NetBackup이 랜섬웨어 공격 차단에 효과적인 5가지 이유

랜섬웨어 공격 소식이 끊임없이 언론의 헤드라인을 장식합니다. 물론 그럴 만한 이유가 있습니다. 2031년에는 랜섬웨어 공격이 2초에 한 번씩 발생할 것으로 예상됩니다.[1] IT 보안 전문가의 절반가량은 본인이 속한 회사가 랜섬웨어 공격에 대처할 만한 상황이 아니라고 생각합니다.[2]

강력한 방어 전선 구축은 랜섬웨어 공격 차단의 출발점이 될 수 있지만 그것만으로는 충분하지 않습니다. 각 기업은 통합적인 멀티레이어 레질리언스 프레임워크를 개발하여 전체 사이버 보안 전략의 보호, 탐지, 복구 구성 요소를 효과적으로 지원해야 합니다. 사이버 범죄 수법이 갈수록 정교해짐에 따라, 이제는 랜섬웨어의 '발생 가능성'보다 '발생 시점'을 파악하는 것이 더 중요합니다.

Veritas NetBackup™을 사용하면 랜섬웨어 공격이 발생해도 성공적으로 레질리언스를 유지할 수 있습니다. NetBackup은 다음과 같은 5가지 방법으로 랜섬웨어 공격을 차단, 탐지하고 실제 공격 상황에서도 효과적으로 복구하도록 지원합니다.

1. 하드웨어 및 소프트웨어 강화

복잡하고 서로 긴밀하게 연결된 IT 시스템의 특성상 랜섬웨어가 단일 진입 지점을 통해, 예컨대 어떤 직원에게 전송된 피싱 이메일 형태로 기업의 모든 데이터를 장악할 수 있습니다.

NetBackup은 통합 하드웨어/소프트웨어 하드닝 전략으로 IT 공격 범위를 최소화하여 그러한 취약점으로부터 보호합니다. 개별 역할 기반 액세스 제어(RBAC), 2단계 인증, 데이터 전송/저장 시 암호화 등 한층 강화된 ID 및 액세스 관리 기능을 갖춘 NetBackup은 날로 심각해지는 보안 위협을 차단하면서 고객 환경의 안전을 보장합니다.

2. 변조 불가 스토리지로 백업 보호

백업은 랜섬웨어 공격에 대한 최종 방어선이라 할 수 있습니다. 하지만 공격자가 백업까지 암호화할 경우 대개는 몸값을 지불할 수밖에 없습니다. 이때 데이터 기록이 가능하지만 변경이나 삭제는 불가능한 변조 불가 스토리지를 사용한다면 효과적인 대응 수단이 됩니다.

랜섬웨어가 일차 방어선을 통과하여 온프레미스 및 클라우드 시스템 전체에 확산되더라도 NetBackup의 변조 불가 이미지 관리 및 스토리지 기능으로 백업이 암호화되거나 지워지지 않게 할 수 있습니다. 결국 데이터를 손상시키거나 암호화하려는 랜섬웨어 공격자의 위협에 굴복하지 않고 더 신속하게 복구할 수 있습니다.

3. 에어 갭 방식의 데이터 보호 지원

네트워크에 연결된 백업은 취약합니다. 물리적으로 연결된 모든 시스템이 공격 표적이 되어 감염될 수 있기 때문입니다. 이러한 상황에서 데이터를 보호하는 방법 중 하나는 저장된 데이터와 네트워크로 연결된 시스템 간에 물리적인 공간, 즉 에어 갭(Air Gap)을 두는 것입니다. 이러한 오프라인 백업은 악의적인 데이터 액세스 및 암호화를 확실히 차단하는 몇 가지 방법 중 하나입니다.

NetBackup은 이러한 에어 갭 전략을 지원합니다. 타사 솔루션에 의존할 필요 없이 NetBackup의 레질리언스 기능을 활용하여 에어 갭 기능을 지원하는 스토리지 미디어에 중복 제거 데이터를 복제할 수 있습니다.

4. 잠재적 보안 위협 자동 탐지

오늘날 기업을 노리는 사이버 범죄자는 데이터 및 인프라스트럭처 환경의 모든 영역을 공격 표적으로 삼습니다. 따라서 데이터, 인프라스트럭처, 사용자 활동을 면밀하게 모니터링하고 제어하면서 보안 위협과 취약점을 탐지하는 것이 중요합니다.

