Enterprise Strategy Group | Getting to the bigger truth.™

ESG 백서

사이버 레질리언스 보장과 스토리지의 역할

ESG 프랙티스 디렉터 겸 선임 분석가 Scott Sinclair 및
ESG 선임 연구 분석가 Monya Keane 공동작성

2022 년 1 월

This ESG White Paper was commissioned by IBM and is distributed under license from TechTarget, Inc.

Contents

전문 요약

혁신 비즈니스 자산으로서 데이터의 역할은 계속해서 커지고 있습니다. 이는 애플리케이션 개발의 투자 증가 덕분입니다. 최신 DevOps 관행; 비즈니스 인텔리전스, 분석 및 기계 학습에 대한 요구가 높아짐에 따라 거의 모든 기업에서 데이터 생성 및 사용이 가속화되고 있습니다. 또한 데이터를 활용하는 지점의 수도 확장되고 있습니다. 이렇게 데이터의 확산과 운영 가속화에 대한 압력이 증가함에 따라 IT 인프라와 IT 운영의 복잡성 또한 증가하고 있습니다.

이러한 요인으로 인해 조직과 해당 인프라는 악의적 공격, 인적 오류 및 부주의한 행동 등을 경험할 위험이 커지고 있습니다. 유감스럽게도 레거시 전략으로는 이러한 유형의 사고가 발생하는 동안 그리고 발생한 이후에 비즈니스 운영의 지속성을 적절하게 보장할 수 없습니다. 기업은 공격 및 기타 침해를 방지하기 위한 기능을 결합할 수도 있으나 기능적 격차, 빈약한 통합 및 관리 복잡성으로 인해 보안 목표를 달성하는 데는 오랜 시간이 걸리고 달성 또한 어렵습니다.

따라서 예방에서 사고대비로 조직의 사고방식을 바꾸는 것(예: 내장형 사이버 레질리언스로 스토리지 솔루션 구현)만이 중요한 데이터 자산을 보호하고 랜섬웨어 및 기타 사이버 공격에 신속하게 대응하고 복구할 수 있는 핵심 비결입니다.

서문

IT 는 새로운 도전에 직면해 있습니다. ESG 설문 응답자의 거의 절반(46%)이 2 년 전에 비해 지금의 IT 가 더 복잡하다고 말합니다. 이러한 복잡성 증가는, 진행 중인 디지털 혁신 과제(29% 응답), 더 많은 데이터 볼륨(35%), 사이버 보안 환경의 급속한 진화(37%) 및/또는 새로운 데이터 보안, 개인정보보호 규정(32%)을 고수하려는 노력의 결과일 수 있습니다.

동시에 조직은 중요한 IT 기술 상의 문제를 해결하기 위해 고군분투하고 있습니다. 실제로 설문에 응한 조직의 48%는 사이버 보안 전문가가 충분하지 않다고 답했는데 이는 부족하다고 응답한 것 중 가장 자주 언급된 영역이었습니다. 또한 이러한 조직은 IT 에서 보호해야 하는 보안 경계의 크기와 범위를 증가시키고 있는 애플리케이션, 장치 및 원격/모바일 작업자의 확산을 처리해야 하는 부담에 시달리고 있습니다.

현대 IT 의 복잡성, 급증하는 데이터, 날로 증가하는 사이버 공격 위협으로 인해 IT 팀은 상호 보조를 맞추기 위해 고군분투하는 경우가 많습니다. 내부 인력만으로 이러한 복잡성을 해결하려고 한다면 결국 지는 싸움이 될 것입니다. 성공하려면 기본 인프라 자체를 현대화해야 합니다. 그러나 그렇게 할 때 IT 의사 결정권자는 애플리케이션 요구 사항을 충족하거나 운영을 단순화하는 데 그치지 않는 혁신 기술을 찾아내야 합니다.

진정한 성공을 달성하려면 이러한 목표를 달성하고 아울러 애플리케이션 환경의 사이버 레질리언스 태세 개선 또한 기할 수 있는 기술을 찾아야 할 것입니다.

