Forcepoint

솔루션 요약

Forcepoint ONE: 일체형 클라우드 플랫폼이 하이브리드 인력의 보안을 간소화합니다

이용 사례

- 웹, 클라우드, 사설 앱의 데이터와 하이브리드 작업자 사이의 상호 작용에 대해 가시성과 관리 능력을 확보합니다.
- 관리형 또는 비관리형 장치에서 액세스하는 민감한 데이터의 오용을 방지합니다.
- 고위험군 웹 콘텐츠에 대한 액세스를 통제합니다.
- VPN의 복잡성을 배제하고 비즈니스 리소스와 사설 앱에 대한 신속하고 안전한 원격 액세스를 제공합니다.

솔루션

- 단일 통합 플랫폼을 이용하면 하나의 콘솔에서 하나의 엔드포인트 에이전트를 통해 모든 앱에 걸쳐 단일 정책 세트를 관리할 수 있습니다.
- 일체형 클라우드 제공 서비스는 보안 웹 게이트웨이(SWG), 클라우드 액세스 브로커(CASB), 제로 트러스트 네트워크 액세스(ZTNA)를 결합하여 액세스와 데이터를 보호합니다.
- 통합된 첨단 위협 방어 및 데이터 보안은 공격자를 차단하고 민감한 데이터를 보호합니다.
- RBI, CSPM, CDR 등의 추가 기능은 공개 클라우드 테넌트를 스캔하여 위험한 구성을 탐지하고, 콘텐츠 위협을 제거

결과

- 간소화 – 웹, 클라우드, 사설 앱에 대한 보안을 단일 정책 세트, 단일 콘솔, 단일 에이전트(에이전트 없는 지원 포함)로 통합합니다.
- 최신화 – 제로 트러스트 원칙을 SASE 아키텍처 그리고 원격 브라우저 격리, 다운로드 파일의 처리 등과 같은 첨단 보안 기능과 결합합니다.
- 모든 장소 – 300개가 넘는 인터넷 액세스 포인트(PoP)를 통해 전 세계적으로 사용 가능합니다.
- 안정성 – 2015년부터 검증된 99.99% 가동 시간을 제공합니다.
- 신속성 – 분산 시행 및 자동 확장을 통해 초크 포인트를 없앱니다.

복잡한 포인트 솔루션은 귀사를 위험에 노출시킵니다

보안이 점점 더 복잡해지고 있습니다. 인력의 75%가 원격으로 근무하면서 집과 사무실 사이의 경계가 모호해졌습니다. 요즘에는 데이터가 웹사이트, 클라우드 앱, 사설 앱을 비롯하여 어디에나 있습니다.

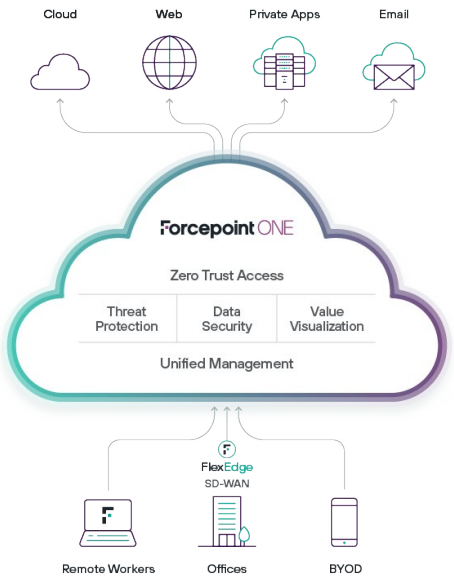
관리되지 않는 장치 및 BYOD를 사용하는 원격 근무자, 파트너, 계약자는 귀사를 취약하게 만듭니다. 느린 구식 VPN을 통해 장치들이 연결되어 있습니다. 심지어 협력 또는 통신을 위해 사용하는 업무 앱이 위험성을 증가시킵니다. 사이버 범죄자와 국가가 데이터를 노리고 모든 속임수를 사용하여 경계를 넘나들고 있습니다.

기존의 포인트 제품 포트폴리오는 이런 용도로 구축된 것이 아닙니다. 더 간소한 접근 방식이 필요합니다.

Forcepoint ONE이 보안을 간소화합니다

Forcepoint ONE은 일체형 클라우드 플랫폼으로 보안을 간소화합니다. 보안 웹 게이트웨이(SWG), 클라우드 액세스 보안 브로커(CASB), 제로 트러스트 네트워크 액세스(ZTNA) 등과 같은 중요한 보안 서비스를 통합했기 때문에 제로 트러스트 및 보안 서비스 에지(SSE, SASE의 보안 구성 요소)를 신속하게 채택할 수 있습니다.

분할된 제품은 더 이상 없습니다. 다양한 솔루션이 포함된 단일 플랫폼, 단일 콘솔, 단일 에이전트를 제공합니다. 단일 정책 세트를 통해 가시성을 확보하고 액세스를 관리하며 관리형 및 비관리형 앱과 모든 장치에서 데이터를 보호합니다.



모든 상호작용에 **종합적인 클라우드 보안 제공**

Forcepoint ONE의 클라우드 네이티브 제로 트러스트 기능

→ **웹, 클라우드, 사설 앱 액세스를 위한 통합형 게이트웨이** – SWG, CASB, ZTNA를 위해 비즈니스 앱에 대한 ID 기반의 엑세스 제어가 한 곳에서 관리됩니다.

