Synology®

Skydda din organisation mot ransomware

Ransomware-attacker beräknas kosta organisationer sammanlagt åtta biljoner USD bara under 2023.[1] Dataskyddsplaner med alternativ för snabb återställning är avgörande för att mildra effekterna av ransomware och andra former av cyberbrottslighet.

Date 13 okt 2023

Säkerhetskopior: den sista försvarslinjen när katastrofen inträffar

När data förloras efter skadlig borttagning eller modifiering kan du återställa uppdragskritiska data och undvika kostsamma driftstopp. Utnyttja Synologys dataskyddslösningar för att utforma en strategi för säkerhetskopiering för hela din IT-infrastruktur.

Fullständigt skydd

Skydda slutpunkter och primära säkerhetskopior för att skapa flera säkerhetsnät för dina data.

Snabb återställning

Minska stilleståndstiden till ett minimum när katastrofen inträffar, med alternativ för omedelbar återställning.

Oföränderlig lagring

Förhindra obehöriga ändringar av data och ögonblicksbilder.

Licensfria säkerhetskopieringar

Säkerhetskopiera så mycket data som din lagring tillåter, utan begränsningar eller dolda avgifter.

Centraliserat försvar mot ransomware

Konsolidera säkerhetskopieringar från flera arbetsstationer, servrar, virtuella datorer och molnapplikationer. Optimera lagringsförbrukningen och undvik flaskhalsar rörande bandbredd med datadeduplicering och stegvis säkerhetskopiering. https://www.synology.com/dsm/solution/infrastructure

Fysiska arbetsbelastningar

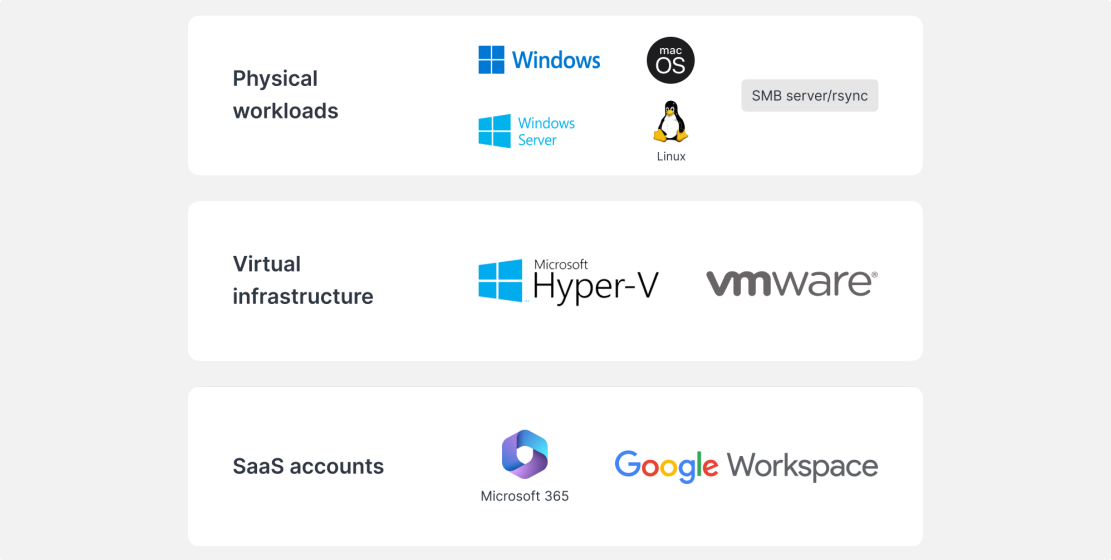
Skydda slutpunkter i händelse av skadliga attacker med omfattande bare-metal-säkerhetskopiering och flexibel filåterställning.

Virtuell infrastruktur

Säkerhetskopiera virtuella VMware® vSphere™-, Microsoft® Hyper-V®-datorer och LUN-enheter med kraftfull teknik för datareduktion.

