

데이터 시트

FortiSASE™

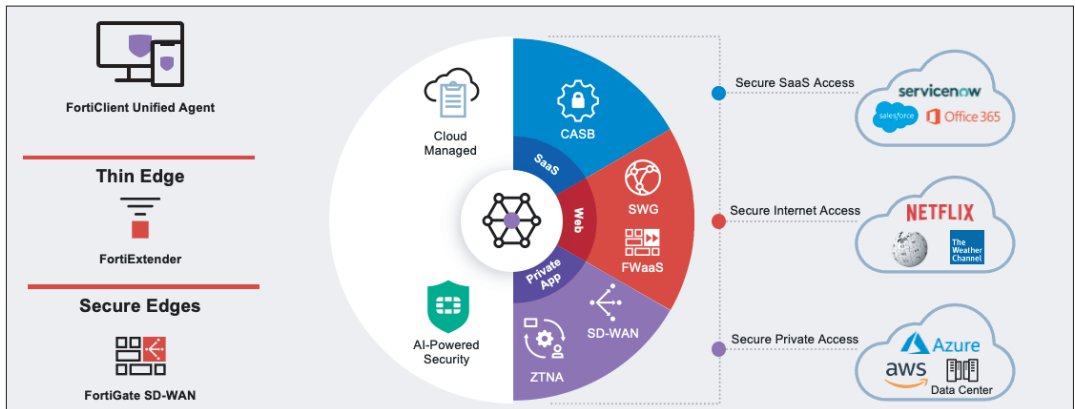


하이브리드 근무 인력을 위한 확장형 클라우드 기반 보안 및 네트워킹

대부분 기업에서 하이브리드 근무 인력의 존재가 새로운 현실로 다가오고 있습니다. 이런 현상으로 인해 공격 표면이 확장되면서 새로운 문제가 나타났고 원격 사용자를 보호하기는 더욱 어려워졌습니다. 새로운 네트워크 엣지와 원격 사용자가 늘어나고 있고, 이들은 별개의 프로젝트로 구현되는 경우가 많아서 사이버 범죄자들이 익스플로잇을 하려고 달려들 수 있는 보안 공백을 만들어냅니다. 그와 동시에 원격 사무실과 하이브리드 근무 인력이 많은 기업의 경우, 보안 네트워크 안팎에 있는 사용자에게 보안 정책을 일관적으로 적용하고 집행하면서도 모든 사람에게 우수한 사용자 경험을 제공하는 데 어려움을 겪는 경우가 많습니다.

시큐어 액세스 서비스 엣지(SASE) 아키텍처는 네트워킹과 보안을 융합함으로써, 사용자가 어디에 있든 보안 액세스와 고성능 연결을 지원합니다. 그러나 많은 클라우드 기반 솔루션이 하이브리드 근무 인력에게 엔터프라이즈급 보안을 제공하지 못합니다. 또한, 네트워크 엣지에 배포된 다양한 물리적, 가상적 네트워크 및 보안 도구와 매끄럽게 통합할 수 없어 모든 곳에서 일관적인 보안 태세와 우수한 사용자 경험을 제공하기가 어렵습니다.

포티넷의 단일 공급업체 SASE 접근법은 모든 엣지에서 기업이 엔터프라이즈급 보안과 우수한 사용자 경험을 일관적으로 적용함으로써 통합된 운영 체제와 에이전트에 네트워킹과 보안을 융합합니다. FortiSASE는 셸 엣지, 보안 엣지, 원격 사용자에게까지 FortiGuard 보안 서비스를 확장하여 사용자가 네트워크 안팎에서 안전하게 액세스할 수 있도록 합니다.