NetBackup은 거시적 관점으로 환경을 모니터링할 수 있습니다. 또한, 인공지능(AI)을 활용하여 이상을 탐지하고, 백업이 생성될 때마다 의심스러운 활동에 대한 알림을 받습니다. IT 팀은 데이터 및 인프라스트럭처에서 행동의 기준선, 이를테면 예상 데이터 활동, 연계 시스템 권한 등을 더 정확히 인식하고 적용합니다. 이상이 탐지되면 IT 팀이 즉시 대응에 나서 문제의 백업을 격리함으로써 만일의 피해를 최소화하고 데이터를 항상 복구 가능한 상태로 유지할 수 있습니다.

5. 자동 오케스트레이션 복구 프로세스 구현

많은 IT 팀이 기업의 요구 사항을 해결하고자 하이브리드 멀티 클라우드 인프라스트럭처를 구축하지만, 관련 복잡성으로 인해 데이터가 더 취약해지고 복구의 어려움이 커질 수도 있습니다. 수백, 수천 대의 서버를 운영하는 기업의 경우 수작업으로 데이터를 복구하려면 많은 시간이 소요되므로 자동화가 필수입니다.

NetBackup이 제공하는 자동 오케스트레이션 복구 프로세스를 위한 통합 옵션을 활용하면 랜섬웨어 공격 상황에서도 주도권을 빼앗기지 않고 대응할 수 있습니다. NetBackup은 VMware를 위한 인스턴트 롤백 기능도 제공하므로 가상 머신을 임의의 시점으로 즉시 롤백하는 것이 가능합니다. 프로덕션 시스템을 롤백하는 데 필요한 고유한 블록만 전송하는 방식이므로, 며칠 또는 몇 시간이 걸리던 복구를 몇 분 또는 몇 초 만에 완료하고 비즈니스 연속성을 보장할 수 있습니다.

안심할 수 있는 Veritas NetBackup

막대한 피해를 일으키는 랜섬웨어 공격을 피하지 못하더라도 NetBackup을 통해 철저히 대비할 수 있습니다. 전 세계 데이터 백업 및 복구 솔루션 시장에서 명실상부한 선두 주자로 인정받는 NetBackup은 단일 통합 플랫폼에서 어떤 워크로드, 클라우드, 아키텍처도 지원하면서 확장 가능한 방식으로 비즈니스 크리티컬 레질리언스를 제공합니다.

NetBackup은 데이터를 노리는 악성 보안 위협으로부터 데이터와 인프라스트럭처를 보호하는 레질리언스 전략으로 보호, 탐지, 복구 요구 사항을 모두 해결하는 동시에 랜섬웨어도 확실히 차단할 수 있습니다.

Veritas NetBackup을 통해 최상의 레질리언스로 랜섬웨어를 차단하는 방법에 대한 자세한 내용은 www.veritas.com/ko/kr/protection/netbackup에서 확인하십시오.

1. Cybercrime Magazine, "2031년에는 전 세계적으로 랜섬웨어로 인한 경제적 피해의 규모가 2,650억 달러를 돌파할 것", 2021년 6월 3일.
2. PurpleSec, "2021년에 반드시 기억해야 할 10가지 사이버 보안 트렌드", 2021년 4월 29일.

Veritas Technologies 소개

Veritas Technologies는 데이터 보호 및 가용성 분야의 글로벌 선도 기업으로, 포춘 500대 기업 중 87%를 포함한 5만개 이상의 전세계 기업이 베리타스 기술을 기반으로 IT 복잡성을 해결하고 데이터 관리를 간소화합니다. 베리타스 엔터프라이즈 데이터 서비스 플랫폼은 데이터의 위치와 관계없이 데이터 보호를 자동화하고 복구를 조정함은 물론, 비즈니스 크리티컬 애플리케이션의 가용성을 항시 보장하고 기업이 데이터 규제 변화를 준수하는 데 필요한 인사이트를 제공합니다. 더불어 높은 신뢰성과 모든 요구사항을 충족하는 배포 모델을 제공하는 베리타스 엔터프라이즈 데이터 서비스 플랫폼은 800개 이상의 데이터 소스와 100개 이상의 운영체제(OS), 1400개 이상의 스토리지 타깃, 60개 이상의 클라우드 플랫폼을 지원합니다. 보다 자세한 정보는 베리타스 홈페이지(www.veritas.com/kr) 또는 베리타스 트위터(@veritastechllc)에서 확인하실 수 있습니다.

VERITAS

서울시 송파구 올림픽로 300
롯데월드타워 35층
Tel: 02 3468 2100
www.veritas.com/kr

V1364 08/21