Forcepoint

Çözüm Özeti

Hastanenizin Personelini ve Verilerini Her Yerde Koruyun

Web, bulut ve veri güvenliği için tek ve birleşik bir hizmetle koruma sağlayacak esnekliğe kavuşun

Zorluklar

- **Tele tıbbın bozulması:** Gitgide daha fazla klinisyen uzaktan çalışıyor ve kablosuz ağlar ve video konferanslar yoluyla konsültasyon yapıyor.
- **Arabada COVID-19 testi:** Mobil test sahaları, EHR veri girişleri için uzaktan erişim gerektiriyor.
- **Geçici tıbbi tesisler:** Yoğun bakım üniteleri, otoparklarda ve hastane güvenlik çevresinin ötesindeki diğer alanlarda kuruluyor.

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 bulutu kullanan uzaktan çalışan ekipleri korur.
- 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.
- Kurumunuz çapında güvenli bulut erişimi sağlarken, riskli bulut ve Gölge BT uygulamalarını tespit eder.
- Tek tedarikçiden gelen birleşik çözüm.
- Ön tanımlı politikalar sayesinde HIPAA ve diğer düzenlemelerle uyumu kolaylaştırır.

Klinisyenleriniz ve sağlık personeliniz sürekli hareket halinde ve hayat kurtarmak için her zamankinden çok çalışıyor. Ancak bu da saldırı yüzeyinin büyümesi anlamına geliyor. Forcepoint ile hastaneniz için kusursuz işleyen bir geleceği güvence altına alabilirsiniz.

Forcepoint Cloud Security Gateway (CSG), dinamik risklere karşı esnek olmanız ve uyum sağlayabilmeniz için gerekli esnek ve ölçeklenebilir korumayı sağlar.

Bir numaralı önceliğiniz her zaman hastalar oldu. Ancak içinde bulunduğumuz dijital çağda, siber güvenlik de hasta güvenliğinin kritik bileşenlerinden biri - hem de risk ortamı değişip büyüdükçe daha da önemli hale gelen bir bileşen.

Pandemi, hastalarınıza bakım sunma yöntemlerinizi değiştirdi. Çalışanlarınız, hastanenizin geleneksel güvenlik çevresinin dışında çalışıyor. Bu yeni çalışma şeklinde verilerinizi koruyabilmek için acil teknoloji alımları yapmış olabilirsiniz. Bu değişiklikler, muhtemelen mevcut gizlilik ve güvenlik politika ve prosedürlerinizde yeni açıklar yarattı. Bu kör noktalar, uzaktan çalışan personelin kablosuz bağlantıları ve yönetimsiz cihazları kullanmaya başlamasıyla birleştiğinde, verilerin kötü amaçlarla veya kaza eseri dışarı sızmasına açık bir davet anlamına geliyor.

Uzaktan çalışan personeli ve kullandıkları verileri nasıl koruyacağınızı düşünürken, kendinize aşağıdaki soruları sorun:

→ **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 güvenli bir şekilde nasıl benimseyebiliriz?

→ **Dağınık tıbbi ekiplerimiz için** nasıl iş birliğine dayalı bir ortam sağlayabiliriz?

Hastanenizin geleceği için veri korumasını tekrar düşünmek

Klinisyenlerinizin daha fazlası hastane dışında çalıştıkça, daha fazla veri ağınızın dışına çıkıyor. Ne kadar veriden bahsediyoruz? Şu son istatistikleri düşünün: COVID-19 karantinası sırasında, hastanelerde ağ dışındaki veri hareketlerinde %80 artış olurken, bu artışa USB sürücülere aktarılan veri hacmindeki %123'lük artış ve bulut depolama hizmetlerine yüklenen verilerdeki büyük artış da dahildi (Data Guardian, 2020).

Bu verilerin çoğu, siber suçlular için son derece değerli. Örneğin, PHI karaborsada kişisel finans bilgilerinden 50 kat daha değerli. Ancak siber suçlular hastanenizi aşağıdakiler gibi diğer bilgiler için de hedef alabilir:

→ **Laboratuvar sonuçları** şantaj veya kimlik hırsızlığı için kullanılabilir

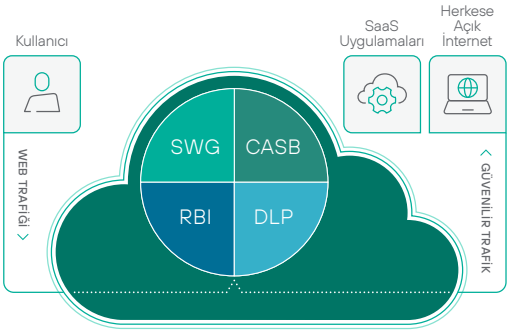
→ **Tıbbi lisanslar** doktorları taklit etmek ve sahte tıbbi belgeler üretmek için kullanılabilir

→ **Sağlık sigorta şirketlerinin oturum açma bilgileri** sahte sağlık sigortası talepleri göndermek için kullanılabilir

→ **İdari evraklar** sahte sağlık sigortası kartları, sahte reçeteler ve ilaç etiketleri oluşturmak için kullanılabilir

Güvenliğiniz, çalışanlarınız uzaktan bağlandığında tüm bu verileri koruyabilecek kadar esnek mi? COVID-19'un yarattığı güvenlik açıklarını kapattınız mı? Hastanenizin 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

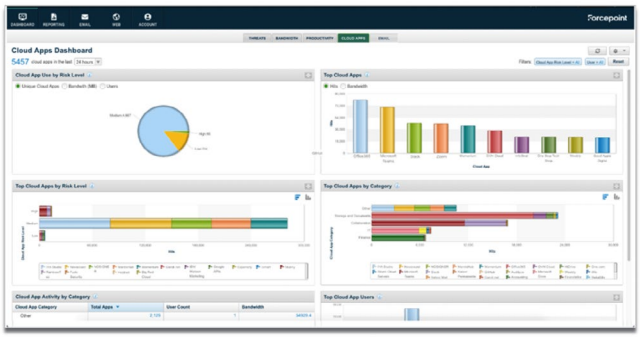
Çalışanlarınız, her nerede çalışıyor olurlarsa olsunlar (hastanenin içinde veya dışarıda), yeni risk çevrenizi teşkil etmektedir. Acil durumlarda veya kriz durumlarında, veri erişimi ve paylaşımını tipik protokollerinize uygun olmayan bir şekilde yapabilirler.

Forcepoint Cloud Security Gateway, hastanenizin 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.

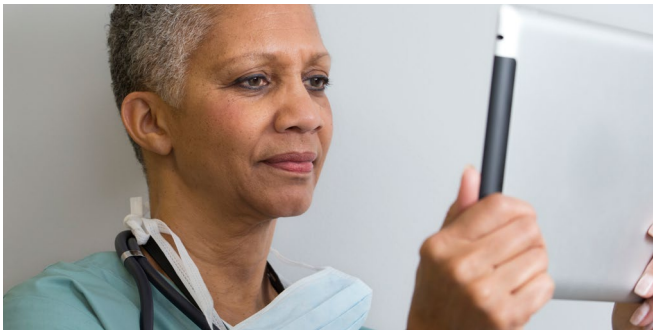
Mevcut ve gelecekteki tehditlere karşı esnek koruma

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.
- → Klinik ve araştırma keşiflerinizi 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 hastaneniz 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 hastanelere özel bir CSG tanıtımı talep edin!

forcepoint.com/contact

[Secure-Your-Hospitlas-Staff-and-Data-Solution-Brief-TR] 19May2021