

에버퓨어 사이버 복원력으로 복구 가속화

사이버 위협으로 인한 위험과 영향을 줄이세요.

사이버 공격은 운영을 며칠 또는 몇 주 동안 중단시킬 수 있습니다. 그럼에도 대부분의 조직은 핵심 애플리케이션과 서비스를 **몇 시간 내**에 복구해야 합니다. 복구에 걸리는 시간이 길어지면 고객 신뢰와 브랜드 평판이 훼손되며, 서비스 중단이 지속될 경우 경쟁사에 시장 점유율을 빼앗길 수도 있습니다. 문제를 더욱 심각하게 만드는 요인은 다운타임으로 인한 비용이 매우 크다는 점입니다. 특히 엔터프라이즈 규모의 조직에서는 그 부담이 더욱 커집니다. 조직에서는 다운타임으로 인해 **분당 약 9 천 달러**, 시간당 약 54 만 달러의 비용이 발생할 수 있습니다. 또한 데이터를 신속하고 안전하게 복구하지 못할 경우 HIPAA, GDPR, SEC 등 관련 규제에 따른 제재를 받을 수도 있습니다.

수동적 대응에서 선제적 대응으로: 사이버 복원력의 새로운 기반

많은 조직이 랜섬웨어 공격으로부터 복구하기 위해 여전히 레거시 재해 복구 기술과 프로세스, 정책에 의존하고 있습니다. 그러나 이러한 방식으로 빠르고 안정적인 복구에 필수적인 격리된 복구 환경(IRE)을 신속하게 프로비저닝해야 하는 등 사이버 복구의 복잡한 요구 사항에 제대로 대응하기 어렵습니다. 또한 가장 중요한 애플리케이션의 백업 스토리지는 대체로 레거시 또는 노후화된 기술을 기반으로 운영되고 있어, 복구 과정에 필요한 데이터를 신속하게 프로비저닝하는 과정에서 병목 현상을 유발합니다. 공격이 발생하기 전에도 보안 정보와 이벤트 관리(SIEM), 사용자와 엔티티 행동 분석(UEBA) 등의 많은 보안 분석 도구는 미션 크리티컬 스토리지의 인사이트를 활용하지 못하며, 네트워크, 엔드포인트, 스토리지, 서버에서 생성되는 방대한 로그 데이터를 분석하는 데 한계가 있습니다.

에버퓨어(Everpure™)는 스토리지가 더는 수동적인 역할에 머물러서는 안 된다고 생각합니다. 네이티브 보안과 복구 기능은 기존의 사이버 보안과 데이터 보호 아키텍처를 보강하여 **스토리지를 사이버 방어와 사이버 복구를 위한 능동적인 기반 계층으로 전환해야 합니다**. 악의적인 접근을 차단하고, 위협을 더욱 신속하게 탐지하며, 그 어느 때보다 확신을 가지고 복구할 수 있도록 데이터 인텔리전스를 기반으로 구축된 에버퓨어 플랫폼(Everpure Platform)은 이러한 과제에 정면으로 대응할 준비가 되어 있습니다.

내장형 보안, 연계형 위협 탐지, 동적 대응과 복구, 데이터 인텔리전스 기반

에버퓨어(Everpure)는 조직이 사이버 공격에 대응하고 사이버 복구와 재해 복구를 모두 가속하도록 지원합니다. **내장형 보안, 연계형 위협 탐지, 동적 대응과 복구**는 효과적인 사이버 복원력 스토리지의 핵심 요소입니다. 에버퓨어 플랫폼(Everpure Platform)은 고성능의 자동화된 계층형 복원력과 복구 기능, 네이티브 위협 탐지, 강력한 데이터 보안과 불변성, 사이버 보안과 데이터 보호 솔루션의 원활한 통합을 통해 랜섬웨어와 사이버 위협으로부터 데이터를 보호합니다. 이를 통해 데이터를 최적의 속도로 복구하고, 데이터의 가용성과 보안을 지속적으로 유지할 수 있습니다. 데이터와 애플리케이션 인텔리전스는 이러한 핵심 요소를 강화하는 데 필요한 컨텍스트별 인사이트, 운영 가시성, 적응형 제어 기능을 제공함으로써 에버퓨어(Everpure)의 사이버 복원력 역량을 뒷받침합니다.