→ **클라우드 및 사설 앱을 위한 비에이전트형 BYOD 보안** – 개인 장치에서 사설 비즈니스 웹 앱을 안전하게 사용하면서, 민감한 데이터의 보안을 유지합니다.

→ **통합된 첨단 위협 방어 및 데이터 보안**은 모든 게이트웨이에 걸쳐 데이터 손실과 유출을 방지하고 해커의 침입을 차단합니다.

→ **글로벌 액세스를 통한 동적 확장성** – AWS에 구축된 300개의 PoP는 장소에 상관없이 대기 시간이 짧은 신속한 연결 및 99.99%의 가동 시간을 제공합니다.

웹, 클라우드, 사설 앱에 대한 통합형 보안

→ **웹:** SWG는 위험성 및 카테고리를 기반으로 모든 웹 사이트와의 상호 작용을 모니터링하고 제어하여, 맬웨어 다운로드 또는 개인 파일 공유 및 이메일 계정에 민감한 데이터를 업로드하는 것을 차단합니다. 당사의 온디바이스 SWG는 장소에 상관없이 관리형 장치에 사용할 수 있는 정책을 시행합니다.

→ **클라우드:** CASB는 모든 장치에서 기업 SaaS 앱 및 데이터에 대한 세분화된 액세스를 시행합니다. CASB는 민감한 데이터의 다운로드와 맬웨어의 업로드를 실시간으로 차단합니다. 자주 사용하는 SaaS 및 IaaS에서 저장 데이터를 스캔하여 맬웨어 및 민감한 데이터를 검색하고 필요에 따라 수정합니다. CASB는 불명확한 IT 앱을 탐지하고 관리형 장치의 액세스를 제어합니다.

→ **사설 앱:** ZTNA는 VPN에 관련된 복잡성이나 위험성 없이 사설 애플리케이션에 대한 액세스를 보호하고 간소화합니다.

통합된 첨단 위협 방어 및 데이터 보안

→ **데이터 손실 방지(DLP):** 파일과 텍스트를 업로드하거나 다운로드할 때 민감한 데이터를 검사하고 적절하게 차단, 추적, 암호화 또는 삭제합니다.

→ **맬웨어 스캔:** 파일을 업로드하거나 다운로드할 때 맬웨어가 있는지 검사하고, 탐지되면 차단합니다.

단일 정책 세트를 통한 시행 간소화

→ **단일 관리 콘솔**은 구성, 모니터링, 보고를 간편화합니다.

→ **단일 로그인 정책 세트**는 사용자 위치, 장치 유형, 장치 상태, 사용자 행동, 사용자 그룹을 바탕으로 웹, 클라우드 또는 사설 앱에 대한 액세스를 통제하고 관리합니다. 이러한 매개 변수는 계정 탈취를 방지할 수 있습니다.

→ **단일 DLP 정책 세트** 는 관리형 SaaS 앱, 사설 앱, 웹사이트뿐만 아니라 관리형 SaaS 및 IaaS에 저장된 데이터와 관련하여, 민감한 데이터 및 맬웨어를 다운로드하거나 업로드하는 것을 통제합니다.

→ **통합형 온디바이스 에이전트**는 Windows 및 MacOS에서 SWG, CASB, ZTNA를 지원하고, 브라우저가 아닌 클라이언트 앱 및 불명확한 IT 앱을 통제합니다.

→ **통합 분석 및 가치 시각화** 는 보안 위험, 전반적인 활용도, 일체형 클라우드 보안 플랫폼의 영향에 대해 즉각적인 분석 자료를 제공합니다.

필요에 따라 사용할 수 있는 추가 기능

→ **클라우드 보안 태세 관리(CSPM):** AWS, Azure, GCP 테넌트 설정에 위험한 구성이 있는지 스캔하고 수동 또는 자동으로 교정합니다.

→ **SaaS 보안 태세 관리(SSPM):** Salesforce, ServiceNow, Office 365 테넌트 설정에 위험한 구성이 있는지 스캔하고 수동 또는 자동으로 교정합니다.

→ **원격 브라우저 격리(RBI):** 클라우드 호스팅 VM에서 브라우저를 실행하여, 로컬 장치의 웹 기반 맬웨어로부터 사용자를 보호합니다.

→ **제로 트러스트 콘텐츠 무력화 및 재구성(CDR):** 문서에 내장된 맬웨어를 제거하고, 사용자가 파일을 열기 전에 재생성시킵니다.

간편함을 제공하는 구독 방식

사용자별 연간 구독 이용 가능:

→ **일체형 에디션**은 웹, 클라우드, 사설 앱 보안에 적합합니다.

→ **웹 보안 에디션**을 이용하면 클라우드 및 사설 앱에 대한 지원을 나중에 추가할 수 있습니다.

→ **모두 구독**에는 중앙집중식 클라우드 관리, 데이터 손실 방지가 포함된 통합 정책, 통합형 엔드포인트 에이전트를 통한 자동 액세스 그리고 포괄적인 보고가 포함됩니다.

forcepoint.com/contact

[FP-Forcepoint ONE-Solution-Brief-KO] 18April2023