



SBY Cockpit

Kurumsal güvenli erişim ve kontrol platformu

Kullanıcıları, cihazları, sunucuları, uygulamaları ve destek oturumlarını aynı kimlik, güvenlik ve politika modeli altında yöneten bütünleşik platform.



Merkezi Yönetim



Güvenli Erişim



Son Kullanıcı Bağlantısı



Uzak Destek

SBY Secure Tunnel

Son kullanıcı güvenli bağlantı istemcisi



SBY Cockpit

Merkezi yönetim, görünürlük ve raporlama



SBY Cockpit
Merkezi Yönetim ve Kontrol



SBY Secure Access Gateway

Güvenli servis erişim katmanı



SBY Secure Remote Support

Kullanıcı onaylı uzak destek



Merkezi Yönetim
Tek kontrol noktası



Güvenli Erişim
Kimlik ve politika tabanlı



Son Kullanıcı Bağlantısı
Sade, hızlı ve güvenli



Uzak Destek
Kontrollü ve izlenebilir

Güvenli erişim, merkezi yönetim ve kontrollü uzak destek tek platformda.

SBY Cockpit

Tüm güvenli erişim operasyonlarının
merkezi yönetim noktası



Ne yapar?



• Kurumları, kullanıcıları ve rolleri yönetir.



• Cihazları, sunucuları ve servisleri
envanterde toplar.



• Erişim ve güvenlik politikalarını tanımlar.



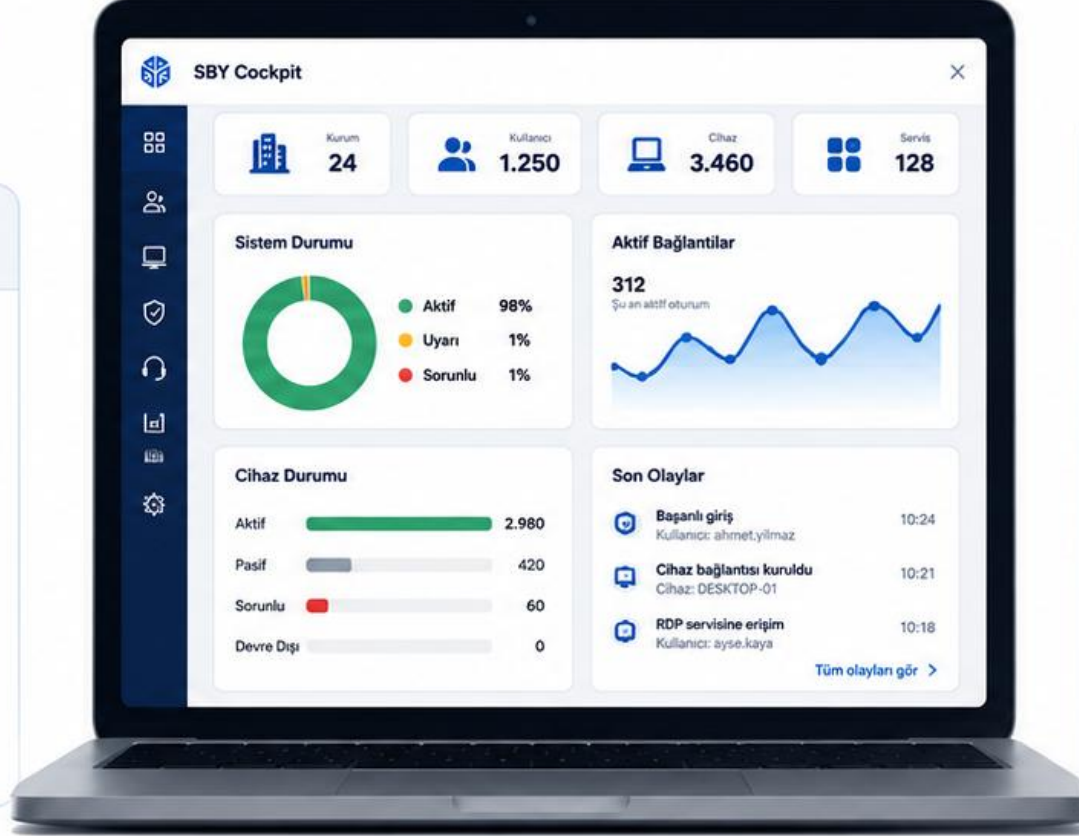
• Gateway ve istemci durumlarını izler.



