DELL Technologies

솔루션 브리프

Sheltered Harbor 용 PowerProtect Cyber Recovery

중요한 고객 데이터를 보호하고 미국 금융 시장에서 소비자의 신뢰 유지

Sheltered Harbor 란?

금융 업계 주도로 2015 년 발의된 Sheltered Harbor 표준에는 다양한 사이버 회복탄력성 및 데이터 보호 모범 사례와 미국 금융 데이터를 보호하는 보호 기능이 통합되어 있습니다. 운영 및 백업 시스템을 대상으로 하는 랜섬웨어, 데이터 파기 또는 도난과 같은 사이버 위협은 소비자와 기업의 재무 데이터를 위험에 빠뜨립니다.

미국의 은행, 신용 조합 또는 증권 회사를 대상으로 사이버 공격이 성공하면 해당 금융 기관의 평판이 손상되고, 미국 금융 시스템에 대한 소비자의 신뢰도가 저하되며, 글로벌 금융 위기가 발생할 수 있습니다.

Sheltered Harbor 는 중요한 고객 계정 기록 및 기타 데이터를 디지털 볼트 내에서 변경 불가능한 상태로 격리하여 미국의 금융 안정성과 금융 기관의 사이버 회복탄력성을 강화합니다. 랜섬웨어 또는 기타 이벤트와 같은 사이버 공격으로 인해 기관의 기본 또는 백업 시스템이 손상되는 경우 중요한 데이터를 신속하게 복구할 수 있으므로 중요한 고객 대상 금융 서비스의 연속성을 보장하여 공신력을 유지할 수 있습니다.

Cyber Recovery 를 선택해야 하는 이유

Dell Technologies 는 Sheltered Harbor Alliance Partner Program 최초의 솔루션 공급업체로서, 미국 금융 기관을 위해 Sheltered Harbor 턴키 데이터 볼팅 솔루션을 개발했습니다.

Sheltered Harbor 용 PowerProtect Cyber Recovery 는 Sheltered Harbor 의 인증을 받은 업계 최초의 온프레미스 턴키 데이터 볼팅 솔루션이며, Sheltered Harbor 표준을 구현하는 참여 기관의 모든 기술 제품 요구 사항을 충족합니다.

데이터 볼트 – 참여 기관 또는 서비스 공급업체가 야간에 중요한 데이터에 대한 백업을 Sheltered Harbor 표준 형식으로 생성합니다. 데이터 볼트는 암호화되고 변경할 수 없으며 백업, 재해 복구, 다른 데이터 보호 시스템을 비롯하여 기관 내 다른 인프라스트럭처와 격리되어 있습니다.

격리 및 거버넌스 – 기업 네트워크에서 분리되어 안전하게 격리된 환경은 적절한 승인을 거친 사용자 이외에는 액세스를 제한합니다. 자동화된 데이터 복사 및 물리적 분리 관리를 통해 데이터 무결성, 가용성, 보안 및 기밀성을 유지할 수 있습니다.

복구 및 문제 해결 – Sheltered Harbor 회복탄력성 계획이 활성화되면 참여 기관은 볼트에서 데이터를 신속하게 복구하여 금융 업무를 빠르게 복원하고 재개할 수 있습니다.

당면 과제: 금융 서비스 업계 대상의 사이버 공격이 글로벌 금융 위기를 유발할 수 있음

모든 조직이 악의적인 사이버 공격이 비즈니스 전반에 미치는 심각한 피해에 대해 우려하면서도 조직의 97%가 디지털 혁신 활동에 기밀 데이터를 사용합니다.[1] 데이터의 잠재적 가치를 제대로 실현하면 큰 보상이 따릅니다.

하지만 기밀 데이터가 부적절하게 유출되어 파기되거나 대중에 공개될 경우 심각한 위험에 빠질 수도 있습니다. Symantec 의 2019 Internet Security Threat 보고서에 따르면 멀웨어 및 랜섬웨어 공격은 날로 증가하고 있으며 기업을 대상으로 한 랜섬웨어 공격은 2019 년 12% 증가하여 전체 랜섬웨어 감염의 81%를 차지하는 것으로 나타났습니다.[2] 또한 최근 Ponemon Institute 의 보고서에 따르면 2020 년에 발생한 전체 데이터 침해 사고 중 52%에서 악의적인 의도가 발견되었으며 이는 5 년 전과 비교할 때 30% 증가한 수치입니다.[3]

무엇보다도 악의적인 행위자의 전술과 툴은 탐지와 공격 예방이 거의 불가능하도록 진화했습니다. Verizon Data Breach Investigations 2020 보고서에 따르면 사이버 범죄 전술은 계속 진화하고 있으며 내부자 관련 사이버 공격은 불과 3 년 전의 25%에서 5% 증가한 30%로 나타났습니다.[4]

Accenture 의 2019 Annual Cost of Cybercrime 보고서 [5]에 따르면 미국 금융 업계는 지난 3 년 동안 사이버 범죄로 인해 가장 큰 손실을 입었으며 이러한 요소들이 결합되어 세계 금융 시장을 한층 더 위협하는 최악의 상황이 발생할 수 있습니다.

Sheltered Harbor 는 미국 금융 기관에서 고객 데이터를 손상시키고 정상적인 금융 서비스를 저해하는 사이버 공격 위험을 줄일 수 있도록 업계가 주도하는 비영리 목적의 이니셔티브 형식으로 2015 년에 시작되었습니다. Sheltered Harbor 생태계는 참여 기관(미국 은행, 신용 조합, 증권 회사, 자산 운용사), 국가 무역 협회, 솔루션 공급업체 및 서비스 공급업체로 구성되어 있으며, 금융 부문의 안정성과 사이버 회복탄력성을 강화하는 데 초점을 맞추고 있습니다.

