Daha Güçlü ve Daha Akıllı Kullanıcı Kimlik Doğrulamasından Faydalanmak

Kim Okumalı-Hedef Kitle:

Kurum-şirket liderleri için. Günümüzün gittikçe karmaşıklaşan güvenlik ataklarını durdurmada şifreler ve geleneksel 2 faktör kimlik doğrulama (2FA) yeterli olmamaktadır. Daha kolay kullanım ihtiyacı duyan, güçlü ve daha akıllı kimlik doğrulama talebi olan herkes okumalı.

Daha Güçlü ve Daha Akıllı Kullanıcı Kimlik Doğrulamasından Faydalanmak
Günümüzün Mobil İş Dünyasında Etkili ve Kullanıcı Dostu Çözüm

İçindekiler

platin
Bilişim Teknolojileri

İdari Özet:

Mobil işgücünün gelişip yaygınlaşmasında katkısı bulunan, bulut tabanlı uygulamalar ve mobil cihaz sayısındaki artış, ofislerde BYOD (Bring Your Own Device) uygulamaları gibi birçok faktör mevcuttur. İş uygulamalarının mobile taşınmasının birçok avantajları vardır, ancak getirdiği yeni zorluklar da bulunmaktadır. Bilişim Teknolojileri (BT) çalışanları halen klasikleşmiş problemler ile başa çıkmaya çalışmaktadırlar. Veri ve uygulamalar yerel ya da remote bir biçimde erişilebilir olduğunda bunları ihlallere karşı korumak ve korumayı garanti altına alan düzenlemeler ile uyumluluğu sağlamak. Ancak BT çalışanları aynı zamanda; çalışanlara basit, güvenli ve heryerden erişilebilir uygulamaları sunmak gibi yeni zorluklarla da karşı karşıya kalmaktalar. Bu yazıda, kurumların veri ve uygulamaları güvenli tutabilmek için bu tür zorlukları, güçlü, daha akılcı kimlik doğrulama ile nasıl karşılayabileceklerine ve kolay kullanıma dair yöntemler sunulmaktadır:

Güvenlik Problemleri:

Çalışma ortamı halihazırda değişmiş bulunmaktadır. Remote erişim ise son günlerde sıkça gündeme gelen bir konu durumundadır. ABD'de gerçekleştirilen 2014 Gartner çalışmasına göre; büyük şirketler için çalışan ABD'deki tüketicilerin yaklaşık %40 I akıllı telefonlara, masaüstü bilgisayarlara veya günlük kullanım amaçlı dizüstü bilgisayarlara sahipler. Fakat bu trend, kurumlar/ şirketler için risk teşkil eden ve mobil cihazların erişiminin güvenliğinin sağlanmasını gerektiren bir unsur durumundadır. Kurumların bir diğer güvenlik problemi ise; "Yazılım Hizmetleri" (Software as a Service)-SaaS dir. Bu model; müşteri ilişkileri, insan kaynakları, işe alım, performans yönetimi, iş seyahatleri gibi birçok süreci ve kritik uygulamayı kapsayan bir modeldir. SaaS uygulamaları, yazılımda internet aracılığı ile esnekliği ve fonksiyonelliği sağlarken, aynı zamanda kurumun /şirketin very ve uygulamaları kurumsal bir güvenlik duvarı ile korunsa dahi, yüksek bir güvenlik riski meydana getirmekteler Dahası güvenlik, bulut tabanlı Dropbox™, Google Drive™, ve Adobe Creative Cloud™ gibi uygulamaların kullanımı ile daha da tehdit edilir bir hale gelmiştir. Veri bu ağlarda serbest bir biçimde akmaktadır ve herhangi bir güvenlik sorunsalı birçok olayda vendorun sorunu gibi sunulmaktadır. Ponemon Enstitüsü tarafından hazırlanan bir rapora göre, birçok BT ve BT Güvenliği vakalarını çalışanların güvenli olmayan paylaşım dosyalarını kullanıp kullanmadıklarından kaynaklanıp kaynaklanmadığı bilinmemektedir. Bu da iş sürekliliğini riske atmaktadır. Sosyal extranetlerin diğer iş birliği araçlarının kullanımı kurum çalışanları dışında, (müşteriler, tedarikçiler ve işortakları gibi) birçok kişinin kurumsal uygulama ve veriye erişimi olduğu anlamına gelmektedir. Her BT güvenlik yöneticisi güvenlik açığı doğurabilecek durumların farkına varabilir. (Veri hırsızlığı, ihlaller, yasal uyumsuzluklar, entellektüel mülk kaybı ,marka itibarının kaybı gibi …) fakat birçoğu güvenlik riskleri ile başaçıkabilmek için en iyi uygulamaları geliştirmeye çalışmaktadırlar. Mobil cihazların kullanımının artması ile birlikte kurumlarda BYOD politikaları geliştirilmeye başlandı. Kasım 2014'te yapılan Tech Pro araştırmasının sonuçlarına göre, kurumların %74 ü halihazırda çalışanların kendi cihazlarını işe getirmelerine izin vermekte ya da gelecekte vermeyi planlamaktadırlar. BYOD gibi inisiyatifleri destekleyen ve yeni çalışma biçimlerinin getirdiği zorluklarla başa çıkmaya çalışan BT uzmanları hem verimliliği hem de kullanıcı deneyimini artırmayı hedeflemektedirler.

