preempt

조건부 접속을 통한 기업 보호와 위협 예방

조직의 모든 사용자와 계정을 식별하고 이들이 무엇을 하고 액세스하는지를 이해하는데 어려움을 겪는다면 위험을 줄이고 위협을 사전에 차단하는 것은 매우 어려울 수 있습니다. Preempt 플랫폼은 인증 및 ID 보안에 대한 현대적인 접근 방식을 취하여, 위험을 줄이고 비즈니스에 영향을 미치기 전에 자동으로 예방할 수 있도록 도와줍니다.

Benefits

- Understand Identity Everywhere
- Detect Threats in Real-time
- Preempt Threats with Conditional Access

위협 예방을 위한 새로운 접근 방식

Preempt 플랫폼은 네트워크에 있는 모든 사용자를 신속하게 발견하고 지속적으로 위험에 대한 통찰력과 행동 분석을 제공함으로써 위협 요소가 비즈니스에 영향을 미치기 전에 실시간으로 더 효과적으로 탐지하고 대응할 수 있도록 지원합니다. 플랫폼의 고유한 적응 능력은 ID, 행위 및 위험에 기반한 올바른 유형의 대처 또는 통지를 통해 위협에 대한 대응을 자동화할 수 있게 해줍니다. 따라서 플랫폼은 위협을 중지하거나 유효한 사용자가 작업을 계속할 수 있게 해주는 적절한 수준의 보안을 제공하게 합니다.

Identity and Risk Insights

- ID에 대한 통합적이고 지속적인 가시성
- Human, service, privileged…

Analytics and Threat Detection

- Detects known/unknown
- 지속적으로 개선되는 즉각적인 값 제공

Conditional Access Anywhere

- 공격, 툴, 위험한 프로토콜 차단
- 위험을 위한 지속적인 감사

플랫폼 구성요소

신원 확인과 위험 감지

조직은 여러 보안 솔루션과 플랫폼을 통해 누가 무엇을, 언제, 어디서, 어떻게 액세스했는지에 대하여 분리되거나 불완전한 가시성을 가지고 있습니다. Preempt는 온 프레미스에서든 클라우드에서든 모든 사용자, 권한, 계정, 및 접속을 자동으로 발견하고 지속적으로 모니터링하여 이를 해결합니다.
사용이 간편한 단일 관리 콘솔을 통해, Identity and Risk Insights는 지속적인 상태 및 위험 평가를 수행하여, 암호 문제, 권한 액세스, 비정규 관리자, AD 구성 문제 등을 밝혀냅니다. 이를 통해, 모든 계정들을 보다 효과적으로 제어할 수 있습니다. 또한, 보안 팀이 리스크와 공격 표면을 신속하면서 간단하게 줄일 수 있기 때문에 감사를 쉽게 수행할 수 있게 합니다.

분석 및 위협 탐지

플랫폼의 사용자 및 엔티티 행동 분석은 권한이 있는 사용자와 서비스 계정을 포함하여 네트워크의 모든 사용자와 장치를 학습하고 위험 점수를 만듭니다. 시스템은 사용자와 기기를 분류하고 클라우드 서비스, SSO, VPN, Supervised와 Unsupervised 학습 및 실시간 인증 트래픽 등의 다양한 요인을 기반으로 위험을 측정합니다.
분석은 위험한 사용자 행동, 악의적인 내부자, 공격자, 손상된 계정 또는 장치, 측면 이동, 권한 상승 시도 및 내부 인프라에 대한 공격을 보여줄 수 있습니다.

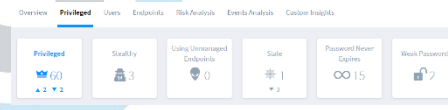
자격 증명을 기반으로 한 공격이 조직을 위태롭게 하는 최고의 방법입니다. Preempt는 위협 탐지에 대하여 다른 방법을 제시합니다. ID, 행동 및 위험에 초점을 맞춘 분석을 실시간 트래픽(passive/sniffer mode 또는 inline)과 결합함으로써 공격 감지에 더 높은 정확도를 얻을 수 있도록 하였습니다.