20년 이상 유기적 혁신을 거듭하고, 공통적인 FortiOS 운영 체제와 FortiGuard AI 기반 보안 서비스를 도입한 FortiSASE는 보안 웹 게이트웨이(SWG), 유니버설 제로 트러스트 네트워크 액세스(ZTNA), 차세대 듀얼 모드 클라우드 액세스 보안 브로커(CASB), 서비스형 방화벽(FWaaS), 클라우드 기반 SD-WAN 연결을 지원하여 기업에서 자본 지출 사업 모델을 운영 지출 사업 모델로 전환할 수 있도록 하면서도 간접비는 낮추고 사용자 경험과 보호는 높입니다. FortiSASE는 배포 위치와 관계없이 웹, 클라우드, 애플리케이션에 사용자와 세션별로 안전한 액세스를 지원하며, 완전히 통합된 엔터프라이즈급 보안이 결합되어 있습니다. 보안과 네트워킹이 매끄럽게 통합되어 있기 때문에 FortiSASE는 어디서나 모든 사용자에게 동일한 수준의 보호, 가시성 및 사용자 경험을 보장합니다.



FortiSASE는 서비스 기업 제어(SOC2) 인증을 받아서 규정 준수에 민감한 기업에 좋습니다. 이 인증은 솔루션 보안 제어가 AIPCA(American Institute of Certified Public Accountants)의 관련 신뢰 서비스 원칙 및 기준에 따라 운영되는지 여부를 독립적으로 검증합니다. SOC 2, II형 표준 인증은 포티넷에서 고객이 다양한 규정 준수 요구 사항을 충족할 수 있도록 보장하기 위한 노력을 기울이고 있다는 증거입니다.

하이라이트



FortiOS

포티넷의 통합 운영 체제인 FortiOS는 20년 이상 업계를 선도하는 혁신을 거듭했습니다. 이를 통해 클라우드에서 네트워킹과 보안을 매끄럽게 융합하는 포티넷만의 고유한 보안 중심 접근법을 지원합니다.



FortiGuard AI 기반 보안 서비스

포티넷의 AI 기반 보안 서비스는 애플리케이션, 콘텐츠, 웹 트래픽, 기기, 사용자를 가리지 않고 적용되며, 최신 공격에 대한 일관적인 실시간 보호를 제공하면서도 신속한 실시간 탐지와 대응을 보장합니다.



클라우드 기반 관리

간단한 클라우드 기반 관리를 통해 여러 곳에 흩어진 사용자와 애플리케이션에 대한 가시성과 제어 기능을 한 곳에서 제공하며, 이 모든 것은 업계 최고의 SLA로 지원됩니다.



주요 비즈니스 성과



어디서나 일관적인 보안 태세 적용

동일한 FortiOS를 기반으로 하는 일관적인 보안 태세로 보안의 공백을 메우고 공격 표면을 최소화합니다.



우수한 사용자 경험

지능적인 애플리케이션 스티어링과 동적인 라우팅을 지원하는 Secure SD-WAN 기능은 원격 사용자에게 우수한 사용자 경험을 기본적으로 제공합니다.



운영 효율

간단한 클라우드 기반 관리에 향상된 보안과 네트워크 분석을 결합하여 운영을 단순화합니다.



운영 지출 사업 모델로 전환

기업에서는 사전 지출이 들어가는 자본 투자에서 벗어나 단순한 사용자 기반 라이선스 모델로 옮겨갈 수 있습니다.

주요 사용 사례



보안 인터넷 액세스

회사 경계의 보호 범위에서 벗어난 원격 사용자 또는 지점에서 인터넷에 직접 연결하면 공격 표면과 관련 위험이 확장됩니다. FortiSASE는 에이전트 및 에이전트리스 접근법을 지원함으로써 관리되는 기기와 관리되지 않는 기기에 모두 포괄적인 보안 웹 게이트웨이(SWG)와 서비스형 방화벽(FWaaS) 기능을 제공합니다.



