COHESITY

RESILIENCE EVERYWHERE

랜섬웨어 시대의 사이버 레질리언스

조직이 NIST 사이버 보안 프레임워크 2.0에 맞게 조정하면서도 사이버 공격을 견디고 그로 인한 피해를 복구하도록 Cohesity가 도움을 주는 방법.

목차

데이터 레질리언스에서 사이버 레질리언스까지

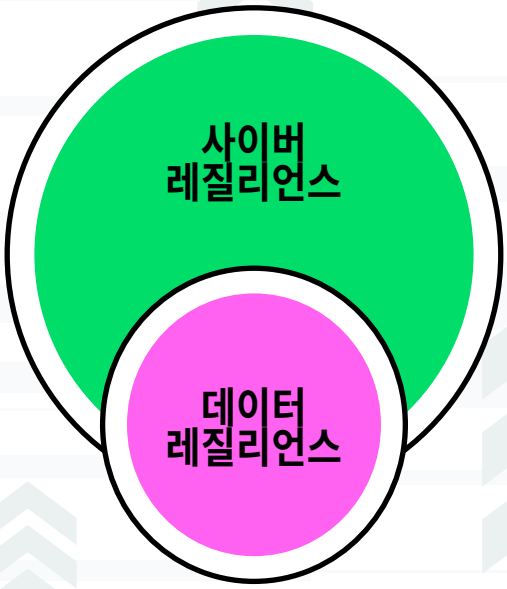
자연재해는 기업 운영에 엄청난 위협을 제기합니다. 낙뢰, 허리케인, 토네이도, 홍수 등으로 인해 심각한 피해를 입어 비즈니스가 중단될 수 있습니다. 이러한 상황에서 데이터 레질리언스 전략은 하드웨어 장애, 실수로 인한 삭제, 자연재해 등이 발생하더라도 데이터가 온전하고 액세스 가능하도록 보장합니다.

하지만 이러한 사건은 귀사를 실질적인 표적으로 삼아 지속적이고 의도적으로 공격하지는 않습니다.

이러한 사건을 사이버 위협과 비교해 보십시오. 위협 행위자는 데이터를 인질로 잡고 귀사를 마비시키기 위해 끊임없이 노력하며 새로운 도구를 활용합니다. 공격 경로는 다양한 형태를 띠며 탐지하기 어려운 경우가 많습니다.
그리고 취약점, 탈취된 계정, 그리고 기타 공격 아티팩트가 다시 환경으로 주입될 위험이 매우 높습니다. 근본 원인이 일반적으로 분명한 기존의 비즈니스 연속성 및 재해 복구 시나리오와 비교하면, 사이버 위협에 대한 대응에는 이러한 원인을 찾아내기 위한 조사가 필요하며 재발 방지를 위한 조치를 시행해야 합니다.

또한 랜섬웨어 공격에서는 보안 인프라와 핵심 증거 데이터가 사고의 영향을 받아 손상되었을 수 있으며, 그로 인해 제품 및 서비스 제공 능력에 치명적인 차질을 초래할 수 있습니다.

사이버 레질리언스를 갖춘 기업을 구축할 때 IT 및 보안 리더에게는 자연재해 또는 기술적 중단으로 인한 일반적인 중단에 대응할 때 사용되는 프로세스에 비해 더 강력하고 역동적이며 협업적인 프로세스가 필요합니다. 사이버 레질리언스는 데이터 레질리언스 관행을 기반으로 구축되며, 사이버 보안 대비, 사고 대응 계획, 직원 교육, 위협 인텔리전스 등의 요소를 포함합니다.



오늘날의 사이버 위협에는 보호 대상 데이터 자산에 대한 글로벌 가시성을 높이고 IT와 보안 실무자 간의 협업을 간소화하는 최신 솔루션이 필요합니다.

Cohesity의 최신 AI 기반 데이터 보안 솔루션은 조직이 사이버 준비태세를 강화하고 사고 대응을 가속화하며 빠르고 안전한 복구를 실행할 수 있도록 지원합니다.

COHESITY를 통해 다음을 수행할 수 있습니다.

- 모든 데이터 보호
- 데이터가 항상 복구 가능하도록 보장
- 백업 데이터의 취약점 및 위협에 대한 가시성 확보
- 공격에 대한 신속하고 효과적인 대응 및 기존의 방어를 회피하는 위협 추적
- 시스템 및 데이터를 신속하고 안전하게 복구

결과적으로, 조직은 사이버 공격에 대해 더 철저히 대비하고, 견뎌내며, 대응하고, 복구할 수 있는 더욱 강화된 사이버 레질리언스를 갖춘 기업으로 거듭나게 됩니다.

자신감과 역량 간의 모순

78%의 조직은 회사의 사이버 레질리언스 전략에 대해 자신감을 가지고 있습니다[1]. 이러한 자신감이 구체적인 역량에 의해 뒷받침된다면 일반적으로 좋은 신호라고 말할 수 있습니다. 하지만 데이터에 따르면 전략적 의도와 실제 역량 사이에는 상당한 괴리가 있습니다.

98%는 공격 발생 후 1일 이내에 데이터 복구 및 비즈니스 프로세스 복원을 목표로 합니다[2].

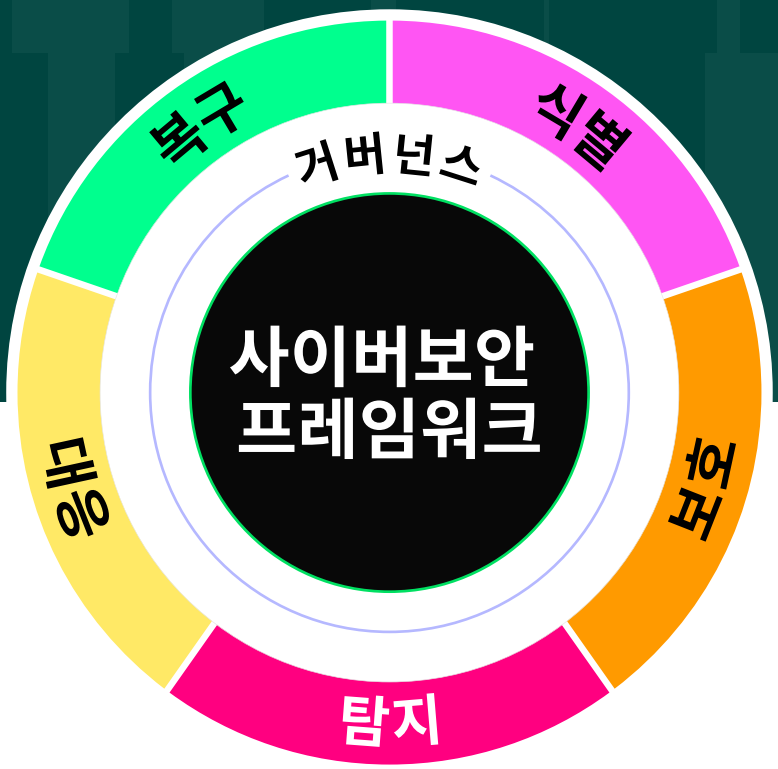
그러나 **2%**만이 이를 달성할 수 있습니다[3].