통합된 가시성을 통한 저장 손실 및 위험 감소

- ✓ 지속적으로 모든 사용자를 발견: Privileged, 서비스 계정, 일반 사용자, 오래된 계정
- ✓ 통합 사용자 액세스 프로필 개발 및 의심스러운 동작 식별
- ✓ 위험 감소 및 공격 실행 전 문제 발견

자격 인증 기반 위협을 실시간으로 탐지 및 조사

- ✓ 의심스럽거나 위험한 동작의 실시간 탐지
- ✓ 결정론적 공격 식별 및 악의적 공격 도구 사용
- ✓ 향상된 조사 및 threat hunting
- ✓ Conditional Access를 통해 향상된 위험 영역 식별



독특하게 Preempt 플랫폼을 사용하면 네트워크 툴(예:PsExec, PowerShell)의 오용과 해킹 툴(예:Mimikatz, Bloodhound 등)의 사용으로 인한 측면 이동 및 무단 도메인 액세스를 방지할 수 있습니다. Preempt는 또한 Kerberoasting, Pass-the-Hash, Golden Ticket과 같은 공격 탐지뿐만 아니라, 불안정한 프로토콜 사용량을 제어하고 자격 증명 전달 및 암호 균열을 포함한 보안 위협의 위험이 될 수 있는 인증 프로토콜(NTLM, Kerberos, LDAP 등)을 심층적으로 검사할 수 있는 기능을 가지고 위험을 줄일 수 있습니다.

위협 방지를 위한 조건부 액세스

보안 사고에 압박을 받고 있는 팀은 결코 모든 위협에 대응할 수 없습니다. 하지만, 플랫폼의 조건부 액세스 기능은 의심스러운 동작이 감지되었을 때, 위협에 즉시 사전 대응하기 때문에 전문가의 개입을 필요로 하지 않으며, 사용자의 업무를 방해하지도 않습니다.

Preempt는 지속적으로 사용자와 상호작용하여 위협을 확인하고 정책을 실행합니다. 세분화된 조치를 통해, 리스크에 적절한 수준의 대응을 할 수 있으며, 이는 상황 변화에 기반하여 자동으로 조정됩니다.

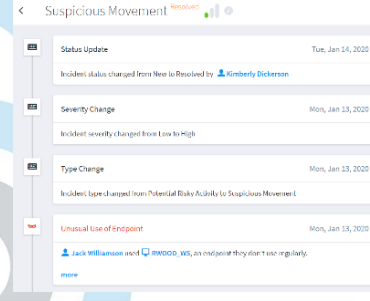
정책 기반 대응(Block, MFA 적용, 격리, 권한 축소, 경보, 허용 등)은 신원, 행동, 리스크에 따라 지속적으로 조정됩니다. 예를 들어, 액세스 권한을 부여하기에 앞서 위험 행동에 따라 사용자에게 MFA를 요구할 수 있습니다.

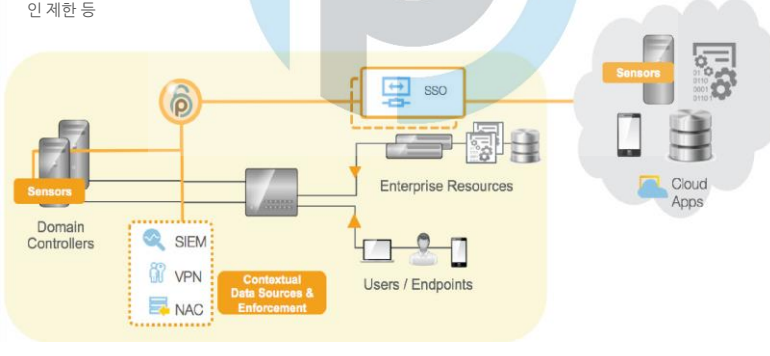
적응형 MFA는 사용자의 요구, 정책에 따라 다양한 유연성을 제공합니다.