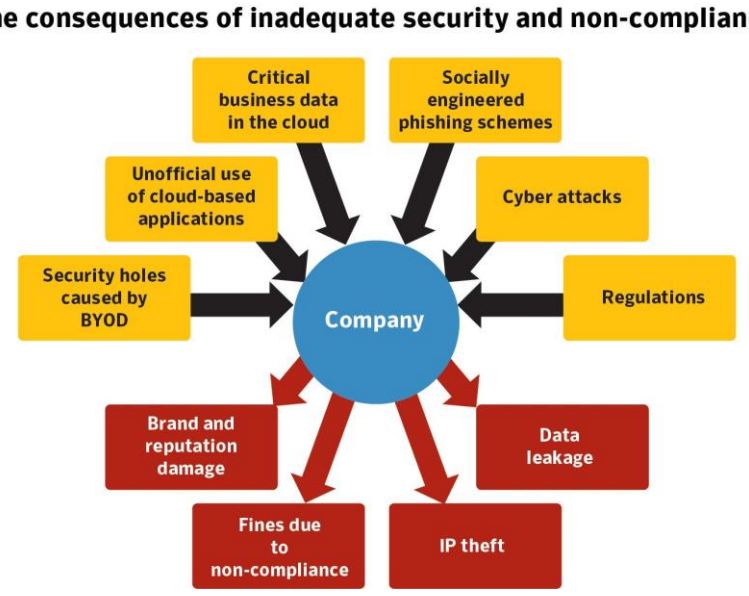
BT Departmanlarının yeni gelişen bu tür taleplerini karşılamak için, ideal bir çözüm olarak kartlı ya da kartsız iki aşamalı kimlik doğrulama gösterilmektedir. 2FA kimlik doğrulama, kurumsal uygulamalara ve veriye hem kurumsal networkten hem de buluttan erişimde yetkisiz erişime karşı korumada geçerliliği kanıtlanmış bir araçtır. Biyometri ve kartsız kimlik doğrulama gibi şifresiz uygulamalar kullanıcıları zora sokmadan yüksek seviyede bir koruma sağlayan yöntemlerdir. Optimum ölçeklendirme, esneklik ve kolay kurulum için, bulut tabanlı bir model göz önünde bulundurulmalıdır. Bulut tabanlı kimlik doğrulama aynı zamanda BT nin finansal ve yönetimsel maliyetleri önemli ölçüde azaltmaktadır. Hatta şifresiz ya da kartsız kombinasyonlar ile tasarruflar artmaktadır.

