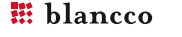


Blancco

Blancco Bilgisayar Sürümü



Blancco bilgisayar sürümü

- PC ve laptop bilgisayarlardan tüm bilgiyi güvenli bir şekilde silmek için dizayn edilmiş profesyonel bir yazılımdır. Yüksek hızlı ve aynı anda birden fazla disk silme kabiliyetine sahip olan yazılım, silme işlemini dünya standartlarında güvenli bir şekilde yapmaktadır. Yazılımın bu kabiliyetleri silinen disklerin güvenli bir şekilde yeniden kullanılmasını sağlamaktadır
- 9 farklı dilde yüklenebilen ürün; MSI, Network PXE, CD ve USB gibi birçok dağıtım seçeneklerine sahiptir.
- Blancco silme işlemi sonrasında PC/laptop'unuzu yeniden kullanabilir veya güvenli satabilirsiniz. Bugünkü var olan herhangi bir teknolojik altyapı ile silinen verinin geri gelmesi olanaksızdır. Yapılan silme işlemi ile alakalı detay rapor yazılım tarafından üretilmekte olup kayıt altına alınabilmektedir.
- Ürün ayrıca opsiyonel olarak donanım fonksiyon testi de yapabilmektedir (sistem operatörü; bellek, işlemci, anakart, görüntü birimi, optik sürücü, ses kartı, klavye ve sabit disk birimlerinin donanım testlerini yapabilmektedir).

Sunucu Sürümü



Bulut Temelli Servisler Blancco Cloud

Blanccocloud.com mükemmel bir merkezi yönetim yazılımıdır (kullanıcı yönetimi, yedekleme servisleri, veri aktarımı vb). Bulut temelli bu servis sayesinde yeni bir altyapı kurulumu ve yatırımı gereksinimi ortadan kalkmaktadır. Internet üzerinden veri yok etme sistemlerine ait tüm ürün portfolyosu sağlanabilmektedir.

Merkezi işlem yönetimi

- Tüm veri silme, yönetme ve monitörize etme işlemleri bulut temelli servisler ile çalıştırılabilir.
- Rapor dağıtımı için çevrim içi merkezi yönetim birimlerine minimum efor ile ulaşılabilir
- Blancco veri silme ürünleri ile ful uyumlu
- Abonelik veya kullanım başına ödeme modeli ile hizmet alımı

Kullanıcı yönetimi

- Kolay kullanıcı yönetimi. Global anlamda kullanıcı haklarının dağıtımı
- Muhtelif basamaklarda kullanıcı hakları (örneğin çözüm ortağı, kurumsal, son kullanıcı vb)
- Blancco'nun yüksek kaliteli teknolojisi sayesinde yönetici ve operatör haklarının profesyonel anlamda dağıtımı

Mobil Sürümü



Mobil Sürüm

Blancco mobil sürüm akıllı telefonların dahili ve harici hafızalarını güvenli bir şekilde silmek için dizayn edilmiş üründür. Akıllı telefonu fabrika ayarlarına almak yüzde yüz anlamda verileri imha ettiniz anlamına gelmemektedir. Muhtelif veri kurtarma yazılımları vasıtası ile ilgi veri geri getirilebilir. Blancco mobil sürümü yardımı ile tüm kullanıcı verileri (e-posta, kontaklar, metin mesajlar) kalıcı olarak güvenli bir şekilde silinebilmektedir. Yazılım aynı zamanda tablet bilgisayarlarda da çalışmaktadır.

Veri Merkezi Sürümü



Blancco Veri Merkezi Sürümü

Yüksek kapasiteli depolama ortamları için dizayn edilmiş sürümdür. Yazılım, güvenli bir biçimde veri merkezi bünyesinde çalışan disk koruncaklarını ve yüksek kapasite yedekleme ünitelerini silbilmektedir. Çözüm geniş donanım desteği sunmaktadır (RAID disk dizilimi için nüfuz etme ve parçalara ayırma özellikleri dahil). Yüksek hızlı ve eşzamanlı çoklu disk silme kapasitesi son derece etkili bir silme işlemi yapabilmeye olanak tanımaktadır.

