jamf | PROTECT

Jamf Protect는 MacOS의 자체 보안 기술과 Jamf의 MacOS 기반의 멀웨어 탐지 기술을 결합하여 단말의 보안 준수 상태를 관리하고 모니터링하는 Mac 전용 통합 엔드포인트 보안 솔루션입니다.

Mac focused AV(Anti-Virus)

MacOS의 자체 보안 프레임워크와 결합하여 Windows 기반 AV솔루션이 제공하는 것보다 훨씬 뛰어난 Mac malware를 방지하고 격리하는 정교한 AV 기능을 제공합니다.

- AV: 알려진 Mac malware 실행 방지
- 가시성: XProtect, Gatekeeper 및 MRT 관리 및 업데이트
- Malware insight: Jamf threat labs를 통한 Apple 전용 위협 탐지 및 타사 위협 정보 활용
- 검역: 악성코드가 식별되면 사용자 환경에서 자동으로 제거하고 분석을 위해 검역

Mac focused EDR (Endpoint Detection and Response)

Mac 전용 EDR 기능으로 오탐을 최소화하며 실시간 분석으로 경고를 수신하며 이로 인한 위협에 능동적으로 대응할 수 있습니다.

- 행위기반 분석: 광범위한 온디바이스 행동 분석을 통해 알려지지 않은 멀웨어 및 지능형 위협 탐지
- 광범위한 경보 적용 범위: Mitre ATT&CK 프레임워크 기반으로 공격 단계에 대한 매핑(초기 액세스, 실행, 지속성, 권한 상승, 방어 회피, 자격 증명 액세스, 검색, 측면 이동, 수집, 유출 및 영향 범주 등)

데이터 및 어플리케이션 제어

허가되지 않은 USB 저장장치로 데이터를 유출하거나 검증되지 않은 어플리케이션으로 인한 위험을 방지하기 위해 USB 통제 및 어플리케이션을 제어합니다.

- USB 사용 제어: 승인된 장치만 사용할 수 있도록 기타 USB의 기능 제한
- 데이터 모니터링: USB로 저장되는 파일에 대한 이력 수집
- 스크린샷 활동 모니터링: 승인되지 않은 앱을 통한 캡쳐 활동에 대한 이력 수집
- 앱 실행 방지: 알려진 취약한 버전의 앱 또는 신뢰할 수 없는 개발자의 앱 실행 방지, 지정된 앱 실행 방지 등

Threat Hunting 및 컴플라이언스 모니터링

규정된 컴플라이언스의 준수 현황을 모니터링하며 악의적인 활동을 식별하고 수집된 정보를 활용할 수 있도록 SIEM연동을 지원합니다.

- 활동 모니터링: 사용자에게 미치는 영향을 최소화하여 Mac에서 파일, 프로세스 등 다양한 정보를 수집
- 디바이스 로그: 외부 분석을 위해 MacOS의 로그를 수집
- 데이터 집계: 수집된 데이터에 대해 SIEM 연동을 할 수 있도록 API 제공

보안 사고 대응

공격이 감지되면 위협을 격리하고 제거하며, 장치 또는 사용자를 신뢰할 수 있는 상태로 만듭니다. 이는 사용자가 알아차리지 못하는 동안 자동으로 이루어집니다.

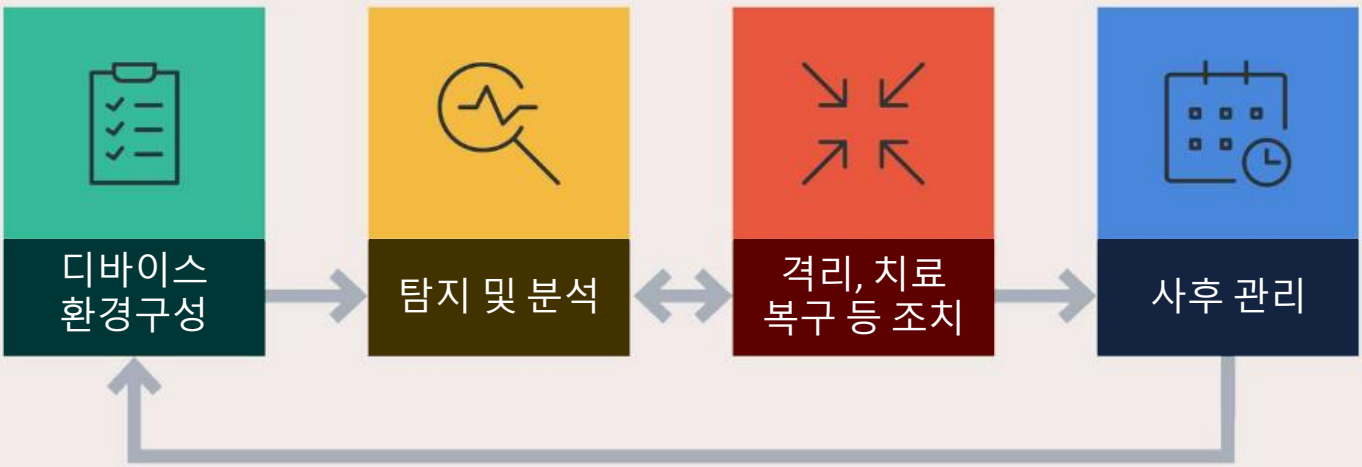
- 격리: 탐지된 malware를 격리하여 후속 피해 발생 방지
- 사용자 알림: 위협 발생 시 사용자 알림을 통해 추가 조치를 할 수 있도록 안내
- 자동 복구: jamf pro를 통해 위협 발생 시 디바이스를 조치
- 디바이스 잠금/격리: 위협의 전파를 차단하기 위해 디바이스를 잠그거나 네트워크 격리 조치(Jamf Pro 연동)

더 나은 사용자 경험

사용자의 안정적이며 생산적인 업무를 위해 사용자의 영향을 최소화합니다.

- 커널 확장 불필요(Kextless): Kextless를 통한 안정성 확보. 필요 시 시스템 확장만 활용
- 당일 지원: 매년 출시되는 신규 MacOS에 대한 당일 지원으로 신규 OS로 인한 이슈 제거
- Mac 전용: Mac 전용 솔루션으로 MacOS의 기본 보안 프레임워크와 결합하여 안정적인 탐지 및 차단을 보장

Jamf Protect는 Jamf Pro(MDM)와 결합하여 MacOS에 대한 보안 관리 Life Cycle을 구현합니다.



jamf | PROTECT

Endpoint Security	Security Operations		Information Technology
Anti-Virus	Custom Analytics	Device Isolation	File Integrity Monitoring
Behavioral Detections	MacOS Security Visibility	Device Lockdown	Application Control
Data Control	Threat Hunting	File Retrieval	Compliance Monitoring
Custom and Automatic Remediation	CIS Benchmarking	User Isolation	Standardized Remediation
	Unified Log Forwarding	User Lockdown	Application Inventory
	SIEM Integration		MacOS Redeployment

Jamf Protect
Jamf Pro
Jamf Connect

Jamf Protect 제품 관련 문의사항은 아래의 메일로 문의 바랍니다.

(문의사항 접수)