사이버 공격 및 랜섬웨어의 위협 증가

조직은 사이버 범죄자에 대한 재정적 인센티브 증가로 인해 점증하는 사이버 보안 위협에 직면해 있습니다. 한 예로, 2020 년 미국 국민이 FBI 의 인터넷 범죄 신고 센터(IC3)에 신고한 랜섬웨어 신고 건수는 2019 년보다 69% 증가했으며 보고된 손실은 41 억 달러를 초과했습니다. 또한 지난 5 년 동안 IC3 는 총 133 억 달러의 총 손실액을 보고했습니다. 미국의 2020 년 4 분기 기준 기업을 표적으로 한 랜섬웨어 공격으로 비즈니스 운영이 중단된 기간은 평균 21 일이었습니다. 랜섬웨어가 비즈니스 운영에 미치는 부정적인 영향은 분명히 상당합니다.

IT 복잡성과 사이버 공격 취약성 사이에는 강력한 상관 관계가 있습니다. IT 가 더욱 복잡해짐에 따라 사이버 공격의 빈도가 증가하고 비용 또한 더 많이 듭니다.

랜섬웨어는 지금 만연한 위협이며 기업의 가장 소중한 자산인 데이터를 집중 공격합니다. IC3 는 2020 년에 총 2,474 건의 랜섬웨어 신고건수를 확인했으며 ESG 는 조사 대상 조직의 63%가 지난 해에 랜섬웨어 공격을 경험한 것으로 나타났습니다. 실제로 9%는 매일 랜섬웨어 공격을 경험했습니다(그림 1 참조).[1]

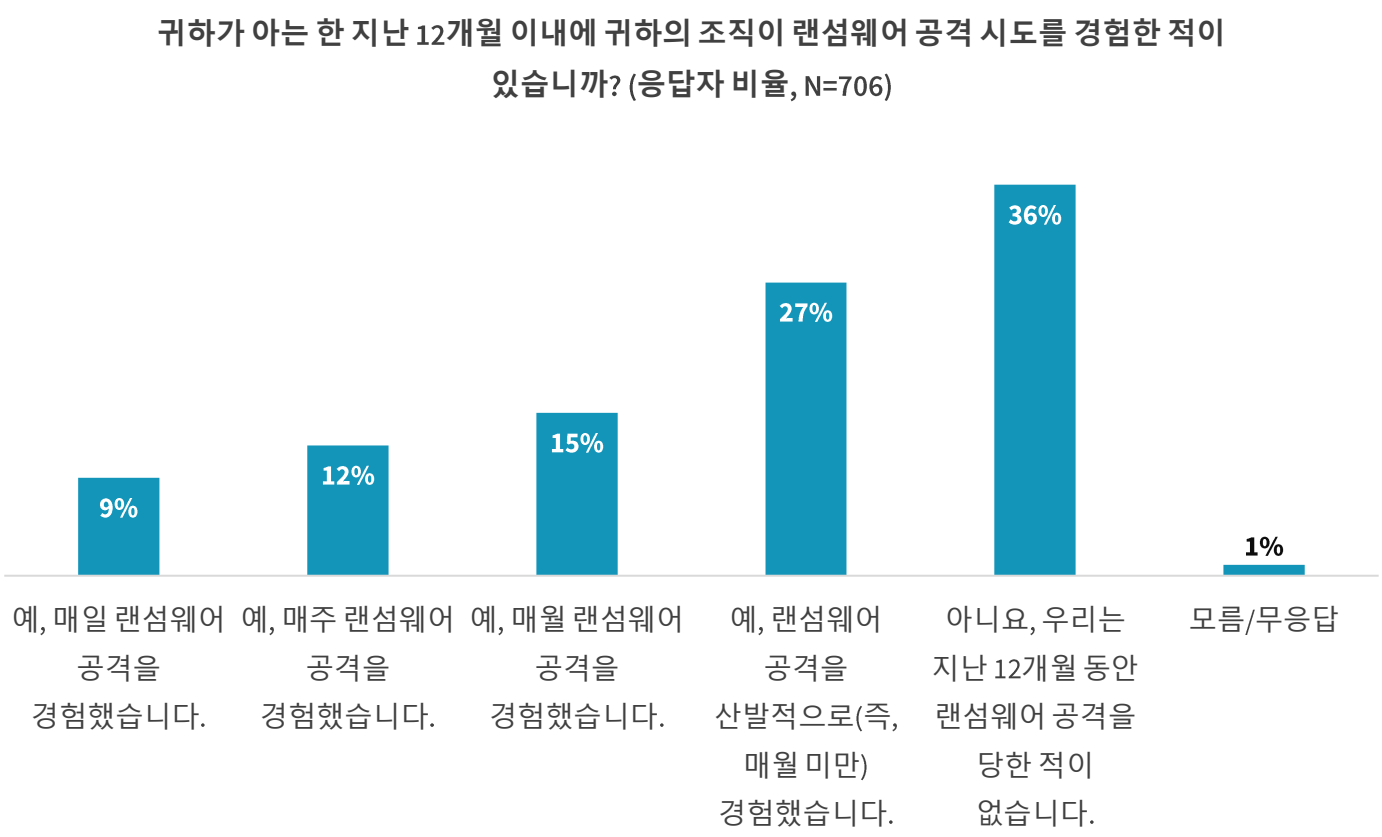
[1] Source: ESG Complete Survey Results, *2022 Technology Spending Intentions Survey*, November 2021.

