Symantec
A Division of Broadcom

Product Brief

Symantec Advanced Authentication

Key Benefits

- 투명한 위험 분석과 소프트웨어 기반 2FA 인증으로 원활한 사용자 경험 제공
- 데이터 유출, 부적절한 액세스, 신원 도용에 대한 노출 감소
- 온라인 사기 감소로 운영 비용 절감
- 더 강력한 인증에 대한 정부 규정 및 업계 가이드라인 준수 지원

Key Features

- 실시간 위험 평가를 기반으로 민감한 로그인 및 트랜잭션 보호
- 디바이스 식별, 지리적 위치, 사용자 행동 및 기타 요인을 기반으로 위험을 평가
- 단계별 인증을 위해 이메일, 문자 또는 음성으로 전달되는 푸시 알림 및 일회용 비밀번호(OTP)와 같은 대역 외 방법을 지원
- 사용 및 사용자 지정이 쉬운 일반적인 사기 패턴을 다루는 기본 규칙 세트 제공
- 비밀번호, 보안 질문부터 2FA 소프트웨어 및 하드웨어 토큰까지 다양한 자격 증명 지원
- 웹 및 모바일 채널을 보호하고 데이터를 통합하여 포괄적인 사기 관리
- 여러 표준 기반 통합 옵션 제공: OATH, RADIUS, REST, SAML, SOAP 등 다양한 표준 기반 통합 옵션 제공
- CA 싱글사인온 및 기타 웹 접속 관리 시스템과 긴밀하게 통합

Lineup

- VIP Authentication - SaaS 기반 서비스로 기본적인 추가 수단 제공
- Advanced Authentication - 온프레미스 환경을 위한 솔루션으로 다양한 추가 인증 수단 제공
- Authentication Hub - 온프레미스와 클라우드 환경을 위해 쿠버네티스 기반 배포를 지원하는 바이오까지 포괄하는 가장 포괄적인 인증 수단 제공

Overview

Symantec Advanced Authentication은 모바일 및 웹 애플리케이션을 보호할 수 있는 안전하고 사용자 친화적이며 비용 효율적인 방법을 제공합니다. 이 솔루션을 통해 조직은 장치 식별, 지리적 위치, 사용자 행동 등을 기반으로 데이터를 조용하고 투명하게 수집하고 위험을 평가할 수 있습니다. 또한, Symantec Advanced Authentication은 다양한 소프트웨어 기반 2단계 인증 자격 증명을 제공하여 로그인을 더욱 안전하게 보호합니다. 위험 평가와 다단계 인증 정보를 결합하면 지능적이고 계층화된 보안 접근 방식을 구현할 수 있습니다. 이러한 접근 방식은 사용자 경험에 영향을 주지 않으면서 부적절한 액세스 및 온라인 신원 사기를 방지합니다.

Business Challenges

직원, 파트너, 고객 모두 온라인 애플리케이션에 쉽게 액세스할 수 있어야 합니다. 그리고 조직은 부적절한 액세스로부터 민감한 데이터를 보호해야 합니다. 이를 실현하려면 다음과 같은 과제를 해결해야 합니다.

- **온라인 트랜잭션 보안 강화:**비밀번호는 쉽게 유출될 수 있습니다. 조직은 사용자를 식별하고 부적절한 액세스로부터 보호할 수 있는 적응형 방법이 필요합니다.
- **모바일 장치 보안 강화:** 모바일 디바이스와 앱은 사용자가 비즈니스와 상호 작용하는 데 선호하는 방법이 되고 있습니다. 조직은 모든 접속 채널과 디바이스를 수용하는 일관된 인증 전략이 필요합니다.
- **규제 준수:** 많은 규정과 업계 지침에서 더 강력한 인증 메커니즘을 권장하거나 요구하고 있습니다. 기업은 이러한 요구 사항을 비용 효율적인 방식으로 해결해야 합니다.
- **사용자 경험 개선:** 사용자는 변덕스럽고 참을성이 없습니다. 조직은 사용자 경험에 영향을 주지 않으면서 보안을 강화해야 합니다.

Solutions Overview

Symantec Advanced Authentication은 두 가지 주요 인증 솔루션을 결합한 패키지 솔루션입니다.