다행히도 Cohesity는 전 세계 고객들이 신속하게 운영을 재개하고 공격의 영향을 완화할 수 있도록 지원하는 프로세스와 도구를 갖춘 입증된 플레이북을 제공합니다.

[1-3] **Cohesity 글로벌 사이버 레질리언스 보고서 2024**

6가지 핵심 요소 사이버 레질리언스를 갖춘 기업을 구축하기 위한

Cohesity의 데이터 보안 솔루션은 조직이 위험을 더 잘 이해하고 관리하며 완화하는 동시에, NIST 사이버 보안 프레임워크의 주요 기능인 거버넌스, 식별, 보호, 탐지, 대응 및 복구에 따라 사이버 레질리언스를 강화할 수 있도록 지원합니다.



거버넌스
- 규제 요건을 이해하기 위해 백업 데이터 분류
- 사이버 보험 프레임워크 준수와 제3자 데이터 관련 기타 계약 의무 사항 지원

식별
- 영향을 주지 않고 취약한 시스템의 취약점 스캔
- 백업되지 않은 중요 시스템 식별
- 향후 사고 대응 및 BC/DR 활동 개선
- 조직의 사이버 레질리언스 프로그램 개선 영역 파악

보호
- 대규모로 엔터프라이즈 데이터 보호
- 공격으로부터 백업 보호
- 백업 및 복원 테스트

탐지
- 랜섬웨어 암호화, 와이퍼 공격 및 악의적인 내부자 탐지
- 침해 지표를 선제적으로 추적하여 회피 기법에 대한 방어력 확보
- 상관관계 분석을 위해 보안 탐지 정보를 SOC 도구로 전송
- 더 많은 포렌식 아티팩트를 캡처하고 EDR/XDR 신호를 기반으로 증분 스냅샷 생성을 실행
- NAS 서버에서 멀웨어 식별

대응
- Cohesity CERT(사이버 이벤트 대응팀)를 가동하여 대응 속도를 높이고 안전한 복구를 보장
- 대응 도구 및 AD를 신뢰할 수 있는 상태로 복원하고 신속한 액세스 제공
- 대응 및 복구를 위한 클린룸을 신속하게 구축
- 영향을 받는 추가 시스템을 식별하기 위해 아티팩트를 수동으로 추적
- 과거 파일시스템 포렌식 검사
- 공격에서 악용된 과거 취약점 이해
- 규제기관, 파트너 및 영향을 받는 데이터 주체에게 통지해야 하는 규제 및 규정준수 의무 이행 지원

복구
- 시스템 및 데이터 복구를 통해 위협 완화

1.

거버넌스로 규제 요건 파악 및 위험 대응을 위한 백업 데이터 관리

오늘날의 데이터 환경은 과도하게 채워진 차고와 같이 무질서하게 확산되고 있어 민감한 데이터의 위치를 찾고 이를 적절하게 보호하기가 점점 더 어려워지고 있습니다. 이러한 가시성 부족으로 인해 데이터 노출 및 규제 미준수의 위험도 높아집니다.

이러한 위험의 관리 목적으로 조직은 법적 및 규제 요건(예: HIPAA, CCPA 및 GDPR)을 충족할 뿐만 아니라 효과적인 사이버 보안 거버넌스를 통해 강력한 내부 통제를 입증해야 합니다. 점점 더 이러한 통제는 단순히 규정준수에만 국한되지 않고 사이버 보안 보험 가입에 필수 요소가 되고 있습니다.

사이버 공격의 빈도와 심각도가 증가함에 따라 사이버 보험은 중요한 위험 이전 전략이 되었습니다. 이 보험은 데이터 복구, 법적 수수료 및 기타 사고 후 여파와 같은 재정적 손실을 보장하는 데 도움이 됩니다. 그러나 보험사는 고객에게 점점 더 많은 것을 요구하고 있으며, 보험증권을 발행하거나 갱신하기 전에 강력한 데이터 보호 및 보안 통제의 증거를 요구하고 있습니다.

이러한 요구 사항에 선제적으로 대응하기 위해 당사는 조직이 다음을 수행할 수 있도록 지원합니다.

민감한 데이터 파악 및 분류.
당사의 변경 불가능한 무제한 백업 스냅샷을 사용하여 환경 전반에서 민감한 데이터를 검색하고 분류합니다. 당사의 내장된 데이터 분류 엔진은 수백 개의 분류기와 AI 기반 알고리즘을 사용하여 규제 대상 및 고위험 정보를 식별 및 라벨링하여, 디지털 자산 인벤토리를 작성하고 적절한 보안 정책을 적용하는 데 도움을 줍니다.

사이버 보험 요구사항 준수와 제3자 데이터 관련 기타 계약 의무 사항을 지원합니다. 당사 플랫폼은 모범사례 통제를 구현하여 보험사 및 규제기관의 높아지는 기대치를 충족하도록 지원합니다.

- 운영 네트워크와 분리된 독립적인 백업 환경
- 전용 클라우드 백업 서비스
- 저장된 데이터와 전송 중인 데이터의 암호화
- 변경 불가능한 백업 스냅샷
- 별도의 자격 증명을 사용하는 역할 기반 액세스
- 내부 및 외부 액세스 모두에 MFA 실행
- 멀웨어가 없음을 보장하는 복원 전 백업 무결성 테스트

2.

사이버 레질리언스 위험 **식별**

사이버 보안 위험을 효과적으로 관리하려면 백업 시스템을 비롯한 IT 환경 전반의 취약점을 명확하게 이해해야 합니다. 또한 그러한 효과적인 관리에는 분류에 따라 데이터 자산의 보호 우선순위를 정하고, 보안 테스트, 훈련, 그리고 과거 사고 대응 및 복구 노력에서 학습한 교훈을 통해 지속적으로 개선하는 작업이 수반됩니다.

CyberScan
Powered by tenable

영향을 주지 않고 취약한 시스템에서 취약점을 스캔합니다.

Tenable 기반의 Cohesity CyberScan을 사용하여 백업 스냅샷에서 취약점 스캔을 실행하고 운영 시스템에 미치는 영향을 방지합니다.

백업되지 않은 중요한 시스템을 식별합니다.