랜섬웨어 보안에는 기존 사이버 보안 영역을 넘어 확장된 기술 전략이 필요합니다. 이는 데이터 저장 및 데이터 보호의 발전도 활용해야 합니다

사이버 레질리언스에 있어 데이터 스토리지의 역할

스토리지 시스템과 스토리지 관리자는 모두 랜섬웨어로부터 조직을 보호하는 데 큰 역할을 합니다. ESG 가 IT 의사 결정권자들을 대상으로 실시한 설문에서, 랜섬웨어 공격을 방지하거나 완화하기 위해 조직에서 어떤

그림 1. 응답자의 63%가 지난 12 개월 동안 랜섬웨어 공격을 경험했습니다.

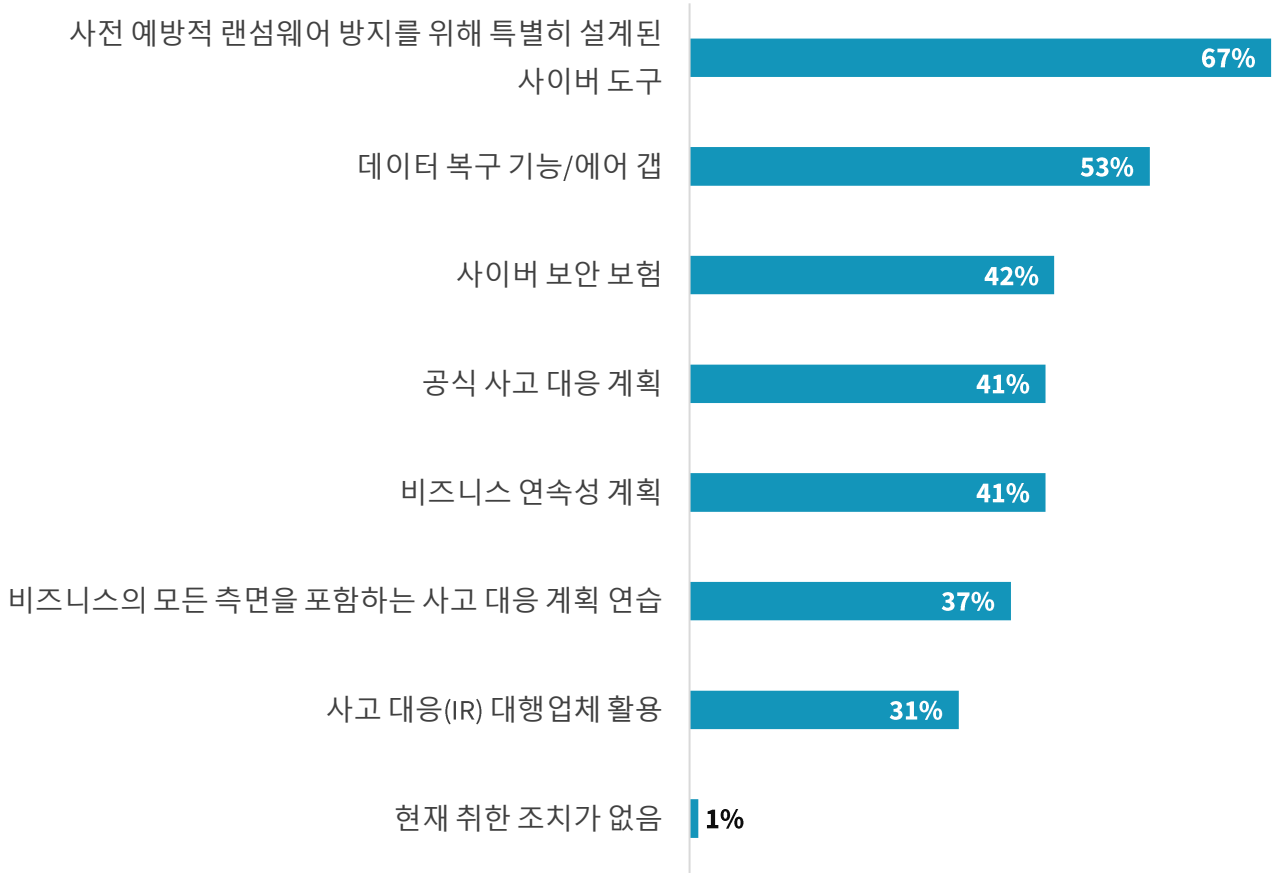


Source: ESG, a division of TechTarget, Inc.

조치를 취하고 있는가라고 질문하자 응답자의 67%는 사전 예방적 랜섬웨어 방어를 위해 사이버 도구를 사용한다고 답했으며 53%는 에어갭과 같은 데이터 복구 기능을 적시해 답했습니다 (그림 2 참조).).
일반적으로 식별되는 이 두 가지 답은 공격을 피하기 위한 조치를 구현하는 것뿐 아니라 불가피하게 공격이 발생할 때 비즈니스가 복구할 준비가 되도록 솔루션에 투자하는 것이 얼마나 중요한지를 잘 보여주고 있습니다. 