Flash Medya Sürümü



Blancco Flash Medya Sürümü

Dijital depolama medyanızı elden çıkarmadan önce, içerisindeki verilerin kesinlikle silindiğini garanti altına alıyor. Ürün USB diskler, SD hafıza kartları, CompactFlash kartlar, mikrosürücüler ve flash hafıza bellekleri gibi birçok yedekleme aygıtlarının içeriğini kalıcı anlamda siliyor.

Güvenli veri silme çözümü Uygulama yedekleme birimi üzerindeki (Windows destekli) verilerin kalıcı olarak silindiğini %100 olarak garantiliyor.

Hızlı ve kullanıcı dostu veri silme işlemi Ürünün kurulumu son derece basit olup kullanımı çok kolaydır.

Mevzuata uygunluk Ürün uluslararası bilinen tüm veri silme standartlarına uygundur. Yazılım aynı zamanda organizasyonunuzun kurumsal politikalarına ve yerel kanunlara uyması (veri silme ve veri kaybı önleme sistemleri) noktasında yardımcı olmaktadır.

Detaylı rapor ve denetim amaçlı izleme Ürün yapılan her veri silme işlemi sonrasında son derece detaylı silme raporlarını otomatik olarak hazırlamaktadır.

**Blanco PCI-DSS Kuralları çerçevesinde Mantıksal Sürücüler Güvenli Bir Şekilde Temizliyor**

Blanco LUN, kurumların depolama sistemi konfigürasyonlarının yeniden kullanımına ilişkin olarak veri merkezlerine güvenli ve maliyet etkin seçenekler sunmaktadır. Bu sayede konfigürasyonların yeniden kurulmasına ya da sabit sürücülerin imha edilmesine gerek kalmamaktadır. Blanco LUN sayesinde, yöneticiler aktif bir depolama ortamında LUN'lar gibi mantıksal sürücüler merkezi olarak silinebilmektedirler. Süreç uzaktan yönetilebilmekte ve çoklu birimlerin eş zamanlı olarak silinebilmesine destek verilmektedir.

Örnek Kullanım Alanları:**PCI DSS uyumluluğu**

PCI DSS zorunluluklarına istinaden ödeme kartı bilgilerinin 5 yıldan fazla bir süre depolanmaması gerekmektedir. Bu da veri merkezlerinin zaman veya vaka bazlı olarak spesifik LUN verilerini hedefleyen bir silme ürününe ihtiyaç duyduklarını göstermektedir.

Yıkım Onarımı Testi

LUN verilerinin çok sayıda kopyası yıkım onarımı testinden sonra da mevcut olduğundan güvenlik gerekçeleri nedeniyle bunların silinmesi gerekmektedir.

Web Barındırma Aboneliğinin Sonlandırılması (End of Hosting Subscription)

Barındırmanın olduğu bir ortamda, mevcut müşterinin ayrıldığı ve hali hazırdaki LUN'a yeni bir kullanıcının atandığı durumlarda LUN'un yeniden kullanımı için silme işlemi gereklidir.

Kart Hamili Verilerinin Korunması**Zorunluluk 3: Depolanmış Kart Hamili Verilerinin Korunması**

Şifreleme, yok etme, maskeleye ve hesaba dayalı adresleme gibi koruma yöntemleri kart hamili veri korumasının hassas bileşenleridir. Davetsiz bir misafir diğer güvenlik kontrollerini alt ederek şifrelenmiş verilere erişim sağlamış olsa bile, uygun şifreleme anahtarlarına sahip değilse, erişmiş olduğu veriler o kişi açısından okunaksız ve dolayısıyla kullanılabilir nitelikte değildir. Veri korunmasına ilişkin diğer etkin yöntemler aynı zamanda, olası riskleri azaltıcı birer fırsat olarak da ele alınmalıdır. Örneğin, riski asgariye indirme yöntemleri arasında mutlak surette gerekli olmadıkça kart hamili verilerinin depolanmaması, PAN'in (Primary Account Number) tamamına ihtiyaç yoksa kart hamili verilerinin kırpmaya tabi tutulması ve koruma altına alınmamış PAN'lerin e-posta ve anlık mesajlaşma gibi son-kullanıcı mesajlaşma teknolojileri kullanılarak gönderilmemesi benimsenebilir. "Güçlü Şifreleme" tanımları ve diğer PCI DSS terminolojisi için lütfen PCI DSS ve PA-DSS Terimler Sözlüğü, Kısaltmalar ve Kısa Ad listelerine başvurunuz.