Cohesity를 선호하는 데이터 보안 태세 관리(DSPM) 벤더와 통합하는 것은 숨겨진 사이버 레질리언스 위험을 발견하는 강력한 방법입니다. DSPM 솔루션은 다양한 클라우드 플랫폼에서 알려진 데이터 저장소와 잊혀진 데이터 저장소 모두에 대한 가시성을 제공하고, 데이터를 분류하여 민감한 정보를 식별하고, 노출 위험을 결정합니다.

민감한 데이터의 대부분은 이미 Cohesity Data Cloud 및 기존 백업 정책에 의해 보호되고 있을 수 있지만, 상당한 격차가 남아 있는 경우가 많습니다. 바로 이 지점이 DSPM과의 통합이 필요한 부분입니다.

DSPM의 인사이트를 Cohesity와 결합하면 백업되지 않은 중요한 시스템과 데이터를 식별하고 백업 정책을 신속하게 확장하여 이를 보호 대상으로 포함하는 방법으로 보안을 강화하고 위험을 줄일 수 있습니다.

기타 주요 운영상의 이점은 다음과 같습니다.

- ☑ Cohesity에서 백업한 데이터 저장소 내 데이터의 중요도를 기반으로 백업 주기 및 보존 기간 최적화
- ☑ 데이터의 업무상 중요도에 따라 데이터 복원의 우선순위 지정
- ☑ 영향을 받은 데이터에 대한 "적시(just-in-time)" 분석을 통해 사고 대응 간소화(대응 기능에서 자세히 다룸)

DSPM과 Cohesity AI 기반 데이터 보안 플랫폼을 결합하면 멀티 클라우드 환경 전반에서 보안 태세를 개선할 수 있습니다.

2.

사이버 레질리언스 위험 **식별**

향후 사고 대응 및 BC/DR 활동을 위한 개선 사항을 파악합니다.

파괴적 사이버 공격 레질리언스 성숙도 모델(DCARMM)을 활용하여 **조직의 현재 대응 및 복구 역량을 평가하고 업계 모범 사례를 향한 경로를 계획합니다.**

Cohesity에서 개발한 이 모델은 SANS 6단계 사고 대응 프로세스, RE&CT, MITRE D3FEND, 그리고 NIST SP 800-61과 같은 주요 프레임워크에 맞게 조정되어 있으므로, 조직은 다음을 수행할 수 있습니다.

- 파괴적 사이버 공격에 대한 준비태세 평가
- 업계 동료 또는 지역 표준을 기준으로 레질리언스 성숙도 벤치마킹
- 격차 파악 및 지속적인 개선을 위한 로드맵 구축

귀사는 이를 사이버 레질리언스 대비 역량을 강화하고 인력, 프로세스 및 기술에 대한 투자에 지침을 제공하는 전략적 도구로 활용할 수 있습니다.

제3자 평가를 활용하여 사이버 레질리언스 프로그램에서 개선이 필요한 영역을 식별합니다.

Cohesity CERT(사이버 이벤트 대응팀) 사이버 레질리언스 컨설팅 서비스는 다음 사고가 발생하기 전에 사이버 레질리언스 역량을 강화하도록 설계된 전문가 주도의 사전 예방적 서비스를 제공합니다. DCARMM을 기반으로 한 심층적인 레질리언스 평가부터 맞춤형 실행 계획에 이르기까지, CERT는 격차를 식별하고 위험을 줄이며 지속적인 방어를 구축하는 데 도움이 됩니다.

3.

대규모로 엔터프라이즈 데이터 보호

데이터 자산의 규모와 다양성으로 인해 데이터 자산 환경이 점점 더 복잡해짐에 따라 사이버 공격이나 데이터 중단으로 인해 비즈니스에 심각한 영향을 줄 위험도 증가합니다.

단일 보안 플랫폼을 사용하여 온프레미스, 클라우드 및 SaaS 환경 전반의 모든 데이터 소스를 백업하면 잠재적 공격의 영향을 극도로 최소화하면서 데이터 보호를 확장할 수 있습니다.

공격 표면 축소

많은 환경은 단편화된 단일기능 제품을 기반으로 설계됩니다. 이와는 대조적으로 Cohesity는 모든 백업 및 복구 구성 요소를 단일 글로벌 플랫폼에 통합합니다. 여기에는 데이터 소스 전반에 걸친 글로벌 가변 길이 중복 제거와 압축이 포함되어 공격 표면을 더욱 축소합니다.

데이터 자산 환경 전반에서 데이터 보호 확장

Cohesity Data Cloud는 하이퍼스케일 아키텍처를 기반으로 설계되었기 때문에 IT 관리자는 Cohesity 클러스터를 무한히 확장하고 성능에 영향을 주지 않고 무제한 스냅샷과 클론을 저장할 수 있습니다. 전례 없는 데이터 중복 제거는 훨씬 저렴한 비용으로 더 많은 데이터를 저장할 수 있도록 보장할 뿐만 아니라, 특정 시점의 스냅샷을 즉시 구동하여 포렌식 조사를 지원할 수 있습니다.

3.

보호

공격으로부터 백업 보호

Cohesity는 제로 트러스트(Zero Trust) 원칙을 사용하여 백업을 표적으로 하는 랜섬웨어의 위험과 의도하지 않거나 악의적인 데이터 삭제의 위험을 최소화하는 다층 보안 접근 방식을 채택했습니다.

- **변경 불가능한 읽기 전용 상태의 스냅샷** Cohesity Data Cloud는 백업 스냅샷을 변경할 수 없는 상태로 저장하는 방법으로 사이버 공격을 막기 위해 특별히 구축되었습니다. 스냅샷은 외부 애플리케이션에 마운트되지 않으며, 승인 없이는 변경 불가능한 백업 스냅샷의 수정 또는 삭제가 불가능합니다.
- **DataLock 정책** – 백업용 WORM(Write-once-read-many) 기능을 통해 특정 역할의 사용자가 선택한 작업에 대해 변경 불가능한 DataLock 정책을 설정할 수 있습니다.
- **다단계 인증(Multifactor Authentication, MFA)** Cohesity 백업에 액세스하는 모든 사람은 두 가지 형태의 검증을 사용하여 인증해야 합니다. Cohesity는 다중 인증 제공업체를 지원하므로, 사이버 사고로 인해 주 서버가 영향을 받더라도 귀사는 강력한 인증 체계를 유지할 수 있습니다.
- **데이터 암호화** – Cohesity는 소프트웨어 기반 FIPS 검증, AES-256 표준 암호화를 통해 전송 중인 데이터와 저장 시 데이터를 보호합니다.
- **역할 기반 액세스 제어 및 최소 권한 -** Cohesity는 IT 직원이 각 개인에게 특정 작업을 수행하는 데 필요한 데이터에 대해 최소 수준의 액세스 권한을 부여할 수 있도록 하여 무단 액세스 위험을 줄입니다.
- **직무 분리** – Cohesity Quorum을 사용하면 내부자 위협과 자격 증명 도난으로부터 데이터를 보호하기 위해 모든 루트 수준 또는 중요한 시스템 변경은 2명 이상이 승인해야 합니다.