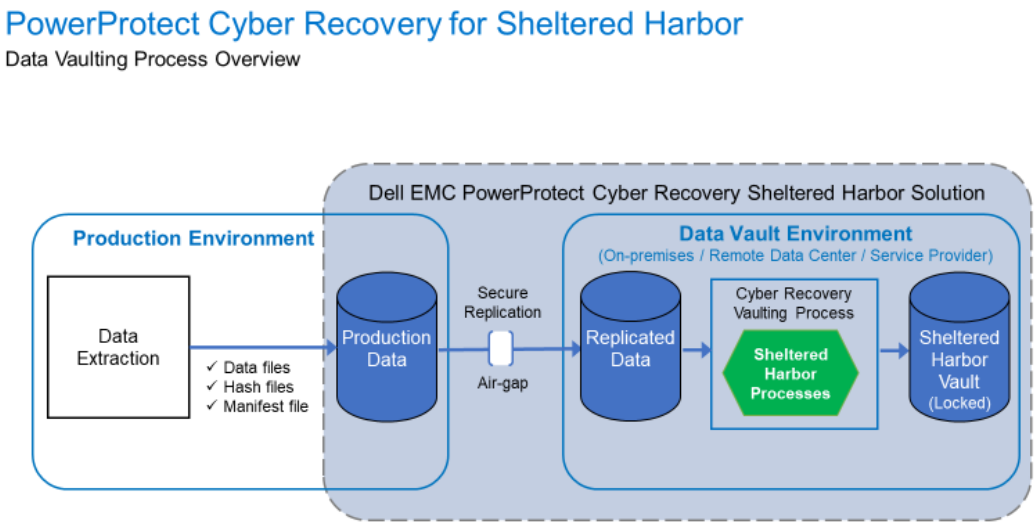
자연 재해나 인재가 발생한 후에 전체 운영 기능을 복원하려면 기존의 재해 복구 및 비즈니스 연속성이 필요합니다. 표적화된 정교한 사이버 공격이 발생하는 경우 Sheltered Harbor 는 전체 복구 절차가 진행되는 동안 기본적인 금융 업무를 복원하는 데 필요한 데이터를 손상되지 않은 상태로 즉시 사용할 수 있도록 하는 것으로 목표로 합니다.

참조 번호: H18199.

Sheltered Harbor 용 Dell EMC PowerProtect Cyber Recovery – 금융 기관의 가장 중요한 데이터를 위한 강력한 사이버 회복탄력성

Dell Technologies 는 Sheltered Harbor Alliance Partner Program 에 참여한 최초의 솔루션 공급업체입니다. Sheltered Harbor 인증을 받은 Dell Technologies 의 솔루션은 거의 5 년 동안 랜섬웨어와 같은 사이버 공격으로부터 조직의 가장 중요한 데이터를 보호해 온 시장 선도 제품인 Dell PowerProtect Cyber Recovery 를 기반으로 합니다.

Sheltered Harbor 스펙을 준수하기 위해 Cyber Recovery 볼트 아키텍처는 아카이브 생성과 안전한 저장소 프로세스를 수행하도록 확장되었습니다. 추출된 Sheltered Harbor 데이터는 운영 환경에 저장된 후 물리적으로 네트워크가 분리된 논리적 전용 연결을 통해 볼팅 환경으로 안전하게 복제되며, 볼팅 환경에서 보존 잠금과 같은 나머지 단계가 수행됩니다.



기업 네트워크 및 백업 시스템과 물리적으로 분리되어 격리된 전용 환경을 구축함으로써 Sheltered Harbor 참여 기관이 보호해야 하는 중요한 데이터 세트를 표준화된 형식으로 제공하므로 고객을 대상으로 하는 기본 금융 서비스를 신속하게 재개할 수 있습니다. 구축은 Sheltered Harbor 스펙을 확실히 준수하면서 몇 달이 아니라 몇 주만에 완료됩니다.

요약

Sheltered Harbor 용 Dell EMC PowerProtect Cyber Recovery 는 Sheltered Harbor 스펙을 준수하기 위해 일회성의 독점 볼트를 구축하는 각 참여 기관에 빠르고 비용 효율적이고 효과적이면서 Sheltered Harbor 의 승인을 받은 대안을 제공합니다. Sheltered Harbor 표준을 구현하려는 은행, 신용 조합 및 증권 회사는 모든 승인을 거쳐 완벽하게 지원되는 Dell Technologies 의 턴키 방식의 데이터 볼팅 솔루션을 사용할 수 있습니다.

Sheltered Harbor 용 PowerProtect Cyber Recovery 를 선택하는 Sheltered Harbor 참여 기관은 완성도 높은 볼트 기반 기술의 이점을 활용함으로써 즉각적인 구축 요구 사항을 충족할 뿐만 아니라 향후 데이터의 볼팅 요구 사항을 충족하는 발판을 마련할 수 있습니다. 참여 기관은 존속 대책을 확보하게 되며 미국 금융 시스템에서 공신력을 유지할 수 있습니다.

출처:

1. 2019 Thales Data Threat 보고서 – www.thalessecurity.com/DTR
2. 2019 Symantec Internet Security Threat 보고서 - https://www.symantec.com/security-center/threat-report
3. 2020 Cost of Data Breach 보고서, Ponemon Institute, LLC - https://www.ibm.com/security/data-breach
4. 2020 Verizon Data Breach Investigations 보고서 - https://enterprise.verizon.com/resources/reports/dbir/
5. 2019 Accenture Cost of Cybercrime 보고서 - https://www.accenture.com/us-en/insights/security/cost-cybercrime-study