Synology®

랜섬웨어로부터 조직 보호

랜섬웨어 공격으로 인해 2023년 한 해에만 조직에 조의 비용이 발생할 것으로 예상됩니다.[1] 빠른 복원 옵션이 포함된 데이터 보호 계획은 랜섬웨어와 다른 형태의 사이버 범죄가 미치는 영향을 완화하기 위해 매우 중요합니다.

Date 2023년 10월 13일

백업: 재해가 발생했을 때 최후의 방어선

악의적인 삭제나 수정 후 데이터가 손실된 경우 백업을 사용하면 업무상 중요한 데이터를 복원하고 값비싼 가동 중지 시간을 방지할 수 있습니다. Synology의 데이터 보호 솔루션을 활용하여 전체 IT 인프라를 위한 백업 전략을 설계할 수 있습니다.

완벽한 보호

끝점과 기본 백업을 보호하여 데이터 안전망을 여러 개 만들 수 있습니다.

빠른 복구

즉각적인 복구 옵션을 사용하면 재해가 발생할 때 가동 중지 시간을 최소화할 수 있습니다.

변조 불가능한 스토리지

데이터 및 스냅샷의 무단 변경 방지

라이센스 무료 백업

제한 사항이나 숨겨진 비용 없이 저장소에서 허용하는 만큼 데이터를 백업할 수 있습니다.

랜섬웨어로부터 중앙 집중식 보호

워크스테이션, 서버, 가상 컴퓨터 및 클라우드 응용 프로그램의 제품군에서 백업을 통합할 수 있습니다. 데이터 중복 제거 및 증분 백업 기술을 사용하여 저장소 소비를 최적화하고 대역폭 병목 현상을 방지할 수 있습니다. https://www.synology.com/dsm/solution/infrastructure

물리적 작업 부하

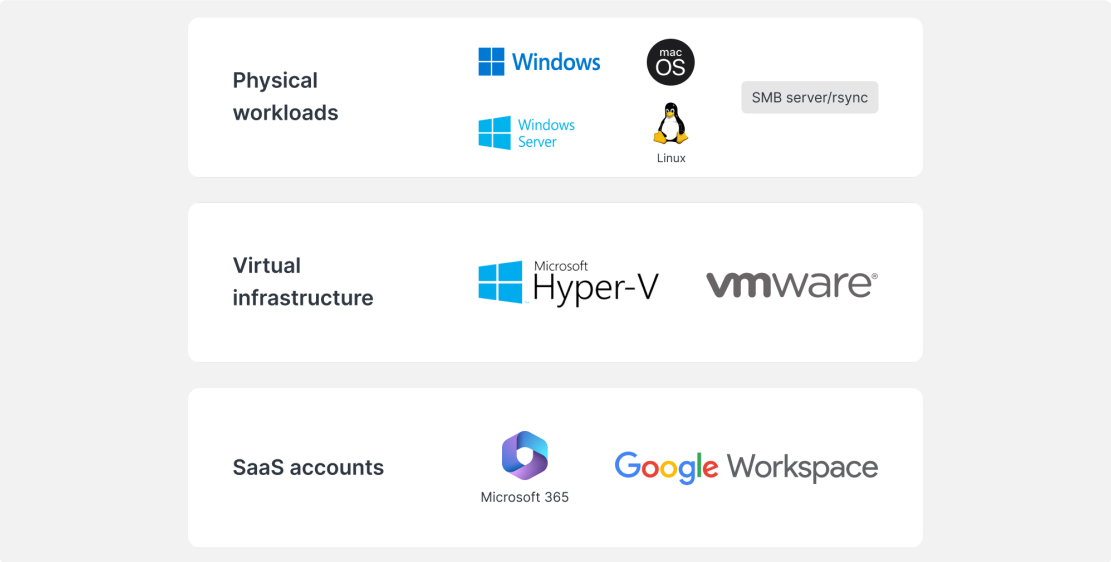
포괄적인 완전 백업과 유연한 파일 수준 복구를 통해 악성 공격이 발생할 때 끝점을 보호할 수 있습니다.

가상 인프라

강력한 데이터 감소 기술을 사용하여 VMware® vSphere™, Microsoft® Hyper-V® VM 및 LUN을 백업할 수 있습니다.

SaaS 계정

새로 추가된 계정을 자동으로 검색하여 클라우드에 저장된 데이터를 연속으로 보호할 수 있습니다.



효율적인 복구

로컬 또는 오프사이트 Synology 시스템에서 백업을 신속하게 복원하여 중요한 프로덕션 시스템의 가동 중지 시간을 최소화할 수 있습니다.