중요한 비즈니스 데이터 격리

온프레미스 또는 퍼블릭 클라우드에서 데이터를 변경 불가능한 다른 Cohesity 클러스터에 자동으로 복제하여 변경 불가능한 추가 데이터 사본을 항상 사용할 수 있습니다.

백업 및 복원 테스트

사이버 복구 오케스트레이션을 사용하면 복구 워크플로우를 자동화하고 운영 외 환경에서 엄격한 테스트를 지원하는 맞춤형 청사진을 생성할 수 있습니다. 이러한 방식으로 귀사는 사이버 사고에 대한 대비를 강화하고 복구를 간소화하여 가동 중단 시간과 데이터 손실을 줄일 수 있습니다.

4.

잠재적인 사이버 공격 및 침해 **탐지**

사이버 범죄자는 데이터 환경의 취약점을 찾아 악용하기 위해 수단과 방법을 가리지 않습니다. 백업 데이터 또는 사용자 행동에서 비정상적인 변화를 조기에 탐지하는 것은 공격의 영향을 최소화하는 데 핵심적 요소입니다.

여기가 바로 AI가 중요한 역할을 하는 곳입니다. AI는 인간이 알아차리지 못할 수 있는 미묘한 데이터 활동 패턴을 식별합니다. 또한 EDR/XDR 도구로 탐지되는 랜섬웨어 공격이 시작될 때 중요한 데이터의 백업 스냅샷을 자동으로 캡처하여 데이터 손실을 줄이고 복구를 가속화할 수 있습니다.

랜섬웨어 암호화, 와이퍼 공격 및 악의적인 내부자를 탐지합니다.

예측 분석을 사용하여 운영을 선제적으로 모니터링, 모델링 및 최적화하여 추세를 평가합니다. Cohesity의 AI 기반 알고리즘은 패턴을 설정하고 시간이 지남에 따라 스냅샷 전반의 데이터에서 이상 징후를 지속적으로 스캔합니다.

이상 징후가 탐지되면 IT 관리자와 Cohesity 지원팀에 알림을 보내 문제 해결을 신속하게 진행합니다.

이를 통해 보안팀은 랜섬웨어 또는 와이퍼 공격, 심지어 악의적인 내부자의 존재를 나타낼 수 있는 행동에 대한 인사이트를 얻을 수 있습니다.

이러한 경고는 이벤트 상관관계 분석 도구(예: SIEM)를 사용하여 귀사의 보안 운영 센터와 공유할 수도 있습니다.

백업 데이터에서 위협을 선제적으로 추적합니다.

랜섬웨어 등의 사이버 공격은 멀웨어를 숨기기 위해 기만적인 전술을 사용합니다. Cohesity 위협 헌팅의 지원을 통해 랜섬웨어 등의 사이버 공격의 최신 변종을 식별하는 AI 기반 위협 탐지를 사용하여 탐지하기 어려운 위협을 찾을 수 있습니다.

Cohesity의 광범위한 행동 패턴 라이브러리는 최신 위협을 포함할 수 있도록 자주 업데이트됩니다.

또한 Cohesity는 CrowdStrike Falcon Adversary Intelligence와 같은 상용 위협 인텔리전스 피드를 지원하며, 다른 제3자 소스의 YARA 형식 IOC를 수집하여 활용합니다.

4.

잠재적인 사이버 공격 및 침해 **탐지**

상관관계 분석을 위해 보안 탐지 정보를 SOC 도구로 전송.

IOC, 백업 데이터 변경의 이상 징후, 민감한 데이터 경고와 같은 중요한 보안 탐지를 SOC 도구(예: SIEM, SOAR)로 전송하여 신속한 위협 탐지 및 대응을 지원합니다.

Cohesity는 CrowdStrike, Splunk, Microsoft와 같은 주요 플랫폼과 통합되어 텔레메트리를 원활하게 공유합니다. 이를 통해 귀사의 SOC는 인프라 전반의 대용량 로그 데이터에 대한 Cohesity 인사이트를 집계, 분석 및 상관관계 분석을 수행할 수 있습니다.

결과물: 가시성을 강화하고 잠재적 랜섬웨어 또는 기타 사이버 위협의 탐지를 가속화하는 통합된 실시간 뷰가 제공됩니다.

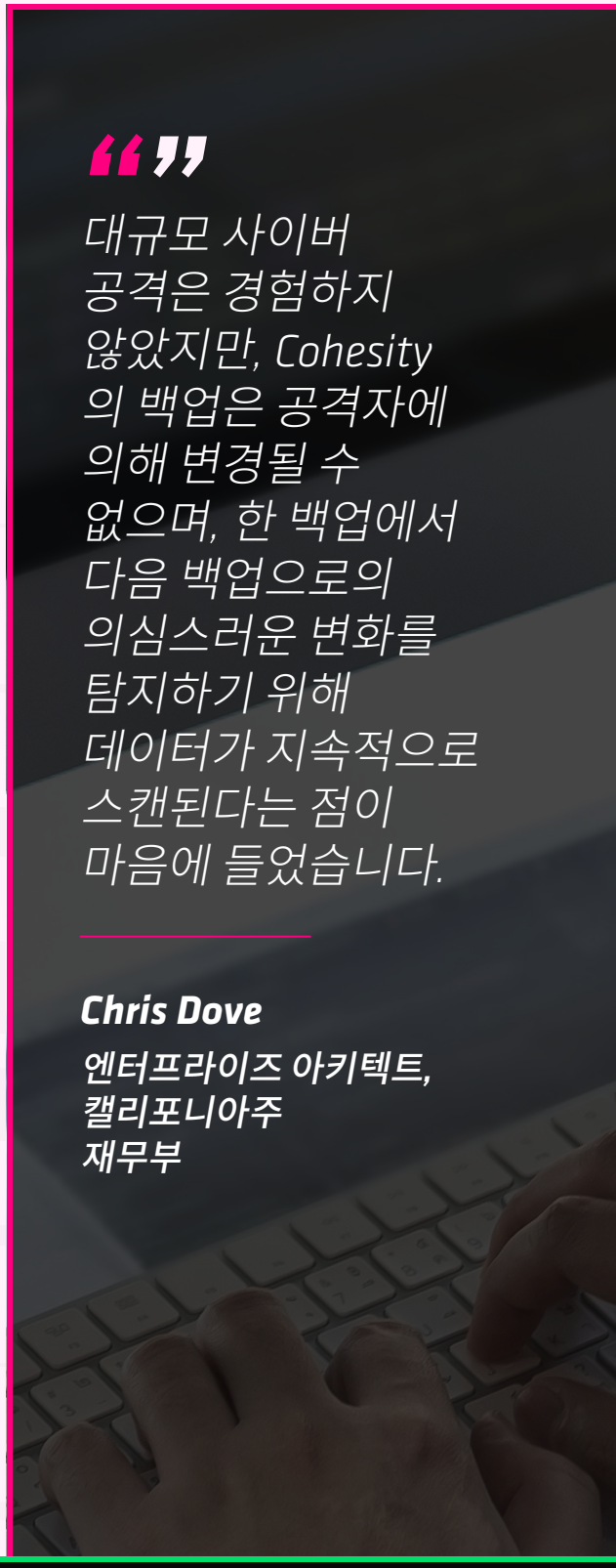
더 많은 포렌식 아티팩트를 캡처하고 EDR/XDR 신호를 기반으로 증분 스냅샷 생성을 실행합니다.