• Uzak destek süreçlerini yönetir.



• Audit ve raporlamayı tek merkezde sunar.



Kuruma ne kazandırır?



Tek kontrol noktası
Tüm süreçler tek ekranda.



Merkezi görünürlük
Kullanıcı, cihaz ve servis durumunu anlık
görünür kılar.



Daha hızlı operasyon
Sorunları daha kısa sürede tespit edip
çözmenizi sağlar.



Daha az karmaşa
Dağılık yönetim yükünü azaltır,
süreçleri sadeleştirir.



Tek Ekran

Tüm bileşenler tek arayüzde.



Ortak Görünürlük

Kurum genelinde net ve anlık
görünürlük sağlar.



Hızlı Müdahale

Sorunlara daha hızlı müdahale
edebilme imkânı sunar.



Daha Az Karmaşa

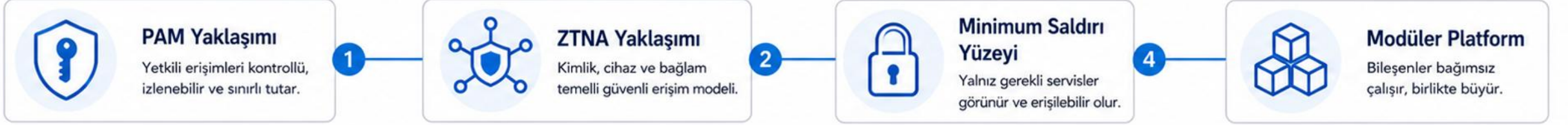
Yönetim süreçlerini sadeleştirir,
operasyonel yükü azaltır.

Dağılık sistemler yerine tek yönetim ve kontrol noktası.



Güvenlik Yaklaşımı ve Modüler Mimari

SBY platformu; kontrollü erişim, minimum saldırı yüzeyi ve modüler büyüme yaklaşımıyla tasarlanmıştır.



Tasarım İlkeleri



- Kimlik, cihaz ve politika temelli erişim kontrolü
- En az yetki ve kontrollü oturum yaklaşımı
- Gereksiz açık yüzeyleri azaltan mimari
- İzlenebilir, kayıt altına alınan erişim modeli
- On-premises ve kurumsal güvenlik ihtiyaçlarına uyum

Ne Anlama Gelir?

	Daha az görünürlük, daha düşük risk Erişime açılmayan servisler saldırı yüzeyini azaltır.
	Her bağlantı doğrulanır Kullanıcı, cihaz ve güvenlik koşulları birlikte değerlendirilir.
	Kontrollü ayrıcalık Yüksek yetkili erişimler kayıtlı ve politika tabanlı yönetilir.
	Büyüyeabilen yapı Yeni bileşenler ve yeni kurum ihtiyaçları modüler şekilde eklenebilir.

Modüler Ürün Yapısı



Bileşenler tek tek konumlandırılabilir, birlikte entegre çalışır.

