
Disaster Recovery és
Business Continuity,
mint szolgáltatás
RelNet technológia
Acronis
Orosz Nándor
Projekt- és
szolgáltatásigazgató

01

Miért van szükség DR szolgáltatásra?

Acronis
Évközi kiberfenyegetési jelentés 2023

Top 5 kiberbiztonsági trend 2023 első felében

01 Az e-mail támadások száma megdöbbentő mértékben, **464%**-kal növekedett

02 Ellátási láncot ért támadások - Több, mint **60 000 ügyfél** érintett

03 A **ChatGPT felemelkedése** - A mesterséges intelligencia használata kibertámadások indítására és rosszindulatú tartalom létrehozására

04 Az **adattolvajok** jelentik a második legelterjedtebb fenyegetést

05 A zsarolóvírusok továbbra is elsősorban a **nagy- és középvállalkozásokra** jelentenek fenyegetést; márciusban jelentősen nőtt a számuk

A márciusban bejelentett 459 sikeres támadás közel fele az Egyesült Államokban történt, 221 károsulttal (48%)

RelNet technológia
Acronis


02
2023-ban napi 270 000 új kártékony kód
Átlagos élettartamuk 1,7 nap
RelNet technológia
Acronis

03

Kinek van szüksége DR szolgáltatásra?

Cégeknek, akik:

- A kritikus fontosságú alkalmazásokra és adatokra támaszkodnak
- Szabályozott megfelelési követelmények hatálya alá tartoznak
- Nagymértékben támaszkodnak az üzleti funkciókat illetően az IT-ra
- Nem rendelkeznek technikai erőforrásokkal (limitált beruházási keret)
- Nincs katasztrófa utáni helyreállítási tapasztalatuk/tervük
- Katasztrófa által veszélyeztetett területeken találhatók
- Audit kötelezettségük van
- Szigorú ellátási láncok partnerei

Kulcs iparágak:


Gyártás


Pénzügy


Szállítmányozás


Törvénykezés


Üzleti folyamatok


Egészségügy


Építőipar

RelNet technológia

Acronis

04

DR és adatmegőrzési képességet előíró hazai jogszabályok (forrás: TrustaaS)

2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.
2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.
41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről.
Az Európai Parlament és a Tanács (EU) 2022/2555 Irányelve az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről (NIS 2 irányelv).
Az Európai Parlament és a Tanács (EU) (EU) 2022/2557 Irányelve a kritikus szervezetek rezilienciájáról.

Ezek mellett érintett lehet mindenki, aki például bizalmi szolgáltatóként tevékenykedik:

2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól.
Az Európai Parlament és a Tanács (EU) 2022/2554 Rendelete a pénzügyi ágazat digitális működési rezilienciájáról (DORA).
Az Európai Parlament és a Tanács (EU) 910/2014/EU Rendelete a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról (eIDAS).

TrustaaS
IT RISK MANAGEMENT

05

Tisztuló kép - NIS2

1. Risk analysis & information system security
2. Incident handling
3. Business continuity measures (back-ups, disaster recovery, crisis management)
4. Supply Chain Security
5. Security in system acquisition, developement and maintenance, including vulnerability handling and disclosure
6. Policies and procedures to access the effectiveness of cybersecurity risk management measures
7. Basic computer hygiene and trainings
8. Policies on appropriate use of cryptography and encryption
9. Human resources security, access control policies and asset management
10. Use of multi-factor, secured voice/ video/ text comn & secured emergency communication

RelNet technológia Acronis

06

Megfelelőség és helyi jelenlét biztosítása

Világszerte több mint 50 adatközpont közül választhat az adatok tárolásához - Acronis Hosted, Google Cloud, AWS és Microsoft Azure.

Acronis Data Centers

Google Data Centers

Azure Data Centers

RelNet technológia

Acronis

06

Megfelelőség és helyi jelenlét biztosítása

Világszerte több mint 50 adatközpont közül választhat az adatok tárolásához - Acronis Hosted, Google Cloud, AWS és Microsoft Azure.

RelNet technológia

Acronis

07

Milyen egy jó DR szolgáltatás egy hazai vállalat számára?

Budapesti adatközpontba telepített, bárki által elérhető technológia

Az **adatközponti beruházás már megtörtént – a felhasználó csak kapacitást vesz igénybe** az általa preferált Acronis viszonteladón keresztül

Pay-as-you-go alapon, **havidíjként fizeti a szolgáltatást**

Hagyományosan előre le kell kapacitásra szerződni – itt nem

„Adat-trezor"-szerű megoldás, **fizikai és logikai védelemmel ellátva**

Külső kontroll lehetősége biztosított – ellenőrizhetőek az adatok, elkülönített kezelés, auditálható mentés, **auditálható** DR képesség

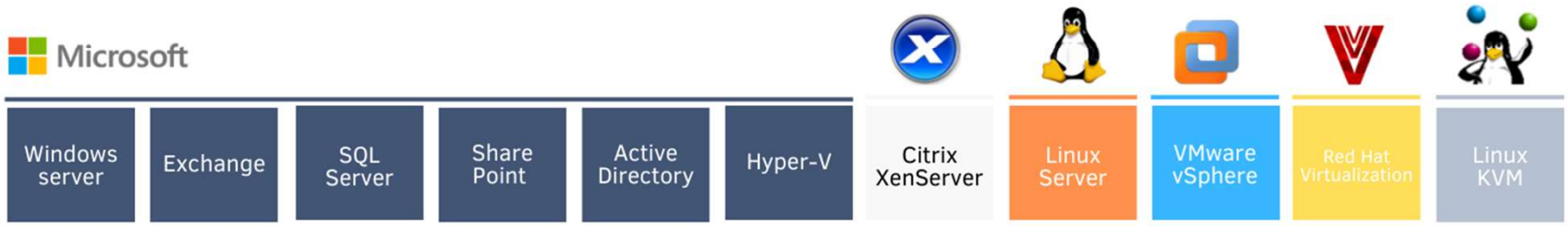
Compliance megfelelőségeket nagyban elősegíti (mentés logok, ellenőrzési felületek, admin ellenőrzés / PAM)