랜섬웨어를 단순 퇴치하거나 완화하기 위한 정책을 설정하고 중지하는 현재의 관행을 탈피하는 것이 중요합니다. 이러한 "부분적" 접근 방식의 경우 공격을 완화하기 위한 노력을 기울이기는 하지만 실제로 필요가 발생하기 전에 효과적인 데이터 복구 계획을 수립하기 위한 노력은 거의 이루어지지 않기 때문에 조직 내에 잘못된 보안 감각을 만드는 맹점이 있습니다.

그림 2. 랜섬웨어 퇴치 또는 완화를 위한 일반적 조치

귀하의 조직은 현재 랜섭웨어 공격을 방지하거나 완화하기 위해 다음 중 어떤 조치를 취하고 있습니까? (응답자 비율, N=706, 복수 문항 답변 허용)



출처: TechTarget, Inc. ESG 사업부

공격에 대처하는 것과 기존의 데이터 복구는 상당히 다르다는 것을 기억하는 것이 중요합니다. 일반적으로 조직에서는 거의 항상 최신 복사본을 사용하여 데이터를 복구하려고 합니다. 그러나 랜섬웨어의 경우 IT 부서는 일반적으로 어떤 "좋은" 복사본을 사용해야 하는지 잘 모릅니다. 따라서 복구작업은 종종 더 위험하고 훨씬 더 오래 걸릴 수도 있습니다. 일부 랜섬웨어 공격은 데이터뿐 아니라 백업 인프라 자체도 공격 목표로 합니다. 이것이 바로 고급 스토리지 기능이 효과적인 랜섬웨어 복구를 위한 전제조건인 이유입니다.