0에 가까운 RTO

백업 이미지를 VMware®, Hyper-V® 또는 Synology Virtual Machine Manager에 탑재하여 가능한 한 빨리 작업을 다시 시작할 수 있습니다. VM을 대체 하이퍼바이저로 복원하여 서비스 중단을 방지할 수 있습니다.

최소 RPO

요구 사항에 따라 백업 빈도를 구성하여 공격 중에 영향을 받을 수 있는 데이터의 양을 최소화할 수 있습니다. 증분 백업과 데이터 중복 제거로 시스템을 빠르게 보호할 수 있습니다.

직관적인 운영

직원들이 이메일, 연락처 및 파일을 복원하기 전에 편리한 포털에서 검색하고 미리 볼 수 있게 할 수 있으므로 보다 사용자 친화적인 환경을 제공하고 IT 팀의 부담을 줄일 수 있습니다.

보호 강화

3번 째 데이터 세트를 오프사이트나 클라우드에 저장하여 화재, 자연 재해 또는 도난으로부터 데이터를 보호함으로써 3-2-1 백업 전략을 준수할 수 있습니다.

오프 사이트 서버로

보조 위치에 있는 Synology 서버에 백업을 저장하여 물리적 재해로부터 보호하고 변경할 수 없는 스냅샷을 복제하여 랜섬웨어 보호를 강화하십시오.

클라우드로

주요 클라우드 저장소 공급자에 백업하여 클라이언트 측 AES-256 암호화를 통해 데이터를 무단 액세스로부터 보호할 수 있습니다. https://c2.synology.com/storage/nas

다양한 업계에서 신뢰

"Synology는 [중략] 우리가 서버 하드웨어 비용을 절감하고 [중략] 동시에 인프라와 워크스테이션 백업, 시스템 로깅 및 파일 관리를 더욱 간편하게 수행할 수 있게 해줬습니다."
https://www.synology.com/company/case_study/Investortools

"Active Backup for Business를 사용하자 모든 백업을 한 곳에서 제어하고 중단 없이 사용할 수 있게 되었습니다. 이로 인해 가동 중지 시간이 최소화되고 FERPA 규정을 준수할 수 있게 되었습니다."
https://www.synology.com/company/case_study/University_of_Washington

"[중략] Active Backup for Business가 백업 속도를 향상시키고 중복 데이터 삭제 면에서 놀라운 성과를 보여줬다는 사실을 확인했습니다. 그 결과 총 서버 용량 58TB 중 28TB만 사용했습니다. [중략]"
https://www.synology.com/company/case_study/SHISEIDO_Taiwan_ABB

"[중략] Active Backup for Business를 사용하면 단일 콘솔 하나에서 모든 백업 작업을 중앙 집중화하여 관리할 수 있습니다. 또한 빠르고 안전적인 복구로 비즈니스 연속성이 보장됩니다."
https://www.synology.com/company/case_study/UNESCO

자주 묻는 질문(FAQ)

랜섬웨어란?

랜섬웨어는 피해자 파일을 암호화하는 맬웨어의 한 가지 유형입니다. 공격자는 데이터 액세스를 복원하려면 금품을 요구하며 금품을 지불하지 않으면 데이터를 영구 파괴하겠다고 위협하는 경우가 많습니다. 랜섬웨어 공격은 큰 지장을 줄 수 있으며 개인과 조직에 상당한 재정적 손실을 초래할 수 있습니다. 소프트웨어를 최신 상태로 유지하고 파일을 정기적으로 백업하는 등 랜섬웨어로부터 자신과 장치를 보호하는 것이 중요합니다.

어떤 유형의 랜섬웨어가 있습니까?

랜섬웨어 종류는 다양하며 새로운 변종이 끊임없이 개발되고 있습니다. 가장 일반적인 유형의 랜섬웨어는 다음과 같습니다.

- **암호화 랜섬웨어** - 가장 일반적인 유형의 랜섬웨어로, 피해자 파일을 암호화하므로 암호화 해제 키가 없으면 파일에 액세스할 수 없습니다. 그러면 공격자는 키의 대가로 금품을 요구합니다.
- **로커(Locker) 랜섬웨어** - 랜섬웨어의 한 가지 유형으로, 로그인 자격 증명을 변경하거나 피해자가 자신의 시스템에 액세스하지 못하도록 하는 메시지를 표시하여 피해자를 컴퓨터에서 차단합니다. 그러면 공격자는 컴퓨터를 잠금 해제하려면 금품을 요구합니다.
- **RaaS(Ransomware-as-a-Service)** - 공격자가 공격을 수행하려는 다른 개인이나 그룹에 랜섬웨어를 제공하는 비즈니스 모델입니다. 전자는 일반적으로 랜섬웨어를 제공하고 금품을 처리하며 후자는 금품의 일정 비율을 가져갑니다.
- **Scareware** - 피해자를 위협하여 금품을 지불하도록 설계된 랜섬웨어입니다. 일반적으로 가짜 보안 경고 또는 피해자의 컴퓨터가 바이러스에 감염되었다고 주장하는 메시지를 표시합니다. 그러면 공격자는 추정된 감염을 제거하려면 금품을 요구합니다.