- **Symantec Risk Authentication**
  이 솔루션을 통해 투명하고 지능적인 위험 분석을 수행하여 사용자가 본인이 맞는지 더욱 확실하게 확인할 수 있습니다. 이 소프트웨어는 모든 온라인 거래에 대해 장치, 지리적 위치 및 사용자 행동을 기반으로 위험을 평가하고 위험 점수가 정의된 임계값을 초과할 경우 단계별 인증을 시작할 수 있습니다.

- **Symantec Strong Authentication**

  이 솔루션은 다양한 자격 증명과 방법으로 웹 및 모바일 앱에 대한 다단계 인증 기능을 제공합니다. 이 소프트웨어를 사용하면 액세스하는 앱에 따라 적절한 보안 수준을 갖춘 올바른 자격 증명을 배포할 수 있습니다.

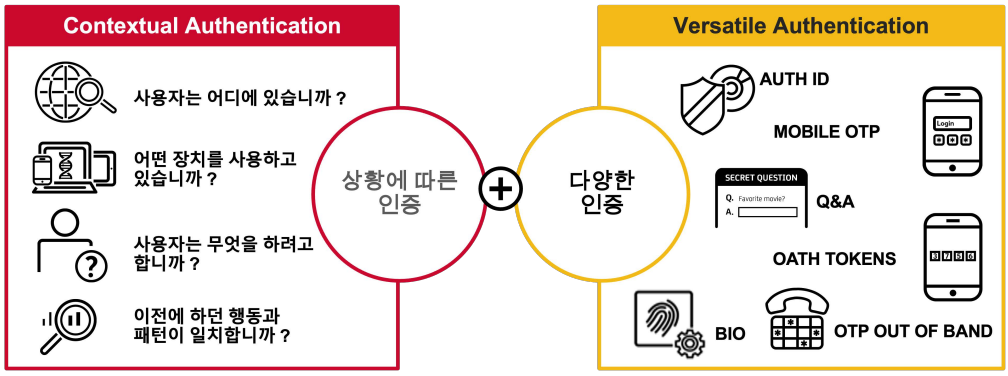
두 개의 솔루션을 함께 사용하면 비용, 편의성, 보안이 적절히 균형을 이룬 계층화된 보안 접근 방식을 통해 애플리케이션과 사용자 ID를 보호할 수 있습니다. 그 결과 보안이 향상되고 규정 준수 프로필이 개선되며 운영 비용이 절감됩니다.

Critical Differentiators

Symantec Advanced Authentication은 다음과 같은 중요한 차별화 요소를 제공하는 완벽한 솔루션입니다.

- 화이트박스 방식으로 각 위험 규칙, 결정 및결과에 대한 가시성을 제공합니다. 또한, 조직에 적합한 위험과 사용자 편의성 간의 황금비를 찾을 수 있습니다.
- 사용자 행동 프로파일링을 통해 사용자의 행동 패턴을 학습하고 표준에서 벗어나는 경우를 감지하여 보안을 강화합니다.
- 유연한 규칙 엔진을 통해 환경을 완벽하게 제어할 수 있습니다. 특히 특정 사용 사례 및 거래에 맞게 위험 엔진을 조정하기 위해 사용자 지정 규칙, 정책 및 조치를 생성할 수 있습니다.
- 다양한 인증 자격 증명과 흐름을 지원하며위험 수준에 따라 다양한 단계별 인증 방법을 설정할 수 있습니다.
- 의심스러운 활동 사례를 검토하고 관리하는 정책 기반 케이스 관리 기능도 제공합니다.
- 암호가 사용자 장치나 백엔드 시스템에 저장되지 않고 인터넷을 통해 암호가 전송되지 않기 때문에 암호 파일 도난의 위험을제거합니다.
- 암호화 위장은 무차별 대입 및 사전 공격으로부터 고유 AuthID 및 모바일 OTP 자격 증명을 보호하기 위해 사용되는 키 은폐 기술로 특허를 획득했습니다.

개별적으로 또는 함께 배포할 수 있는 토털 솔루션.

