
# Acronis Advanced Security + Endpoint Detection and Response (EDR)

## 서비스 제공업체 전용

### 엔드포인트 보안 간소화

현재 침해의 60% 이상이 해킹[1]과 관련되어 있기 때문에 기업은 이제 고급 보안 솔루션과 제공업체를 통해 오늘날의 정교한 위협 환경에 대처해야 합니다. 그러나 이러한 위협에 대응할 수 있는 선도적인 EDR 솔루션은 다음과 같은 단점이 있습니다.

- 높은 비용과 복잡성으로 인해 저렴하게 이용할 수 없음
- 가치 창출에 오랜 시간 소요, 까다로운 교육 및 온보딩 요건
- 불완전한 보호, 비즈니스 연속성을 위해서는 추가적인 통합이 필요
- 운영하는 데 있어 보안 전문가로 구성된 대규모 팀이 필요하다는 확장성 문제

안타깝게도 이제 막 업무를 시작한 서비스 제공업체의 경우 자체 EDR 기반 서비스를 실행하는 데 필요한 기술과 비용이 부족할 수 있습니다. 보안 전문성이 확립된 제공업체의 경우, 선도적인 솔루션으로 탐지 및 대응 서비스를 구축하려고 시도하면 터무니없는 가격으로 미드 마켓 또는 중견중소기업 고객에게 배척당할 수도 있고, 솔루션 공급업체의 MDR 서비스와 경쟁하게 될 수도 있습니다.

### 서비스 제공업체용으로 설계된 Acronis Advanced Security + EDR

**아크로니스**는 서비스 제공업체가 효과적인 서비스를 제공하고 다양한 고객 요구 사항 및 예산을 맞추는 데 있어 균형을 유지해야 한다는 점을 잘 알고 있습니다.

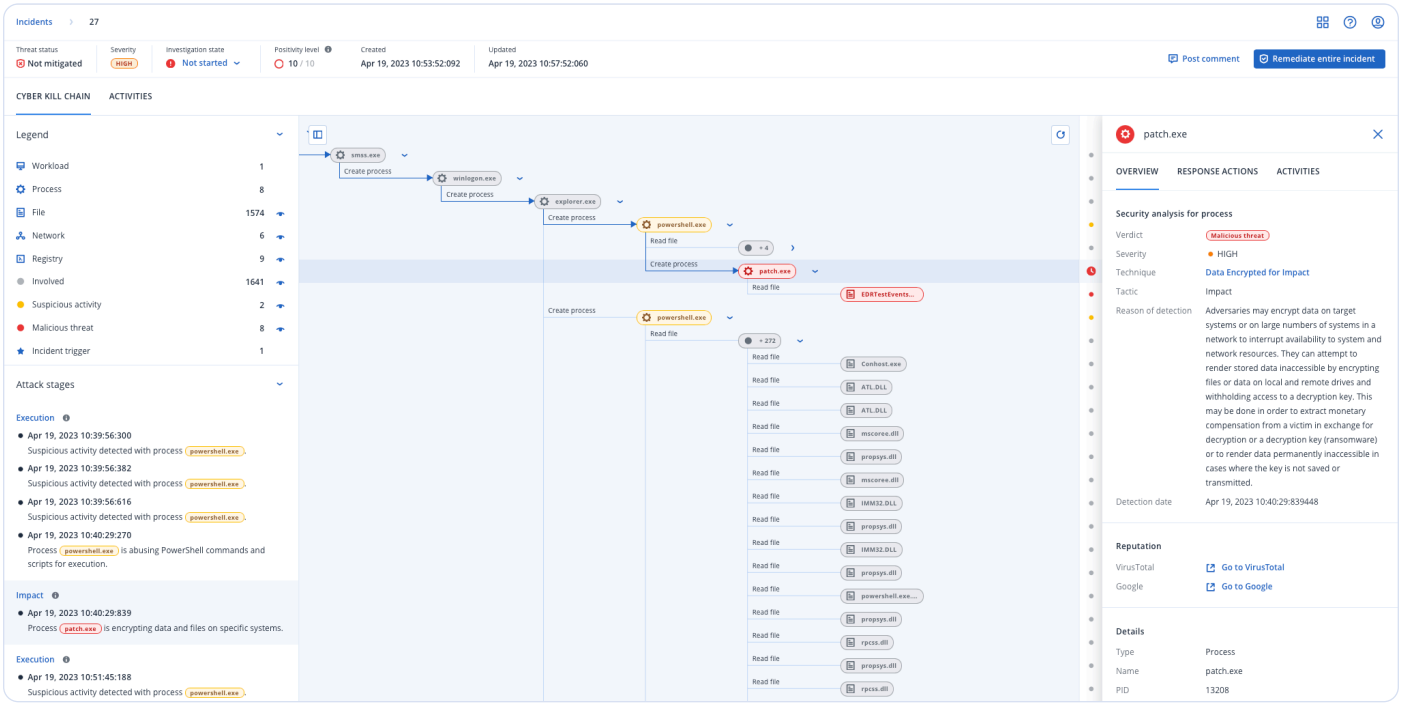
아크로니스는 또한 서비스 제공업체가 필요로 하는 고급 보안 솔루션은 수익과 사내 기술을 적정 규모로 조정할 수 있고, 멀티테넌트이고 SaaS 기반이며, 더 나은 보안 결과를 제공하고, 적절한 정도의 자동화 및 사용 편의성에 초점을 맞춰 여러 고객에게 그리고 고유한 환경에서도 신속하게 개시 및 확장할 수 있는 솔루션이라는 점도 알고 있습니다.