SaaS-konton

Aktivera kontinuerligt skydd för data som lagras i molnet, med automatisk detektering av nyligen tillagda konton.



Effektiv återställning

Minimera driftstopp för kritiska produktionssystem genom att snabbt återställa säkerhetskopior från ett lokalt eller off-site Synology-system.

Nära noll återställningstid

Montera säkerhetskopierade bilder på VMware®, Hyper-V® eller Synology Virtual Machine Manager för att återuppta arbetet så snabbt som möjligt. Återställ virtuella datorer till en alternativ hypervisor för att undvika tjänsteavbrott.

Minimal RPO

Konfigurera säkerhetskopieringsfrekvensen enligt dina behov, vilket minimerar mängden data som kan påverkas under en attack. Skydda systemen snabbt tack vare stegvis säkerhetskopiering och teknik för deduplicering.

Intuitiv användning

Låt anställda bläddra och förhandsgranska e-post, kontakter och filer från en smidig portal innan de återställs, vilket ger en mer användarvänlig upplevelse och minskar belastningen på IT-teamen.

Ett extra lager skydd

Följ 3-2-1-strategin för säkerhetskopiering genom att lagra en tredje uppsättning data på en annan plats eller i molnet, vilket skyddar dina data mot brand, naturkatastrofer eller stöld.

Till servrar utanför anläggningen

Lagra säkerhetskopior på en Synology-server på en sekundär plats för att försvara dig mot fysisk katastrof och replikera oföränderliga ögonblicksbilder för extra skydd mot ransomware.

Till molnet

Säkerhetskopiera till alla större molnlagringsleverantörer och skydda dina data från obehörig åtkomst genom AES-256-kryptering på klientsidan. https://c2.synology.com/storage/nas

Betrodda inom olika branscher

"Synology [...] gjorde det möjligt för oss att minska kostnaderna för servermaskinvara [...] samtidigt som vår infrastruktur och säkerhetskopiering av arbetsstationer, systemloggning och filhantering blev mycket enklare."
https://www.synology.com/company/case_study/Investortools

"Tack vare Active Backup for Business är alla våra säkerhetskopior nu centraliserade och tillgängliga dygnet runt, vilket hjälper oss att minimera driftstopp och att efterleva FERPA:s bestämmelser."
https://www.synology.com/company/case_study/University_of_Washington

"[...] Active Backup for Business har förbluffande säkerhetskopieringshastigheter och gör underverk när det handlar om att radera duplicerade data – bara 28 TB av de totala 58 TB på servern togs upp. [...]"
https://www.synology.com/company/case_study/SHISEIDO_Taiwan_ABB

"[...] Active Backup for Business [...] kan vi centralisera och hantera alla säkerhetskopieringsuppgifter från en enda konsol. Snabb och tillförlitlig återställning säkerställer också kontinuitet i verksamheten."
https://www.synology.com/company/case_study/UNESCO

Vanliga frågor

Vad är ransomware?

Ransomware är en typ av malware som krypterar offrens filer. Angriparna kräver sedan en lösensumma för att återställa dataåtkomst, och hotar ofta att permanent förstöra data om ingen lösensumma betalas. Ransomware-attacker kan vara mycket störande och kan orsaka betydande ekonomiska förluster för individer och organisationer. Det är viktigt att skydda dig själv och dina enheter mot ransomware, till exempel genom att hålla din programvara uppdaterad och säkerhetskopiera dina filer regelbundet.

Vilka typer av ransomware finns det?

