
ESCARE
NeuShield® Data Sentinel
랜섬웨어 순간 복원 솔루션
NeuShield®
How much is your data worth?

목차

- Ransomware 현황 및 대응 방안
- 제품 소개
- 사례 분석

Ransomware 현황 및 대응방안

NeuShield®
How much is your data worth?

Ransomware 방어 솔루션이 존재하는가?

> “FireEye에서 분석한 랜섬웨어 공격을 당한 기업은 당시 보안솔루션 및 안티바이러스 제품들이 **최신 업데이트가 반영된 상태**였습니다.”

- FireEye (WC Docket No. 13-184) FireEye™

랜섬웨어 분석 보고서에 따르면 **2019년에 14초** 마다 기업이 랜섬웨어 공격을 받고 있으며, **2021년에는 11초** 마다 공격을 받게 될 것입니다.

Ransomware 복원 시 고민 사항은?

- **랜섬웨어 제거 방안**
  - 감염 단말의 완벽한 악성코드 분석 및 제거가 불가능함
  - 이메일, 어플리케이션 및 시스템 재 구성이 어려움
  - 단말 재 설치 과정에 다시 감염되는 현상 발생

- **데이터 복구 방안**
  - 완벽한 암호화 복구 방안이 존재하지 않음
    (34% 기업이 데이터를 완전히 유실함)
  - 백업 존재 시 복구에 막대한 시간이 소요됨.

- **업무 장애 및 손실**
  - 비즈니스 중단으로 인한 수익 손실 발생
  - 기회 비용 상실
  - 기업 평판 및 브랜드 손상
  - 법률 소송

제품 소개

NeuShield®

How much is your data worth?

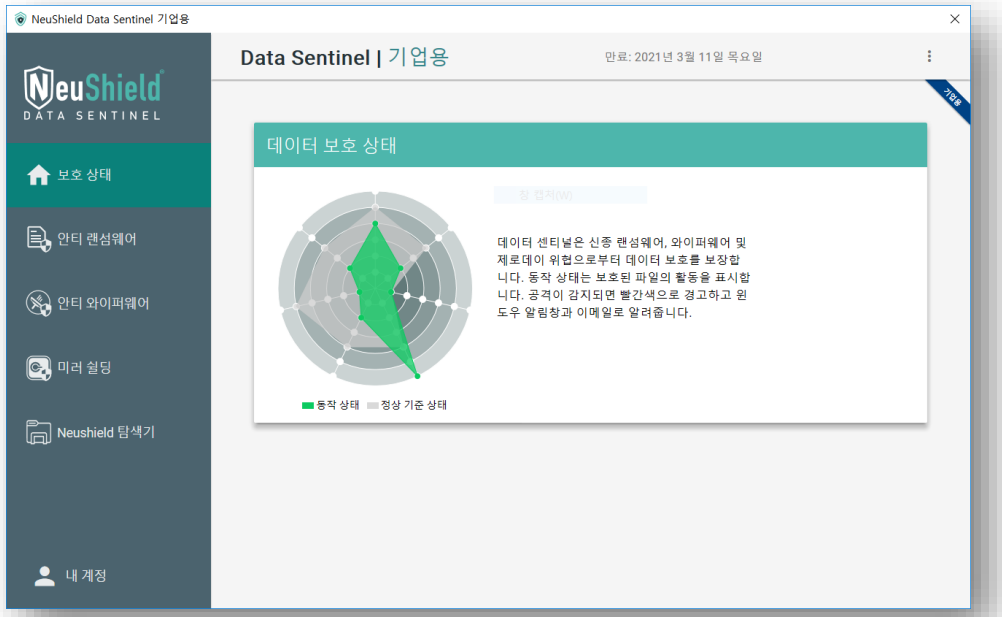
NeuShield Data Sentinel

Data Sentinel 지원 범위 :

- 클라우드 기반의 Endpoint 관리 지원
- 다양한 시스템 보호 기술 지원 (Boot 이미지, Disk 이미지, 문서보호)
- 랜섬웨어 등 의도하지 않은 방법에 의한 파일 변조를 보호
  - 랜섬웨어는 보호 필름 위에 암호화를 시도함.
  - 보호 필름 제거를 통한 암호화 영역 제거 (문서 순간 복원)
  - 보호 필름 영역을 위하여 로컬 디스크를 사용함.
  - 클라이언트 인증 시 인터넷 연결이 필요함.