Güvenlik Riskleri ve Gelişen İhtiyaçlar

Kurumları ve çalışanlarını etkileyen Siber Saldırılar her geçen gün hızla artmaktadır. 2015 Symantec Internet Güvenlik Saldırıları Raporunda, tecrübeli saldırganların 2014'te geçen yıla göre %40 büyüyen 6 büyük firmadan 5 ini hedef aldıkları ortaya çıkmıştır. Bu da sarsılan itibar ve kaybolan dolarlar demektir. Veri kaybı, entellektüel bilgi hırsızlığı,soygunu ve bu türden zararlı aktiviteler b.irçok firmaya yıllık olarak milyon dolarlarca kayıp verdirmektedir. Gerçekte, siber suçların kurumlara yıllık olarak 9 milyon dolar kayıp verdirdiği ortaya çıkmıştır. Kaldı ki, bu kayıplar geri çevrilemez niteliktedir. 2013 yılında %34 olan saldırganlar tarafından yaratılan zarar 2014 yılında %49 a çıkmıştır. Rapor edilen vakalar yalnızca siber buzdağının ucunu oluşturmaktadır.Çalışanlar ise bireysel olarak sosyal mühendislik yoluyla organize edilen fishing türü ve diğer türden saldırılar hergün hedef alınmaktadır. Ek olarak, kurbanı saldırı altında bıraktıkları zaman; entellektüel bilgiden hassas müşteri bilgilerine kadar herşeyi tehlike altına atmış olmaktalar.

İki Aşamalı Kimlik Doğrulama Nasıl Çalışır?

İki aşamalı kimlik doğrulama (2FA) iki şeyi talep etmektedir: kullanıcının bildiği birşey (kullanıcı adı ve şifre) kullanıcının sahip olduğu birşey (donanımsal bir yetki belgesi* kart, akıllı kart, cep telefonu, davranış profili gibi, ya da kullanıcının olduğu birşey (biyometrik parmakizi gibi). Kurumlar için, bu ikili mekanizma gizli datanın korunması için daha yüksek bir güvenlik seviyesini ve aynı zaöanda uyumluluğu karşılayan uygualamaları gerektirmektedir.



Uyumsuzluk ve Güvenlik Açığı Sebepleri

Bu türden ihlal riskleri kurumları daha yüksek seviyede bir güvenlik arayışı konusunda etkileyen en önemli itici güçlerdendir. Daha da ötesi, devlet tarafından öngörülen birtakım kamusal ve endüstriyel güvenlik düzenlemeleri daha sıkı bir güvenliği zorunlu kılmaktadır. Bu tür düzenlemelerin bir çoğu tarafından veri ve uygulamalara erişimin kontrolü aranmaktadır ve bu konular uyumluluk denetimlerinde en dikkat edilen hususlardan biri olmaktadır. Ancak sözkonusu kontrol özellikle bireysel kullanıcı düzeyinde oldukça zordur. Şifreler ve kullanıcı kimlikleri günümüzde artık güvensiz ölçütlerdir. Herhangi bir kurumsal BT departmanının iyi bildiği gibi, kimlik/şifre sistemlerinde çok fazla sayıda akış vardır. Şifreler ise onları kullanan kişiler kadar güvenlidir. Bu kişiler de insan olduklarından dolayı her zaman için yanılma payları vardır. Kullanıcıların %26sı hesaplarını sadece farklı şifreler ile korumaktadırlar. Bu durumda kişinin sosyal networkune dair bir şifre ele geçirildiğinde aynı zamanda kurumsal hesabının şifresi de tehlike altına girmiş demektir. Kişiler arasında şifrelerini yapışkan notlara yazıp bir yerlere asma gibi güvensiz bir durum çok da yaygın değildir ancak, hackerlar için korumalı şifreler bile kırılabilir veya tahmin edilebilir. Bundan çok da uzun olmayan bir zaman önce, Elektrik ve Elektronik Mühendisleri Ensitütüsü (IEEE) kazaen 100,000 kullanıcının şifrelerini serverları üzerinden kamunun bilgisine açtılar. Bu durumu inceleyen bloggerlar, en yaygın şifrelerin 123456, ieee2012,12345678 olduğunu keşfettiler. Kullanıcının talep ettiği bu kullanım kolaylığı bazen güvenlik sınırlarını aşmaktadır. Kurumların birçoğu günümüzde, BYOD (Bring your own device) ve BYOE (Bring Your Everything) politikalarına izin vermektedirler.Evet, kurumlar bu tür inisiyatiflerdeki tasarruf avantajlarını bugün artık anlamış durumdalar. Fakat system yöneticileri ise tüm bu cihazları mevcut güvenlik sistemlerine nasıl uyum sağlayabileceklerini düşünmekten uykusuz kalmaktadırlar. Tüm bu faktörler bizi bir sonuca götürmektedir. Kurum ve işletmeler hassas veriyi korumak için yeni, daha esnek daha güçlü araçlara ihtiyaç duymaktadırlar. Geleneksel kullanıcı şifreleri/ kimlikleri dışında, iki aşamalı kimlik doğrulama gibi daha akılcı, güvenilir güvenlik politikalarına ihtiyaç duymaktadırlar. Kurumlar çalışanlarına daha kolay ve güvenli çözümler sunabilmelidirler.