사이버 위협에 대비된 스토리지

스토리지는 핵심 복구 메커니즘으로, 보호, 복제, 통합, 자동화를 통해 사이버 복원력을 강화하고 복구 시간을 단축합니다.



보안 분석 가속화

에버퓨어(Everpure)는 중요 워크로드를 겨냥한 위협에 대한 가시성을 제공하고 온프레미스 SIEM 환경에서 위협 탐지를 가속화합니다.



데이터 보호 강화

에버퓨어(Everpure)는 뛰어난 성능과 세이프모드 스냅샷(SafeMode™ Snapshots) 통합을 통해 백업 시간과 복구 시간을 단축합니다.

솔루션 개요

내장형 보안은 네이티브 예방 기능과 기본적으로 안전하게 설계된(Secure-by-Default) 아키텍처를 제공합니다. 삭제와 변경이 불가능한 스토리지, 제로 트러스트 원칙, 업계를 선도하는 데이터 보안 솔루션과 긴밀한 통합을 바탕으로 플랫폼과 데이터를 보호합니다.

- 에버퓨어(Everpure)의 삭제와 변경이 불가능한 스냅샷은 랜섬웨어나 악의적인 공격자가 중요 데이터를 변경, 삭제, 암호화하지 못하도록 보호합니다. 이러한 스냅샷은 스토리지 계층에서 자동으로 버전이 관리되고 보호되므로, 데이터를 빠르게 복구할 수 있는 안전한 변조 방지 사본으로 활용됩니다. 즉각적인 접근성과 내장된 삭제 방지 기능을 결합하여, 조직은 고도화된 사이버 공격 상황에서도 규정 준수 요구 사항을 충족하고, 복구 시간을 단축하며, 비즈니스 연속성을 유지할 수 있습니다.
- 에버퓨어(Everpure)는 데이터 인프라의 모든 계층에 제로 트러스트 원칙을 적용하여 모든 접근 요청을 검증하고, 모든 작업을 인증하며, 모든 구성 요소를 검증합니다. 기본적으로 안전하게 설계된 아키텍처를 기반으로, 에버퓨어(Everpure)는 역할 기반 접근 제어(RBAC), 다중 인증(MFA), 종단 간 암호화를 적용하여 관리 영역과 데이터 영역을 모두 보호합니다. 또한 신뢰할 수 있는 플랫폼 모듈(TPM), UEFI 보안 부팅(Secure Boot) 등 하드웨어 기반 보안 기능과 고객이 자체 암호화 키를 직접 관리할 수 있는 자체 키 사용(BYOK) 기능을 제공합니다. 이러한 보안 제어 기능은 제로 트러스트 프레임워크에 부합하는 강화되고 검증 가능한 기반을 구축하여 엔터프라이즈 전반에서 데이터의 기밀성, 무결성, 복원력을 보장합니다.
- 에버퓨어 IAM 2.0(Everpure IAM 2.0)은 엔터프라이즈급 ID 관리와 접근 제어 기능을 제공하여 다양한 환경에서 데이터 보안을 한층 강화합니다. 제로 트러스트 원칙을 기반으로 구축된 IAM 2.0은 세분화된 역할 기반 접근 제어(RBAC), 페더레이션 ID 통합, 다중 인증(MFA)을 제공하여 오로지 검증된 사용자와 서비스만 중요 데이터와 관리 기능에 접근할 수 있도록 보장합니다. 또한 IAM 2.0은 중앙 집중식 정책 관리와 감사 대응에 필요한 가시성을 제공하여 관리를 간소화하는 동시에 에버퓨어(Everpure) 생태계 전반의 보안, 규정 준수, 운영 효율성을 높입니다.
- 에버퓨어 에버그린(Everpure Evergreen®) 모델은 중단 없는 업그레이드, 펌웨어 검증, 지속적인 혁신을 통해 이러한 기본 보안 아키텍처를 지속적으로 확장합니다. 이를 통해 고객의 환경은 시간이 지나도 높은 가용성을 유지하고, 규정을 준수하며, 보안이 강화되고, 최적화된 상태로 운영됩니다.

에버퓨어(Everpure)는 위협을 식별하고 대응하기 위한 내장 기능과 통합 기능을 기반으로 **연계형 위협 탐지** 기능을 제공하며, 네이티브 위협 탐지와 대응, 지속적인 보안과 랜섬웨어 평가, 업계를 선도하는 사이버 보안 플랫폼과 원활한 통합을 지원합니다.