Data Sentinel 비 지원 범위:

- 안티바이러스 및 백업 기능
- 랜섬웨어 실시간 탐지 및 암호화 차단

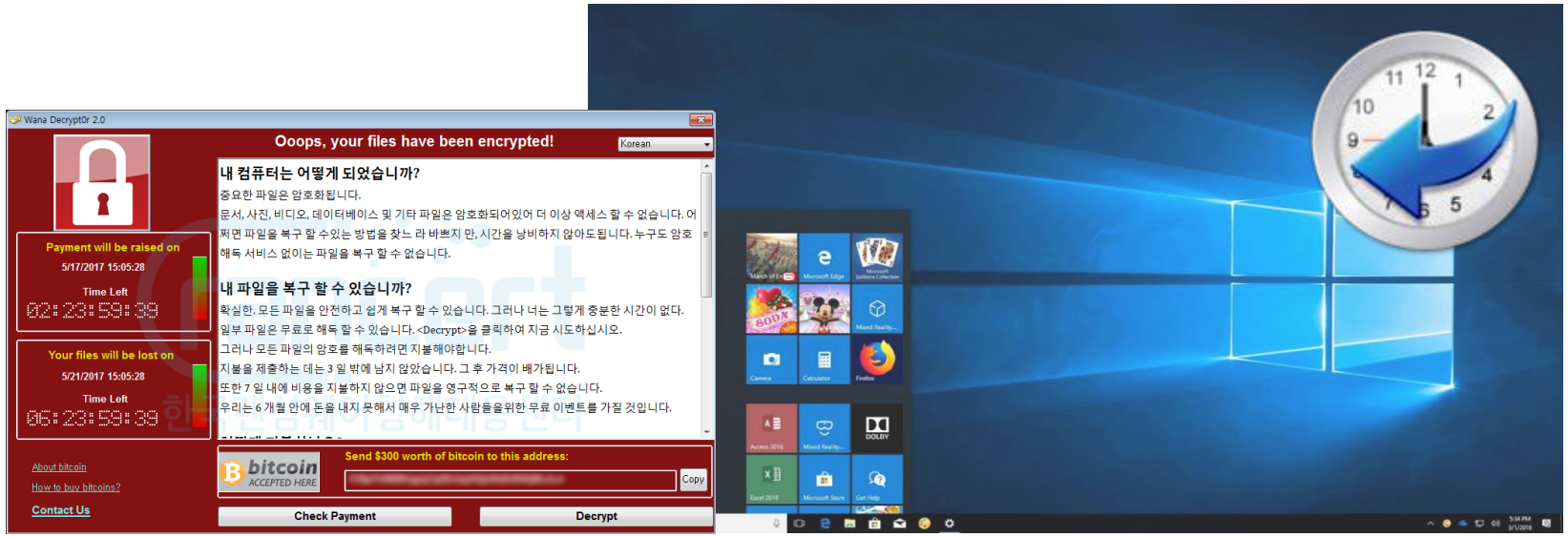


Mirror Shielding 기술 소개

1. NeuShield는 보호 필름을 구성
2. 램섬웨어는 보호필름 위에 암호화 수행
3. 원본파일은 변경되지 않음
4. 보호필름 제거로 암호화 영역을 제거

원 클릭 시스템 복원

- 의도하지 않은 시스템 구성 변경 또는 프로그램 설치 시, 시스템 복원 수행
- 악성코드 감염 시 악성코드 설치 전으로 빠른 시스템 복원을 수행
- 알려지지 않은 시스템 장애 발생 시, 정상 시점으로 시스템 복원 수행
- Microsoft 패치 오류로 부터 빠른 정상 시점으로 시스템 복원 수행



원격 시스템 / 파일 복원

- **관리자 콘솔을 통한 원 클릭 시스템 복원**
  - 컴퓨터 환경을 문제 시점 이전으로 원격 복원
  - 의도하지 않은 시스템 변경의 시점 복원
  - 악성 코드 설치 이전으로 복원

- **관리자 콘솔을 통한 원 클릭 파일 복원**
  - Mirror Shielding™ 보호필름 기술 지원
  - 기업용 보호 폴더 지정 및 관리 수행
  - 특정 시점으로 문서 및 보호 파일 복원

NeuShield 필요성

- **단말 보안 솔루션의 문제점**
  - 어떠한 보안 솔루션도 100% 단말을 보호하지 못함.
  - 악성코드 감염 시, 완벽한 치료를 보장하지 않음.