서비스 제공업체를 위해 설계된 **Acronis Advanced Security + EDR**을 사용하면 엔드포인트 보호를 간소화하여 지능적인 공격을 신속하게 탐지, 분석 및 해결하는 동시에 탁월한 비즈니스 연속성을 보장할 수 있습니다. 다중 포인트 제품의 비용과 복잡성을 제거하고 관리 및 디플로이가 간편한 하나의 완전한 사이버 보호 솔루션으로 팀을 지원하십시오.



Copyright © 2002-2023 Acronis International GmbH.

# 아크로니스로 탐지 및 대응 서비스를 간소화 하십시오.




| 신속한 대응을 위한 최적화된 공격 우선순위 지정 및 분석 | 탁월한 비즈니스 연속성을 위한 통합 백업 및 복구 기능 | 단일 에이전트에서 MSP용으로 설계된 완전한 사이버 보호 솔루션 |
|---|---|---|
| ▪ 잠재적인 인시던트의 우선순위를 지정하고 경보 피로도를 줄여 조사를 간소화합니다.<br>▪ 자동화된 상관관계 및 AI 기반 공격 해석을 통해 몇 시간이 아닌 몇 분 만에 대규모 분석을 수행합니다.<br>▪ MITRE ATT&CK® 전반의 가시성을 높여 공격이 어떻게 유입되었는지, 어떤 피해를 줬는지, 잠재적으로 어떻게 확산되었는지 등 공격 분석과 영향을 신속하게 파악합니다. | ▪ 포인트 보안 솔루션이 실패할 경우 탁월한 비즈니스 연속성을 제공하는 통합 백업 및 복구 기능을 제공합니다.<br>▪ 간소화된 원클릭 문제 해결 및 복구<br>▪ 식별, 보호, 탐지, 대응, 복구를 통해 NIST 사이버 보안 프레임워크 전체의 완전한 통합 보호 기능을 단일 솔루션에서 제공합니다. | ▪ 단일 아크로니스 에이전트 및 콘솔을 디플로이, 관리, 확장에 사용하여 쉽고 빠르게 새로운 서비스를 시작합니다.<br>▪ 안정적인 수익을 유지하고 운영 비용(OpEx)을 최소화하면서, 여러 고객에게 쉽게 확장 가능하고 고도로 숙련된 인력으로 구성된 대규모 팀을 운영할 필요가 없습니다.<br>▪ 비즈니스를 위해 경쟁하는 것이 아닌, 성공과 지원에 초점을 맞춘 공급업체와 협력합니다. |

## 수상 경력으로 검증된 엔드포인트 보호 기반 서비스

↘ Editors' choice

↘ AV-TEST 참여자 및 테스트 1위

↘ VB100 인증

↘ ICSA Labs 엔드포인트 안티맬웨어 인증

↘ AV-Comparatives 인증


Copyright © 2002-2023 Acronis International GmbH.

