귀사의 사이버 복원력을 개선하기 위한 5가지 주요 단계

COHESITY

어디에서나 중요한 레질리언스

서론

랜섬웨어 공격이 증가하고 그 영향이 점점 더 심각해짐에 따라 불편한 진실이 드러납니다. 예방에 상당한 투자를 하더라도 이러한 조치만으로는 오늘날의 위협에 대응하기에 충분하지 않습니다.

좋든 싫든(그리고 우리는 좋아하지 않음) 사이버 공격은 사라지지 않습니다. 그리고 현 상태를 유지하지도 않을 것입니다. 빈도, 심각도 또는 규모 측면에서 더욱 그렇습니다.

그러므로 이것은 안 좋은 소식입니다.

이제 좋은 소식을 전해 드리겠습니다. 사이버 복원력을 개선하기 위한 검증된 플레이북이 있으며, 귀사와 같은 조직은 이를 사용하여 접근 방식을 재고하여 더 나은 결과를 창출할 수 있습니다.

이 전자책에서는 이러한 플레이북을 사이버 복원력을 위한 5단계 진행 상황으로 제시합니다. 5단계 모두에 걸쳐 구체적인 조치를 취함으로써 사이버 대응 및 복구의 모범사례에 부합하게 됩니다. 또한 보안, 비용 절감 및 위험 감소 측면에서도 상당한 이점을 확인할 수 있게 됩니다.

몇 가지 간략한 배경

랜섬웨어와 같은 사이버 위협에 대한 인식이 높아졌음에도 불구하고 사이버 공격은 계속해서 운영, 재정 및 평판에 대한 막대한 손실을 야기하고 있습니다. 사실상 사이버 공격은 전 세계 기업에 가장 큰 위협입니다.

재정적 피해가 실제로 발생합니다.

540,000 달러
가동 중단 시간당 손실액[1]

미화 10억 달러 이상
매년 랜섬웨어 지급액[2]

Sophos[3]의 2024년 랜섬웨어 현황에는 모두 냉정하게 받아들여야 하는 다음과 같은 통계가 포함되어 있습니다.

지난해 랜섬웨어로 피해를 입은 조직 중 설문조사에 응한 59%의 조직 중에서 **94%의 응답에 따르면, 공격자가 백업을 표적으로 삼았으며 이러한 백업 침해 시도의 57%가 성공했습니다.**

또한

- **공격의 70%가 데이터 암호화로 이어짐**
- **평균 200만 달러가 몸값으로 요구됨**
- **34%의 조직이 복구에 한 달 이상 소요됨**

새롭고 더 효과적인 전략, 기능 및 솔루션이 필요한 시간은 바로 지금입니다.

[1] The Hidden Costs of Downtime Splunk The $400B problem facing the Global 2000: https://www.splunk.com/en_us/pdfs/gated/ebooks/the-hidden-costs-of-downtime.pdf

[2] Chainalysis, Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline, 2/7/24: https://www.chainalysis.com/blog/ransomware-2024/

[3] Sophos, The State of Ransomware 2024: https://www.sophos.com/en-us/content/state-of-ransomware

사이버 복원력이 특히 어려울 수 있는 두 가지 이유:

1. 사이버 복구는 재해 복구와 다릅니다.

소속 조직에 견고한 재해 복구 프로세스가 마련되어 있더라도 이와 동일한 프로세스에 의존하여 사이버 공격으로부터 복구할 수 없습니다.

화재, 홍수, 정전 또는 심지어 구성 오류와 같은 재해에서 근본 원인을 신속하게 분석하여 무엇이 잘못되었는지 파악할 수 있습니다. 사이버 공격에서, 철저한 조사와 시정 조치가 필요한 수백 가지 상황이 발생할 수 있습니다. 또한 적대세력은 적극적으로 복구 노력을 약화시키고 몸값을 지불하도록 압박하고 있습니다.

2. 경험이 많은 조직과 전문가조차도 랜섬웨어 공격이 얼마나 파괴적인지 과소평가할 수 있습니다.

신뢰할 수 있는 시스템이 온라인 상태로 복귀하는 데 도움이 되거나 데이터와 증거에 의존하여 무슨 일이 일어났는지 파악할 수도 있다고 가정할 수 있습니다.