Cohesity Data Cloud와 Cisco XDR의 통합을 통해 Cisco XDR이 랜섬웨어 공격을 탐지하는 순간 중요한 데이터의 백업을 자동화하여 복구 시점 목표(RPO)를 줄이고 비즈니스 중단을 최소화할 수 있습니다.

또한 이러한 백업 스냅샷은 사고 대응자에게 파일 시스템 변경에 대한 보다 세분화된 맥락을 제공하여 포렌식 조사를 더 빠르고 효과적으로 수행할 수 있게 합니다.

NAS 서버에서 멀웨어를 식별합니다.

백업 데이터 변경 속도를 모니터링하여 잠재적인 랜섬웨어 공격을 탐지하는 것 외에도, Cohesity는 비정형 파일 및 객체 데이터에서 파일 수준 이상 징후를 고유하게 탐지하고 이에 대해 경고할 수 있습니다.



"대규모 사이버 공격은 경험하지 않았지만, Cohesity의 백업은 공격자에 의해 변경될 수 없으며, 한 백업에서 다음 백업으로의 의심스러운 변화를 탐지하기 위해 데이터가 지속적으로 스캔된다는 점이 마음에 들었습니다.

Chris Dove
엔터프라이즈 아키텍트, 캘리포니아주 재무부

5.

사이버 사고에 신속하게 **대응**

사이버 사고가 탐지되면 조직은 신속하게 대응하여 해당 사고를 억제하고 피해 범위를 조사하며 위험을 완화하여 안전한 복구를 가능하게 해야 합니다.

랜섬웨어, 와이퍼 공격과 같은 중요한 사고는 고객에게 제품과 서비스를 제공하는 데 필요한 시스템과 해당 시스템 관리에 중요한 내부 IT 시스템을 방해할 수 있습니다. 이러한 시나리오에는 표준 데이터 침해 프로토콜을 넘어서는 보다 체계적인 다른 워크플로우가 필요합니다.

위협을 조사 및 완화하지 않고 서둘러 복구하면 근본적인 취약점이 그대로 남아 재감염과 가동 중단 시간 연장의 위험이 있습니다.

이러한 공격으로부터 안전하게 복구하려면 사고 발생 경위와 그 근본 원인을 시정하는 방법을 파악해야 합니다. 이러한 절제된 접근 방식은 모든 모범사례 사이버 보안 사고 대응 프레임워크의 핵심입니다.

1. **Cohesity CERT를 가동하여** 사고 대응 초기에 신속한 전문가 지원을 받으십시오. Cohesity 팀은 위협 확산을 차단하고, 가동 중단 시간을 최소화하며, 백업 인프라에 대한 포렌식 분석을 지원하고, 규제 준수 및 침해 알림 요구 사항을 지원하며, 운영 환경의 안전한 복구를 촉진합니다.

2. **대응 도구를 신뢰할 수 있는 상태로 복원하고 신속한 액세스를 제공합니다.** 사이버 공격이 발생하고 비즈니스가 중단되면 낭비할 시간이 없습니다. 신속한 대응이 매우 중요하며, **Digital Jump Bag™**을 사용하면 즉시 조치를 취할 수 있습니다.

   사고에 대비해서 이상적으로 준비된 디지털 점프백은 효과적인 대응을 시작하는 데 필요한 도구, 소프트웨어, 구성 파일 및 문서에 신속하게 액세스할 수 있는 보호되고 신뢰할 수 있는 저장소입니다. 공격자의 손이 닿지 않는 금고에 보관되는 이 데이터는 Cohesity 클린 룸 솔루션 전체의 기반이 되어 사고 대응의 핵심 단계를 지원하고 안전하고 확실한 복구를 가능하게 합니다.

3. **클린 AD(Active Directory) 인프라를 복원합니다.** AD만큼 비즈니스에 중요하거나 더 많이 표적이 되는 시스템은 별로 없습니다. 사고 대응 초기에는 다른 대응 도구를 다시 온라인으로 전환하기 전에, 그리고 무엇보다 AD를 운영 환경으로 복원하기 전에 AD 환경을 철저히 조사하고 정리하는 것은 필수적입니다. 이 단계를 건너뛰면 공격자가 다시 침입할 수 있어, 복구 노력을 저해하고 업무 중단 상황이 장기화될 수 있습니다.

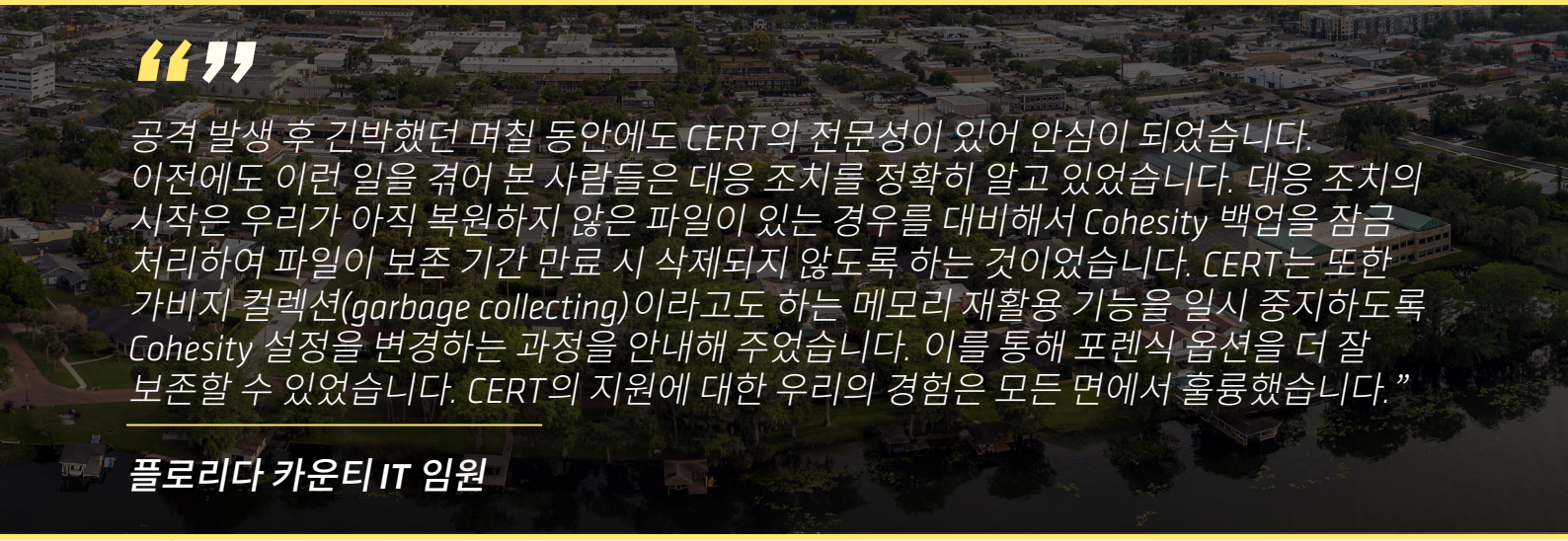
   Semperis가 지원하는 Cohesity Identity Resilience를 사용하면 AD를 최대 90% 더 빠르게 신뢰할 수 있는 상태로 복원할 수 있습니다.

