Privia SECURITY

Güvenli Veri Silme Hizmeti

Profesyonel Forensic Hizmetleri

"DoD Standartlarında Güvenli Veri Silme!"

Küçükbakkalköy Mah. Kocasinan Cad.
Privia Plaza No:42 Ataşehir, İstanbul

+90 (216) 514 72 14

www.priviasecurity.com

“Güvenli Veri Silme Hizmeti, ABD Savunma Bakanlığı'nın DoD 5220.22-M standardı gibi askeri veri silme protokolleri ile uyumlu şekilde gerçekleştirilir. Askeri protokoller, verilerin geri döndürülemez şekilde silinmesini garanti eder.”

Güvenli Veri Silme Hizmeti, verilerin yasal düzenlemelere ve güvenlik standartlarına uygun bir şekilde verinin kalıcı olarak silinmesini sağlar. Organizasyonlar, disk yüzeylerinde saklanan hassas bilgilerin güvenliğini sağlamak için bu hizmete ihtiyaç duyar. Verilerin kalıcı olarak silinmesi, bilgi sızıntısı ve bilginin başkaları tarafından ele geçilmesi risklerini minimize ederek organizasyon içi güvenliği güçlendirir.

Günümüzde, yalnızca verileri disk yüzeyinden silmek yetersizdir çünkü birçok silme işlemi verilerin geri döndürülebilir hale getirir. Güvenli Veri Silme Hizmeti, verilerin geri dönüşümünü imkânsız hale getirmek için çeşitli teknikler kullanır. Kullanılan teknikler arasında yazılımsal veri yok etme, manyetik alan kullanımıyla silme ve fiziksel imha yöntemleri bulunur. Kullanılan yöntemler, hassas verilerin tamamen yok edilmesi için titizlikle seçilir ve uygulanır. Verilerin güvenli bir şekilde silinmesi, yasal uyumluluk açısından da kritik bir rol oynar. Özellikle kişisel veri güvenliği ve gizlilikle ilgili düzenlemelere uymak için verilerin güvenli bir şekilde yok edilmesi gerekmektedir. Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği Genelgesi gibi ulusal ve uluslararası düzenlemelere uyum sağlayarak olası yasal riskleri önlemeye katkı sunar.

Kişisel veya kurumsal bilgilerin güvenli bir şekilde silinmemesi hem maddi hem de manevi zararlara neden olabilir. Gizli bilgilerin geri döndürülerek kötüye kullanılması, organizasyonların itibarını zedeleyebilir ve güven kaybına yol açabilir. Güvenli Veri Silme Hizmeti, hassas bilgilerin güvenliğini sağlama ve veri yönetiminde güvenli bir süreç oluşturmak için sunulan önemli bir hizmettir. Verilerin kalıcı olarak yok edilmesi, bilgi güvenliğinin temel taşlarından biri olarak kurumsal kullanıcıların veri yönetimini güvenli hale getirir.

Hizmete Ait Bileşenler

Yazılımsal Veri Yok Etme

Yazılımsal veri yok etme yöntemi, verilerin yazılımlar aracılığıyla güvenli bir şekilde silinmesini sağlar. Özel olarak geliştirilen yazılımlar, verilerin üzerine birden fazla kez rastgele veri yazarak geri dönüşümünü imkânsız hale getirir. Yazılımsal yok etme, özellikle çok sayıda dosyanın güvenli bir şekilde silinmesi gerektiğinde etkili bir yöntemdir. Bu yöntemle silinen verilerin hiçbir izi kalmaz, böylece veri sızıntısı riski en aza indirilir. Özellikle hard disk ve SSD gibi depolama birimlerinde yaygın olarak tercih edilir.

Fiziksel İmha Yöntemleri

Fiziksel imha, verilerin bulunduğu cihazların kalıcı olarak yok edilmesi anlamına gelir. Bu işlemde hard disk, SSD, CD gibi depolama birimleri parçalanarak verilerin geri döndürülmesi tamamen imkânsız hale getirilir. Parçalama, cihazların fiziksel olarak küçük parçalara ayrılmasıyla gerçekleştirilir. Kullanılan yöntem, özellikle hassas verilerin tamamen güvence altına alınması gereken durumlarda tercih edilir.

