

Yedeklerinizi Korumak Artık Bir Seçenek Değil, Zorunluluk!

İşNet Güvenli Bulut Yedekleme hizmetimiz kötü amaçlı girişimlerde yedeklerin silinemediği, değiştirilemediği ve şifrelenemediği yeni nesil veri koruma yaklaşımıdır. Yedekler belirli bir dönem boyunca yalnızca okunabilir (read-only) şekilde saklanır. Bu sayede kurumunuzun veri bütünlüğü ve iş sürekliliği garanti altına alınır.

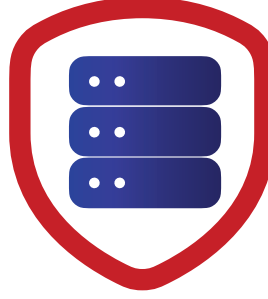


Değiştirilemez - Güvenli Yedekleme (Immutable Backup)

İnsan Hatası



Silinme



Fidye Yazılımı



Yazılımsal Hatalar

Neden İşNet Güvenli Bulut Hizmetimizi Tercih Etmelisiniz?

Fidye Yazılım Saldırılarına Karşı Tam Koruma

Saldırganların hedef aldığı ilk yer genellikle yedeklerdir. İşNet Güvenli Bulut Yedekleme hizmetimiz ile verileriniz, belirlenen süre boyunca değiştirilemez ve silinemez. Saldırı anında bile yedekleriniz güvenli korunur.

Hızlı Kurtarma

Olası bir felaket anında, kritik verilerinizi saniyeler içerisinde geri yükleyerek operasyonlarınızı hızlı bir şekilde devam ettirir.

Regülasyon Uyumu

Regülasyonlar kapsamında talep edilen yedek bütünlüğü, yetkisiz erişimin engellenmesi gibi gereksinimleri karşılar. Böylece hem denetim süreçleriniz kolaylaşır, hem de uyumluluk riskleri ortadan kalkar.

Daha Az Risk, Daha Az Maliyet

Fidye yazılım saldırıları sonrasında kurumların maddi kayıpları yüksek olabilir, bununla beraber yaşanan durum itibar kaybına da sebep olabilir. İşNet Güvenli Bulut Yedekleme hizmetimiz bu kayıpları önler.

İşNet Güvencesi

Kurulum, izleme, test gibi süreçleriniz uzman ekiplerimiz tarafından 7/24 yönetilir.

Bu Hizmet Kimler için Uygundur?

Veri kaybı; itibar kaybı, finansal zararlar ve regülatif cezalar anlamına gelir.

İşNet Güvenli Bulut Yedekleme hizmetimiz;

- Verilerini garanti altına almak isteyen tüm kurumlar,
- Fidyeye yazılım riskini minimize etmek isteyen kurumlar,
- Regülasyona tabi kurumlar,
- Yedeklerini yönetilen hizmetler kapsamında Tier-IV sertifikalı veri merkezimizde güvenli şekilde barındırmak isteyen kurumlar için uygundur.

Neden İşNet'i Tercih Etmelisiniz?



Tier-IV sertifikalı veri merkezi üzerinde modern bulut ve yedekleme altyapısı



Sertifikalı ve deneyimli uzman ekip



7/24 izleme ve müdahale



Müşteri odaklı yaklaşım

%23

2024 yılında incelenen tüm ihlallerin %23'ü fidye yazılımı içeriyor.

%30

Küresel fidye yazılımı zararları için öngörülen yıllık büyüme oranı %30.

%25

2024'ün 4. çeyreğinde fidye yazılımı mağdurlarının %25'i fidye ödedi.

\$3,5 Milyon

2024'te ortalama fidye talebi 3,5 milyon dolardı.

Kaynak: Mandiant, Fortinet, Halycon

%32

2025'teki fidye yazılımı olaylarının %32'si istismar edilen güvenlik açıklarıyla başladı; bu da bunu en yaygın teknik neden yapıyor.

%23

2025'teki fidye yazılımı saldırılarının %23'ü ele geçirilmiş kimlik bilgileriyle başladı; 2024'te bu oran %29'du.

%19

2025'te fidye yazılımından etkilenen kurumların %19'u, kötü amaçlı e-postanın giriş noktası olduğunu söyledi.

%40,1

2025'te fidye yazılımı mağdurlarının %40,1'i, saldırıda ana etkenin bilinmeyen güvenlik açıkları olduğunu bildirdi.

%39,4

2025'te fidye yazılımı mağdurlarının %39,4'ü, saldırıya uğramalarının nedeni olarak yetersiz personel veya kapasiteyi gösterdi.

Kaynak: Sophos State of Ransomware 2025

\$5,2B+

2025 yılında küresel veri ihlali maliyetleri %9 düşerek 5,2 milyar dolar oldu.

\$1M

Uygulanan güvenlik ve yedekleme politikaları ile 2025 yılında ortalama fidye ödeme tutarı %50 düşerek 1 milyon dolar oldu.

%29

2025'teki fidye yazılımı saldırılarının %23'ü ele geçirilmiş kimlik bilgileriyle başladı; 2024'te bu oran %29'du.

%18

2025'te fidye ödeyen kurumların %18'i, ilk talep edilenden daha fazla ödeme yaptı.

Kaynak: Fortinet, Sophos

%50

2025'teki fidye yazılımı saldırılarının %50'si veri şifrelemesiyle sonuçlandı.

%97

2025'te verileri şifrelenen kurumların %97'si bu verileri geri almayı başardı.

%16

2025'teki kurumların %16'sı fidye yazılımından bir gün içinde kurtuldu; 2024'te bu oran %7'ydi.

%53

2025'teki kurumların %53'ü bir hafta içinde kurtuldu; 2024'te bu oran %35'ti.

Kaynak: Sophos State of Ransomware 2025