그러나 사이버 공격이 발생하면 사고 조사에 의존하는 바로 그 시스템이 다운되거나 회피 또는 손상되었을 수 있습니다. 좋은 데이터가 나쁜 데이터와 섞이면 복구로 가는 길이 더 멀고 험난해집니다. 그렇기 때문에 많은 스마트한 조직도 여전히 빠르고 클린하며 확실한 복구를 진행하는 데 어려움을 겪고 있습니다.

5가지 중요한 단계를 살펴보겠습니다

이것을 실제적인 블루프린트로 생각하십시오. 여기서 각 단계를 거치면 진행 상황에 따라 다음 단계로 이동하게 됩니다.

1단계

모든 데이터를 보호합니다.

간단하게 보이지만, 여전히 많은 조직이 이 중요한 첫 걸음을 내딛지 못하고 있으며, 문제의 원인은 데이터 스프롤일 가능성이 큽니다.

유기적인 데이터 증가로 인해 단편화와 사일로가 발생하여, 공격 표면이 크게 확대되고 조직이 그 어느 때보다 많이 노출되었습니다. 이와 동시에 대규모 데이터 관리 및 보안은 운영 효율성에 점점 더 큰 부담을 줍니다.

효율적으로 관리할 수 있는 능력 부족과 더 많은 장소에서 더 많은 데이터를 처리해야 하는 상황의 조합으로 공격자가 큰 피해를 입힐 수 있는 완벽한 조건이 조성되었습니다.

1단계의 주목할 만한 이점

- ☑ 향상된 보안
- ☑ 위험 감소
- ☑ 규정준수 및 거버넌스 개선
- ☑ 비용 절감 및 ROI 개선
- ☑ IT 효율성 증대

1단계를 이행하기 위한 주요 조치

1. **다음을 포함하여 1000개 이상의 데이터 소스를 지원하는 최신 데이터 플랫폼을 채택합니다.**

- 가상 머신(VM)
- SaaS 애플리케이션
- 데이터베이스
- NAS 환경(비정형 데이터)

2. **플랫폼이 온프레미스, 클라우드 및 SaaS 환경 전반에서 실행되도록 합니다.**

모든 곳에 데이터가 있기 때문에 플랫폼에는 공통 UI 및 API로 통합된 유연한 배포 모델이 있어야 합니다.

3. **직관적인 UI로 작업을 간소화합니다.**

UI 사용이 간편하면 비교적 소규모 팀에서 거대한 자산을 운영할 수 있고, 오히려 잘 운영할 수도 있습니다. 고객은 당사 플랫폼에서 워크플로우 자동화를 위한 단일 UI와 API 세트를 통해 탁월한 운영 효율성을 얻을 수 있습니다.

4. **강력한 스토리지 압축 기능을 활용하십시오.**

강력한 데이터 압축 기능을 갖춘 플랫폼을 사용하는 것이 좋습니다. 이를 통해 페타바이트 규모로 실행할 때 상당한 절감 효과를 얻을 수 있습니다. 당사에는 업계 표준인 고유한 파일 시스템이 있습니다. 정말 강력한 스토리지 압축으로 TCO를 절감할 수 있습니다.

2단계

데이터가 항상 복구 가능하도록 보장합니다.

공격자는 백업을 표적으로 삼습니다. 이들은 이 마지막 방어선에 영향을 미칠 수 있는지 여부를 알고 있으며, 귀사는 다른 구제 수단을 가지고 있지 않으므로 몸값을 지불할 가능성이 훨씬 더 높습니다.

그리고 최신 데이터 플랫폼이 즉시 복구 가능한 백업을 보장한다고 가정하는 것은 좋은 일이지만, 이는 사실이 아닙니다.

몇 가지 조치를 취해서 공격자의 액세스를 더 어렵게 만들고, 침해가 발생하면 귀사가 클린 백업을 복구해야 합니다.

