve sağlık hizmeti koordinasyonu sorumluluklarını net bir şekilde tanımlayacaksınız. Nihai amacınız, sağlık hizmetlerinizin kalitesini artırırken, maliyetleri ve yeniden hastaneye yatma vakalarını azaltmak olacaktır.

Değer tabanlı sağlık hizmetleri, kurumunuzun şu anki hedeflerinden biri olmasa da bugünden hazırlanmak için adımlar atabilirsiniz. İşe, uzaktan çalışanların güvenliği ile birlikte web, e-posta ve bulut üzerinden halihazırda yürütmekte oldukları veri paylaşımı ve dijital işbirliği süreçlerinin güvenliğini iyileştirerek başlayın.

Son olarak da son sağlık krizi sırasında aldığınız güvenlik derslerini ve varsa henüz nelerin tamamlanmadığını düşünün. Kurumunuzun olabilecek başka bir sağlık krizine hazır olabilmesi için, güvenliğinizi nasıl ölçeklendirmeyi planlıyorsunuz?

Forcepoint Cloud Security Gateway



CSG, bulut tabanlı ve merkezi olarak yönetilen tek ve birleşik bir hizmette web, bulut ve veri güvenliği sunar. Secure Web Gateway (SWG), Cloud Access Security Broker (CASB) ve Data Loss Prevention özelliklerini tek bir SKU'da sunar.

Diğer çözümler: Özel uygulamalara VPN'lerin getirdiği karmaşıklık, darboğaz ve riskler olmadan gerçek Sıfır Güvenle erişilmesini sağlayan Forcepoint Private Access.

Çalışanlarınız = Yeni risk çevresi

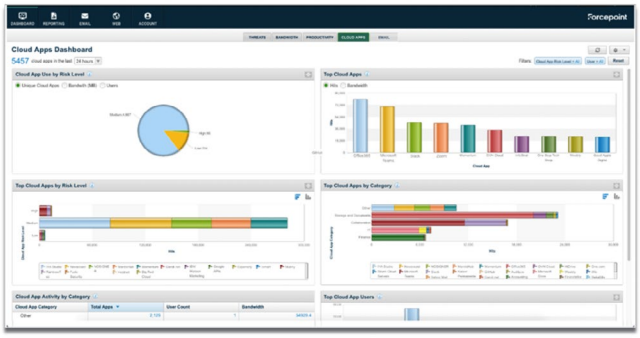
Çalışanlarınız, her nerede çalışıyor olurlarsa olsunlar (tesis içinde veya dışarıda), yeni risk çevrenizi teşkil etmektedir. Acil durumlarda veya kriz durumlarında, veri erişimi ve paylaşımını tipik protokollerinize uygun olmayan bir şekilde yapabilirler. Ayrıca, ağınızın dışındaki tıbbi uzmanlarla iş birliği yapıyor da olabilirler.

Forcepoint Cloud Security Gateway, kurumunuzun yeni gerçeklerine uygun esnek ve ölçeklenebilir koruma sağlar. Nerede çalıştıklarına bakılmaksızın personelinizin web ve bulut üzerinden herkese açık uygulamalara güvenle erişmesini sağlar. CSG sayesinde, kritik verileriniz ve fikri mülkiyet haklarınız daha düşük maliyetle ve sadeleştirilmiş güvenlik politikası yönetimiyle korunur.

Mevcut ve gelecekteki tehditlere karşı esnek koruma

Forcepoint Cloud Security Gateway şunları yapmanızı sağlar:

- → Derin içerik denetimi, cloud sandboxing ve remote browser isolation (eklenti olarak sunulmaktadır) özellikleriyle öldürme zincirinde tam görünürlük sağlama.
- → Kötü amaçlı kullanıcıları durdurmak ve en iyi uygulamalara uygun olmayan personel faaliyetlerine engel olmak için buluttaki anormal ve riskli kullanıcı davranışlarını tespit etme.
- → Uzaktan çalışanların, PHI ve diğer hassas verileri yönetim kurallarını ve/veya federal, eyalet veya yerel düzenlemeleri ihlal edecek şekilde yetkisiz kullanıcılara ifşa etme riskini azaltma.
- → Potansiyel olarak uygunsuz olabilecek ayrıcalık yükseltme durumlarını tespit etme ve uzaktan çalışan gerçek personel ve kötü amaçlı aktörler için konum tabanlı erişim ve faaliyet takibi özelliklerini uygulama.
- → Özel süreç, yöntem ve prosedürlerinizi küçük ve büyük her türlü veri kaybı ve büyük dosya hırsızlığına karşı koruma.



Forcepoint Cloud Security Gateway, kullanıcılar ve veriler için %100 bulut tabanlı ve merkezi olarak yönetilen tek güvenlik platformudur.

Çalışanlarınızı siber güvenliğin merkezine yerleştirin

Cloud Security Gateway'in kurumunuz için neler yapabileceğini mi merak ediyorsunuz? Bulut güvenliği uzmanlarımız size açıklamaktan mutluluk duyacaktır. Birleşik güvenlik hizmetimizin aşağıdakileri nasıl yaptığına ilk elden şahit olun:

- → Tedarikçi sayısını ve özel amaçlı ürün sayısını azaltmak
- → Operasyonel iş yükünü ve ilgili maliyetleri azaltmak
- → Her kullanıcı için her yerde tek tip web koruması ve politikaları sağlamak
- → Kurumunuz çapında Gölge BT'yi keşfetmek ve güvenli bulut erişimi sağlamak

Hemen bir CSG tanıtımı talep edin!

forcepoint.com/contact

[Secure-Your-Patient-Care-Every-Step-Solution-Brief-TR] 19May2021