

Sınıflandırılmış Yazılımlar için Ticari Çözümler: Forcepoint NGFW

Genel bakış:

Kamu kurumları ve yükleniciler, hassas ve sınıflandırılmış verileri güvence altına almak için giderek daha fazla Sınıflandırılmış Ticari Çözüm programlarına (CSfC) yöneliyor. Forcepoint'in Yeni Nesil Güvenlik Duvarı (NGFW) çözümleri, gizli bilgileri korumak için gerekli olan sıkı uyumluluk gereksinimlerini karşılayan güçlü bir güvenlik sunarken, CSfC çözümünde kritik bir rol üstlenmek için ideal bir noktadadır.

CSfC nedir?

Ulusal Güvenlik Ajansı (NSA) tarafından yönetilen CSfC programı, kuruluşların sınıflandırılmış veriler için koruma gereksinimlerini karşılayan katmanlı güvenlik çözümlerinde piyasada bulunan teknolojileri kullanmasını sağlar. Bu program, kurumların yalnızca maliyetli, geleneksel devlet onaylı çözümlere bağlı kalmadan güvenli iletişimi hızla kurlmalarına ve aynı zamanda en yüksek veri koruma standartlarını sürdürmelerine olanak tanır.

Forcepoint NGFW çözümleri, güvenli ve uyumlu CSfC uygulamaları için kritik bir yapı taşı olarak kamusal kurumların ve yüklenicilerin NSA tarafından belirtilen titiz gereklilikleri karşılarken sınıflandırılmış verileri koruyabilmesini sağlar. Forcepoint NGFW çözümleri, kuruluşların en hassas verileri için etkili, geleceğe hazır güvenlik kullanmalarını sağlar.

Forcepoint NGFW çözümü hakkında bilgi edin
CSfC programları hakkında daha fazla bilgi edin

Forcepoint NGFW CSfC Çözümleri için Neden Önemlidir:

FIPS FIPS 140-3 Uyumluluğu:

Forcepoint NGFW, FIPS 140-3 onaylı kriptografik modülleri entegre ederek hassas devlet ve savunma verilerinin hem aktarılırken hem de durağan haldeyken güvenli bir şekilde şifrelenmesini sağlar.

Kapsamlı Veri Koruma:

Forcepoint NGFW, sınıflandırılmış bilgileri korumak için gelişmiş tehdit koruması, uygulama kontrolü ve derin paket denetlemesini güçlü şifreleme özellikleriyle birleştirir.

Katmanlı Güvenlik Mimarisi:

Bir CSfC çözümünün parçası olarak Forcepoint NGFW'ler, katmanlı bir savunma mimarisi oluşturmak üzere güvenli yönlendiriciler ve uç nokta koruması gibi diğer ticari teknolojilerle sorunsuz bir şekilde entegre olur. Bu katmanlı yaklaşım, gelişmiş kalıcı tehditlere (APT'ler) ve sofistike siber saldırılara karşı direnci artırır.

Ölçeklenebilirlik ve Esneklik:

Forcepoint NGFW çözümleri yüksek oranda ölçeklenebilirdir ve kamu kurumlarının ve yüklenicilerin güvenlik yaklaşımlarını belirli görev gereksinimlerini karşılayacak şekilde uyarlanmalarını sağlar. Bu esneklik, CSfC çözümlerini çeşitli ortamlarda ve coğrafyalarda dağıtırken çok önemlidir.

Operasyonel Verimlilik ve Uyumluluk Raporlaması:

Forcepoint'in merkezi yönetimi, kurumların güvenlik politikalarını etkili bir şekilde yönetmesine, trafiği izlemesine ve uyumluluk raporları oluşturmasına olanak tanır. Bu sayede çözüm, CSfC sertifikasyonu için mevzuata uygunluğun ve denetim takibinin sürdürülmesine yardımcı olur.

Zero Trust Erişimi:

VPN ve Endpoint Context Agent ile Forcepoint NGFW, Zero Trust Application Control özelliğini kullanarak güvenli ve içeriğe duyarlı erişim sağlar. Sıkı politikalar ve gerçek zamanlı cihaz istihbaratı uygulaması yaparak, Zero Trust Network Access'i destekler, hassas verileri korur ve ağ genelinde riskleri azaltır.