## 아크로니스에서 제공하는 탁월한 비즈니스 탄력성

아크로니스를 통해 NIST와 같이 확립된 업계 표준의 사이버 보안 프레임워크에 따라 종합적인 엔드포인트 보호 및 비즈니스 연속성을 제공하는 단일 플랫폼을 활용하여 취약한 자산과 데이터를 식별하고, 이를 사전에 보호하고, 위협을 탐지 및 차단하고, 공격에 대응하고, 그로부터 복구할 수 있습니다.

## 아크로니스: NIST 프레임워크에 부합하는 비즈니스 연속성과 사이버 복원력

### 식별

### 보호

### 탐지

### 대응

### 복구

| | | | | |
|---|---|---|---|---|
| **Advanced Security + EDR** | | | | |
| • 하드웨어 인벤토리<br>• 보호되지 않는 엔드포인트 검색 | • 취약점 평가<br>• 익스플로잇 방지<br>• 장치 제어<br>• 보안 구성 | • 새로운 위협 피드<br>• 새로운 위협의 IOC 검색<br>• 안티맬웨어와 안티랜섬웨어<br>• AI 및 ML 기반 행동 감지<br>• URL 필터링 | • 신속한 인시던트 분석<br>• 격리를 통해 워크로드 문제 해결<br>• 포렌식 백업 | • 공격에 대한 신속한 롤백<br>• 원클릭 대량 복구<br>• 자가 복구 |
| **Acronis Cyber Protect Cloud** | | | | |
| • SW 인벤토리<br>• 데이터 분류 | • 패치 관리<br>• DLP<br>• 백업 통합<br>• 사이버 스크립팅 | • 이메일 보안 | • 원격 연결을 통한 조사 | • 재해 복구 기능과의 사전 통합 |

## EDR 핵심 기능

### 인시던트의 우선순위 지정

인시던트 경보의 형태로 의심스러운 이벤트 체인의 우선순위를 지정하여 엔드포인트 이벤트를 모니터링하고 자동으로 상관관계를 지정하십시오.

### MITRE ATT&CK®에 매핑된 인시던트 자동 해석

MITRE ATT&CK®에 매핑된 공격에 대한 AI 기반 해석을 활용하여 대응을 간소화하고 위협에 대한 반응성을 높여

단 몇 분 만에 다음을 파악할 수 있습니다.

- 공격자가 침입한 방법
- 공격자가 흔적을 숨긴 방법
- 공격으로 인한 피해 및 발생 방식
- 공격이 확산된 방식



Copyright © 2002-2023 Acronis International GmbH.