Yönetilebilir Hizmetler

Iki aşamalı kimlik doğrulama yeni bir konsepttir. Kurum verisini koruma konusunda artık olgunlaşmış ve kanıtlanmış bir yöntemdir. Ancak en konvansiyonel 2FA çözümleri güvenlikte en geleneksel bakış açılarına yoğunlaşmaktaydı yani kartlı yazılımlara. Ek olarak, birçok on-premise uygulama yüksek maliyetli ve büyük entegrasyon çabaları ve yönetimsel destek gerektiren çabalardır.

Bugün kurumların ihtiyacı olan temek şey, güçlü bir 2FA ile endüstriyel entegrasyonu konmbine eden ve kimlik doğrulama seçenekleri sunabilen yönetilebilir hizmetlerdir. Doğru konumlandırılmış bir yönetilebilir hizmetler desteği, SaaS için avantajlı çözümler sunmaktadır. Bu çözümler içerisinde donanımsal ve yazılımsal olarak daha düşük maliyetler, daha az yazılımsal işgücü ödemesi, ölçeklendirilebilir yapı, güvenirlik, uzun sürelilik ve SLA ler ile mevcut altyapınıza mükemmel entegrasyon sağlar.

Kimlik doğrulama seçenekleri, geleneksel çift aşamalı 2FA modeline uysalar bile, biyometri ve profilleme gibi yeni modeler aracılığı ile kurumlar artık tüm uygulamalarda kendileri için neyin doğru olduğunu görmeye başladılar. Bunlardan biri de BT şirketleri için kartsız kimlik doğrulama sistemleridir. Gartner raporuna göre, 2017 yılı sonunda, kurumların %30 undan fazlası, işgücü ve remote erişim konularında adapte edilebilir teknikler kullanacaklar.