랜섬웨어는 어떻게 확산됩니까?

랜섬웨어는 일반적으로 피싱 이메일을 통해 또는 컴퓨터 시스템의 취약점을 악용하여 전파됩니다. 피싱 공격에서 공격자는 은행이나 유명한 회사와 같은 합법적인 출처에서 보낸 것처럼 보이는 이메일을 보냅니다. 이메일에는 링크나 첨부 파일이 포함되는 경우가 많으며 이를 클릭하면 피해자의 컴퓨터에 랜섬웨어가 설치됩니다. 시스템에서 취약점을 악용하는 것은 비슷하지만 공격자가 시스템 보안의 결함을 사용하여 피해자 모르게 랜섬웨어를 설치한다는 점이 다릅니다. 두 경우 모두 랜섬웨어가 설치되면 같은 네트워크의 다른 컴퓨터로 빠르게 확산될 수 있습니다.

랜섬웨어 공격의 일반적인 프로세스는 어떻게 됩니까?

일반적으로 랜섬웨어 공격 프로세스는 다음 단계를 수행합니다.

1. 공격자는 피싱 이메일을 보내거나 시스템의 취약점을 악용하여 피해자 컴퓨터에 대한 액세스 권한을 획득합니다.
2. 공격자가 피해자의 컴퓨터에 액세스하면 시스템에 랜섬웨어를 설치합니다.
3. 그러면 랜섬웨어는 피해자 파일을 암호화하여 사용자가 액세스하지 못하게 합니다.
4. 그런 다음 공격자는 피해자에게 암호화된 파일의 잠금을 해제하는 암호화 해제 키에 대한 대가로 금품(일반적으로 비트코인과 같은 디지털 통화)을 요구합니다.
5. 피해자가 금품을 지불하면 공격자는 암호화 해제 키를 제공하고 피해자는 다시 파일에 액세스할 수 있습니다. 그러나 공격자가 실제로 키를 제공한다는 보장이 없으며 제공한다고 해도 암호화 프로세스로 인해 피해자의 파일이 손상될 수 있습니다.

이 프로세스에는 다양한 변형이 있으며 모든 랜섬웨어 공격이 이러한 단계를 정확하게 따르지 않습니다. 예를 들어 일부 공격은 파일을 암호화하지 않을 수 있지만 다른 공격은 강탈이나 협박 등 다른 형태일 수 있습니다.

어떻게 랜섬웨어에 감염되나요?

랜섬웨어에 감염되는 방법은 여러 가지입니다. 가장 일반적인 방법 중 하나는 피싱 이메일의 악성 링크나 첨부 파일을 클릭하는 것입니다. 이 유형의 이메일은 합법적으로 보이도록 설계되었으며 유명한 회사나 조직에서 보낸 것처럼 보입니다. 링크나 첨부 파일을 클릭하면 컴퓨터에 랜섬웨어가 설치됩니다. 랜섬웨어에 감염되는 또 다른 방법은 손상된 웹사이트에 방문하는 것입니다. 이러한 웹사이트는 공격자에 의해 해킹되었으며 공격자는 사이트를 방문하면 컴퓨터에 자동으로 랜섬웨어가 설치되는 코드를 삽입합니다. 인터넷에서 감염된 파일을 다운로드해도 랜섬웨어에 감염될 수 있습니다. 의심스러운 웹사이트에서 파일을 다운로드하거나 모르는 사람이 공유한 파일을 다운로드하면 감염될 수 있습니다. 즉, 인터넷을 탐색할 때 주의해야 하며 링크를 클릭하지 않거나 낯선 출처에서 파일을 다운로드하지 않는 것이 중요합니다. 이렇게 하면 랜섬웨어와 다른 유형의 맬웨어에 감염되지 않도록 보호하는 데 도움이 됩니다.

랜섬웨어의 공격 대상은 누구입니까?