Genişleme ve Platform Desteği

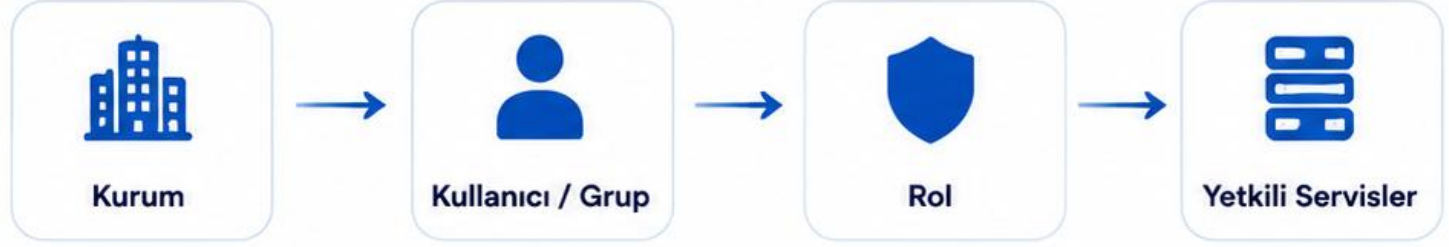


SBY platformu, PAM ve ZTNA yaklaşımını kurumsal ihtiyaçlarla birleştirerek daha kontrollü, daha güvenli ve daha yönetilebilir bir erişim modeli sunar.

Modüler. Güvenli. Kontrollü.

Kullanıcı, Kurum ve Yetki Yönetimi

Doğru kullanıcıya, doğru yetkiyi,
doğru kapsamda verir.



Yönetim Kabiliyetleri

- Kurum ve organizasyon yapısı tanımlama
- Kullanıcı ve grup yönetimi
- Rol ve yetki tanımları
- Servis ve cihaz atamaları
- Hesap aktif / pasif yönetimi
- Son giriş ve oturum görünürlüğü
- Kullanıcı yaşam döngüsü yönetimi



Güvenlik Yaklaşımı

- Kişisel kullanıcı hesapları
- Rol bazlı yetki sınırları
- En az yetki prensibi
- İki faktörlü kimlik doğrulama (MFA) desteği
- Kullanıcı ve rol değişikliklerinde audit kaydı
- Yetki devri ve onay süreçleri
- Oturum süreleri ve zaman kısıtları



Yetki Kapsamı

- Kullanıcı yalnız yetkili olduğu servisleri görür.
- Servis bazlı erişim kontrolü
- Cihaz bazlı erişim sınırları
- Zaman ve lokasyon tabanlı kısıtlamalar
- Bağlantı modu ve özellik kısıtları
- Politika ihlallerinde erişim engelleme



Kişisel Hesap

Ortak hesap yok,
bireysel sorumluluk var.



En Az Yetki

Kullanıcı yalnız
ihtiyacı kadar yetkiye sahiptir.



İzlenebilirlik

Tüm işlemler kayıt altına alınır
ve raporlanır.



Yaşam Döngüsü

Kullanıcılar kurum politikalarına göre
yönetilir.

Doğru kullanıcı, doğru rol, doğru yetki, doğru kapsam.

Cihaz, Sunucu ve Servis Envanteri

Sahiplik, durum ve gerçek kullanılabilirlik görünürlüğü.



CİHAZLAR

Son kullanıcı cihazları ve istemciler



SUNUCULAR

Altyapı ve uygulama sunucuları



SERVİSLER

Yayınlanan uygulama ve kaynaklar



CİHAZLAR

-  Cihaz adı ve sahibi
-  İşletim sistemi ve istemci sürümü
-  Cihaz kimliği ve sertifika durumu
-  Atanmış kullanıcı
-  Son bağlantı (heartbeat)
-  Durum: Aktif / Pasif / Devre dışı
-  Son görülen zaman
-  Gateway ilişkisi



SUNUCULAR

-  Sunucu adı ve organizasyon
-  Sunucu türü ve lokasyon
-  Çalışma ve erişilebilirlik durumu
-  Atanmış servisler
-  Gateway bağlantısı
-  Yetkili kullanıcı ve gruplar
-  Son heartbeat
-  Uptime ve olay özeti



SERVİSLER

-  Servis adı ve türü
-  Erişim protokolü (RDP, HTTPS, SMB vb.)
-  Bağlı olduğu sunucu
-  Yetkili kullanıcı ve gruplar
-  Erişim politikası
-  Servis sağlık durumu
-  Aktif bağlantı sayısı
-  Son kontrol ve olay kaydı



Neden Önemli?

Tüm varlıkları tek yerde görünür kılar, sorunları hızlı tespit etmeyi sağlar.



Tek Noktadan Görünürlük

Cihaz, sunucu ve servislerin tamamı tek ekranda.