Durumsal Kartsız Kimlik Doğrulama

Artan bir oranda kurumlar, kullanıcı deneyimlerini artırmak ve maliyetlerini azaltmak adına kartsız kimlik doğrulamaya geçmenin yollarını aramaktalar. BT çalışanları artık tüm kimlik doğrulama türlerinin donanım kartlarından ve mobil doğrulama bilgileri gibi dinamik güvenlik kodu gerektirmediğini anladılar. Symantec™ Doğrulama ve Kimlik Koruma hizmeti, (VIP) kartsız sistemi, cihaz üzerinde parmak izi doğrulama seçeneği ve kullanıcı davranışı risk analizi gibi donanım temelli tanıtıcı özellikleri de içermektedir. Kartsız kimlik doğrulamanın cazipliği,, kullanıcı deneyimini kullanıcıyı doğrulamanın ikinci aşamasından muaf tutarak büyük oranda basitleştiriyor. Kullanıcıların algısı ise sadece basit bir şifre ve kullanıcı adına sahip olmanın networke erişmek için yeterli olduğu noktasında. Tüm bunların ötesinde, Doğrulama ve Kimlik Koruma hizmeti; bilgisayarları etiketleme, giriş davranış analizi özelliklerini çıkarma ve giriş profile analizlerini gerçekleştirme işlemlerinin hepsini kendisi yapıyor. Tüm bu kartsız kombinasyonlar, kullanıcı adı/şifresini karmaşık cihaz analizleri ve davranış analizleri ile combine ederek geçerliliği kanıtlanmış bir giriş güvenliği sağlamaktadır. Symantec™Doğrulama ve Kimlik Koruma Akıllı kimlik doğrulama sistemi (risk bazlı doğrulama) cihaz üzerinde tam bir risk analizi yaparak; olası tehditleri analiz ediyor ve kullanıcı davranış profillerini çıkarıyor. Kullanıcılar için kullanıcının normal giriş ve davranış profilini çizebiliyor. Örneğin; bir kullanıcının normalde girş yaptığı yeri ve cihazı tanımlayabiliyor. Bir saldırı analizi, Symantec'in diğer çözümlerinden de very toplamaktadır. Örneğin Global Zeka Ağı gibi günümüzün en yaygın saldırılarını tanımlayabilen ağlar ile korelasyonlar kurabilmektedir. Giriş davranışı normal olduğu zaman, basit bir şifre Kabul edilebilir gözükmektedir. Ancak bilinmeyen bir cihazdan veya mekandan şüpheli bir durum içerebilecek bir giriş aksiyonu fark edildiğinde, kullanıcı, bir yazı, e-posta ya da ses bilgisi ile bilgilendirilmektedir. Çünkü, akıllı kartlar, biyometri gibi kartlı bir system mevcut değildir. Üstelik maliyet daha düşüktür ve kullanıcı deneyimi arka planda karmaşık olsa da kullanıcı deneyimi açısından geleneksel bir kullanıcı adı/şifre bilgisi şeklindedir. Kartsız kimlik doğrulama, vakit sıkıntısı çeken ve ağa erişim ile vakit harcamak istemeyen yöneticiler için biçilmiş kaftandır. Kartsız seçenek, dikey piyasalarda faaliyet gösteren firmalar için de tercih edilir bir hale gelmiştir. Düşük maliyetler ve kullanım kolaylığı sayesinde, eğitimciler için de tercih edilir bir seçenektir.

Güçlü ve Daha Akıllı Kimlik Doğrulama ve ID Koruma

Başarı Hikayesi: Esneklik ve Hız

Global bir danışmanlık firması, donanım kartlarını ekarte ederek kullanıcı deneyimini artırmayı ve PC lere ve mobil cihazlara olan desteği geliştirmeyi talep etmekteydi.

Aynı zamanda da maliyetleri düşürmeyi hedefliyordu. Symantec™ VIP hizmetini iki sebeple tercih etti: esneklik ve hızlı kurulum.VIP hizmeti, Akıllı Kimlik Doğrulama hizmeti ile geniş bir doğrulama desteği ve entegre destek sunmaktadır.

Ek olarak, VIP Hizmeti girş şifrelerinin indirlebildiği kişisel bir portal ile hazır gelmektedir.Hızlı kurulabilir ve ölçeklenebilir. Danışmanlık firması, bu hizmeti 325,000 kullanıcına açmış durumda ve Akıllı Kimlik Doğrulama hizmetine remote erişim sağlamaktadır.

Daha Güçlü ve Daha Akıllı Kullanıcı Kimlik Doğrulamasından Faydalanmak
Günümüzün Mobil İş Dünyasında Etkili ve Kullanıcı Dostu Çözüm