- 에버퓨어(Everpure)는 데이터 계층에 실시간 가시성과 실행 가능한 인텔리전스를 제공하는 네이티브 위협 탐지 기능을 제공합니다. 조직은 고급 행동 분석과 휴리스틱 분석을 활용하여 이상 징후, 무단 접근, 의심스러운 데이터 활동을 탐지할 수 있습니다. 또한 플랫폼은 침해 징후를 초기에 선제적으로 식별하고 풍부한 컨텍스트 인사이트를 제공하여 운영 부담을 최소화하면서도 신속하고 정확하게 대응하도록 지원합니다.
- 에버퓨어 AI 코파일럿(Everpure AI Copilot) 기반의 에버퓨어 시큐리티 어세스먼트 2.0(Everpure Security Assessment 2.0)은 조직의 보안 상태를 심층적으로 분석하여 공통 취약점 및 노출(CVE)을 포함한 위험 요소, 취약점, 이상 징후를 신속하게 식별합니다. 내장된 에이전트는 위협을 자동으로 탐지하고 대응하도록 지원하여, 운영 부담을 최소화하면서도 선제적으로 위협을 해결하고 사이버 복원력을 강화하도록 합니다.
- 에버퓨어(Everpure)는 SIEM, UEBA, 확장형 탐지와 대응(XDR) 솔루션에 원활하게 통합되어 스토리지 계층에서 발생하는 위협에 대한 실시간 가시성을 제공함으로써 위협 탐지와 대응 속도를 높입니다. 보안 분석을 위한 전용 스토리지 계층으로 활용할 경우 에버퓨어(Everpure)는 뛰어난 성능과 확장성을 제공하여 대규모 보안 워크로드까지 효율적으로 처리하면서, 동시에 포괄적인 위협 모니터링과 데이터 보호를 지원합니다.

동적 대응과 복구는 업계를 선도하는 기능과 통합을 통해 워크로드에 신속하게 대응하고 복구할 수 있도록 하며, 자동화된 계층형 복원력, 온디맨드 복구 영역, 원활한 데이터 보호 통합 기능을 제공합니다.

- 에버퓨어(Everpure)의 자동화된 다계층 복원력은 에버퓨어 레질리언스(Everpure Resilience) 서비스 자동화 기능과 프로비저닝 기능을 기반으로 하며, 변경 불가능하고 삭제할 수 없는 데이터 스냅샷, 데이터 복제, 스트리밍 데이터 보호, 서비스형 재해 복구(DRaaS)를 결합하여 활용합니다. 이를 통해 진화하는 사이버 위협에 대응해 데이터 가용성을 보장하고, 단순한 운영 중단부터 복잡하고 파괴적인 사이버 공격까지 복구할 수 있는 성능과 역량을 제공합니다.
- 에버퓨어(Everpure) 복구 영역은 완전하게 구성된 IRE 를 자동으로 프로비저닝하여, 사이버 사고 발생 후 복구를 위한 깨끗하고 안전한 공간을

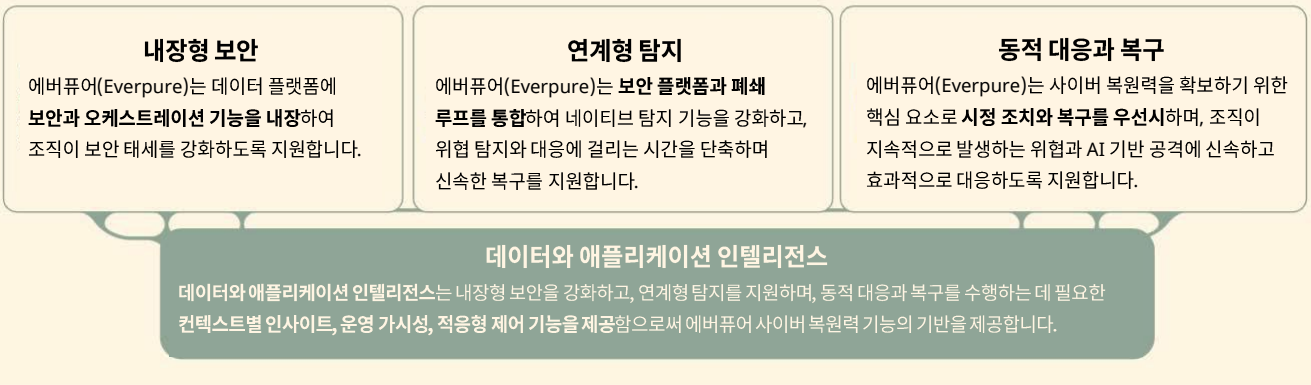
보장합니다. 각 IRE는 컴퓨팅, 네트워킹, 스토리지 리소스 구성이 완료된 상태이므로 필요시 즉시 사용할 수 있습니다. 복구 영역은 자동화된 프로비저닝과 스크립트 기반 워크플로우를 활용하여 정확한 설정을 보장하고, 배포 속도를 높이며, 수동 작업에 따른 오류 발생 위험을 제거합니다. 이러한 자동화는 복구 운영을 간소화하고 복원력을 강화하며, 조직이 중요 워크로드를 신속하고 안정적으로 복원할 수 있도록 지원합니다.

