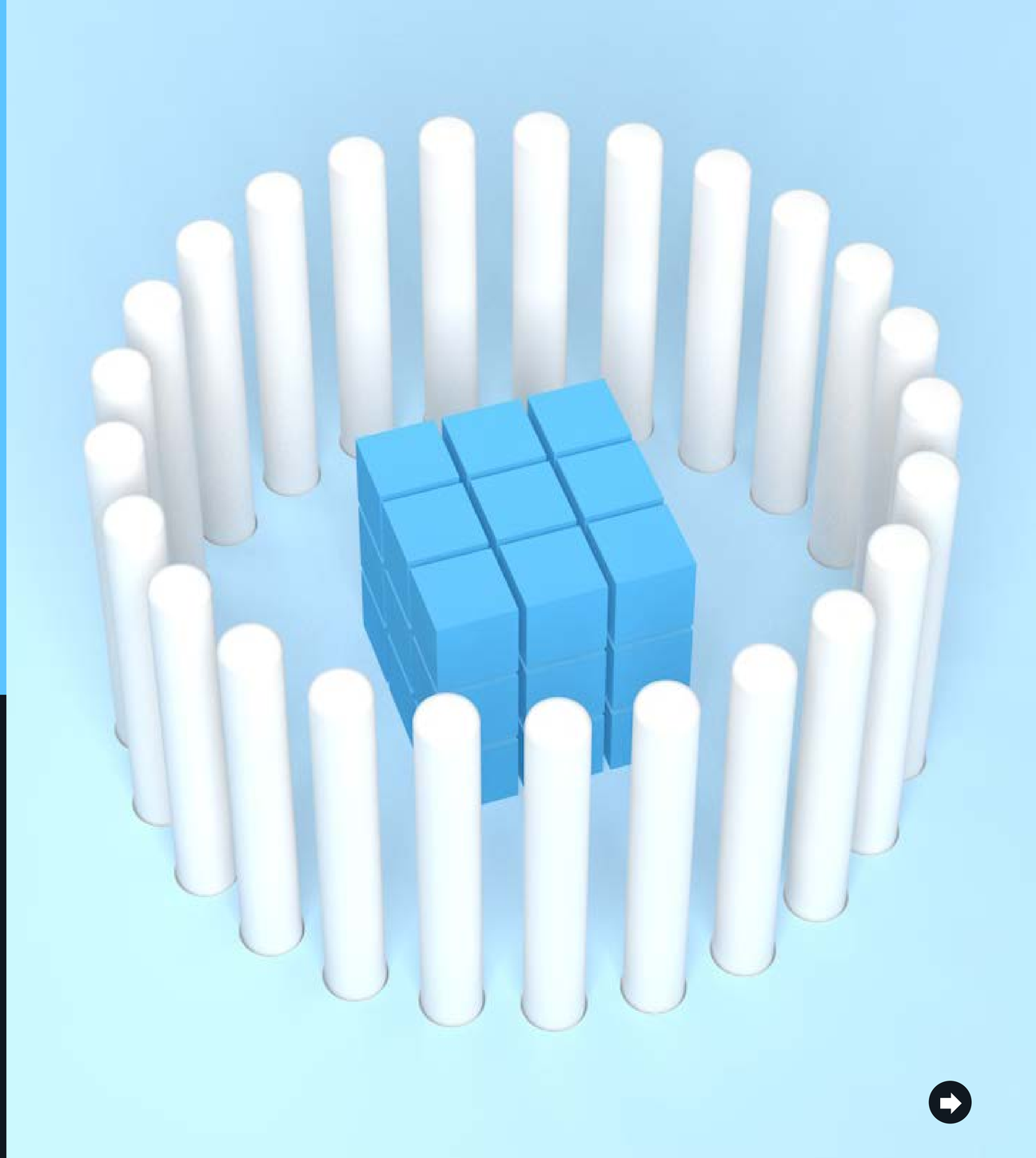
E-BOOK

사이버 레질리언스: 데이터를 전방위적으로 보호하는 방법

NetApp



목차

IT 조직 중심의 체제로 전환하는 과정

일주일간 먹을 식료품을 사러 갈 시간입니다. 일회용 쇼핑백과 열쇠를 챙긴 다음, 은색의 커다란 졸음 방지약을 입안에 털어 넣고 집을 나섭니다.

이제 어떠한 상황도 견딜 수 있는 초인적인 힘이 생겼으니 마트까지 안전하게 운전할 수 있습니다.

신통한 피로회복제를 복용하거나, 침입자를 막아줄 벽돌로 집을 짓거나, 도둑이 손에 쥘 수 없는 보석을 살 수만 있다면 안전벨트, 자물쇠 또는 경보 시스템을 거의 신경 쓰지 않아도 될 것입니다.

현실에서는 좀처럼 찾아보기 힘든 이런 강력한 보호 수단이 가상 세계에 등장하기 시작하면서 기존의 보호 수단과 통합되고 있습니다. IT 업계에서는 지난 수십 년 동안 '안전벨트 및 경보 시스템'과 유사한 사이버 보안 전략을 사용해 왔습니다.

그런데 최근 더 스마트한 방식이 등장했습니다. 바로 ***사이버 레질리언스(Cyber resilience)*** 입니다.