보안 비공개 액세스

기존의 VPN으로는 오늘날의 하이브리드 근무 인력이 경험하는 어려움을 해결할 수 없습니다. 이런 VPN은 연결을 검사하지 않기 때문에 의도치 않게 공격 표면을 확장하고 위협의 내부망으로 이동할 위험을 증가시키게 됩니다. FortiSASE 보안 비공개 액세스는 회사 애플리케이션에 업계에서 가장 유연한 보안 연결을 제공합니다. 기업에서는 보편적 ZTNA를 통해 애플리케이션에 세분화된 액세스 권한을 부여하고, 애플리케이션별 명시적 액세스 권한과 묵시적 신뢰에서 명시적 신뢰로의 중요한 전환을 지원합니다. 또한, FortiSASE 보안 비공개 액세스는 SD-WAN 네트워크와 매끄럽게 통합할 수 있으며, FortiSASE를 기반으로 지능적인 스티어링 및 동적인 라우팅을 기반으로 최단 경로를 자동으로 찾아내 회사 애플리케이션에 대한 액세스도 제공합니다.



보안 SaaS Access 액세스

SaaS 도입이 급격히 늘어나면서 많은 기업이 새도우 IT 문제와 데이터 유출 문제를 해결하는 데 어려움을 겪고 있습니다. FortiSASE 보안 SaaS 액세스는 인라인 및 API 기반 지원을 모두 사용하는 차세대 듀얼 모드 CASB와 함께 사용하면, 중요한 SaaS 애플리케이션을 찾아내고 위험한 애플리케이션을 보고하여 종합적인 가시성을 확보할 수 있고 새도우 IT 문제를 극복하는 데 도움을 줍니다. 또한, 차세대 CASB는 관리되는 기기와 관리되지 않는 기기에서 모두 애플리케이션의 민감한 데이터를 보호하고 멀웨어를 찾아내 복구 업데이트하기 위한 세분화된 액세스 제어 기능을 제공합니다.



주요 기능

서비스형 보안



보안 웹 게이트웨이(SWG)

암호화된 트래픽 등과 같이 웹 트래픽을 보호하기 위한 다양한 기능으로 가장 지능적인 웹 위협까지 모두 차단합니다. SWG는 웹 필터링, 안티바이러스, 파일 필터링, DLP(데이터 손실 방지) 등을 통해 관리되는 기기와 관리되지 않는 기기에 심층적 방어 전략을 지원합니다.



서비스형 방화벽(FWaaS)

독립적인 인증을 받고 호평을 받고 있는 FortiOS의 기능을 활용하는 포티넷의 FWaaS 기술은 클라우드에서 우수한 성능의 SSL 검사와 지능적 위협 탐지 기술을 제공합니다. 또한, 안전한 연결을 설정하여 유지하고 사용자 경험에는 아무런 영향 없이 인바운드 및 아웃바운드 트래픽을 분석합니다.



유니버설 ZTNA

위치와 관계없이 어디서나 모든 사용자와 기기에 ZTNA를 적용하면 묵시적 액세스를 명시적 제어로 전환할 수 있습니다. 애플리케이션별로 적용되는 세분화된 제어 기능은 사용자 인증, 연속적 자격 증명 및 컨텍스트 검증, 모니터링이 결합되어 있습니다.



차세대 듀얼 모드 CASB

인라인 및 API 기반 지원을 모두 제공하는 차세대 CASB는 중요한 SaaS 애플리케이션을 식별하여 새도우 IT 애플리케이션을 신고하며, 제재된 SaaS 애플리케이션에 안전한 액세스를 제공하고, 신뢰할 수 있는 엔드포인트만 SaaS 앱에 액세스할 수 있도록 제한하고, 애플리케이션 액세스를 위한 ZTNA 준비 검사를 지원합니다.

서비스형 네트워킹



소프트웨어 정의 WAN(SD-WAN)

포티넷의 클라우드 기반 SD-WAN 기능에는 회사 애플리케이션으로의 최단 거리를 찾아내는 애플리케이션 스티어링 및 동적 라우팅이 포함되며, 이러한 연결의 무결성이 변화함에 따라 경로를 수정하여 원격 근무자에게 우수한 사용자 경험을 제공하고 이를 유지합니다.



애플리케이션 가시성 및 제어

FortiSASE에는 애플리케이션에 대한 깊이 있는 가시성과 세분화된 제어를 보장하고 유지하기 위한 5,000개 이상의 애플리케이션 서명, 첫 패킷 식별, 딥 패킷 검사, 사용자 지정 애플리케이션 서명, SSL 복호화, 암호화가 필수로 적용되는 TLS1.3, 심층적 검사 등이 포함됩니다.