Manyetik Alan Yardımıyla Silme

Degaussing yöntemi, verilerin manyetik alan yardımıyla silinmesini sağlar. Bu yöntemde, yüksek güçlü manyetik alanlar verilerin depolandığı disklerdeki manyetik bilgileri siler. Degaussing, özellikle manyetik depolama birimlerinde bulunan verilerin kalıcı olarak silinmesi için tercih edilen etkili bir yöntemdir. Silme işlemi sonrasında, veriler geri döndürülemez hale getirilir.

SSD Veri Silme Protokolleri

SSD'lerde veri silme, özel protokoller kullanılarak gerçekleştirilir çünkü SSD yapısı, geleneksel sabit disklerden farklıdır. SSD'lerde veriler, hücrelerdeki elektrik yükleri üzerinden saklanır ve bu nedenle geleneksel yöntemler yetersiz kalmaktadır. Kullanılan özel protokoller, SSD üzerindeki verilerin kalıcı olarak yok edilmesini ve cihazın güvenli hale getirilmesini sağlar. Özel yazılımlar veya donanımlar kullanılarak SSD'lerde yer alan veriler güvenli bir şekilde yok edilir.

Bulut Veri Silme

Bulut veri silme, bulut ortamında saklanan verilerin güvenli bir şekilde silinmesini sağlar. Bulut sağlayıcıları, kullanıcıların talepleri doğrultusunda verilerin güvenli silinmesini sağlamak için çeşitli protokoller kullanır. Veriler, bulut depolama alanından tamamen silinir ve geri dönüşü mümkün olmayacak şekilde kaldırılır.

Şifreleme Tekniğiyle Silme

Veri şifreleme ile güvenli silme yöntemi, verilerin özel şifreleme algoritmalarıyla şifrelenmesi ve ardından silinmesi işlemidir. Veriler önce güçlü bir şifreleme ile korunur ve ardından güvenli bir şekilde yok edilir. Şifreleme, verilerin çalınsa bile anlaşılamaz hale gelmesini sağlar. Veri şifreleme, özellikle yüksek güvenlik gerektiren hassas bilgiler için önemli bir koruma sağlar.

Sık Sorulan Sorular

Güvenli veri silme işlemi nedir ve nasıl yapılır?

Güvenli veri silme, verilerin geri döndürülemez şekilde yok edilmesi sürecidir. Standart silme işlemlerinden farklı olarak, güvenli veri silme yöntemlerinde veriler üzerine rastgele veriler yazılır veya cihaz manyetik alanlarla silinir ve verilerin kurtarılmasını imkânsız hale getirir. Özellikle hassas bilgiler içeren ortamlarda, özel yazılımlar veya fiziksel imha yöntemleri ile güvenli veri silme gerçekleştirilir. Yazılım tabanlı güvenli silme işlemleri genellikle hard diskler ve SSD'ler gibi dijital depolama birimleri üzerinde uygulanır.

Fiziksel imha ile güvenli veri silme arasındaki fark nedir?

Fiziksel imha, verilerin depolandığı cihazların fiziksel olarak parçalanmasıyla gerçekleştirilir. Güvenli veri silme ise verilerin üzerine birden fazla kez veri yazılarak geri getirilemez hale getirilmesi sürecidir. Fiziksel imha cihazların yeniden kullanılamaz hale gelmesini sağlarken, yazılım tabanlı güvenli silme yöntemi ise cihazlar kullanılabilir durumda kalır. Özellikle çok hassas veriler barındıran cihazlar için fiziksel imha daha çok tercih edilir. Manyetik alan kullanımı (degaussing) veya parçalama işlemleri ile fiziksel imha gerçekleştirilir. Her iki yöntem de farklı ihtiyaçlara hitap eder.

Hangi cihazlar güvenli veri silme işlemine tabi tutulabilir?