사이버 레질리언스에는 데이터 보호 체제에 기존의 IT 보안 체제가 접목되어 있기 때문에 조직이 사이버 공격을 극복할 수 있습니다. 침입자가 방어막을 돌파하거나 내부자가 악의적인 행동을 취하더라도 자체적인 보호 기능이 이미 갖춰져 있기 때문에 데이터를 보호할 수 있습니다.

사이버 레질리언스가 중요한 이유

사이버 레질리언스가 중요한 이유는 네트워크 침입을 원천 봉쇄하는 식의 사이버 보안 수단으로는 날로 진화하는 범죄 수법을 감당할 수 없기 때문입니다. 대다수 보안 전략은 방어막을 강화하여 출입구에서 적을 막는 데 중점을 둡니다. 그러나 오늘날에는 급증한 엔드포인트, BYOD 정책, 각광받는 재택근무 때문에 하나였던 출입구가 수백 개로 늘었습니다. 그로 인해 사이버 범죄자는 복잡한 네트워크 환경을 철저히 모니터링하느라 이미 과부하가 걸린 조직을 한결 수월하게 공격할 수 있습니다. 게다가 많은 조직은 본질적인 목표가 침입을 방지하는 것이 아니라는 사실을 잊은 지 오래입니다. 주요 목표는 가장 중요한 자산인 데이터를 보호하는 것입니다.

데이터 계층을 기점으로 한 사이버 레질리언스 전략 추구

모든 곳에서 보안 위협이 발생할 수 있는 상황이라면 어디서부터 시작해야 할까요?

이와 같은 상황에서는 데이터 중심의 보안 및 보호 체제를 구축하는 것이 급선무입니다. 그리고 이는 사이버 레질리언스 계획의 핵심 요소이기도 합니다.

전 세계적으로 랜섬웨어가 62% 증가[1]하고, 랜섬웨어 유형이 3.4% 증가[2]한 가운데 사이버 공격자들은 데이터를 볼모로 삼는 데 날로 능숙해지고 있습니다. 랜섬웨어 공격을 받은 조직 중 약 1/3은 암호화된 데이터를 되찾기 위해 대가를 지불합니다.[3] 같은 맥락에서 랜섬웨어 공격을 해결하는 데 드는 평균적인 비용은 미화 기준으로 2020년 768,106달러에서 2021년 185만 달러로 증가했습니다.[4]

게다가 이중 갈취 수법의 랜섬웨어 공격도 증가하고 있습니다. 데이터 손실 위험뿐만 아니라 데이터 유출 위험마저 조직이 떠안게 된 것입니다.[5] 그 어느 때보다 위험이 커졌으며, 랜섬웨어 공격은 오늘날 컴퓨팅 환경에서 언제든지 발생할 수 있는 현실이 되었습니다.

그렇다면 언젠가는 랜섬웨어 공격의 또 다른 희생양이 될지 모른다는 두려움을 안고 살아야만 할까요? 그렇지 않습니다. 데이터 중심의 사이버 보안 전략을 수립하면 **랜섬웨어를 두려워할 필요가 없을뿐더러 사이버 레질리언스를 실현할 수 있습니다.**

데이터 중심의 사이버 보안 전략에서는 방어막이 아니라 데이터와 최대한 가까운 곳을 보안의 기점으로 삼습니다.

데이터 계층으로 이동하여 데이터 보호

IT 조직 중심의 데이터 보호 체제로 전환하려면 약간의 작업이 필요합니다. 다행히 다른 선구적인 조직들이 남긴 유용한 지침이 있습니다.

파악

대응

보호

복구

감지

이러한 지표가 유용하긴 하지만, 포괄적인 사이버 레질리언스 계획을 수립하는 데는 여전히 어려움과 큰 비용이 수반됩니다. 팀은 한정된 자원을 최대한 효율적으로 활용하고, 기술 격차를 해소하며, 규제 요구사항을 일원화하고, 다른 우선순위에도 관심을 기울여야 합니다.[6] 사이버 레질리언스는 많은 에너지를 요하고 기억하기도 쉽지 않습니다.

각 단계를 진행하는 방법은 다음과 같습니다.

62%

전 세계적으로 랜섬웨어가 62% 증가[1]하고, **랜섬웨어 유형이 3.4% 증가**[2]한 가운데 사이버 공격자들은 데이터를 볼모로 삼는 데 날로 능숙해지고 있습니다.

파악: 데이터 환경 조사

보호가 필요한 항목을 파악하고 중요도에 따라 각 항목의 우선순위를 정하십시오. 어떤 시스템이 비즈니스 운영에 필수적인지 조사하십시오. 사용 중인 하드웨어와 소프트웨어를 빠짐없이 파악하여 이러한 인프라가 어디에 있고, 비즈니스 운영에 각기 어떤 역할을 하며, 악의적인 사용자가 이를 어떻게 악용할 수 있는지 알고 있어야 합니다. 정보의 흐름을 문서화하고, 사이버 보안 활동과 관련된 역할과 책임을 배정하며, 위협 파악 및 위험 관리 계획을 수립하십시오.[7]

다시 말해서, 현재의 데이터 보호 및 보안 실태를 점검해야 합니다. 또한 데이터를 유형별로 분류하고, 각 유형의 데이터가 저장된 곳을 파악하며, 데이터 액세스 권한을 평가해야 합니다.