- **백업 솔루션의 문제점**
  - 백업은 대규모 구성비용과 백업 시간이 소요 됨
  - 시점 복원이 어려우며 단말에 적용되기 어려운 기술임
  - 백업용 네트워크 드라이브도 공격 대상임

- **클라우드 스토리지 및 백업의 문제점**
  - 대용량 데이터 백업 시, 과대한 비용이 소요됨
  - 외부에 주요정보가 저장되는 리스크가 발생됨
  - Cloud 스토리지도 공격 대상임

클라우드 스토리지 보호 (부가기능)

- **클라우드 스토리지 데이터 보호**
- **클라우드 스토리지 자동 탐지**
- **지원 가능한 클라우드 스토리지**
  - OneDrive Personal
  - OneDrive for Business
  - Google Drive
  - DropBox
  - Box Sync
- **별도 클라우드 스토리지 사용 시 커스트마이징 지원**

사례 분석

NeuShield®
How much is your data worth?

시스템 복원 사례

랜섬웨어 또는 악성코드 공격으로 시스템 복구

- **시스템 복원**
  - 관리자 콘솔을 통한 시스템 복원
  - 그룹별 정책 관리 지원
  - 침해 전 정상 상태로의 시스템으로의 복구 지원

- **의도하지 않은 프로그램 및 악성코드 감염 시 복원**
  - 악성코드 및 악성 플러그인 등 설치 시점 전으로 복원

- **스크린락커 및 랜섬웨어 감염 시 복원**
  - 다양한 랜섬웨어 감염 시점 전으로 복원

데이터 복구 사례

랜섬웨어 또는 악성코드 공격으로 데이터 복구

- **랜섬웨어 또는 악성코드로 인한 데이터 손상 복구**
  - 사용자 단말의 악성코드 감염 현상 확인
  - 사용자 화면 또는 관리자 콘솔을 통한 시스템 복원
  - 침해 전 정상 시점으로 시스템으로의 복원
  - 손상된 문서 등 파일 복원
  - AD 침해 등으로 지속 공격 시, 데이터 보호 및 백업 지원
- **사용자 실수로 인한 데이터 손상 복구**
  - 보관된 필름 영역 확인 후, 정상 시점 복원
- **삭제 데이터 복구**
  - 삭제된 데이터의 정상 시점 복원

관련 기술 제품 비교표

	백신솔루션	NeuShield (실시간 백업복원)	백업솔루션
안티바이러스 / 안티스파이웨어	✓		
룰 기반 분석 탐지 및 차단	✓		
개인 방화벽	✓		
호스트 침입 탐지	✓		
비정상(악성) 프로세스 행위 탐지 및 차단	✓		
실시간 데이터 보호		✓	
데이터 순간 복원		✓	
디스크 삭제 보호		✓	
부팅 레이어 보호		✓	
Resilient from malware		✓	
하드웨어 장애 복원			✓
분실 장비 데이터 복원			✓
네트워크 백업			✓
데이터 아카이빙			✓
손실 데이터 복구			✓

관련 기술 제품 비교표

NeuShield 기능 소개 및 랜섬웨어 데이터 복원 동영상

- **NeuShield 기술 소개**
  - https://www.youtube.com/watch?v=CvVqhdAYyk4
- **Ransomware 복원 영상 (사용자가 직접 복원)**
  - https://www.youtube.com/watch?v=L_lkY06GaRE
- **Ransomware 복원 영상 (보안관리자가 복원)**
  - https://www.youtube.com/watch?v=ckbfqoBFk2g&t=17s

※ 현재는 클라우드 제품이지만 금년 내 데이터센터 설치형 지원 예정

NeuShield®

How much is your data worth?

ESCARE