포티넷의 장점

FortiSASE는 격리된 채 클라우드에서만 서비스를 제공하는 것이 아니라, 포티넷 보안 패브릭을 연장하는 역할을 하며 어디서나 FortiOS(포티넷 보안 솔루션 포트폴리오 전체를 묶어주는 공통 운영 체제)의 기능을 확장하고 활용합니다. 이 솔루션에는 다음과 같은 장점이 있습니다.

일관적인 보안 및 우수한 사용자 경험

포괄적인 클라우드 기반 보안 및 네트워킹이 모든 사용자에게 적용되는 보편적 ZTNA와 결합됩니다.

하나의 통합 에이전트

포티넷의 통합 에이전트는 여러 사용 사례를 지원합니다. FortiClient는 다른 솔루션과 달리 각 사용 사례에 여러 에이전트를 사용할 필요 없이 ZTNA, SASE에 대한 트래픽 리디렉션, CASB, 엔드포인트 보안에 사용할 수 있습니다.

간단한 관리 및 사용

고유한 셀프 서비스 디자인을 적용한, 간단한 온보딩 및 관리 기능에는 업계에서 가장 유연하게 작동하는 계층적 사용자 기반 라이선싱 모델이 포함됩니다.

라이선스 정보

원격 사용자	대역	사용자 라이선스
FortiSASE Remote	100-499	FC2-10-EMS05-547-02-DD
	500-1999	FC3-10-EMS05-547-02-DD
	2000-9999	FC4-10-EMS05-547-02-DD
	10 000+	FC5-10-EMS05-547-02-DD



www.fortinet.com/kr

서울특별시 강남구 영동대로 325 에스타워 14 /15층

전화: 080-559-8989

Email: kr-callcenter@fortinet.com

Copyright © 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® 및 FortiGuard® 및 기타 상표는 Fortinet, Inc.의 등록상표입니다. 본문에 기재된 기타 포티넷 관련 상품명/상호 등 또한 포티넷의 등록 및/또는 관습법상 등재 상표일 수 있습니다. 다른 모든 제품 또는 회사명은 각각 해당하는 소유주의 등록상표일 수 있습니다. 본문에 기재된 성능 및 기타 지표는 이상적인 실험 조건으로 수행한 사내 연구소 테스트 결과로 획득한 것이며, 실제 성능 및 기타 결과는 다양하게 나타날 수 있습니다. 네트워크 번수, 서로 다른 네트워크 환경 및 기타 조건 등이 성능 결과에 영향을 미칠 수 있습니다. 본문에 기재된 어떠한 내용도 Fortinet에서 법적인 효력이 있는 약속을 한다는 의미가 아니며, Fortinet은 명시적이든 묵시적이든 모든 보장에 대한 책임을 부인하는 바입니다. 다만 Fortinet에서 법적 구속력이 있는 서면 계약을 체결하여 Fortinet 법무 자문위원(General Counsel)이 서명하고, 계약서에 기재된 제품이 분명하게 명시된 특정 성능 지표대로 성능을 발휘할 것이라고 구매자에게 분명히 보장한 경우는 예외입니다. 이러한 경우, 그와 같이 법적 구속력이 있는 서면 계약서에 분명히 기재된 특정 성능 지표만이 Fortinet에 법적 효력을 발휘합니다. 의미를 확실히 해두기 위하여, 그와 같은 보장은 포티넷의 사내 연구소 테스트를 실시한 조건과 동일한 이상적인 조건 하에서의 성능에만 국한됩니다. Fortinet은 명시적이든 묵시적이든 본문에서 거론한 각종 약속, 대변 및 보장 등에 대한 책임을 전면 부인하는 바입니다. Fortinet에는 본 출판물의 내용을 변경, 수정, 전송 또는 여타의 형태로 개정할 권한이 있으며 본 출판물의 내용은 최신 버전을 적용하는 것으로 합니다.