파악 단계에서 해결해야 할 과제

파악 단계에서는 많은 시간이 소요됩니다. IT 책임자는 이미 엄청나게 많은 인프라 및 데이터 관리 작업을 날마다 담당하고 있습니다. 보유 중인 모든 IT 인프라를 파악하는 데만 상당한 시간이 소요될 수 있습니다. 특히 자동화 툴이 없으면 더더욱 그렇습니다. 그리고 구체적인 계획이나 표준화된 분류 절차에 따라 IT 인프라를 파악하지 않으면 데이터가 훨씬 더 복잡해져서 팀이 암호를 해독하고 실용화하는 데 어려움을 겪을 수 있습니다.

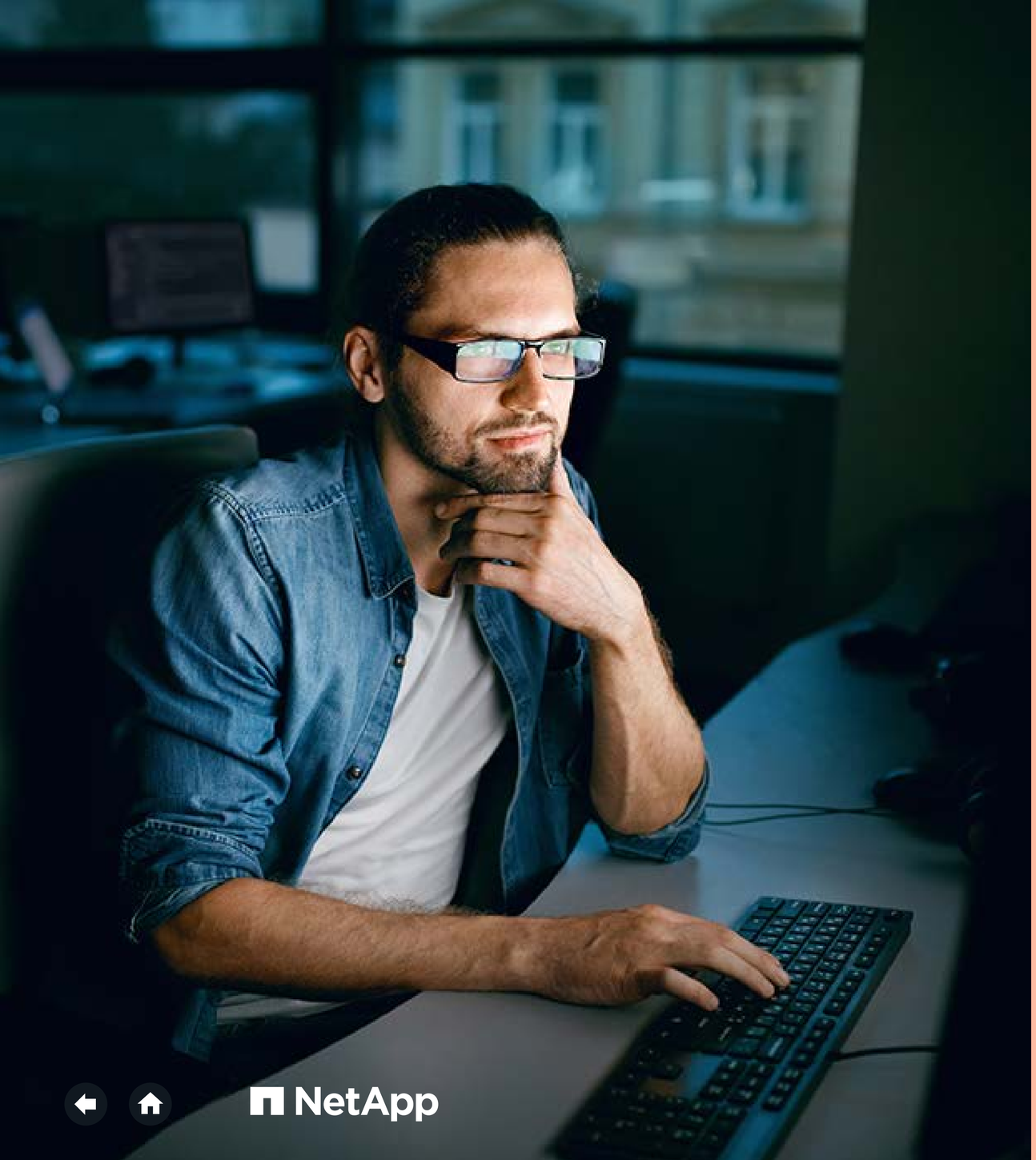
보호: 적소에 방어망 배치

보호 단계의 핵심은 방어벽을 구축하는 것입니다. 데이터 암호화, 주기적인 백업, 액세스 제어, 방어망 구축, 취약한 운영 체제 및 애플리케이션 업데이트를 수행하고 사용자에게 사이버 보안 모범 사례에 대해 교육하십시오.[8]

이 단계에서 수반되는 사항으로는 악의적인 사용자 차단, 오류 가능성이 있는 데이터 격리, 디스크에 데이터를 추가로 기록할 수 없도록 조치, 감염 방지 차원에서 세분화된 수정 불가능한 복사본 생성, 데이터 삭제 방지 차원에서 삭제 불가능한 백업 수행 등이 있습니다.