Sabit diskler (HDD), katı hal sürücüler (SSD), USB bellekler ve mobil cihazlar güvenli veri silme işlemine tabi tutulabilir. Bulut sistemlerde saklanan veriler de güvenli silme işlemiyle tamamen silinebilir. Gerçekleştirilen işlemler sırasında kullanılan yöntemler, cihazın türüne göre değişiklik gösterir. Örneğin, SSD'lerde kullanılan veri silme protokolleri, mekanik disklerde uygulanan protokollerden farklıdır. Her cihaz, kendine özgü teknikler kullanılarak kurtarılamaz hale getirilir.

Güvenli veri silme yasal gereklilikler ile nasıl ilişkilidir?

Güvenli veri silme, KVKK, GİB, GDPR, NATO gibi ulusal ve uluslararası düzenlemelere uyumluluğu sağlamak için kritik bir gerekliliktir. Yasal düzenlemeler, hassas ve kişisel bilgilerin güvenli bir şekilde imha edilmesini zorunlu kılar. Verilerin güvenli silme yöntemleriyle yok edilememesi durumunda, organizasyonlar ciddi yasal yaptırımlarla karşılaşabilir. Güvenli veri silme işlemi, bu gereklilikleri yerine getirerek yasal uyumluluğu sağlar.

Veri silme yazılımlarının güvenliği nasıl sağlanır?

Veri silme yazılımları, özel olarak geliştirilmiş algoritmalarla çalışarak verilerin geri döndürülemez şekilde silinmesini sağlar. Veri silme yazılımları, ABD Savunma Bakanlığı (DoD 5220.22-M) gibi belirli güvenlik standartlarına göre geliştirilmiştir. Yazılımların doğru kullanılması için kullanıcıların eğitim alması ve bu yazılımların güvenliğine dair periyodik denetimlerin yapılması önerilir. Güvenli veri silme

yazılımları, kullanıcıların verileri kalıcı olarak yok etmesine olanak tanır ve güvenli bir veri imha süreci sağlar.

Güvenli veri silme işlemi ne kadar sürer?

Güvenli veri silme süresi, silinecek verinin büyüklüğüne ve kullanılan silme yöntemine bağlıdır. Birkaç MB boyutunda küçük dosyalar hızlıca silinebilirken, tüm bir diskin güvenli bir şekilde temizlenmesi saatler sürebilir. Fiziksel imha yöntemleri genellikle daha kısa sürerken, yazılım tabanlı tekrar yazma döngüleri daha uzun zaman (disk yapısına ve büyüklüğüne bağlı) alabilir. Kullanılan yönteme göre, süreç birkaç saatten birkaç haftaya kadar değişebilir. Veri güvenliğini sağlamak için işlem sonrası doğrulama yapılması gerektiğinden süreç uzayabilmektedir.

Yedekleme yapılmadan veri silme neden önerilmez?

Veri silme işlemi, verilerin geri döndürülemez şekilde yok edilmesine neden olduğu için önemli dosyaların yedeklenmesi gerekir. Özellikle iş süreçlerinde gerekli olan dosyalar yok edilmeden önce harici bir cihaza veya sisteme yedeklenmelidir. Yedekleme yapılmadığında, önemli verilerin kaybı büyük zararlara yol açabilir. Güvenli silme işlemi geri dönüşü olmayan bir işlem olduğundan, yedekleme ihtiyacı her zaman değerlendirilmelidir.

Fiziksel olarak imha edilen veriler geri getirilebilir mi?

Fiziksel olarak imha edilen veriler, cihazların parçalanması veya manyetik alan kullanılarak silinmesi nedeniyle geri getirilemez hale gelir. Fiziksel imha işlemi, cihazların tam anlamıyla kullanılamaz hale gelmesini sağlar, böylece verilerin geri döndürülmesi mümkün olmaz. Özellikle kritik bilgi içeren depolama birimleri için fiziksel imha önerilir. Degaussing gibi yöntemler, cihazlardaki verileri tamamen silerek güvenlik sağlar. Fiziksel imha sonrasında, cihazlar bir daha kullanılmayacak şekilde yok edilir.

Fabrika ayarlarına döndürmek veri silme işlemi yerine geçer mi?