그림 2 에서 식별된 조치를 채택하는 것은 물론 현명하고 앞으로 증가해야 하지만, 어떤 방어조치도 그 자체로 랜섬웨어 복구에 100% 효과적이지 않다는 점 또한 조직은 이해해야 합니다. 랜섬웨어 식별 및 방지와 데이터 복구를 전문으로 하는 도구를 고려하는 것은 물론 중요하지만 이는 전체 노력의 일부일 뿐입니다. 수비가 아무리 좋다 해도 외부 공격에 뚫릴 수 있습니다. 조직은 이러한 상황에 대비하고 가능한 한 빨리 복구하여 비즈니스 운영에 미치는 영향을 최소화할 수 있는 방법을 평가해야 합니다. 전반적인 랜섬웨어 노출을

최소화하기 위해 조직은 얼마나 빨리 공격을 식별할 수 있는지, 얼마나 신속하게 손상을 완화할 수 있는지, 알려진 정상 복사본으로 얼마나 빨리 복구할 수 있는지 이를 가속화할 수 있는 방법을 찾아야 합니다.

하드웨어, 소프트웨어, 사람 및 프로세스 등 모든 데이터 처리 구성 요소를 고려하여 강력한 사이버 레질리언스 전략이 실행되어야 하는 이유가 바로 그 때문입니다. 사이버 레질리언스 태세를 개발할 때 조직은 "어떻게 보호합니까?"라는 질문에서. "랜섬웨어에 감염되면 얼마나 빨리 복구할 수 있습니까? 우리 사업은 얼마나 빨리 정상으로 돌아올 수 있습니까?" 라는 질문으로 전환해야 합니다"

데이터 저장 및 데이터 보호: 랜섬웨어 위험을 최소화하기 위해 어디에 집중해야 하는지 파악하기

랜섬웨어 복구는 재난 복구의 한 형태지만 랜섬웨어의 영향은 화재나 홍수의 영향과 상당히 다릅니다. 결국 화재가 완전히 진압된 시점은 상식적으로 잘 알 수 있지 않습니까? 랜섬웨어는 언제든지 다시 발화할 수 있는 벽 안에 숨겨진 불꽃과 같습니다. 스토리지 관리자는 랜섬웨어와 관련된 위험을 줄이기 위해 특정 영역에 집중해야 합니다. 속도가 필수적이므로 조직에서 다음 사항을 수행할 수 있는 속도를 결정해야 합니다:

- 위험을 식별한다.
- 피해를 수량화한다.
- 정상 작동이 확인된 사본을 식별하고 정상 작동이 확인된 사본을 사용하여 복구하고 궁극적으로 작업을 복원하여 손상을 완화한다.

"이것은 우리에게 일어나지 않을 것"이라는 접근 방식이야말로 가장 위험합니다. 조직은 사전 예방적이어야 하며 실제로 필요하기 전에 효과적인 데이터 저장 및 보호 솔루션을 마련해야 합니다.

IBM 과 함께 사이버 보안에서 사이버 레질리언스로 전환

사이버 보안 및 위험 관리에 대한 광범위한 경험을 바탕으로 IBM 은 사이버 레질리언스 분야에서 인정받는 리더이며 다음과 같은 포괄적인 고급 스토리지 및 데이터 보호 솔루션 제품 군을 제공합니다:

- **IBM FlashSystem, IBM Cloud Object Storage 및 IBM Spectrum Scale,** 데이터 불변성 및 암호화 기능과 함께 제공되는 기본 스토리지 솔루션.
- 데이터 불변성 및 암호화도 지원하고 에어 갭을 통해 보호 기능을 제공하는 **IBM 테이프 스토리지**.
- **IBM Spectrum Copy Data Management** 소프트웨어는 데이터 사본을 관리하고 보호합니다.
- 추가 보호를 위한 **IBM Spectrum Protect Suite. Spectrum Protect** 소프트웨어 정의 스토리지는 플래시, 디스크, 개체 스토리지, 물리적 또는 가상 테이프에 데이터를 저장할 수 있습니다. 그런 다음 정상적인 액세스 패턴에서 큰 편차를 식별하여 맬웨어 및 랜섬웨어 활동을 감지합니다.
- **QRadar 및 Storage Insights** 솔루션은 AI 강화 기능을 사용하여 잠재적 위협 탐지를 가속화합니다.