2단계의 주목할 만한 이점

- ☑ 더 빠르고 안전한 복구
- ☑ 공격에 대한 강력한 보호
- ☑ 감사에 대한 대비
- ☑ 제로 트러스트 조정

2단계를 이행하기 위한 주요 조치

1. **다음과 같은 강력한 기능을 구성하여 플랫폼을 강화합니다.**

- 다단계 인증(MFA)
- **불변성**(데이터를 변경하거나 삭제할 수 없음)
- **역할 기반 액세스 제어**(RBAC)
- **직무 분리**(다양한 개인 간의 중요 업무 분할)

2. **사이버 볼트 구현**

가장 중요한 데이터의 에어갭 처리된 사본을 보유하고 **3-2-1-1 백업 규칙**(데이터 사본 3개, 서로 다른 미디어 2개, 오프사이트 1곳, 변경 불가 사본 1개)을 준수하면, 비상 시 항상 데이터 사본을 이용할 수 있습니다.

또한 Cohesity는 첨단 키 관리 시스템을 제공하므로 공격 발생 시 고객에게 데이터에 대한 액세스를 계속 제공할 수 있습니다.

이러한 액세스를 통해 백업을 항상 복구할 수 있습니다.

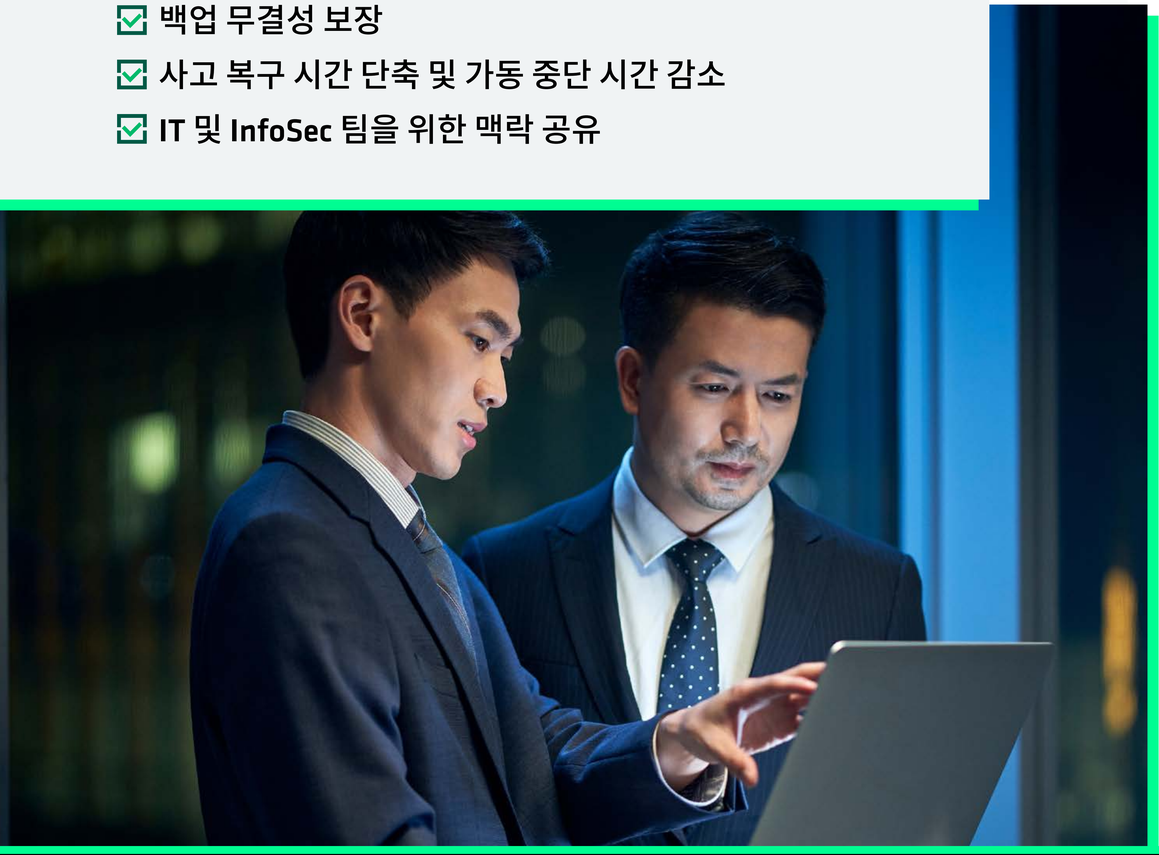
3단계

위협 탐지 및 조사

이 단계는 위협 스캐닝 및 위협 헌팅 기능의 결합과 관련이 있습니다.