보호 단계에서 해결해야 할 과제

보호 단계에서는 사이버 보안 전략의 최근 변화를 엿볼 수 있습니다. 조직은 수십 년 전부터 방화벽과 네트워크 침입 방지 툴로 IT 환경을 보호해왔지만, 데이터 급증으로 인해 이러한 전략이 복잡해졌습니다. 이에 따라 이 단계에서는 해결해야 할 과제가 몇 가지 있습니다. 즉, 제대로 파악하기 버거울 정도로 빠르게 생성되고 있는 대량의 데이터를 암호화하는 방법, 생산성 저하나 안전하지 않은 차선책으로 귀결될 수도 있는 사용자 경험의 심각한 훼손을 막으면서 데이터 액세스를 제어하는 방법, 수많은 사각지대가 발견된 와중에도 빈틈없는 보안을 유지하는 방법을 강구해야 합니다.



감지: 선제적 조치

예방이야말로 최고의 해결법입니다. 위협이 나타나기 전에 의심스러운 활동을 감지하는 다음과 같은 시스템을 구축하십시오.

- 업데이트된 감지 프로세스
- 비정상적인 활동을 감지하고 근절할 수 있도록 주기적으로 로그 모니터링
- 데이터 도난 징후로 의심되는 비정상적인 활동을 인지할 수 있도록 주기적인 데이터 흐름을 철저히 파악
- 보안 사고를 감지하고 관련 여파(또는 피해 범위)를 가늠할 수 있는 기능[9]

다시 말해서, 사용자 행동을 모니터링하여 의심스러운 활동을 포착하고 데이터 트래픽의 이상 징후를 감지해야 합니다.

감지 단계에서 해결해야 할 과제

감지 단계의 최대 과제로는 조직이 걸러내야 하는 다량의 불필요한 경고가 손꼽힙니다. 수동으로 처리해야 하는 경우가 많은 위협 경고는 사이버 보안 팀과 보안 운영 센터(SOC)에 큰 부담이 됩니다. 이들은 허위 경고와 우선순위가 낮은 경고를 자동으로 조사하고 배제하여 보다 까다로운 경고에 집중할 방법을 강구해야 합니다. 또한 사이버 보안 팀은 이러한 위협을 더 빨리 감지하여 심각한 피해가 발생하기 전에 대응할 방법도 강구해야 합니다. 특히 사이버 범죄자가 탈취한 자격 증명을 사용해 무단으로 데이터에 액세스할 경우 상당량의 데이터를 암호화하기 전에 관련 상황을 즉시 파악할 수 있어야 합니다.

대응: 위기 대응 능력 확보

보안 수단이 발전하면서 보안 위협도 진화하고 있습니다. 따라서 사이버 레질리언스 계획의 실효성을 지속적으로 점검하는 것이 중요합니다. 모든 팀원은 각자의 책임을 숙지하고 있어야 합니다. 즉, 일반적인 사이버 보안 모범 사례뿐 아니라 비상 상황에 맞게 정해진 역할도 모두 알고 있어야 합니다. 위협의 진화 양상과 공격의 여파로 얻은 교훈을 토대로 사이버 레질리언스 계획을 업데이트하는 것도 중요합니다. 마지막으로, 공격이 발생했을 때 모두가 합심해서 대응할 수 있도록 업데이트한 계획을 내외부의 다른 이해 관계자와 빠짐없이 공유하는 것이 중요합니다.[10]

데이터 보호를 위해 대응 단계에서는 공격 감지 시 스냅샷을 생성하고 악성 사용자 계정을 차단하는 작업이 수반됩니다.

대응 단계에서 해결해야 할 과제

대응 단계를 성공적으로 완료하려면 시스템을 전반적으로 파악해야 합니다. 그래야 데이터가 저장된 곳을 평가하고, IT 환경에서 어떤 유형의 활동이 이뤄지는지 모니터링하며, 사이버 레질리언스 계획을 적절히 업데이트할 수 있습니다. 일상적인 인프라 및 데이터 관리에 이미 큰 부담을 느끼는 조직은 이 단계에서도 많은 시간을 들여야 합니다.

그리고 개인이 가장 철저하게 준비하여 수동으로 계획을 실행하는 데 걸리는 시간보다 빨라야만 효과적으로 대응할 수 있습니다. 사이버 보안 팀은 시스템이 의심스러운 활동을 감지하는 즉시 미리 정해진 조치(예: 데이터 스냅샷 생성)를 자동으로 취하는 툴을 갖춰야 합니다.

복구: 적시에 정상화

사이버 공격으로 인해 비즈니스 운영에 차질이 생긴 경우 신속하게 복구하여 정상화할 수 있어야 합니다. 이를 위해서는 공유해야 하는 정보가 무엇인지와 이 정보에 누가 액세스해야 하는지 파악해야 할 뿐 아니라 이러한 이해 관계자가 필요한 정보를 적시에 얻을 수 있게 하려면 어떻게 해야 하는지도 알고 있어야 합니다. 또한 보안 사고를 대중에게 공개하고, 개인정보가 유출된 것으로 보이는 사용자에게 관련 사실을 알리며, 규제 기관에 연락을 취하는 계획도 마련해야 합니다.