Gerçek Durum Bilgisi

Sadece kayıt değil, gerçek çalışma durumunu gösterir.



Hızlı Müdahale

Sorunların kaynağına hızlı ulaşmayı kolaylaştırır.



Doğru Karar

Güvenilir verilerle doğru planlama ve kapasite yönetimi.

Doğru envanter, güvenli ve kesintisiz erişimin temelidir.

SBY Secure Access Gateway

Kullanıcı ile yetkili servis arasında güvenli erişim katmanı

Kullanıcıyı yalnız yetkili olduğu servislere güvenli, kontrollü ve izlenebilir şekilde ulaştırır.



Ne yapar?

- ✓ Kullanıcı ve cihaz kimliğini doğrular.
- ✓ Yalnız yetkili servislere erişime izin verir.
- ✓ Politika kontrollü bağlantı uygular.
- ✓ Güvenli servis erişim tüneli oluşturur.
- ✓ Oturumları izler ve kayıt altına alır.
- ✓ Olayları ve sağlık verilerini toplar.
- ✓ On-prem veya bölgesel erişim noktası olarak çalışır.



GÜVENLİK KAZANIMI

- ✓ Daha küçük saldırı yüzeyi
- ✓ Servis bazlı erişim
- ✓ Kontrollü yayın modeli
- ✓ Merkezi politika uygulaması
- ✓ İzlenebilir bağlantı kayıtları
- ✓ Ağ segmentasyonu ile uyumlu yapı
- ✓ Erişim kayıtlarında tam izlenebilirlik



KONUMLANDIRMA



On-Premises

Kurumsal ağ içinde çalışır.



Bölgesel / Dağıtık

Farklı lokasyonlarda konumlanarak daha iyi performans sağlar.

GATEWAY ÖZELLİKLERİ



TLS 1.2+ ile uçtan uca şifreleme



Kullanıcı ve cihaz doğrulaması



Politika tabanlı erişim kontrolü



Çoklu Gateway desteği



Yüksek erişilebilirlik ve yedeklilik



Yüksek performans ve düşük gecikme



Detaylı oturum izleme ve raporlama



Kolay kurulum ve merkezi yönetim



Erişim, ağ adresine göre değil; kimlik, yetki ve politika kararına göre şekillenir.



Güvenli. Kontrollü. İzlenebilir.

SBY Secure Tunnel

Son kullanıcı için güvenli erişimi
sade ve hızlı hale getirir

Kullanıcı ne görür?

-  Kurum hesabıyla giriş
-  Gerektiğinde MFA doğrulaması
-  Yalnız yetkili servisler
-  Bağlantı durumu ve sağlık bilgisi
-  Bağlan / bağlantıyı kes
-  Uzak destek talebi
-  Bildirim ve duyurular
-  Dil ve tema seçenekleri

 SBY SECURE TUNNEL

 Ana Sayfa

 Servisler

 Destek

 Bildirimler

 Ayarlar

 Hakkında

 **Bağlı**
Güvenli tünel aktif
Süre: 00:12:48

Cihaz Durumu
Cihaz Kimliği 
Sertifika 
Tünel 
Son Senkronizasyon 1 dk önce

Yetkili Servisler

 **Web Uygulaması**
https://app.sirket.com
Bağlan

 **RDP Sunucusu**
rdp.sirket.com:3389
Bağlan

 **Dosya Sunucusu**
files.sirket.com
Bağlan

 **Veritabanı**
db.sirket.com
Bağlan

 **API Servisi**
api.sirket.com
Bağlan

 **Yönetim Paneli**
admin.sirket.com
Bağlan

 Tünel: Aktif | Gateway: SBY-GW-01 | Sürüm: 2.1.6.0 |  Tüm trafik şifreli

Arka planda ne olur?

-  Kullanıcı kimliği doğrulanır.
-  Cihaz sertifikası kontrol edilir.
-  Yetkili servis listesi alınır.
-  Güvenli bağlantı yolu kurulur.
-  Bağlantı ve servis sağlığı izlenir.
-  Durum bilgisi Cockpit'e iletilir.