Det finns många olika typer av ransomware, och nya typer utvecklas ständigt. Några av de vanligaste typerna av ransomware är:

- **Krypterande ransomware**. Den vanligaste typen av ransomware krypterar offrets filer så att de inte kan nås utan dekrypteringsnyckeln. Angriparna kräver sedan en lösensumma i utbyte mot nyckeln
- **Locker-ransomware**. En typ av ransomware som låser ut offer från sin dator genom att ändra inloggningsuppgifterna eller visa ett meddelande som hindrar offret från att komma åt sitt system. Angriparna kräver sedan en lösensumma för att låsa upp datorn
- **Ransomware-as-a-Service (RaaS)**. En affärsmodell där angriparna erbjuder ransomware till andra individer eller grupper som vill utföra attacker. Den förstnämnda tillhandahåller ransomware och hanterar betalningarna, medan den senare får en procentandel av lösensumman
- **Scareware**. Ransomware som är utformad för att skrämma offren till att betala lösensumman. Det innebär vanligtvis att visa falska säkerhetsvarningar eller meddelanden som hävdar att offrets dator är infekterad med ett virus. Angriparen kräver sedan en lösensumma för att ta bort den förmodade infektionen

Hur sprids ransomware?

Ransomware sprids vanligtvis via nätfiske i e-post eller genom att utnyttja sårbarheter i ett datorsystem. Vid ett nätfiskeangrepp skickar en angripare ett e-postmeddelande som verkar vara från en legitim källa, t.ex. en bank eller ett välkänt företag. E-postmeddelandet innehåller ofta en länk eller en bilaga som installerar ransomware på offrets dator om man klickar på den. Att utnyttja sårbarheter i ett system liknar nätfiske, förutom att angriparen utnyttjar en svaghet i systemets säkerhet för att installera ransomware utan offrets vetskap. När ransomware är installerat kan det i båda fallen snabbt sprida sig till andra datorer på samma nätverk.

Hur ser det typiska förloppet för en ransomware-attack ut?

En ransomware-attack går vanligtvis till så här:

1. Angriparen får tillgång till en offrets dator, antingen genom att skicka ett nätfiskemeddelande via e-post eller genom att utnyttja en svaghet i systemet.
2. När angriparen har tillgång till offrets dator installerar de ransomware på systemet.
3. Ransomware krypterar sedan offrets filer, vilket gör att användaren inte får åtkomst.
4. Angriparen kräver en lösensumma från offret, vanligtvis i form av en digital valuta som Bitcoin, i utbyte mot dekrypteringsnyckeln som låser upp de krypterade filerna.
5. Om offret betalar lösen skickar angriparen dekrypteringsnyckeln och offret får åtkomst till sina filer igen. Det finns dock ingen garanti för att angriparen faktiskt skickar nyckeln, och även om de gör det kan offrets filer vara skadade eller korrupta till följd av krypteringsprocessen.

Det är viktigt att notera att det finns många variationer på denna process, och alla ransomware-attacker följer inte ovanstående förlopp exakt. Vissa attacker kanske inte krypterar filerna alls, till exempel, medan andra kan innebära andra former av utpressning.

Hur kan jag få ransomware?

Man kan få ransomware på olika sätt. Ett av de vanligaste sätten är att klicka på en skadlig länk eller bilaga i ett nätfiskemeddelande. Denna typ av e-post är utformad för att se legitima ut och verkar ofta vara från ett välkänt företag eller organisation. När du klickar på länken eller bilagan installeras ransomware på datorn. Man kan också få ransomware genom att besöka en komprometterad webbplats. Dessa webbplatser har hackats av angripare som har infört kod som automatiskt installerar ransomware på datorn om du besöker webbplatsen. Du kan också få ransomware genom att ladda ner infekterade filer från internet. Det kan hända om du hämtar en fil från en misstänkt webbplats eller om du hämtar en fil som har delats av någon du inte känner till. Kort sagt är det viktigt att vara försiktig när du surfar på Internet och att undvika att klicka på länkar eller ladda ner filer från okända källor. Detta kan hjälpa dig att skydda dig från ransomware och andra typer av malware.

Vilka utgör mål för ransomware?