복구 단계에서는 몇 분 만에 데이터를 복원하고, 감염되지 않은 애플리케이션을 다시 정상화하며, 디지털 포렌식을 통해 위협의 근원을 파악해야 합니다.

복구 단계에서 해결해야 할 과제

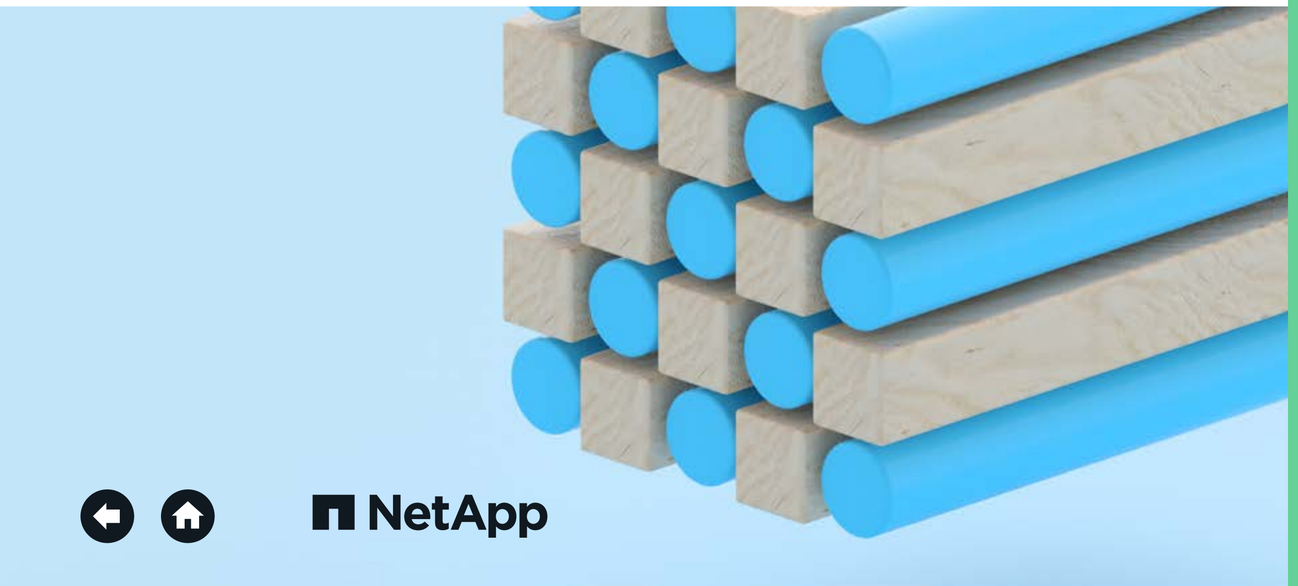
공격이 발생한 이후에는 감염된 인프라와 감염 정도를 파악하는 데 상당한 시간이 걸릴 수 있습니다. 그러나 내부 대응력과 외부 감시망을 모두 관리하려면 이러한 정보를 빠르게 확보해야 합니다.[11]

NetApp® 사이버 레질리언스 솔루션은 사이버 레질리언스 계획의 5가지 단계인 파악, 보호, 감지, 대응, 복구를 지원합니다. 그러나 많은 조직이 여러 가지 사이버 보안 툴을 무분별하게 도입한 탓에 다른 공급자의 솔루션으로 교체할 엄두도 내지 못하고 있습니다.

NetApp과 함께하면 이러한 고충에서 벗어날 수 있습니다. 토털 솔루션 역할을 하거나 기존 솔루션을 보완하는 랜섬웨어 솔루션을 도입할 수 있는 것입니다.

전방위적이고 현대적인 사이버 레질리언스 전략 수립

데이터 계층에 초점을 맞추면 사이버 레질리언스 문제를 더 쉽게 해결할 수 있습니다. 첫 번째 단계는 다음과 같은 질문을 통해 실태를 파악하는 것입니다.



예방이야말로 최고의 해결법입니다. 위협이 나타나기 전에 의심스러운 활동을 감지하는 다음과 같은 시스템을 구축하십시오.

- 클라우드, 온프레미스, 에지 중 어디에 데이터가 저장되어 있는가? 데이터가 지리적으로 분산되어 있는가?
- 어떤 유형의 데이터를 보유하고 있는가?
- 데이터에 어떤 유형의 권한이 적용되어 있는가?
- 악의적인 활동을 신속하게 파악하고 차단하려면 어떻게 해야 하는가?
- 신속하게 '자체 보호'를 진행하면서 위협을 파악하고 해소할 수 있도록 데이터 안팎에 보호 체제를 직접 구축하려면 어떻게 해야 하는가? 글로벌 네트워크에서 사용자 행동을 모니터링하여 의심스러운 활동을 포착하려면 어떻게 해야 하는가?
- 공격으로 인한 피해 범위를 파악하는 동안 모든 데이터의 보안을 유지하려면 어떻게 해야 하는가?
- 공격이 발생했을 때 몇 분 만에 데이터와 애플리케이션을 다시 정상화하려면 어떻게 해야 하는가?
- 위협의 근원을 조사하여 향후 유사한 공격을 방지하려면 어떻게 해야 하는가?