RelNet technológia Acronis

08

Legyen Disaster Recovery szolgáltatás a következő rendszerekhez

Fizikai és virtuális gépek	Windows	Linux
Virtualizációs platformok	VMware vSphere Microsoft Hyper-V Linux KVM	Red Hat Virtualization Citrix XenServer
Felhős szerverek a valós idejű alkalmazás replikációhoz	For applications with built-in replication like SQL Server AlwaysOn	



RelNet technológia

Acronis

09

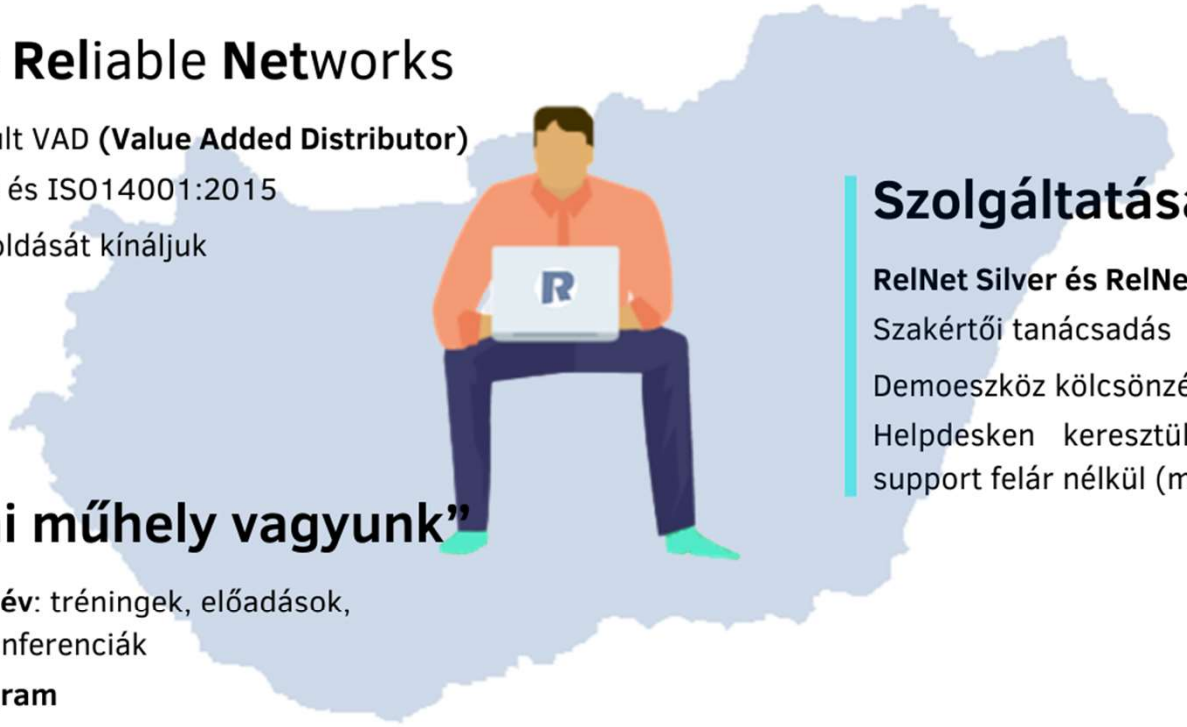
Bemutatkozás

RelNet = Reliable Networks

2004-ben alakult VAD **(Value Added Distributor)**

ISO 9001:2015 és ISO14001:2015

22 gyártó megoldását kínáljuk



„Szakmai műhely vagyunk”

~50 esemény /év: tréningek, előadások, workshopok, konferenciák

eLearning program

Szolgáltatásaink

RelNet Silver és RelNet Gold támogatások

Szakértői tanácsadás

Demoeszköz kölcsönzés + POC

Helpdesken keresztül **7/24 magyar nyelvű** support felár nélkül (már 1 licensz vásárlásától)

Akit mélyebben érdekel – RelNet eLearning

Acronis – Ötvektoros kibervédelem az Acronis backup technológiájával

Bővebben

Acronis – Az Acronis Cyber Infrastructure backup szolgáltatásának telepítése és konfigurálása

Bővebben

Acronis Cyber Protect Cloud – Integrált kiberbiztonság IT-szolgáltatók számára

Bővebben

Acronis – MI védelemmel a támadások ellen – új kihívások az MSP-k előtt

Bővebben

Acronis – A ransomware támadás anatómiája

Bővebben

Acronis – A Cyber Protect Cloud funkciói és licencelése

Bővebben

Acronis Cyber Protect Cloud – Van élet a backupon túl

Bővebben

RelNet technológia

Acronis

11

Kint a vízből...


Köszönjük a figyelmet!
Az Acronis megoldásaival kapcsolatban keressék a RelNet vezető termékmenedzserét, Veréb Stellát: svereb@relnet.hu
Compliance audit felkészítés igénye esetén keressék a TrustaaS szakértőit, Magyar Márton: marton.magyar@trustaas.hu
RelNet technológia