Ransomware-attacker kan rikta sig till alla som använder en dator eller en annan enhet som är ansluten till internet. Vissa grupper är dock mer benägna att drabbas än andra. Ransomware-attacker riktar sig till exempel ofta mot företag, eftersom de ofta har mer värdefulla data och kan vara mer villiga att betala en lösensumma för att återfå den. Sjukhus, skolor och andra organisationer som tillhandahåller kritiska tjänster är också vanliga mål, eftersom en ransomware-attack kan störa deras verksamhet och sätta människors liv i fara. Individer kan också utgöra mål för ransomware-attacker. I dessa fall kan angriparna försöka utpressa pengar från offret genom att hota med att radera deras personliga filer eller publicera känslig information om inte lösensumman betalas. Målen för ransomware-attacker väljs ofta ut baserat på värdet av deras data och deras vilja att betala en lösensumma för att återfå den.

Vilka är riskerna med att betala ransomware?

Att betala en lösensumma till en ransomware-angripare kan verka som det enklaste sättet att få dina filer tillbaka, men det kan faktiskt vara ett mycket riskabelt beslut. Det finns flera risker förknippade med att betala en lösensumma, inklusive:

- Det finns ingen garanti för att angriparen faktiskt tillhandahåller dekrypteringsnyckeln. I många fall får offren som betalar lösensumman aldrig nyckeln och får aldrig tillgång till sina filer.
- Att betala lösensumman uppmuntrar angripare att fortsätta med attackerna. Om angriparna vet att offren är villiga att betala lösensumman kan de vara mer benägna att utföra fler attacker i framtiden.
- Att betala lösensumman kan göra dig till ett mål för framtida attacker. Om angriparen vet att du är villig att betala en lösensumma ökar risken att du blir attackerad i framtiden.
- Det kan vara olagligt att betala lösensumman. I vissa fall kan betalning av en lösensumma till en kriminell organisation betraktas som en form av finansiering av terrorism eller annan olaglig verksamhet

Samtidigt som utbetalning av lösensumman faktiskt kan tyckas vara det enklaste sättet att återfå filerna, kan det faktiskt vara ett mycket riskabelt beslut. Det är viktigt att noga överväga riskerna innan du fattar ett beslut.

Vad är kostnaden för ransomware?

Kostnaden för en ransomware-attack kan variera kraftigt beroende på ett antal faktorer, såsom vilken typ av ransomware som används, hur många filer som har krypterats och attackens effektivitet. I vissa fall kan kostnaden för en ransomware attack vara relativt låg, med angripare som kräver några hundra dollar i lösen. I andra fall kan kostnaden vara mycket högre, med angripare som kräver tusentals dollar eller ännu mer för att återställa tillgången till offrets filer. Förutom de direkta kostnaderna i samband med att betala en lösensumma kan ransomware-attacker också medföra betydande indirekta kostnader. Till exempel kan en ransomware-attack orsaka driftstopp och förlust av produktivitet, vilket kan resultera i förlorade intäkter och inkomster. Det kan också skada ett företags rykte och kundförtroende, vilket kan ha långsiktiga negativa effekter på verksamheten. Dessa indirekta kostnader är ofta mycket högre än själva lösensumman.

Vilka är symtomen på ransomware?

Symptomen på en ransomware-attack kan variera beroende på den specifika typen av ransomware som används. Några vanliga symptom är dock:

- Dina filer är krypterade och du kan inte komma åt dem.
- Du får ett meddelande från angriparen som kräver en lösensumma i utbyte mot dekrypteringsnyckeln.
- Du märker att obekanta program eller processer körs på din dator.
- Din dator blir långsam eller svarar inte.
- Datorn visar ovanliga felmeddelanden eller popup-fönster.

Om du misstänker att din dator har smittats med ransomware är det viktigt att agera snabbt. Koppla bort din dator från internet för att förhindra ransomware från att sprida sig.

Hur förhindrar man ransomware-attacker?