위의 질문에 대한 답을 모두 구하면 랜섬웨어 공격을 '두려워할 필요 없는' 데이터 중심의 사이버 레질리언스 계획을 위한 뼈대가 완성됩니다.

그러나 예상보다 많은 질문에 답하지 못한 조직을 위해 NetApp은 새로운 랜섬웨어 방지 및 복구 계획을 실행하는 데 필요한 툴이 포함된 솔루션을 제공합니다.

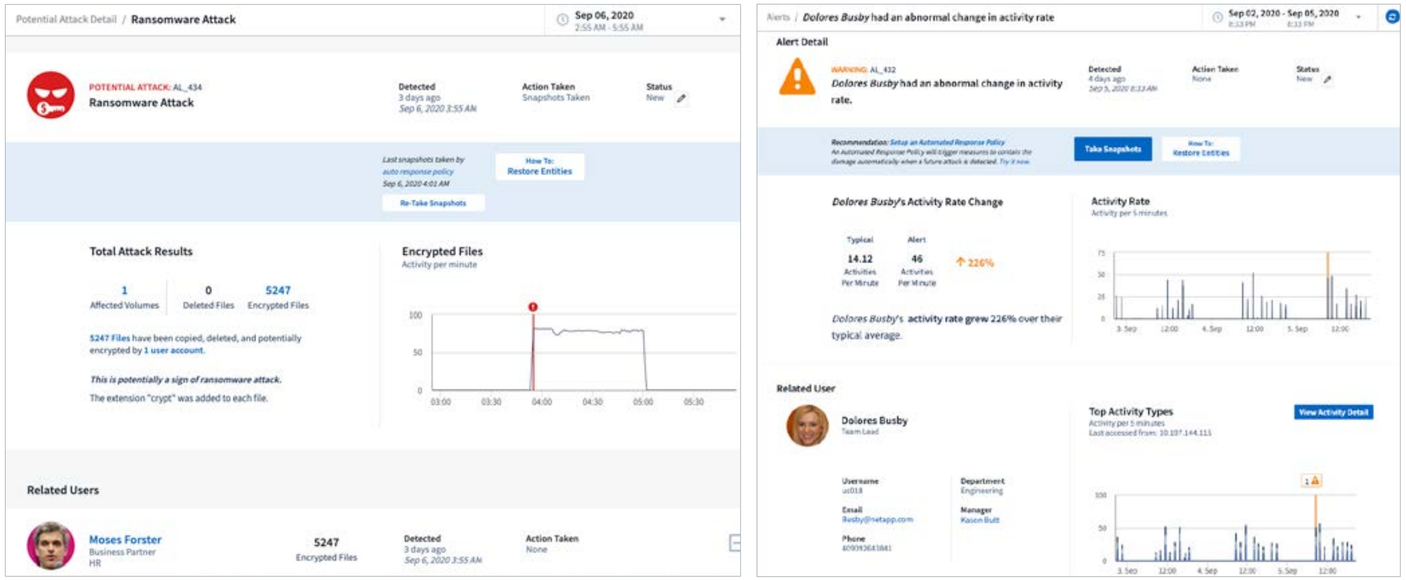
NetApp과 함께 사이버 레질리언스 계획 실현

다음 시나리오를 염두에 두고 실제 랜섬웨어 공격이 발생했을 때 바로 위에서 제시한 질문에 답하며 수립한 사이버 레질리언스 계획과 NetApp이 팀에 어떤 도움이 될지 생각해보십시오.

팀은 보유한 데이터 유형과 데이터 저장 위치를 알 수 있어야 합니다. AI 알고리즘을 사용하여 자동으로 데이터를 검색, 매핑, 분류하는 툴인 NetApp Cloud Data Sense는 이러한 정보를 제공합니다. 한편, 하이브리드 클라우드 인프라를 한눈에 보여주는 NetApp Cloud Insights는 전체 환경을 모니터링하고 보호하는 데 이상적입니다. 이 솔루션은 자사의 방어 수준을 파악하는 데도 유용합니다.

"최근에 랜섬웨어 사고가 있었는데 Cloud Insights 랜섬웨어 감지 기능의 효과를 직접 보고 완전히 반했습니다."