5.

사이버 사고에 신속하게 **대응**

4. **대응 및 복구를 위한 클린룸을 신속하게 구축합니다.** 클린룸은 분석가와 조사관이 포렌식 조사를 수행하고, 공격에서 악용된 취약점을 파악하며, 감염된 데이터가 운영 환경에 다시 유입되지 않도록 하는 신뢰할 수 있는 환경으로 구현되어야 합니다.

5. **영향을 받는 추가 시스템을 식별하기 위해 아티팩트를 수동으로 추적합니다.** Cohesity 위협 추적 기능은 귀사 인프라 전반에서 IOC를 탐지합니다. 심지어 피해 확산을 막기 위해 시스템이 격리된 상태에서도 탐지가 가능합니다. 이 기능은 기존의 엔드포인트 보안 도구가 탐지를 무력화하거나 지연시킬 수 있는 일반적인 방어 회피 기술에 대해 레질리언스를 갖추고 있습니다.



"공격 발생 후 긴박했던 며칠 동안에도 CERT의 전문성이 있어 안심이 되었습니다. 이전에도 이런 일을 겪어 본 사람들은 대응 조치를 정확히 알고 있었습니다. 대응 조치의 시작은 우리가 아직 복원하지 않은 파일이 있는 경우를 대비해서 Cohesity 백업을 잠금 처리하여 파일이 보존 기간 만료 시 삭제되지 않도록 하는 것이었습니다. CERT는 또한 가비지 컬렉션(garbage collecting)이라고도 하는 메모리 재활용 기능을 일시 중지하도록 Cohesity 설정을 변경하는 과정을 안내해 주었습니다. 이를 통해 포렌식 옵션을 더 잘 보존할 수 있었습니다. CERT의 지원에 대한 우리의 경험은 모든 면에서 훌륭했습니다."

플로리다 카운티 IT 임원

6. 과거 파일시스템에 대해 포렌식 검사를 수행합니다. Cohesity의 데이터 보호를 사용하면 UI 및 API를 통해 변경 불가능한 스냅샷의 전체 시계열에 액세스할 수 있으므로 대응자는 보존된 백업 데이터 전반에서 상세한 파일 수준 포렌식 조사를 수행할 수 있습니다.

7. **공격에서 악용된 과거 취약점을 파악합니다.** Cohesity CyberScan 솔루션을 사용하면 백업 스냅샷에서 알려진 취약점을 스캔할 수 있습니다. 이를 통해 보안팀은 시스템이 격리로 인해 이용할 수 없거나, 지워졌거나, 침입 후 적대세력에 의해 패치가 적용된 경우에도 공격 중에 취약점을 식별할 수 있습니다.

8. **규제기관, 파트너 및 영향을 받는 데이터 주체에게 통지해야 하는 규제 및 규정준수 의무 이행을 지원합니다.** Cohesity AI 기반 데이터 분류는 백업을 스캔하여 민감하고 규제 대상인 데이터를 식별함으로써, 중요 데이터 저장소가 암호화되거나 삭제되는 파괴적인 사이버 공격에서도 조직이 규제 요구사항을 충족할 수 있도록 지원합니다. 또한 Cohesity 클린룸 솔루션의 일부로 사고 관리에 필요한 커뮤니케이션 기능을 복원하는 작업도 지원합니다. 이해 관계자에게 통지하기 위한 커뮤니케이션 템플릿을 디지털 점프백에 보관하여 빠르게 액세스할 수 있습니다.

6.

시스템 및 데이터를 안전하게 **복구**

사고 대응의 복구 단계는 위협을 철저히 근절하는 것을 지원하여 재감염을 방지하고 향후 유사한 공격 가능성을 줄여야 합니다.

Cohesity 클린룸 솔루션을 사용하면 기존 시스템을 복구 및 정리하든 처음부터 다시 구축하든 원하는 복구 전략을 유연하게 선택할 수 있습니다.

이 솔루션은 신속한 볼륨 복구를 지원하므로, 위협 근절을 위해 완화 조치를 시행하기 전에 전체 파일 시스템을 복구할 수 있습니다. 또한 신뢰할 수 있는 소프트웨어 이미지와 검증된 정상 구성에 기반하는 신속한 재구축을 지원합니다.

"우리 조직은 심각한 랜섬웨어 공격으로 전체 인프라가 사실상 마비되었습니다. Cohesity를 통해 시스템과 파일 공유를 복구하고, 안전성을 확인한 후, 애플리케이션을 다시 온라인 상태로 전환할 수 있었습니다.