Fabrika ayarlarına döndürmek, cihazdaki verilerin çoğunu silse de veri kurtarma yazılımları ile bazı silinen veriler geri getirilebilmektedir. Fabrika ayarları yalnızca yüzeydeki verileri temizler, ancak gizli veya önemli dosyaların bazı izleri cihazda kalabilir. Güvenli veri silme işlemleri ise, verilerin geri getirilemeyecek şekilde yok edilmesini sağlar. Veri güvenliğini sağlamak için, fabrika ayarları yerine güvenli veri silme yöntemleri kullanılmalıdır. Bu yöntemler, cihazı tamamen temizler ve veri sızıntısı riskini azaltır.

Veri silme sonrası geri döndürme mümkün müdür?

Güvenli veri silme işlemlerinde, verilerin üzerine birden fazla kez veri yazılması, manyetik silme veya fiziksel imha gibi yöntemler kullanıldığı için geri döndürme mümkün değildir. Standart silme işlemleriyle silinen veriler özel yazılımlarla kurtarılabilirken, güvenli veri silme işlemi bu riski ortadan kaldırır. Veriler, kalıcı olarak silindiğinde, herhangi bir kurtarma yazılımı veya yöntem ile geri getirilemez.

Siber Güvenlikte Doğru Çözüm Ortağınız

2018 yılında siber güvenliğin geleceği için yola çıkan Privia Security, kuruluşundan bu yana, müşterilerine yüksek kaliteli hizmet sunmayı amaçlamaktadır. Güçlü ve yetenekli ekibimiz, siber güvenliğin her alanında hizmet verdiğimiz organizasyonlara en güvenilir ve kapsamlı çözümleri sunarak, organizasyonların dijital dünyadaki güvenlik ihtiyaçlarını karşılamaktadır.

Günümüzde hızla gelişen ve karmaşık hale gelen siber tehditlerle mücadele etmek giderek zorlaşıyor. Bu noktada Privia Security olarak, müşterilerimize ihtiyaç duydukları hem defansif hem de ofansif siber güvenlik stratejilerini en ileri teknolojiyle sunuyoruz. İnovatif AR-GE ürünlerimiz ve stratejik danışmanlığımız sayesinde organizasyonların siber güvenlik olgunluğunu artırmayı ve onlara proaktif çözümler sunmayı hedefliyoruz. Şu anda 300'den fazla büyük kuruluşun güvenliğini sağlamaktan gurur duyuyoruz.

Uluslararası ve Yerel Siber Güvenlik Çözümleri

Privia Security olarak, Avrupa, Asya, Ortadoğu ve Amerika dahil olmak üzere geniş bir coğrafyaya siber güvenlik hizmetleri sunmaktayız. Offensive, Defensive ve Forensic alanlarında uzmanlaşmış ekiplerimiz, kritik altyapılar, aviyonik sistemler, kurumsal ağlar ve askeri alanlar gibi farklı sektörlerde faaliyet gösteren organizasyonlara özel çözümler geliştirmektedir.

Ayrıca savunma kapasitelerini güçlendirmek isteyen ülkelere yönelik geliştirdiğimiz PriviaHub siber savaş simülasyonu ile siber savaş stratejilerinin test edilmesi, tatbikatların yürütülmesi ve uzmanların niteliklerinin ölçülmesi için kapsamlı çözümler sunuyoruz. Bu inovatif platform özel sektör, akademi ve askeri alanlarda tatbikat ihtiyaçlarını karşılamak üzere tasarlanmıştır.

İleri Teknoloji ile Güvenli Gelecek

İstanbul, Ankara, Londra ve Cumhuriyet Teknopark'taki Ar-Ge merkezimizde, müşterilerimize değer katan projeler geliştiriyoruz. Penetrasyon testleri, Red Team operasyonları, siber güvenlik eğitimleri ve kurumlara özel siber güvenlik çözümlerimizle sektörde fark yaratmaya devam ediyoruz. "Privacy For You" sloganımızla, güvenlik ve gizliliğe yenilikçi bir bakış açısı getiriyor ve müşterilerimizin dijital geleceğini güvence altına alıyoruz.

Privia
SECURITY