IBM 사이버 볼트와 함께하는 사이버 레질리언스

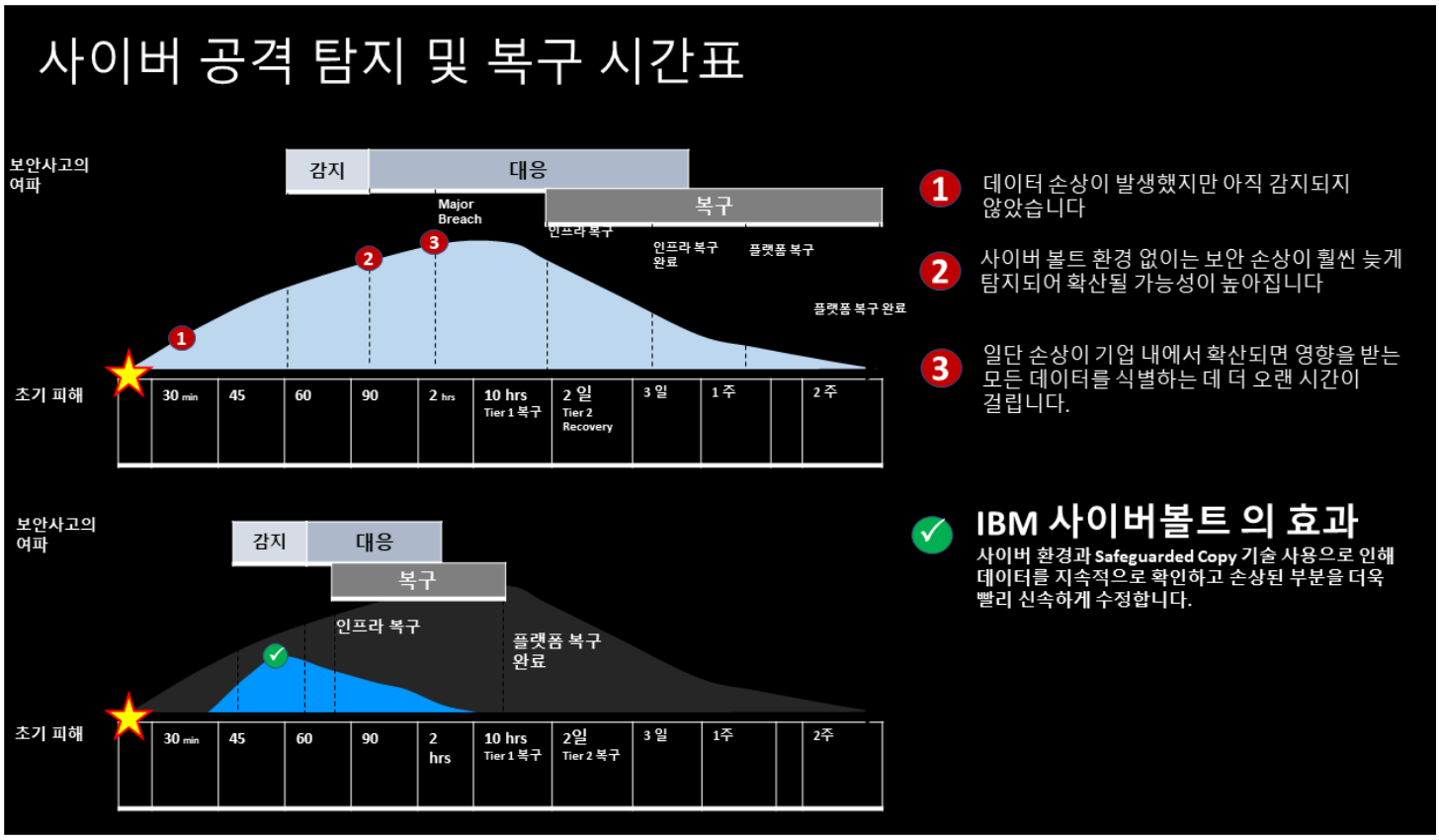
랜섬웨어로부터 보호하는 스토리지의 역할은 아무리 강조해도 지나치지 않습니다. 스토리지 소프트웨어는 기본 데이터의 변경 사항을 확인하고 이러한 변경 사항을 확인하기 때문에 공격이 시작되는 시점을 식별할 수 있는 우위가 있습니다. 보조 복사본을 가져와 보호하는 것도 기술입니다. 따라서 스토리지는 복구를 지원하는 데 매우 중요합니다. 이러한 사실을 감안할 때 IBM 의 사이버 레질리언시 도구 상자에서 가장 유용한 도구 중 하나는 아마도 IBM 사이버 볼트일 것입니다.