랜섬웨어 공격은 인터넷에 연결된 컴퓨터나 다른 장치를 사용하는 모든 사람을 대상으로 합니다. 그러나 일부 그룹은 다른 그룹보다 공격 대상이 될 가능성이 높습니다. 예를 들어 랜섬웨어 공격은 기업을 공격 대상으로 삼는 경우가 많습니다. 더 중요한 데이터를 보유하고 있고 이를 검색하기 위해 금품을 지불하는 경우가 많기 때문입니다. 중요한 서비스를 제공하는 병원, 학교 및 기타 조직도 일반적인 공격 대상입니다. 랜섬웨어 공격이 운영을 방해하고 사람들의 생명을 위험에 빠뜨릴 수 있기 때문입니다. 개인도 랜섬웨어 공격 대상이 될 수 있습니다. 이러한 경우 공격자는 금품을 지불하지 않는 한 개인 파일을 삭제하거나 중요한 정보를 게시하겠다고 위협하여 피해자에게 금품을 갈취하려고 할 수 있습니다. 랜섬웨어 공격 대상은 데이터의 가치와 데이터를 회수하기 위해 금품을 지불할 의사에 따라 선택되는 경우가 많습니다.

랜섬웨어 지불 위험에는 어떤 것이 있습니까?

랜섬웨어 공격자에게 금품을 지불하는 것이 파일을 다시 가져올 수 있는 가장 쉬운 방법처럼 보일 수 있지만 실제로는 매우 위험한 결정일 수 있습니다. 몸값 지불과 관련된 위험은 다음과 같습니다.

- 공격자가 실제로 암호화 해제 키를 제공한다고 보장할 수 없습니다. 대부분의 경우 금품을 지불한 피해자는 키를 받지 못하며 파일에 계속 액세스할 수 없습니다.
- 금품 지불은 공격자가 공격 활동을 계속하도록 부추길 수 있습니다. 공격자가 피해자가 금품을 기불할 의사가 있음을 알게 되면 향후에 더 많은 공격을 시도할 가능성이 더 높아집니다.
- 금품을 지불하면 향후 공격 대상이 될 수 있습니다. 공격자가 금품을 지불할 의사가 있음을 알게 되면 향후에 공격 대상이 될 가능성이 더 높아집니다.
- 금품 지불은 불법입니다. 경우에 따라 범죄 단체에 금품을 지불하는 것은 테러리즘 또는 기타 불법 활동에 자금을 제공하는 형태로 간주될 수 있습니다.

금품을 지불하는 것이 파일을 가져올 수 있는 가장 쉬운 방법처럼 보일 수 있지만 실제로 매우 위험한 결정이 될 수 있습니다. 결정을 내리기 전에 위험을 신중하게 고려하는 것이 중요합니다.

랜섬웨어 비용은 얼마입니까?

랜섬웨어 공격 비용은 사용된 랜섬웨어 유형, 암호화된 파일 수 및 공격 효과와 같은 다양한 요인에 따라 크게 달라질 수 있습니다. 경우에 따라 랜섬웨어 공격의 비용은 공격자가 수백 달러의 금품을 요구하므로 상대적으로 낮을 수 있습니다. 또 다른 경우 공격자가 피해자의 파일에 대한 액세스 권한을 복원하는 데해 수천 달러 이상을 요구하므로 비용이 높아질 수 있습니다. 랜섬웨어 공격으로 인해 금품 지불과 관련된 직접 비용 외에도 상당한 간접 비용이 발생할 수 있습니다. 예를 들어 랜섬웨어 공격은 가동 중지 시간과 생산성 저하를 유발하여 수익이 손실될 수 있습니다. 또한 회사 명성과 고객 신뢰가 훼손될 수 있으며, 이로 인해 비즈니스에 부정적인 영향이 장기적으로 미칠 수 있습니다. 이러한 간접 비용은 금품 그 자체보다 훨씬 높은 경우가 많습니다.

랜섬웨어 증상에는 어떤 것이 있습니까?

랜섬웨어 공격 증상은 사용되는 랜섬웨어의 특정 유형에 따라 달라질 수 있습니다. 그러나 몇 가지 일반적인 증상은 다음과 같습니다.

- 파일이 암호화되어 액세스할 수 없습니다.
- 공격자로부터 암호화 해제 키의 대가로 금품 지불을 요구하는 메시지를 받습니다.
- 평소에 보지 못한 프로그램이나 프로세스가 컴퓨터에서 실행되고 있음을 확인합니다.
- 컴퓨터가 느려지거나 응답하지 않습니다.
- 컴퓨터에 비정상적인 오류 메시지가 팝업 창이 표시됩니다.

컴퓨터가 랜섬웨어에 감염된 것으로 의심되면 신속하게 조치를 취하는 것이 중요합니다. 랜섬웨어 확산을 방지하기 위해 인터넷에서 컴퓨터를 연결 해제합니다.