Kullanıcı kazanımı

-  IP adresi bilmez.
-  Port bilgisi girmez.
-  Karmaşık ağ ayarı yapmaz.
-  Yalnız yetkili olduğu servisi görür.
-  Tek tıkla güvenli bağlantı kurar.
-  Destek ihtiyacını kolayca iletir.



Basit ve Hızlı

Tek tıkla güvenli erişim,
karmaşık ayar yok.



Güvenli

Kimlik ve cihaz doğrulaması ile
uçtan uca şifreli bağlantı.



Zaman Kazancı

Yetkili servislere hızlı erişim,
iş süreçlerini hızlandırır.



Kullanıcı Dostu

Anlaşılır arayüz, herkes için
kolay kullanım.



Destek Entegrasyonu

Uzak destek talebiyle
sorunlara hızlı çözüm.



Kullanıcı için kolay, kurum için kontrollü ve güvenli erişim deneyimi.



Güvenli. Basit. Kontrollü.

Politika, MFA ve Firewall Entegrasyonu

Erişim kararı birden fazla güvenlik koşuluyla birlikte verilir

POLİTİKA YÖNETİMİ

- Kullanıcı ve grup bazlı politikalar
- Cihaz ve sertifika kontrolleri
- Servis ve kaynak bazlı kurallar
- Zaman ve çalışma saati kısıtları
- Lokasyon ve ağ koşulları
- Risk ve davranış temelli kurallar
- Bağlantı modu (Relay / Direct / Hybrid)
- Öncelik ve istisna tanımları
- Tüm değişikliklerde audit kaydı

ERİŞİM KARARI NASIL VERİLİR?



MFA GEREKTİREBİLECEK DURUMLAR

- Yeni cihazdan giriş
- Cihaz kimliğinde değişiklik
- Olağandışı ülke veya bölge erişimi
- Kısa sürede uzak konum değişimi
- Yenilenmiş cihaz sertifikası
- Uzun süre kullanılmayan cihaz
- Yönetici tarafından zorunlu MFA



FIREWALL ENTEGRASYONU

- Ağ segmentasyonu ve izolasyon
- Servis bazlı erişim sınırlandırma
- İç ve dış trafik kontrolü
- Güvenlik olaylarının ilişkilendirilmesi
- Erişim politikalarının ağ politikaları ile uyumu



DAHA GÜVENLİ

Çok katmanlı kontrol ile saldırı yüzeyi azalır.



DAHA KONTROLLÜ

Erişim kararları net kurallara göre otomatik verilir.



DAHA HIZLI

Uygun koşullar sağlandığında erişim kesintisiz sağlanır.



DAHA GÖRÜNÜR

Tüm kararlar ve olaylar merkezde izlenir.



DAHA UYUMLU

Kurumsal güvenlik ve ağ politikaları ile tam uyum.



Doğru kullanıcı, doğru cihaz, doğru koşullar sağlandığında erişim izni verilir.



Güvenli. Kontrollü. İzlenebilir.

Sağlık, Görünürlük ve Self-Healing

Uçtan uca görünürlük, proaktif izleme ve otomatik iyileştirme ile kesintisiz erişim.



İSTEMCİLER

SBY Secure Tunnel
Ajanları



GATEWAY'LER

SBY Secure Access
Gateway



SERVİSLER

Uygulama ve
Sunucular



COCKPIT

Merkezi İzleme ve
Yönetim

SİSTEM SAĞLIK DURUMU



GENEL DURUM
Sağlıklı



1.284
İstemciler
Sağlıklı



12
Gateway'ler
Sağlıklı



256
Servisler
Sağlıklı



1.678
Aktif Oturumlar
Sağlıklı



PROAKTİF İZLEME

- ✓ 7/24 durum kontrolü
- ✓ Eşik tabanlı uyarılar
- ✓ Anormal durum tespiti
- ✓ Kapasite ve kullanım raporları



SELF-HEALING YETENEKLERİ

- ✓ Bağlantı kaybında yeniden bağlanma
- ✓ DNS ve ağ sorunlarında otomatik onarım
- ✓ Servis erişim hatalarında akıllı yönlendirme
- ✓ İstemci ajan kendini kontrol ve iyileştirme



HIZLI TESPİT

Sorunları erken tespit eder,
etkiyi en aza indirir.