- **에버퓨어(Everpure)**는 주요 데이터 보호 솔루션을 위한 업계 최고 수준의 성능과 확장성을 제공해 백업 속도를 높이고 핵심 워크로드를 신속하게 복구할 수 있도록 합니다. 에버퓨어(Everpure)는 루브리크(Rubrik), 컴볼트(Commvault), 빔(Veeam)과 같은 선도적인 공급업체와 원활하게 통합되어, 종단간 데이터 복원력을 보장하며, 운영 환경에 미치는 영향을 최소화하면서도 조직이 데이터를 효율적으로 보호, 관리, 복구할 수 있도록 지원합니다.

데이터 인텔리전스 기반은 업계를 선도하는 에버퓨어 데이터 인텔리전스(Everpure Data Intelligence, 기존 1 터치) 솔루션을 기반으로 하여, 데이터를 보호하고, 탐지 대상을 설정하며, 대응 조치와 복구의 우선순위를 정하는 데 필요한 맥락 기반 인텔리전스를 제공합니다.

- **내장형 보안:** 민감 데이터를 분류하고, 인프라 수준을 넘어 설계상의 보안 보호 기능을 확장하며, 중요 데이터를 식별하여 규정 준수를 강화하고 위험을 줄입니다.
- **연계형 탐지:** 데이터 인텔리전스를 활용해 탐지 정책을 수립하고, 실행 가능한 컨텍스트로 SIEM과 보안 오케스트레이션, 자동화, 대응(SOAR)을 강화하며, 텔레메트리와 데이터 인텔리전스를 결합해 우선순위 기반 대응을 지원합니다.
- **동적 대응과 복구:** 데이터와 애플리케이션 컨텍스트를 사용하여 복구 우선순위를 지정하고, 정책과 워크플로우에 필요한 정보를 제공합니다.

수동적 공격 대상에서 능동적 방어자로: 최후의 방어선



솔루션 구성 요소

에버퓨어(Everpure)는 업계를 선도하는 여러 기능과 통합 지원을 바탕으로 조직이 사이버 공격과 재해로부터 신속하게 운영을 복구하고 위협을 탐지하여 대응하도록 지원합니다.

에버퓨어 데이터 인텔리전스

- 조직의 네트워크 전반에서 데이터, 소스, 흐름을 자동으로 탐색합니다.
- 지속적으로 고도화되는 AI/ML 기반의 실행 가능한 인텔리전스를 활용하여 데이터 민감도를 정확하게 컨텍스트별로 분류합니다.
- 통합된 데이터 소스 전반에서 규정 준수와 보고를 위해 단일한 맥락 기반 정보를 생성하는 통합된 확장형 데이터 인텔리전스를 제공합니다.

퓨리티(Purity), 플래시어레이(FlashArray™),

플래시블레이드(FlashBlade®) 시스템을 갖춘 에버퓨어 플랫폼

- 복구 워크로드를 동적으로 프로비저닝하여 블록과 파일 워크로드를 통합하고 데이터 사일로를 제거합니다.
- 최고 수준의 데이터 절감 기술과 99.9999%의 고가용성을 바탕으로 150μs~1ms의 초저지연 성능을 제공하여 데이터에 신속하게 접근할 수 있습니다.
- 전체 플릿에 걸쳐 애플리케이션과 워크로드를 실시간으로 인식하여 애플리케이션 수준의 복구를 지원합니다.