- 정책 기반 시행을 추가하여 내부 자원을 즉각적으로 보호할 수 있습니다.
- 응용 프로그램을 수정하거나 단말 에이전트를 설치할 필요 없이, MFA를 어떤 네트워크 리소스 앞이든 쉽게 추가할 수 있습니다.
- 누가, 어떤 리소스에, 어떠한 상황(역할, 장치, 위치)에 액세스할 수 있도록 할 것인지를 설정할 수 있습니다.예 : 협력사의 중요 서버 액세스 제한, 서비스 계정 별로 대화형 로그인 제한 등

공격 실행 전에 위협을 사전관리

- ✓ 실시간으로 위협 제거
- ✓ 자동 대응으로 효율성 극대화
- ✓ 온 프레미스 또는 클라우드 앱에 조건부 접속 추가
- ✓ 개발 또는 단말 에이전트 없이 모든 리소스에 MFA 추가





연관성 있는 데이터 소스 :
Network Traffic/Logs/Third Party Integrations

강제화 옵션 :
적응형 MFA/권한 축소/격리, 차단 + 기타

ShinwooTNS

PREEMPT 플랫폼을 사용하는 방법

적응형 MFA

+ ID, 행동 및 위험을 기반으로 한 조건부 접속
+ 워크스테이션 로그인 ID 확인
+ 고가 서버 및 애플리케이션 액세스 관리
+ 정책에 따른 조건부 접속
+ 모든 애플리케이션에 MFA 추가
+ 모든 환경(클라우드/ 온프레미스/ 하이브리드)에 적용

권한 계정 보안

+ 권한 있는 계정 사용/탐지
+ 권한 사용자에 대한 위험도 측정
+ 권한 상승, 측면이동 방지
+ 권한 액세스 남용 탐지
+ 숨겨진 관리자 계정 탐지
+ 정책 기반 제어

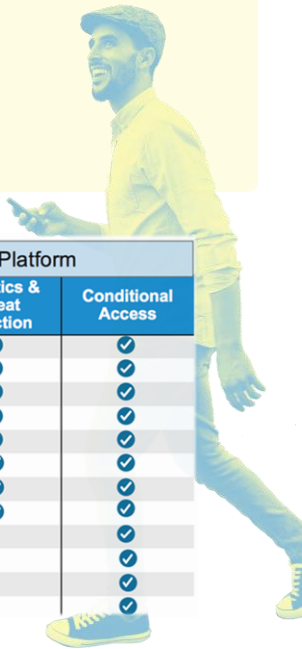
"우리는 네 가지 다른 솔루션을 검토했지만, 어떤 제품도 위협을 실시간으로 차단하고 대응할 수 없었다."
CISO AT LARGE INSURANCE ASSOCIATION

내부자 위협+인증 침해 탐지

+ 침해된 계정/기기 탐지
+ 측면이동 탐지
+ Golden Ticket, Kerberoasting과 같은 인프라 공격 탐지
+ 변칙적이거나 위험한 행동 탐지
+ 데이터 액세스 제한
+ 랜섬웨어 / 멀웨어 확산 탐지

Active Directory 보안

+ 워크스테이션 로그인 ID 확인
+ 고가 서버 및 애플리케이션 액세스 관리
+ 정책에 따른 액세스
+ 모든 애플리케이션에 MFA 추가



Value at Every Step

	Preempt Platform		
	Identity & Risk Insights	Analytics & Threat Detection	Conditional Access
User and Account Access Visibility	✓	✓	✓
Discovery of Privileged Accounts	✓	✓	✓
Discovery of Stealthy Admins & Service Accounts	✓	✓	✓
Password Health Visibility	✓	✓	✓
Compliance & Reporting	✓	✓	✓
Risky User Behavior & Anomaly Detection		✓	✓
Attack Tools & Misuse of Protocols		✓	✓
Lateral Movement & Threat Hunting		✓	✓
Adaptive Response and Policy Enforcement			✓
Secure Federated Access to Cloud Apps			✓
Secure Access Control for Any App			✓
Real-Time Threat Prevention			✓