한 운송업체의 IT 담당 이사



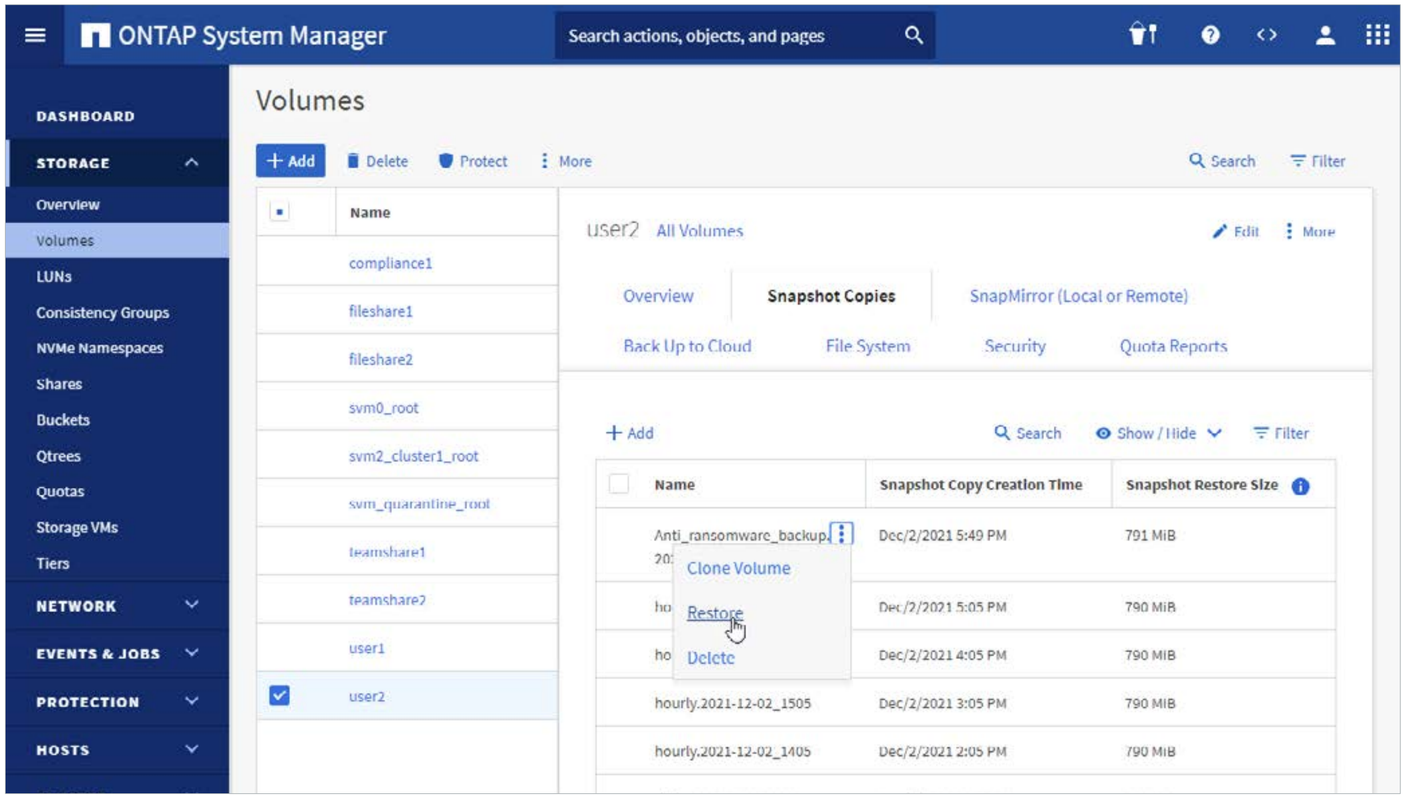
Cloud Insights는 비정상적인 사용자 활동을 찾아낸 후 스냅샷 복사본을 생성합니다. (출처: NetApp)

어느 날 아침 뉴욕 사무실에 출근한 IT 팀은 런던 사무실에 근무 중인 어떤 직원이 수상한 이메일 링크를 클릭했다는 사실을 알게 됩니다.

아무도 이 공격을 직접 모니터링하지 않았는데도 NetApp ONTAP® 데이터 관리 소프트웨어에 포함된 NetApp FPolicy가 제로 트러스트 데이터 보호 기능을 사용하여 알려진 악성 파일 확장자를 차단했습니다.

그래도 해커는 공격을 멈추지 않습니다. 해커는 노출된 사용자 계정을 통해 제로 데이 맬웨어 익스플로잇을 유포하여 파일을 감염시킵니다. 감시망에 포착되지 않기를 바라면서 여러 개의 노출된 사용자 계정에 더 많은 맬웨어를 심어 서서히 데이터를 암호화합니다.

소수의 직원으로는 이런 활동을 모조리 찾아내 근절하기란 쉽지 않습니다. 특히 다른 시간대에서 여러 가지 직무를 수행하느라 분주한 직원의 경우 더더욱 그렇습니다. 그러나 IT 팀에는 네트워크 상의 파일 공유를 모니터링하고 비정상적인 사용자 활동을 포착하는 NetApp Cloud Insights가 있습니다. IT 팀이 공격을 인지하지 못하더라도 Cloud Insights가 대신 공격을 감지하고 즉시 NetApp Snapshot™ 복사본을 생성하여 데이터를 보호합니다. IT 팀이 Cloud Insights를 사용하여 공격의 근원을 파악하고 나면 노출된 사용자 계정을 자동으로 차단할 수 있습니다.



조직은 NetApp을 활용하여 몇 분 만에 테라바이트 단위의 데이터를 복원할 수 있습니다. (출처: NetApp)

파일 스토리지에 서서히 침투하는 맬웨어도 문제없습니다. ONTAP에 내장된 자율형 랜섬웨어 방지 기능이 워크로드 활동과 데이터 엔트로피를 모니터링하여 필요시 경고 메시지를 발송합니다. 또한 경고 메시지가 발송되면 스냅샷이 자동으로 복사되어 여러 개의 복구 지점을 확보할 수 있습니다.