에버퓨어 레질리언스 서비스

- 온디맨드 IRE: 필요시 신속히 복구할 수 있도록 컴퓨팅, 네트워크, 스토리지 리소스를 포함한 IRE 를 자동으로 프로비저닝합니다.
- 자동화된 프로비저닝: 스크립트 기반 워크플로우를 통해 펌웨어를 오케스트레이션하고, 다양한 환경에서도 정확하고 일관된 설정을 보장하여 수작업과 오류를 줄입니다.
- 자동화된 계층형 복원력: 에버퓨어 레질리언스(Everpure Resilience) 서비스는 스냅샷, 복제, 복구 워크플로우를 자동으로 오케스트레이션하여 에버퓨어 계층형 복원력의 프로비저닝과 관리 과정을 간소화하고, 최소한의 수작업만으로 일관되고 안정적인 보호가 가능하도록 지원합니다.

퓨어 1(Pure1®)

- 선제적 위협 완화: 퓨어 1(Pure1)은 실행 가능한 평가를 제공하고, 취약점을 예측하며, 공격이 발생하기 전에 스냅샷과 세이프모드(SafeMode™) 설정을 비롯한 스토리지 모범 사례 구성을 제안하여 보안 태세를 강화합니다.
- 지능형 탐지와 대응: AI 기반 이상 징후 탐지 기능은 스토리지 동작을 모니터링하여 의심스러운 활동을 식별하고, SIEM, SOAR, XDR 플랫폼과 통합하여 변경 불가능한 스냅샷 생성, 잠재적 위협 격리 같은 자동화된 보호 조치를 실행합니다.
- 간편하고 안전한 복구: 퓨어 1(Pure1)은 마지막으로 확인된 정상 스냅샷을 식별하고 위협 인텔리전스를 연계 분석하여 비즈니스 중단을 최소화하는 동시에 신속하고 안정적인 복구를 지원하고 재감염을 방지합니다.

에버그린 구독 모델

에버그린(Evergreen)은 중단 없이 환경을 지속적으로 발전시켜 보안, 규정 준수, 최적화 상태를 유지함으로써 사이버 복원력을 강화합니다.

- 에버그린 교체 서비스: 에버그린(Evergreen)은 사이버 사고로 인해 하드웨어가 손상되거나 침해된 경우 신속하고 중단 없는 하드웨어 교체를 지원하여 신뢰할 수 있는 안전한 기반을 복원하고 복구와 지속적인 운영을 보장합니다.
- 지속적인 보안 강화와 규정 준수: 에버그린(Evergreen)은 지속적인 펌웨어 검증, 선제적인 패치 적용, 변화하는 보안 표준 준수를 통해 다운타임이나 서비스 중단 없이 스토리지 환경을 기본적으로 안전한 상태로 유지합니다.
- 중단 없는 업그레이드: 하드웨어와 소프트웨어 업데이트를 중단 없이 원활하게 적용하여 성능, 가용성, 중요 데이터 보호 수준을 유지하면서 복원력을 강화합니다.

사이버 보안 통합

- SIEM, UEBA, XDR 솔루션과 통합하여 스토리지 위협에 대한 실시간 가시성을 제공합니다.
- SIEM, UEBA, XDR 의 스토리지 계층으로 사용할 경우 향상된 성능과 확장성을 제공합니다.

데이터 보호 통합

- 선도적인 데이터 보호 솔루션에 필요한 성능과 확장성을 제공하여 더 빠른 백업과 신속한 복구를 지원합니다.
- 루브릭(Rubrik), 컴볼트(Commvault), 빔(Veeam)과 같은 선도적인 데이터 보호 공급업체의 최신 솔루션과 긴밀하게 통합되어 중단간 데이터 복원력을 제공합니다.

참고 자료

- 에버퓨어 [기술 협력 파트너\(TAP\)](#)에 대해 자세히 알아보기
- [조직이 진화하는 랜섬웨어 위협에 대응하는 방법](#) 알아보기
- [에버퓨어 사이버 복원력 구매자 가이드](#) 확인하기

에버퓨어 사이버 복원력 살펴보기

웹사이트 방문하기

02-6001-3330