Birçok firma, artık mobil cihazlardan ve dışarıdan ofise erişim sağlayan önemli bir çalışan sayısına sahip durumda. Ancak halen, kullanıcı adları ve şifreler yetkisiz erişime karşı cihazları tam bir koruma altına alabilmiş değildir. Çoğu firma 2FA e geçiş yaptı ancak hassas şirket verisine otomatik erişimi gereken, az sayıda bir çalışan tarafından bu system kullanılmakta. Neden bu şekilde? Çünkü kullanıcılar, karmaşık 2FA süreçlerinin iş yüküne katlanmayı reddetmekteler. Hatta BT çalışanları ve ekipleri için bile bu süreçler kimi zaman ekstra işyükü şeklinde algılanabilmektedir. Bu tür on-premise çözümler çoğu zaman çok pahalı ve ekstra altyapı yatırımları gerektiren süreçlerdir. Oysa BT ekipleri daha ziyade uzun sürelilik ve ölçeklenebilirlik özelliklerine odaklanmaktadır. Doğrulama ve Kimlik Koruma hizmeti, mobil bir işgücünü koruma altına alma konusundaki problemleri çözmektedir ve birçok on premise 2FA sistemine göre avantajlıdır. Kısacası, Doğrulama ve Kimlik Koruma hizmeti, bulut tabanlı güçlü, daha akıllı ve etkin bir güvenlik sisteminin tüm özelliklerini de sağlamaktadır. Yönetilebilir hizmetler daha düşük bir maliyete gelmektedir ve daha ölçeklenebilirdir. Çünkü, yerinde kurulum gerektiren hiçbir altyapı yatırımı gerektirmez ve güçlü bir kimlik doğrulama sunarken, daha esnek oluşu ile ön plana çıkar. Aynı zamanda farklı risk modellerine göre ve politikalara uyarlanabilir özelliğinin yanısıra maliyet avantajı çözümü cazip kılmaktadır. Özel Sanal Ağlarda (VPN), veri ambarlarında, web mail programlarında kullanılabilir ve entegre edilebilir bir durumdadır. Şifresiz olduğu için kişisel hizmet seçenekleri ile BT çalışanlarının iş yükünü azaltmaktadır. VIP hizmetinin doğrulama sistemi bir portal üzerinden çalışır. Kullanıcı kendi kendine bunları test edebilir, isim değiştirebilir veya kaldırabilir. Herhangi bir destek hattından yardım almanıza gerek kalmaz. Kurumlar IT masrafları VIP servisi ile %75 e kadar azaltabilmektedirler. CitriXSistemi kurulduğunda, %60 a kadar bir maliyet azaltımı olmaktadır. Gartner raporuna göre destek hatları aramarının %30 u şifre kaynaklı sorunların çözümü ile ilgili aranmaktadır. VIP hizmeti, kullanıcı, cihaz veya case e göre kurumun çeşitli modelleri seçebilmesini sağlar. Zira bugünün işgücü mobil olduğu için çoğu çalışan mobil erişimi tercih etmektedir, ancak bu seçeneklerin çoğu şifrelidir. Kartsız sistemlerde en avantajlı çözümlerden biri VIP servisidir.

Başarı Hikayesi: Çalışma Zamanı ve Ayrılan Kaynak Azaldı: CitriXSisteminde, çoğu çalışan şirketin VPN ine ulaşmak için otomatik olarak mobil sistemler üzerinden ağa erişmektedir. Citrix, Symantec VIP ile kurulduğunda, birçok avantajı beraberinde getirmektedir. Büyük bir işletme, BYOD politikasını getirdi ve çeşitli politikalar geliştirdi. Bu süreçte, VIP servisinin kişisel portal ile kullanıcı deneyimini geliştirdi ve çalışanları arasında; adaptasyonu sağladı. Aynı zamanda kurum, yönetimsel masraflarını azalttı ve çalışma zamanından tasarruf etti. Özellikle, BT güvenliği desteklemek için ayrılan zaman önemli ölçüde azaldı. VIP hizmeti, 10,000 kullanıcıya ulaştı.

platin
Bilişim Teknolojileri

Daha Güçlü ve Daha Akıllı Kullanıcı Kimlik Doğrulamasından Faydalanmak
Günümüzün Mobil İş Dünyasında Etkili ve Kullanıcı Dostu Çözüm

Symantec Doğrulama ve Kimlik Koruma Hizmeti

Koruma: Doğrulama ve kimlik koruma hizmeti, yetkisiz erişim riskini azaltır, veriyi korur ve güvenlik problemlerinin çözülmesini sağlar. 2FA, kurumların veri ve uygulamalarının güvence altına alınması için hem şirket netwoku hem de bulut bazında sektör lideri konumunda bir çözümdür. Symantec VIPi kurarak, işletmeniz hem kurumsal anlamda bir güvenlik çözümüne hem de bulut bazlı bir güvenlik çözümüne kavuşmuş olmaktadır.