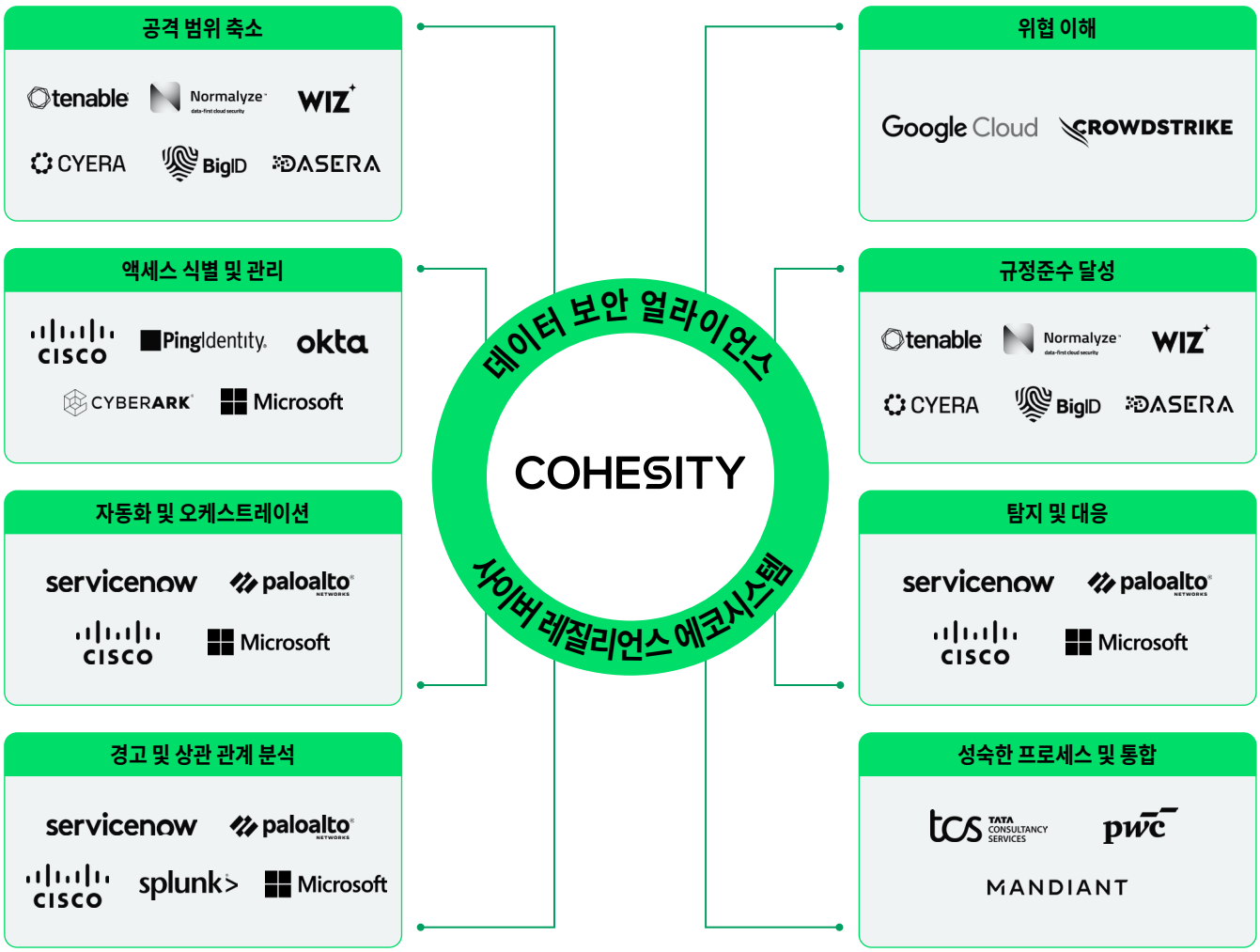
Cohesity는 말 그대로 수백 시간의 작업을 절약해 주었으며, 몸값을 지불하지 않도록 막아 주었습니다. 우리가 아직 일자리를 갖고 있고 지역사회에 제 기능을 하는 병원이 남아있는 이유는 Cohesity 도입이 큰 성과를 거두었기 때문입니다."

Sam Stewart
Sky Lakes Medical Center
네트워크 시스템 분석가

파트너십을 통한 사이버 레질리언스 강화

사이버 레질리언스는 협력이 중요한 역할을 하는 팀 스포츠입니다. 단일 공급업체의 솔루션만으로는 사고 전체를 조사하고 시정 조치를 취할 수 없습니다.

이것이 바로 우리가 데이터 보안 얼라이언스(Data Security Alliance)라는 사이버 복구 위험을 줄이고, 보안 운영 센터의 효율성을 높이며, 이미 보유하고 있는 도구를 사용하여 더 많은 데이터 자산 환경을 보호하는 데 도움이 되는 선도적인 보안 및 사이버 복구 기업의 에코시스템을 설립한 이유입니다.