PCI DSS Zorunlulukları

3.1 Kart Hamili Veri Depolamasını asgari düzeyde tutabilmek adına, tüm kart hamili verilerinin depolanmasına (CHD) ilişkin olarak en azından aşağıda belirtilen unsurları içeren, veri saklama ve veri imha politikalarını, prosedürlerini ve süreçlerini uygulamaya koyun.

- * Veri depolama miktarını ve saklama süresini yasal gereklilikler, düzenleyici gereksinimler ve sektör ihtiyaçlarına göre sınırlandırmak.
- * Verilere artık ihtiyaç duyulmadığında güvenli bir şekilde silinmesine ilişkin süreçleri uygulamak
- * Kart hamili verilerine yönelik özel imha zorunluluklarını yerine getirmek
- * Tanımlanmış saklama süresini aşan veriler söz konusu olduğunda depolanmış verileri üçer aylık dönemler zarfında tespit etmek ve güvenli bir silme işlemine tabi tutmak

Test Süreçleri

3.1.a Veri saklama ve imha politika, prosedür ve süreçlerinin en azından aşağıdaki koşulların sağlanıp sağlanmadığını doğrulamak amacıyla incelenmesi

- * Aşağıda belirtilen hususlar da dahil olmak üzere veri saklamaya ilişkin yasal, düzenleyici ve sektörel zorunluluklar
- * Kart hamili verilerinin saklanması yönelik özel birtakım zorunluluklar (örneğin Y sektör gereksinimlerine istinaden kart hamili verilerinin X süre ile tutulması gibi)
- * Artık ihtiyaç duyulmayan verilerin yasal, düzenleyici ve sektörel zorunluluklara istinaden güvenli bir şekilde silinmesi
- * Kart hamili verilerinin eksiksiz depolanmasına ilişkin kapsam
- * Tanımlanmış saklama süresini aşan veriler söz konusu olduğunda depolanmış verilerin üçer aylık dönemler zarfında tespit edilmesi ve güvenli bir şekilde silinmesi

3.1.b Aşağıda belirtilen hususları teyit maksadıyla personelle görüşülmesi

- * Depolanmış kart hamili verilerine ilişkin tüm konuların saklama ve imha süreçlerine dahil edilmesi
- * Depolanmış kart hamili verilerinin tespit edilmesi ve güvenli bir şekilde silinmesine yönelik olarak üçer aylık dönemler itibarı ile otomatik veya manuel olarak yürütülebilecek süreçlerin yerli yerinde olması
- * Üçer aylık dönemlerde yürütülen söz konusu otomatik veya manuel süreçlerin kart hamili verilerinin bulunduğu tüm lokasyonlarda eksiksiz olarak gerçekleştirilmesi

Yönlendirme

Usule uygun bir veri saklama politikası hangi verilerin saklanması gerektiğini ve söz konusu verilerin nerede bulunduğu tespit edebilir böylelikle veriler-ihtiyaç duyulmadığı noktada- güvenli bir şekilde imha edilebilir veya silinebilir.

Kart hamiline ilişkin verilerden yetkilendirme sonrası saklanması gerekenler, yalnızca ana hesap numarası veya okunaksız hale dönüştürülen Ana Hesap Numarası (PAN), son kullanım tarihi, kart hamilinin ismi ve hizmet kodu olabilir.

Kart hamili verilerine artık ihtiyaç duyulmadığı noktada, verilerin düzgün bir şekilde imha edilmesi veya silinmesi için söz konusu verilerin tam olarak nerede bulunduğunu kavramak gereklidir. Bir kurumun uygun imha etme zorunluluklarını tanımlayabilmesi için, ilk olarak hem kendi bünyesine özgü ihtiyaçları hem de yasal ve düzenleyici zorunluluklarla, faaliyet gösterdikleri sektörü ilgilendiren ve/veya saklanmakta olan verileri ilgilendiren yükümlülükleri iyice kavramış olması gerekmektedir.