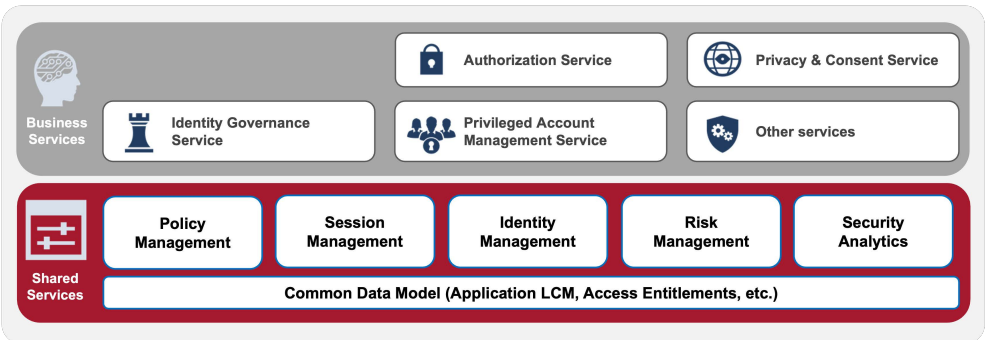


Continuous Authentication

위험 컨텍스트를 바탕으로 지속해서 신원을 확인하는 것을 뜻하는 지속적 인증(Continuous Authentication)은 최신 IAM 관리 접근 방식의 핵심 구성 요소입니다. 보안을 개선하고 비용을 절감하며 생산성을 높이는 데 도움이 될 수 있습니다. 또한, 위험 컨텍스트를 통한 지속적인 인증은 사용자의 신원과 행동을 지속적으로 확인하여 제로 트러스트 접근 방식을 구현하는 데 도움이 될 수 있습니다.지속적 인증에 대한 다양한 기업의 환경과 요구를 수용하기 위해 브로드컴 소프트웨어는 세 가지 솔루션을 제공합니다. VIP Authentication은 쉽고 빠른 구현이 가능한 SaaS 기반 서비스로 기본적인 추가 수단 제공합니다. Advanced Authentication은 온프레미스 환경을 위한 솔루션으로 다양한 추가 인증 수단 제공합니다. Advanced Hub는 온프레미스와 클라우드 환경을 위해 쿠버네티스 기반 배포를 지원하는 바이오까지 포괄하는 가장 포괄적인 인증 수단 제공합니다.

Authentication Hub와 SiteMinder의 결합

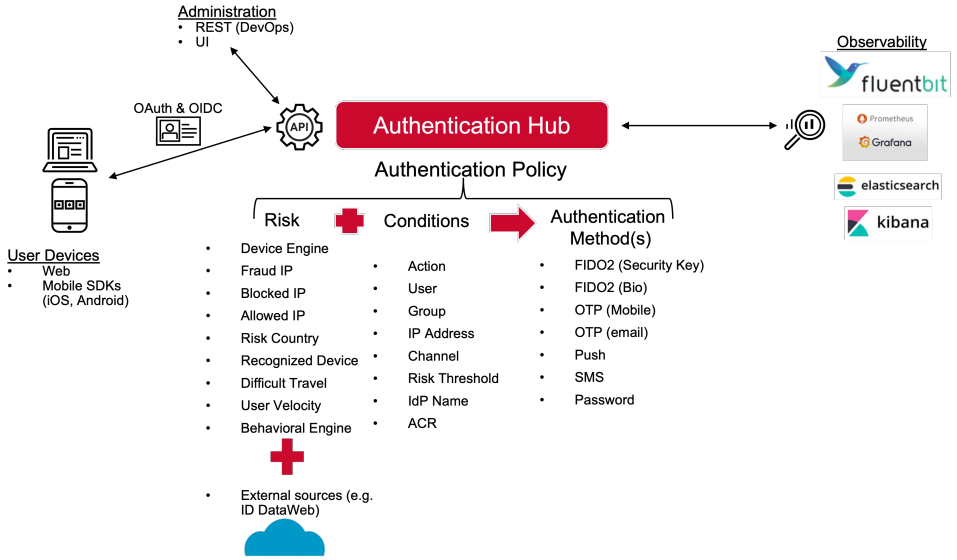
Authentication Hub와 SiteMinder를 결합하면 전사 수준의 지속적 인증 체계를 신속하게 구현하여 제로 트러스트로의 전환을 가속할 수 있습니다. Authentication Hub를 사용하여 SiteMinder로 보호되는 애플리케이션에 SSO를 제공하면 사용자가 단일 자격 증명 세트로 여러 애플리케이션에 로그인할 수 있어 사용자 경험을 개선하는 데 도움이 됩니다. 편의성만 높은 것이 아닙니다. 보안도 크게 강화됩니다. Authentication Hub는 SiteMinder로 보호되는 애플리케이션에 위험 기반 인증을 제공하는 데 사용할 수 있습니다. 이는 사용자가 액세스하려는 애플리케이션 또는 리소스의 위험 수준에 따라 사용자의 인증 요구 사항을 동적으로 조정하여 보안을 개선하는 데 도움이 될 수 있습니다.