## 공격에 대한 원클릭 대응으로 탁월한 비즈니스 연속성 보장

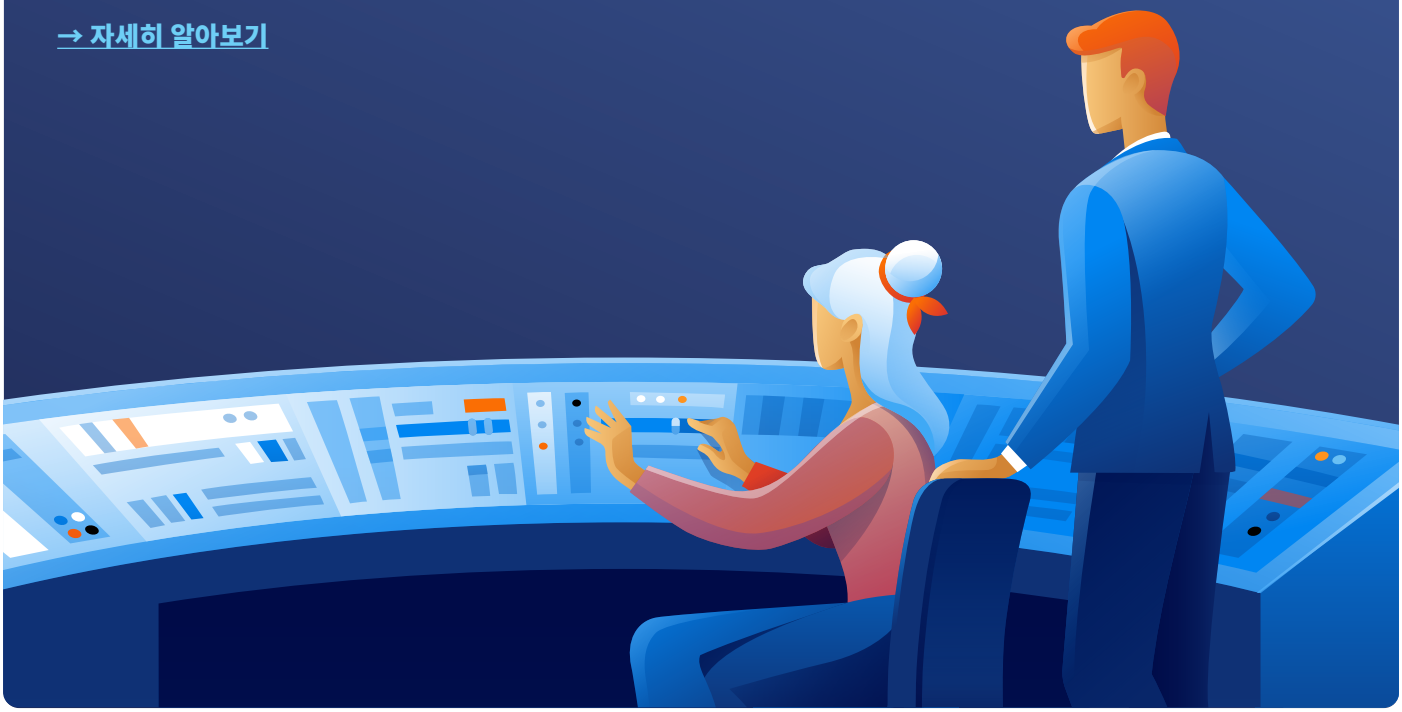
포인트 솔루션이 실패한 영역에서 성공하고 인시던트에 대한 원클릭 대응으로 다음과 같이 사이버 보안, 데이터 보호, 엔드포인트 보안 구성 관리 간의 통합 기능을 최대한 활용하십시오.

- 엔드포인트를 분리하고 위협을 격리하여 **문제 해결**
- 원격 연결 및 포렌식 백업을 사용하여 **추가로 조사**
- 공개된 취약점을 완전히 해결하여 **향후 공격 방지**
- 공격 롤백과 통합 백업 및 복구를 통해 **비즈니스 연속성 보장**


### 엔드포인트 보안 간소화, 지금 바로 바꿀 수 있습니다.

엔드포인트를 보호하는 데 있어 여러 도구를 사용하거나 여러 방면의 고급 보안 지식에 의존하지 않아도 됩니다. Acronis EDR로 엔드포인트 보안을 간소화하십시오.

→ 자세히 알아보기




1. 출처: "2022년도 데이터 위반 조사 보고서", Verizon



Copyright © 2002-2023 Acronis International GmbH. All rights reserved. 아크로니스와 아크로니스 로고는 미국 및/또는 기타 국가에서 Acronis International GmbH의 상표입니다. 기타 등록 상표 및 상표는 모두 해당 저작권자의 소유물입니다. 내용상의 오류를 제외한, 기술적 변경 또는 그림과의 차이점이 있을 수 있습니다. 2023-05