IBM 사이버 볼트는 사이버 공격으로부터 신속한 복구를 위한 보안 방법론입니다. 이는 격리되고 변경 불가한 스냅샷을 정기적으로 생성하는 기술인 IBM Safeguarded Copy 를 기반으로 구축되었습니다. 사이버 볼트는 이러한 스냅샷을 분석하여 랜섬웨어의 존재를 나타낼 수 있는 잠재적인 악성 변경 사항을 찾아냅니다. 또한 IBM Cyber 볼트는 IBM QRadar 및 IBM Storage Insights 와 통합하여 더욱 빠르게 위협을 탐지합니다. 변경 불가한 복사본의 유효성 검사를 통해 관리자는 좋은 복사본을 빠르게 식별하고 테스트한 다음 복원할 수 있습니다.

특히 속도 향상 측면에서 IBM 사이버 볼트는 스토리지 관리자가 다음을 가속화할 수 있도록 지원합니다.

- **식별** - QRadar 와 Storage Insights 의 통합은 더욱 향상된 감지 및 모니터링을 제공합니다.
- **피해 완화 및 정량화** - 이것은 자동화된 프로세스입니다. 공격을 조기에 자동으로 탐지하면 공격으로부터 더 빠르게 복구할 수 있습니다.
- **정상 작동이 확인된 복사본 식별** - 위협이 감지되면 변경할 수 없는 데이터 복사본이 자동화됩니다.
- **운영 복구** - 며칠 또는 몇 주가 아닌 몇 시간 내에 신속한 복구가 가능합니다(그림 3 참조).

그림 3. IBM Cyber 볼트가 사이버 복구를 가속화하는 방법



출처: IBM

더 큰 진실

IT 인프라는 날이 갈수록 복잡해지고 있어 인적 오류, 시스템 장애 또는 과실이 발생할 가능성이 높아집니다. 동시에 조직 내외부의 악의적인 행위자들은 취약한 링크를 찾아 악용하기 위해 끊임없는 노력을 기울입니다.

결국 틀림없이 보안 사고가 발생합니다. 이러한 사실은 조직의 사고 방식을 사후 대응에서 사전 예방으로, 즉 공격을 방지하기 위한 시도에서 보안 실패 발생 시 대비하고 대응하는 것으로 변화해야 한다는 것을 시사합니다. 이것이 바로 사이버보안에서 사이버 레질리언스로 나아가는 기업이 취해야 할 혁신입니다.

많은 조직이 NIST 사이버 보안 프레임워크에서 제공하는 지침에 따라 사이버 레질리언스 전략을 모델링하고 있습니다. 이 지침은 조직이 중요 리소스를 식별하고, 해당 리소스를 보호하고, 보안실패 및 보안위반을 감지하고, 사이버 사고에 대한 대응 및 복구를 계획할 것을 권장하고 있습니다. 지금 주요 선진 조직은 여러 데이터 복구 옵션을 유지하면서 데이터 검색, 복사 관리, 암호화, 액세스 제어, 불변 저장과 같은 기능을 통해 사이버 레질리언스를 향상시킬 수 있는 IT 인프라 기능에 특별한 관심을 기울이고 있습니다.

IT 및 비즈니스 리더에게 있어 사이버 레질리언스란 비즈니스 운영의 유지를 목표로 올바른 기술을 선정하고 올바른 비즈니스 결정을 내리는 것입니다.

Enterprise Strategy Group 은 글로벌 IT 커뮤니티에 마켓 인텔리전스, 이행 가능한 통찰력 및 시장 출시 콘텐츠 서비스를 제공하는 통합 기술 분석, 연구 및 전략 회사입니다.

www.esg-global.com

contact@esg-global.com

+1.508.482.0188