Ölçeklendirilebilirlik: Çünkü VIP güvenlik sistemi, bulutta da sunulabilmektedir. Böylece donanımsal ve yazılım kaynaklarına ilişkin maliyetlerin azaltılmasını sağlamaktadır. İhtiyaçlar değiştikçe farklı ölçeklerde sunulabilmektedir. Konvansiyonel bir on-premise hizmet olduğu için kapasite aşımı problem yaşamazsınız.

Hız: Bazen başarı gelen talepleri en hızlı biçimde karşılama yeteneğiniz ile doğru orantılı olarak tanımlanmaktadır. Symantec VIP hizmeti ile yeni server kurulumu, işletim sistemleri, yeni uygulamalar ile vakit kaybetmezsiniz. Herşey kurulu ve kullanıma hazır bir şekilde sunulmaktadır. Bulut tabanlı hizmetlerin hepsine uygun olduğu için rekabet avantajı sağlar.

Esneklik: Symantec VIP servisi, biyometri ve mobil cihazlardaki gibi şifreyi devre dışı bırakabilme özelliğinden ötürüolağanüstü bir esneklik sunmaktadır. Kurumlara kendileri için en etkili çalışabilecek yöntemi seçme konusunda farklı kimlik doğrulama seçenekleri sunmaktadır. Kullanıcılar veya kurumlar tek kullanımlık şifre, kartsız güvenlik kodları, şifresiz kullanım, biyometrik parmak izi ya da risk temelli kimlik doğrulama seçeneklerinden birini seçebilmektedir. Neyi seçerlerse seçsinler, 2FA maliyet avantajları ve esnek yapısı ile kullanıcılar ve kurumlar için güçlü bir kimlik doğrulama ve etkili bir çözümdür.

Zeka: Doğrulama ve Kimlik Koruma servisi gittikçe daha akıllı bir hal alıyor ve kullanıcı dostu bir biçime dönüşüyor. Kartsız kimlik doğrulama seçeneği, sofistike cihaz analizleri ve Akıllı kimlik doğrulama davranış analizi kullanıcıya daha basit bir system sunuyor. Tabiiki güçlü bir Symantec kurumsal koruması sağlıyor. Risk temelli kimlik doğrulama seçeneği ile kullanıcıların işini kolaylaştırırken, riskli giriş aksiyonları teşhis edilebiliyor ve bloklanabiliyor.

Erişilebilirlik: VIP uygulaması, Symantec Global altyapısı ile yüksek seviyede entegredir. Aynen orduların güvenlik seviyelerindeki tier-4 veri koruma seviyelerini sizlere sunmaktadır. Symantec in internet altyapısı, günlük olarak 30 milyar etkileşimi koruma altına almaktadır.

Öngürüler: Saldırganlar, hergün taktik değiştirmektedir. Bu sebepten kurumların kullanıcılarının hem şimdiki hem de gelecekteki kimlik doğrulama çözümlerine ihtiyaçları vardır. Global Zeka Ağı size gelecekteki tehditlere karşı da korur ve güncel olmanızı sağlar.

platin
Bilişim Teknolojileri

SONUÇ:

Günümüzde, kurumlar çalışanları mobil teknolojilere entegre olduğu ve uygulamalarını buluta taşıdıkları için herzaman olduğundan daha fazla güvenlik meselelerini önemsemek durumundalar. Aynı zamanda da esnek, ölçeklendirilebilir, etkili ve maliyet avantajı olan çözümlere her zamandan daha fazla ihtiyaçları bulunmaktadır. Çıta her geçen gün daha fazla yükselmektedir. Veri hırsızlıkları ve kötü yazılımlara bağlı güvenlik olayları artıkça, kurumların kayıpları milyonlara hatta marka imajının yerle bir olmasına mal olabilmektedir. Aynı zamanda, mesele kimlik doğrulama olduğu zaman, herkes ve her kurum daha basit, daha akıllı kullanıcı deneyimine sahip olmak istemektedir. Symantec™ Doğrulama ve Kimlik Koruma aradığınız çözümdür. Bu çözüm, sektör lideri, bulut tabanlı bir 2FA çözümüdür. Otomatik güvenlik sağlar ve kullanıcı dostu kullanım deneyimi sunar. Hassas veri ve uygulamalara yetkisiz erişim konusunda size ve kurumunuzu korur. Kurulumu kolay, maliyet avantajlı ve akıllıdır.

Platin Bilişim, "Veri Koruma, "Veri Güvenliği" ve "Profesyonel Hizmetler" konularında faaliyet gösteren bir teknoloji firmasıdır.

Uzman kadrosu ile tüm müşterilerine, yerinde ve uzaktan güvenli erişim metoduyla "Yönetilebilir Hizmetler" vermektedir. Satın alma ve kiralama modelleri ile değişik finansal çözümler sunulabilmektedir. IBM, Veritas, Symantec, Hitachi, Bluecoat, Arcserve gibi konularında uzman, lider firmaların çözüm ortağıdır. Platin Bilişim, çözüm sağladığı ürün ve konularda uzmanlaşarak BT sektöründeki yerini almıştır. Uzmanlığındaki konularda, farklı müşteri ihtiyaçlarına uygun implementasyonlarla, müşterilerinin yaptıkları yatırımların hızlı geri dönüşü sağlanmaktadır.

Modern Profesyonel Hizmetler anlayışı ile uzmanlaşmış "Kurulum Uyarlama Servisleri" dışında, "Durum Değerlendirme (Healthcheck)", "Göç (Migration)", "Sürüm Yükseltme (Upgrade)" gibi kompleks servisleri de müşterilerine sağlamaktadır. "Arşivleme" ve "İş Sürekliliği" konularında deneyimli mühendislerinin güncel proje tecrübeleri ile farklılık yaratılmaktadır. Destek verilen ürünler arasında : Netbackup, SSR, Enterprise Vault, Storage Foundation, IBM Bigfix, IBM Qradar, Symantec DLP, SEP, Brightmail, VIP, Clearwell, Transvault,

Hitachi Content Platform sayılabilir. BT Altyapıları konusunda yüksek standartlara sahip firmaların ürünleri ile sorunsuz, uzun vadeli ve güvenilir çözümler üreten Platin Bilişim'i rakiplerinden ayıran en önemli farkı, sağladığı Profesyonel Hizmetlerin yüksek standartları ve uyguladığı başarısı kanıtlanmış metodolojilerdir.

Faaliyet alanımızdaki bir çok çözüm ve gelişmiş IT altyapılarının günlük yönetimi için, eğitimli ve deneyimli kaynakların olması gereklidir. Bu konulardaki tecrübeli insan gücünün kıtlığı, yetiştirilmesi veya istihdam edilmesindeki güçlükler hastalık ve izin vb. ek insan kaynağı

ihtiyacı yaratan durumlarda, bu kaynakların yedeklenmesinde güçlüğüne neden olmakta vefirmalar için risk oluşturmaktadır. Platin Bilişim tüm bu güçlükleri ortadan kaldırmak için, sistemlerinizin günlük yönetimlerini profesyonel olarak üzerine alabilmektedir.

Platin Bilişim, IBM Qradar , Veritas NetBackup , Veritas Enterprise Vault , Symantec DLP , Symantec SEP çözümlerini müşterilerine yazılım ve donanım dahil olmak üzere bütünleşik cihazlar (appliances) şeklinde PLA markası altında sunmaktadır.

www.platinbilisim.com.tr

platin
Bilişim Teknolojileri