Continuous Authentication with Enhanced Risk Context

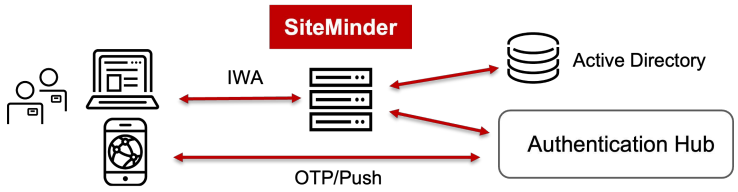
Authentication Hub와 SiteMinder를 연계하여 사용자 경험을 개선하고 보안을 강화하는 방법은 다음과 같습니다:

- **Authentication Hub 설정:** Authentication Hub는 보안 액세스를 위한 계층화된 접근 방식을 제공하는 유연한 인증 솔루션입니다. 먼저 선택한 인증 형식(예: 생체 인증, 디바이스 기반, 위치 기반 또는 행동 기반 인증)을 사용하도록 설정합니다. 이러한 요소는 요구 사항에 따라 지속적인 인증을 구현하기 위해 선택할 수 있습니다.
- **SiteMinder와 통합:** SiteMinder는 웹 애플리케이션에 대한 사용자 액세스를 제어하는 데 도움이 되는 액세스 관리 솔루션입니다. Authentication Hub가 구성되면 SiteMinder와 통합합니다. SiteMinder는 Authentication Hub에서 인증된 ID를 가져와 리소스에 대한 액세스를 제공하는 데 사용할 수 있습니다.
- **지속적 인증 및 위험 컨텍스트 설정:** 지속적인 인증을 설정하려면 위험 컨텍스트를 지속적으로 모니터링하고 평가해야 합니다. 갑작스러운 위치 변경이나 새 디바이스 등 비정상적인 동작이 감지되면 재인증 또는 추가 인증 요소를 요청하도록 시스템을 구성해야 합니다.
- **정책 개발 및 구현:** IAM 프로세스를 위한 정책을 개발합니다. 예를 들어 일정 기간 동안 활동이 없는 경우 또는 민감한 리소스에 액세스할 때와 같이 추가 인증이 필요한 시기를 결정합니다.

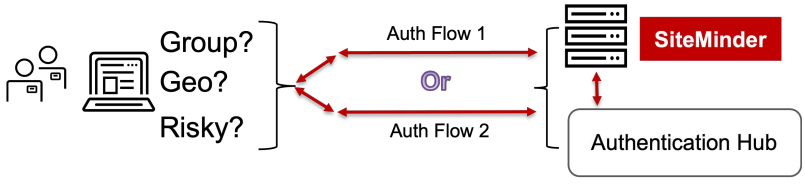


Common Use Case

-시나리오: 보조 OTP 또는 푸시가 있는 IWA
-적용 효과 : 사용자를 위한 간편함, 보안 강화, 상황에따른 자동 인증



-시나리오: 사용자 컨텍스트 기반 인증 정책 적용
-적용 효과: 컨텍스트에 기반한 지능형 인증



Symantec
A Division of Broadcom

Related Products

- **Symantec SiteMinder.** 고객 및 비즈니스 파트너를 위해 온프레미스, 호스팅 또는 파트너 기반 애플리케이션에 웹 싱글 사인온을사용하도록 설정합니다.
- **Layer7 API Gateway.** 앱, 디바이스 및비즈니스 전반에서 통합할 수 있는 신뢰할 수있는 API 보안 솔루션을 제공합니다.

For product information, visit our website at: broadcom.com/symantec-iam