Det finns flera åtgärder som du kan vidta för att förhindra ransomware-attacker:

- Använd välrenommerade antivirus- eller säkerhetsprogram och håll det uppdaterat. Detta kan hjälpa till att skydda din dator från ransomware och andra typer av skadlig kod.
- Var försiktig när du öppnar e-postbilagor eller länkar. Ransomware levereras ofta via nätfiske i e-post, så det är viktigt att vara försiktig med vad du klickar på.
- Håll operativsystem och annan programvara uppdaterad. Programuppdateringar innehåller ofta säkerhetskorrigeringar som kan hjälpa till att skydda din dator från ransomware och andra hot.
- Säkerhetskopiera dina filer regelbundet. Detta kan hjälpa till att skydda dina data om din dator är infekterad med ransomware. Följ en av de rekommenderade strategierna för säkerhetskopiering, som 3-2-1-strategin.
- Var medveten om riskerna med ransomware och utbilda andra i din organisation om dessa hot. Detta kan hjälpa till att förhindra ransomware-attacker och gör det lättare att upptäcka dem och vidta åtgärder om de inträffar.

Det bästa sättet att förhindra ransomware-attacker är att vara vaksam och vidta åtgärder för att skydda din dator och dina data. Detta kan bidra till att minska risken för en ransomware-attack och göra det lättare att återhämta sig från en om det inträffar.

Hur kan Synology skydda mig mot ransomware?

Förebyggande åtgärder är nödvändiga som skydd för att inte falla offer för ransomware. Använd dessa Synology-lösningar utöver ditt val av antivirusprogram:

- **Förhindra åtkomst**. Minska spridningen av ransomware genom att ange fil-, program- och åtkomstbehörigheter och konfigurera säkra inloggningsuppgifter med hjälp av Secure SignIn och C2 Password.
- **Skydda enheter**. Föråldrade system löper större risk att drabbas. Uppdatera alla NAS-enheter samtidigt med Synology Central Management System (CMS) och skydda andra enheter med hjälp av gruppolicyer i Synology Directory Server och C2 Identity.
- **Undvik misstänkta filer**. Spam och nätfiske-e-post som innehåller misstänkta filer är vanliga metoder för att sprida ransomware. Synology MailPlus ger ett starkt skydd mot skadlig programvara och skydd mot skräppost.
- **Kontrollera om det finns sårbarheter**. Använd Synology Security Advisor för att regelbundet söka efter skadlig programvara, sårbarheter och onormala inloggningsaktiviteter. Implementera rekommenderade ändringar för att förbättra säkerheten för din NAS-enhet. https://www.synology.com/dsm/overview/security

Fler sätt att skydda dina data

Hantera dina enheter

Dra nytta av omfattande funktioner för att centralt hantera behörigheter för dataåtkomst, programvarustatus, systemhälsa och mycket mer.
https://www.synology.com/dsm/overview/administration

Övervaka alla dina system

Identifiera misstänkta inloggningsaktiviteter, hantera uppdateringar och övervaka enheternas tillstånd, oavsett var dina enheter finns.
https://www.synology.com/dsm/feature/active-insight

Skydda dina data.

Följ 3-2-1-regeln för säkerhetskopiering för att skydda dina data mot oavsiktliga och skadliga ändringar eller raderingar.
https://www.synology.com/dsm/solution/data_backup

Kom igång

Kontakta oss

Kontakta regionala säljare för mer information
https://www.synology.com/form/inquiry/sales

Var de finns att köpa

Hitta en Synology-partner i din region
https://www.synology.com/wheretobuy

Anteckningar:

1. eSentire, 2022 Official Cybercrime Report
   https://www.esentire.com/resources/library/2022-official-cybercrime-report

Skydda din organisation mot ransomware

https://www.synology.com/sv-se/dsm/solution/ransomware

Synology-webbplats

https://www.synology.com/

Kontakta oss

https://www.synology.com/company/contact_us