따라서 IT 팀은 NetApp 툴을 사용하여 몇 분 만에 테라바이트 단위의 데이터를 복원할 수 있습니다. 그리고 매우 극단적인 상황에서도 팀 전원은 데이터를 안전하게 보호할 수 있어 걱정할 필요가 없습니다. NetApp SnapLock® 소프트웨어는 데이터 삭제를 방지하는 논리적 에어갭(Air gap) 기술을 지원하기 때문입니다.

모든 클라우드를 고려한 데이터 중심의 사이버 레질리언스 계획

IT 팀이 온프레미스로 데이터를 관리하는 경우에도 앞서 설명한 시나리오가 유효할까요? 클라우드, 하이브리드 환경 또는 에지에 데이터를 저장하는 경우는 어떨까요? 물론 유효합니다. 사이버 레질리언스는 데이터 중심으로 설계되었으므로 온프레미스, 원격 위치, 클라우드 등 어디에 데이터를 저장하든 완벽한 보안, 복원력, 가용성이 항상 유지됩니다. NetApp 사이버 레질리언스 솔루션은 하이브리드 클라우드와 호환되며 모든 주요 퍼블릭 클라우드와 통합됩니다.

기존의 인프라 활용도 극대화

데이터 중심의 NetApp 사이버 레질리언스 솔루션은 지금까지 설명한 사이버 레질리언스 계획의 5가지 단계에 모두 유용합니다. 이미 사이버 보안 툴을 도입한 조직도 혜택을 볼 수 있습니다. NetApp ONTAP 소프트웨어 기능은 기존의 사이버 보안 툴과 통합될 수 있으므로 전면적인 교체 없이도 보안 공백을 메울 수 있습니다.

데이터 보호

ONTAP Snapshot과 통합하고 SnapMirror를 통해 효율적으로 복제

NetApp

COMMVAULT, rubrik, veeam, CLEONDRIS, CATALOGIC, druva, IBM, ProLion, VERITAS

사용자 행동

파일과 사용자 행동을 지능적으로 모니터링할 수 있는 FPolicy API와 통합

NetApp Cloud Insights

Brainwave GRC, CLEONDRIS, ProLion, STEALTHbits, VARONIS, VERITAS

감사/로깅

포렌식 분석 시스템 로그 또는 SIEM 툴과 통합

NetApp Cloud Insights, splunk>

Brainwave GRC, CLEONDRIS, ProLion, STEALTHbits, VARONIS, VERITAS

클릭 몇 번으로 수립할 수 있는 사이버 레질리언스 계획

사이버 범죄자가 없어지게 할 수는 없지만, 적절한 툴로 조직의 사이버 레질리언스를 실현할 수 있습니다. 데이터 중심의 사이버 레질리언스 계획을 실행하는 데 NetApp이 어떤 도움이 되는지 자세히 알아보십시오.

- NetApp 데이터 보호
- NetApp 랜섬웨어 솔루션
- NetApp으로 철통같은 보안 유지

www.netapp.com/kr에서 자세히 알아보십시오.

1. PBS NewsHour, 랜섬웨어 공격이 증가하는 이유와 이를 막을 방법, 2021년 7월 8일
2. Business Wire, 랜섬웨어 인덱스 스포트라이트 보고서: 2021년 3분기 조사에서 새로운 랜섬웨어 취약점 및 유형이 양적·질적으로 꾸준히 증가한 것으로 확인, 2021년 11월 9일
3. Statista, 2021년 2월을 기준으로 랜섬웨어에 감염된 조직이 암호화된 데이터를 되찾는 방법
4. Sophos News, 2021년 랜섬웨어 상태, 2021년 4월 27일
5. Deloitte, 이중 갈취 보안 사고, 2020년 10월
6. Infosec, NIST CSF: NIST 사이버 보안 프레임워크 구현, 2020년 2월 19일
7. Infosec, NIST CSF: NIST 사이버 보안 프레임워크 구현, 2020년 2월 19일 - *상동*
8. Infosec, NIST CSF: NIST 사이버 보안 프레임워크 구현, 2020년 2월 19일
9. Infosec, NIST CSF: NIST 사이버 보안 프레임워크 구현, 2020년 2월 19일
10. Infosec, NIST CSF: NIST 사이버 보안 프레임워크 구현, 2020년 2월 19일
11. Infosec, NIST CSF: NIST 사이버 보안 프레임워크 구현, 2020년 2월 19일

NetApp 정보

평범함으로 가득한 세상에서 NetApp은 특별함을 선사합니다. NetApp은 귀사가 데이터를 최대한 활용할 수 있도록 돕는다는 한 가지 목표에 주력하고 있습니다. NetApp은 귀사에서 사용 중인 엔터프라이즈급 데이터 서비스를 클라우드로 전환하고, 클라우드의 유연성을 데이터 센터에 제공합니다. 업계 최고 수준의 NetApp 솔루션은 다양한 고객 환경과 세계 최대의 퍼블릭 클라우드에서 작동합니다.

클라우드 주도형 데이터 중심 소프트웨어 회사인 NetApp만이 고유한 Data Fabric을 배포하고, 클라우드를 단순화하고 연결하며, 언제 어디서나 원하는 사람에게 원하는 데이터와 서비스, 애플리케이션을 안전하게 제공하도록 지원할 수 있습니다.

NetApp

+1 877 263 8277