랜섬웨어 공격을 어떻게 방지할 수 있습니까?

랜섬웨어 공격을 방지할 수 있는 몇 가지 단계는 다음과 같습니다.

- 신뢰할 수 있는 안티 바이러스나 보안 소프트웨어를 사용하고 최신 상태로 유지합니다. 이렇게 하면 랜섬웨어와 기타 유형의 맬웨어로부터 컴퓨터를 보호할 수 있습니다.
- 이메일 첨부 파일 또는 링크를 열 때 주의하십시오. 랜섬웨어는 피싱 이메일을 통해 전달되는 경우가 많으므로 클릭하는 대상에 주의해야 합니다.
- 운영 체제와 기타 소프트웨어를 최신 상태로 유지합니다. 소프트웨어 업데이트에는 랜섬웨어와 기타 위협으로부터 컴퓨터를 보호하는 데 도움이 되는 보안 패치가 포함된 경우가 많습니다.
- 정기적으로 파일을 백업합니다. 이렇게 하면 컴퓨터가 랜섬웨어에 감염된 경우에 데이터를 보호할 수 있습니다. 3-2-1 백업 전략과 같은 권장 백업 전략 중 하나를 준수해야 합니다.
- 랜섬웨어의 위험을 인식하고 조직의 다른 사람들에게 이러한 위협에 대해 교육합니다. 이렇게 하면 랜섬웨어 공격을 예방할 수 있으며 랜섬웨어 공격이 발생할 경우 이를 보다 쉽게 감지하고 대응할 수 있습니다.

랜섬웨어 공격을 방지하는 최선의 방법은 경계를 늦추지 않고 컴퓨터와 데이터를 보호하기 위한 조치를 취하는 것입니다. 이렇게 하면 랜섬웨어 공격의 위험을 줄일 수 있으며 랜섬웨어 공격이 발생할 경우 쉽게 복구할 수 있습니다.

Synology가 랜섬웨어로부터 어떻게 사용자를 보호할 수 있습니까?

랜섬웨어에 의한 피해를 받지 않으려면 예방 조치가 필수적입니다. 선택한 안티 바이러스 소프트웨어와 함께 이러한 Synology 솔루션을 사용할 수 있습니다.

- **액세스 방지** - 파일, 응용 프로그램 및 액세스 권한을 설정하여 랜섬웨어 확산을 줄이고 Secure SignIn 및 C2 Password를 사용하여 보안 로그인 자격 증명을 구성할 수 있습니다.
- **Protect devices** — 오래된 시스템은 위험에 노출될 가능성이 더 높습니다. Synology Central Management System(CMS)을 사용하여 한 번에 모든 NAS를 업데이트하고 Synology Directory Server 및 C2 Identity의 그룹 정책을 사용하여 다른 장치를 보호합니다.
- **의심스러운 파일 피하기** - 스팸과 의심스러운 파일이 포함된 피싱 이메일은 랜섬웨어를 유포하는 일반적인 방법입니다. Synology MailPlus는 강력한 맬웨어 방지 보호 및 스팸 방지 기능을 제공합니다.
- **취약점 확인** - Synology 보안 어드바이저를 사용하여 맬웨어, 취약점 및 비정상적인 로그인 활동을 정기적으로 검사합니다. 구현 권장 변경 사항을 따르면 NAS 보안이 강화됩니다.
  https://www.synology.com/dsm/overview/security

데이터를 보호하는 다양한 방법

제품군 관리

다양한 기능을 활용하여 데이터 액세스 권한, 소프트웨어 상태, 시스템 상태 등을 중앙에서 관리할 수 있습니다.
https://www.synology.com/dsm/overview/administration

모든 시스템 모니터링

장치 위치에 관계없이 의심스러운 로그인 활동을 식별하고 업데이트를 관리하며 장치 상태를 모니터링할 수 있습니다.
https://www.synology.com/dsm/feature/active-insight

데이터 보호

3-2-1 백업 규칙을 따라 실수로 인하거나 악의적으로 데이터를 수정 및 삭제하지 못하도록 보호할 수 있습니다.
https://www.synology.com/dsm/solution/data_backup

시작하기

문의

자세한 내용은 각 지역 영업팀에 문의
https://www.synology.com/form/inquiry/sales

구입처

사용자 지역에서 Synology 파트너 찾기
https://www.synology.com/wheretobuy

주의 사항 :

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

랜섬웨어로부터 조직 보호

https://www.synology.com/ko-kr/dsm/solution/ransomware

Synology 웹사이트

https://www.synology.com/

문의

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