3단계의 주목할 만한 이점

- ☑ 조기 위협 탐지 및 완화
- ☑ 백업 무결성 보장
- ☑ 사고 복구 시간 단축 및 가동 중단 시간 감소
- ☑ IT 및 InfoSec 팀을 위한 맥락 공유



3단계를 이행하기 위한 주요 조치

1. 백업에서 위협을 정기적으로 스캔하여 선제적으로 대응하십시오. 이러한 선제적 **위협 스캐닝**을 일관된 위생 관행을 실천하는 것처럼 생각하십시오. 이는 다음을 수행하는 데 도움이 됩니다.

- 최대한 신속히 변경 사항 파악
- 멀웨어 또는 기타 취약점 식별

2. 특정 위협을 찾을 때는 **위협 헌팅** 기능을 시작하십시오. 당사의 선별된 위협 피드와 CrowdStrike, Palo Alto Networks, Cisco 등 당사의 데이터 보안 얼라이언스의 보안 에코시스템 공급업체와 통합하면 이러한 시스템에 당사가 제공할 수 있는 데이터와 함께 이러한 공급업체의 집단적 지혜의 결합된 이점을 얻을 수 있습니다.

InfoSec과 IT 팀도 동일한 세트의 정보로 운영됩니다.

당사는 수년 동안 고객이 사이버 공격으로부터 복구할 수 있도록 지원해 왔으므로 기본 제공 위협 스캔 및 위협 헌팅 기능이 데이터 플랫폼의 일부가 되어야 합니다.

왜일까요? 다른 보안 시스템은 공격을 받으면 비활성화되거나 오프라인 상태가 될 수 있기 때문입니다.

4단계

애플리케이션 복원력 연습

"연습"과 관련하여 위의 1-3단계를 수행했다면 이미 좋은 상태를 유지하고 있는 것입니다. 여러분은 이미 플랫폼을 구축하고, 그에 대한 보안을 강화하며, 사이버 볼트를 통해 배포를 확장했습니다.

또한 정기적인 위협 스캐닝과 위협 헌팅에 대한 약간의 유용한 경험을 쌓았습니다. 잘하셨습니다!

여기 4단계에서는 인프라, 데이터 및 애플리케이션에 대한 대응 및 복구 프로세스를 연습하여 다음 단계를 준비하게 됩니다. 어쨌든, 시스템이 다운되고 다양한 압박이 가해지는 실제 공격에서 처음으로 이 작업을 수행해서는 안 됩니다.

"모든 것을 다시 온라인 상태로 만드는 것은 시간이 많이 걸리는 프로세스입니다. 정기적으로 테스트하면서도 여전히 일상 업무를 수행하는 것이 가능한가요?"라고 생각할 수 있습니다.

4단계의 주목할 만한 이점

- ☑ 더 빠르고 안전한 복구
- ☑ RTO 개선
- ☑ 재감염 위험 감소
- ☑ 운영 중단 및 재무 위험 감소

여기서 오케스트레이션이 필요하게 됩니다.

오케스트레이션을 사용하면 대응 및 복구 워크플로우를 자동화하고 공격 후 시스템을 다시 온라인 상태로 전환하는 "예행연습"을 시작할 수 있습니다. 이러한 예행연습은 대응과 복구를 원활이 수행하는 데 도움이 되며, 오케스트레이션을 통해 수동 작업을 줄이면서 이러한 연습을 정밀 조정하는 데 도움이 될 수 있습니다.