OTOMATİK İYİLEŞTİRME

Self-healing ile çoğu sorun
insansız çözülür.



TAM GÖRÜNÜRLÜK

Uçtan uca görünürlük ile
kontrol sizde olur.



YÜKSEK KULLANILABİLİRLİK

Kesintisiz ve güvenilir
erişim deneyimi.

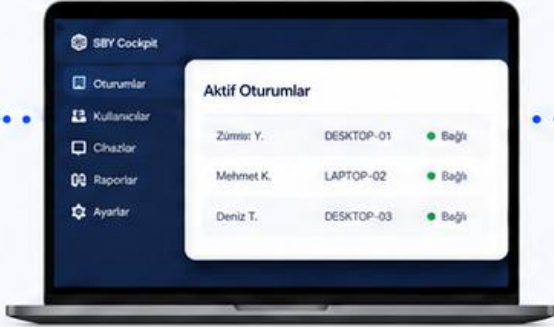
SBY Secure Remote Support

Güvenli uzak destek, SBY altyapısı üzerinde kurum içinde kalır.

Nasıl Çalışır?



Teknisyen
Destek Başlatır



Kullanıcı Onayı
Kodu girer ve onaylar.



Güvenli Bağlantı
SBY altyapısı üzerinden güvenli bağlantı kurulur.

Öne Çıkan Özellikler

-  Güvenli tünel ile bağlantı
-  Kullanıcı onayı
-  6 haneli geçici kod
-  Viewer / Tam kontrol
-  Dosya aktarımı
-  Oturum bitince otomatik kapanış

Güvenlik Avantajları



İnternete açık
bağlantı gerekmez



Tüm trafik şifreli
altyapıdan geçer



Kullanıcı onayı
olmadan erişim yok



Politika ve MFA
kontrolleriyle uyumlu



Oturum sonunda
istemiçi kapanır

Uçtan Uca Güvenli Erişim Yaşam Döngüsü

SBY Secure Tunnel ile kullanıcıdan yetkili servise, kontrollü ve güvenli erişim akışı



Doğru kullanıcı, doğru cihaz ve doğru güvenlik koşulları sağlandığında erişim güvenli biçimde kurulur.

**SBY**

SBY Cockpit Ürün Ailesi: Kullanıcı Sabah İşe Geldiğinde Nasıl Kullanır?

Son kullanıcı için 5 adımda günlük kullanım akışı

1

Bilgisayarı Açma

Kullanıcı Windows veya Linux bilgisayarını açar.

2

SBY Secure Tunnel Başlar

İstemci otomatik açılır ve kurumsal bağlantı ekranı hazır olur.

3

Cihaz Kontrolü

Cihaz kontrol edilir. Güvenli cihaz sınıfındaysa bağlantı otomatik devam eder; değilse veya politika gerektirirse MFA istenir.

**4**

Yetkili Servisler

Kullanıcı yalnız yetkili olduğu servisleri görür ve kullanmaya başlar.

5

Güvenli Kullanım ve Destek

Kullanıcı servisini güvenli şekilde kullanır. Sorun varsa SBY Secure Remote Support ile destek talep eder.



Kullanıcı İçin Ne Kadar Kolay?



IP veya port bilgisi gerekmez



Yalnız yetkili servisler görünür



Güvenli cihazda hızlı giriş



Sorun varsa kontrollü destek



Arka Planda Güvenlik



Kimlik doğrulama



Cihaz kontrolü



Politika değerlendirmesi



Şifreli bağlantı



SBY

Teşekkürler

Sorularınızı memnuniyetle yanıtlarız.

SBY Bilişim Yazılım Ltd.

Web: <https://sbybilisim.com>

E-posta: info@sbybilisim.com

Kurumsal dijital çalışma ve sanallaştırma çözümleri için yanınızdayız.