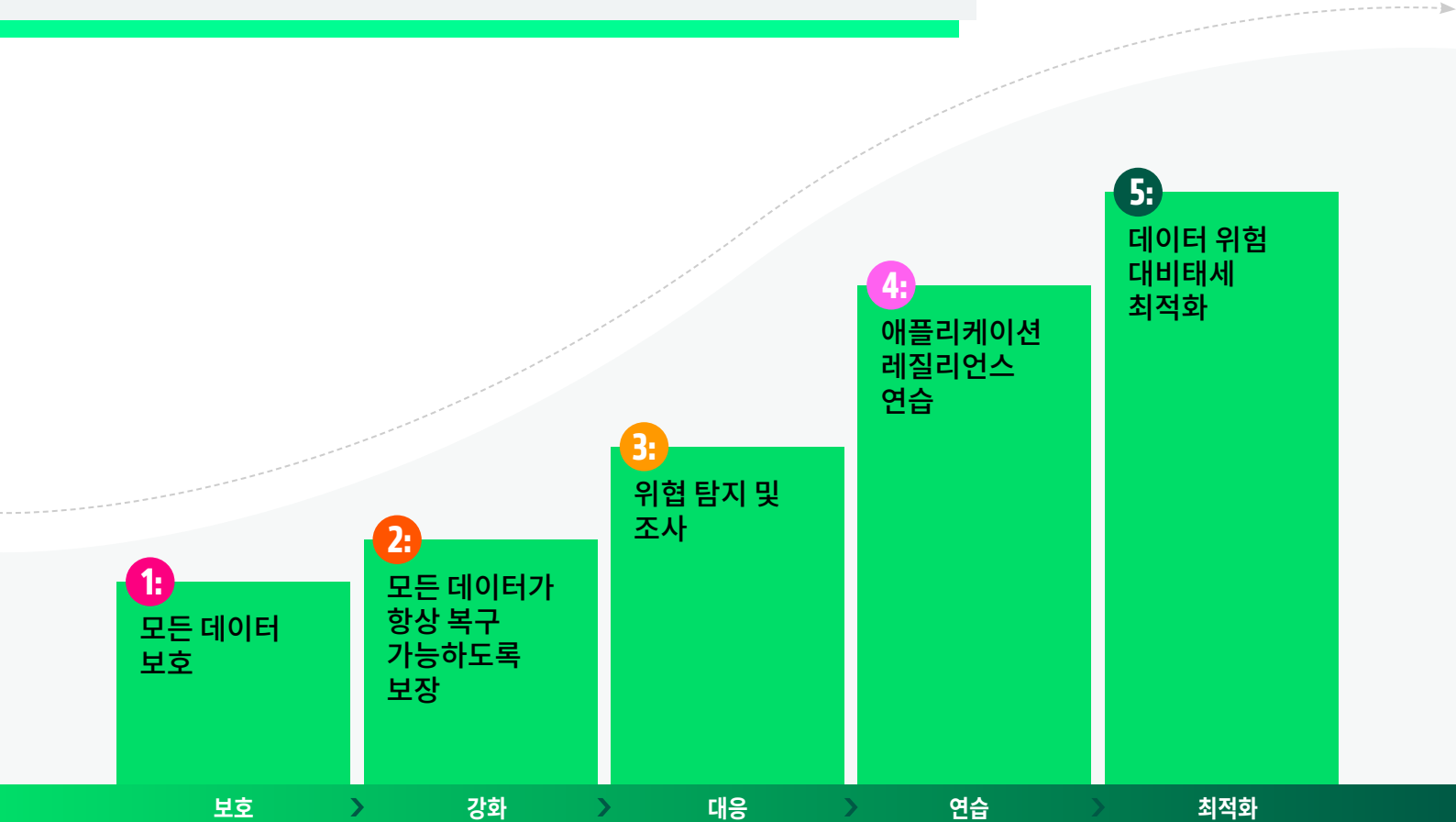
다음 단계

귀사에 적용할 수 있는...

Cohesity 사이버 레질리언스의 5단계

사이버 레질리언스를 갖춘 기업을 구축하기 위한 6가지 핵심 요소와 NIST 사이버 보안 프레임워크(CSF)의 각 단계를 지원하는 방법을 살펴보았습니다. 이제 이러한 인사이트를 실행에 옮길 시간입니다.

시작하는 데 도움을 주기 위해 Cohesity에서는 사이버 대응 및 복구를 위한 업계 모범사례에 부합하는 **5단계 사이버 레질리언스 플레이북**을 개발했습니다. Cohesity Data Cloud 및 서비스를 사용해 구체적이고 반복 가능한 작업을 구현하는 방법을 보여주는 실용적인 가이드입니다. 각 단계는 NIST 핵심 기능의 결과물을 도출하는 데 도움이 됩니다.



Cohesity 사이버 레질리언스의 *5단계*

1. 전체 데이터 보호

NIST CSF 준수: *보호*

엔터프라이즈 규모로 데이터가 어디에 있든 보호하여 레질리언스를 구축합니다. Cohesity Data Cloud는 VM, SaaS 앱, 데이터베이스, NAS 환경 등을 포함한 **1,000개 이상의 데이터 소스**를 지원하는 동시에 글로벌 중복 제거 및 압축을 통해 비용과 위험을 줄입니다.

이러한 접근 방식을 통해 IT의 스토리지 비용을 절약하고 보안팀의 공격 표면을 축소할 수 있습니다. 이러한 효과는 더 강력한 보호 기능을 위한 두 가지 중요한 요소입니다.

2. 데이터 복구 가능 여부 확인

NIST CSF 준수: *보호 및 복구*

보호 능력은 복구 능력에 의해 규정됩니다.

- **플랫폼 강화:** MFA, 역할 기반 액세스 제어 및 쿼럼과 같은 방어 수단을 활성화하여 직무 분리를 시행하고 내부자 위험을 최소화합니다.
- **중요 데이터 격리:** Cohesity 관리형 클라우드 볼트 또는 자가 관리형 솔루션으로 제공되는 Cohesity의 사이버 볼트를 사용하여 안전하고 복구 가능한 사본을 생성합니다.

이러한 단계를 통해 가장 중요한 순간에 신뢰할 수 있는 사본을 복원할 수 있습니다.

3. 위협 탐지 및 조사

NIST CSF 준수: *식별 및 탐지*

레질리언스는 조기 탐지에 달려 있습니다. Cohesity를 통해 다음을 수행할 수 있습니다.

- ☑ 취약점을 식별합니다.
- ☑ 랜섬웨어 및 멀웨어 지표가 있는지 백업을 지속적으로 스캔합니다.
- ☑ 백업 데이터에서 특정 위협을 추적하여 회피 기법에 대한 방어력을 확보합니다.
- ☑ 발견 내용을 SIEM/SOAR 도구로 보냅니다.

결과물: 위협을 더 빨리 포착하고 대응팀이 더 신속하게 조치를 취합니다.

4. 애플리케이션 복원 연습

NIST CSF 준수: *대응 및 복구*

마지막 단계 알아보기 >

공격이 발생할 때까지 복구 계획 테스트를 미루지 마십시오.

- **정기적 예행연습:** 복구 프로세스와 준비태세를 검증하기 위해 모의 공격 상황에서 복구 계획을 연습합니다.
- **자동화된 복구:** Cohesity 플랫폼의 복구 오케스트레이션을 사용하여 워크플로우를 간소화하고 사고 발생 후 시스템 복원을 가속화합니다.

이 단계에서는 복구를 수동적이고 스트레스가 많은 프로세스에서 반복 가능하고 충분히 연습된 플레이북으로 전환합니다.

Cohesity 사이버 레질리언스의 *5단계*

5. 데이터 위험 대비 태세 최적화

NIST CSF 준수: *거버넌스, 식별 및 대응*

- **데이터 보안 거버넌스 강화:** Cohesity 데이터와 데이터 분류 기능을 사용하여 귀사가 보유한 데이터를 파악하고, 그 위험 수준을 평가하며, 적절한 보안 통제를 적용합니다.
- **백업되지 않은 중요 시스템 식별:** 백업을 포함하여 전체 데이터 자산 환경 전반에서 민감한 데이터를 식별하고 적절하게 보호되도록 합니다. 선호하는 데이터 보안 태세 관리(DSPM) 도구와 Cohesity 플랫폼의 기능을 결합하여 이 프로세스를 간소화할 수 있습니다.
- **사고 영향 평가:** 침해가 발생하는 경우, 특히 중요한 데이터 저장소가 암호화되거나 삭제된 경우, 백업을 사용하여 어떤 민감한 규제 대상 데이터가 노출되었을 수 있는지 신속하게 평가할 수 있으므로 규제기관, 파트너 및 영향을 받는 데이터 주체에게 통지해야 하는 규제 및 규정준수 의무를 이행할 수 있습니다.

사이버 레질리언스 활용 사례 보기

다양한 산업에서 활동하는 7개의 기업이 랜섬웨어 공격으로부터 빠르고 안전한 복구를 이행한 방법을 알아보세요.

전자책 다운로드

요약 및 종합

종합적으로 5단계 사이버 레질리언스 플레이북은 NIST CSF를 운영할 수 있는 명확하고 실행 가능한 절차를 안내합니다.

Cohesity의 최신 데이터 보안 플랫폼을 사용하면 보호 및 복구뿐만 아니라 사이버 레질리언스 준비태세를 지속적으로 최적화할 수 있습니다.

사이버 레질리언스 솔루션에 대해 자세히 알아보기

COHESITY
RESILIENCE EVERYWHERE

6100008-006-KO 11-2025