실행 중인 자동화의 한 가지 주요 사례: 당사의 클린룸 솔루션을 사용하면 포렌식 분석을 수행하고, 감염된 데이터 비트에 대해 자세히 알아보며, 무엇이 발생했는지 파악한 다음, 공격 아티팩트를 근절하여 시스템이 복구하기에 안전한지 확인할 수 있는 별도의 환경을 활용할 수 있습니다. 이러한 접근 방식은 속도, 자동화 및 강력한 포렌식의 고유한 조합을 제공하여 사고 대응자가 IT 팀과 협업할 수 있도록 지원합니다. 그 결과 사이버 대응 및 복구가 더 빨라집니다.

이 단계에서는 Cohesity CERT(사이버 이벤트 대응팀)와도 협력하게 됩니다. 이 전문가 팀은 정교한 랜섬웨어 및 데이터 침해에서 표적 공격에 이르기까지 사고에 대응하고 이를 처리하는 것을 지원합니다. 혼자서 문제를 감당할 필요가 없습니다.

4단계를 이행하기 위한 주요 조치

1. 오케스트레이션 및 예행연습을 통한 연습
- 대응 및 복구 프로세스 자동화
- 예행연습을 통해 인프라, 데이터 및 애플리케이션에 대한 복구 순서를 지정하는 방법을 포함하여 대응 계획을 정밀 조정

2. 클린룸 사용
- 포렌식 분석을 위한 별도의 안전한 환경 활용
- 인프라, 데이터 소스 및 애플리케이션을 복원하기 전에 위협 식별 및 근절

3. 전문가 지원 받기
- 공격 발생 시 Cohesity CERT에 문의

5단계

데이터 위험 대비태세 최적화

랜섬웨어 조직의 악의적인 양상이 심화되는 것 외에도 온프레미스, SaaS, 클라우드, 엣지 등 그 어느 때보다 많은 데이터를 관리해야 하는 상황입니다. "음, 아무도 모르거나 감시하고 있지 않은 보안이 취약한 S3 버킷에 무엇이 들어 있습니까?"라고 모든 사람은 항상 생각하고 있습니다.

보안이 취약한 S3 버킷 외에도 숨겨진 위험에는 고아 데이터베이스, 노출된 자격 증명 등이 포함될 수도 있습니다.

데이터 보안 태세 관리(DSPM) 및 데이터 분류와 같은 선제적 조치는 이러한 위험을 줄이는 데 도움이 됩니다.

5단계의 주목할 만한 이점

- ☑ 향상된 데이터 가시성 및 분류
- ☑ 선제적 위험 식별 및 완화

5단계를 이행하기 위한 주요 조치

1. 어떤 데이터가 어디에 있는지 알아보기

- 환경을 스캔하여 어떤 데이터가 어디에 있고 어떤 보호 수준이 있는지 평가하십시오. DSPM을 사용하는 전체 범주의 도구들이 이것을 가능하게 합니다.
- Cyera 및 BigID를 포함한 업계 최고의 일부 공급업체와 당사의 완전한 기능 통합을 통해 백업 자산에 무엇이 있는지 이해하고 올바른 방식으로 보호되는지 확인하십시오.

2. **침해로 인해 영향을 받았을 수 있는 사항 또는 데이터 유출 시 발생했을 수 있는 사항을 평가하십시오.**

- 당사 제품에 내장된 데이터 분류를 통해 필요한 올바른 보장 범위를 확보하고 위험을 줄이십시오.
- 사고 발생 시 신속하게 답변하고 변호사는 다음과 같이 질문합니다. 어떤 데이터가 영향을 받았습니까? 그것은 얼마나 민감합니까? 우리의 위험은 무엇입니까? 영향을 받은 고객은 몇 명입니까? 어떤 유형의 레코드가 영향을 받았습니까?

결론

이제 조직의 사이버 복원력을 개선하기 위한 5가지 중요한 단계를 이해했으며, 이러한 단계를 소속 환경에서 구현하는 데 필요한 실용적인 정보를 얻었습니다.

Cohesity는 이러한 과정을 안내하여 실현 가능한 가장 강력한 사이버 복원력을 확보할 수 있도록 지원할 수 있는 독보적인 위치에 있습니다.

랜섬웨어에서 안전하고 빠르게 복구하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

"파괴적인 사이버 공격에 대한 전시 대응 전략을 수립하는 방법"

COHESITY

어디에서나 중요한 레질리언스

2000056-002-KO 4-2025