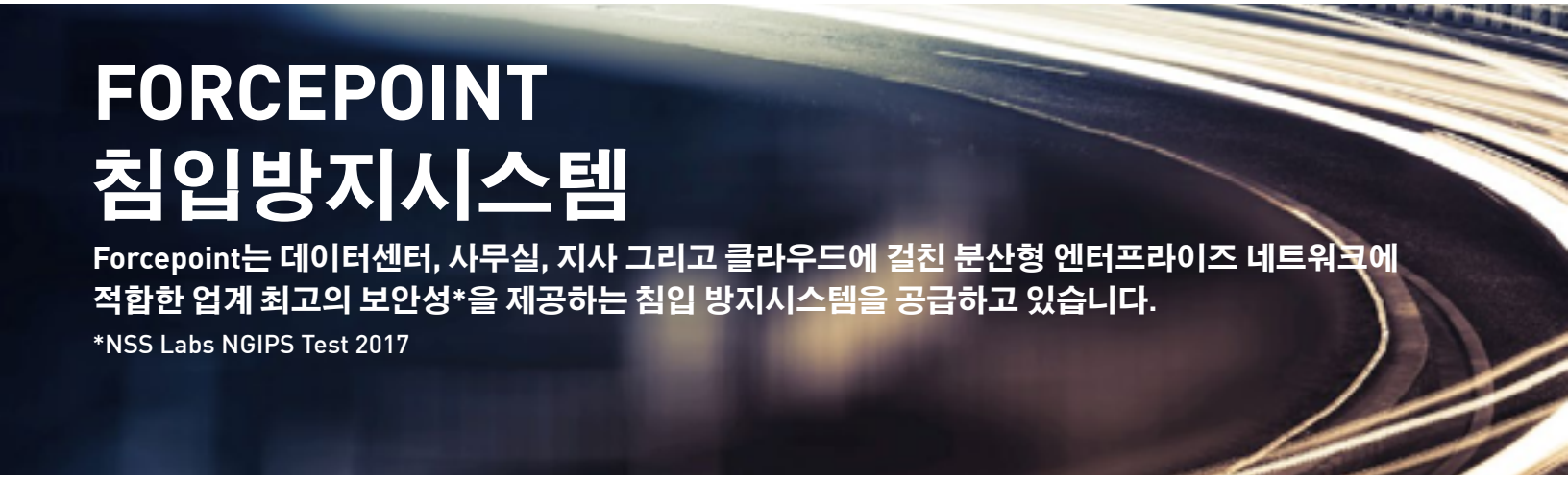
FORCEPOINT

데이터시트



FORCEPOINT 침입방지시스템

Forcepoint는 데이터센터, 사무실, 지사 그리고 클라우드에 걸친 분산형 엔터프라이즈 네트워크에 적합한 업계 최고의 보안성*을 제공하는 침입 방지시스템을 공급하고 있습니다.

*NSS Labs NGIPS Test 2017

Forcepoint의 네트워크 보안시스템은 업계에서 가장 보안이 뛰어난 침입 방지시스템을 제공합니다. 독립기관에서 시행한 시험에서 최고 등급을 받은 Forcepoint IPS는 독립형 레이어2 IPS 장치 또는 물리적, 가상 및 클라우드 환경에서 모든 기능을 지원하는 레이어 3 차세대 방화벽[NGFW]으로 적용이 가능합니다. 이는 공격자들이 엔터프라이즈 네트워크의 침투와 확산에 이용하는 회피기법, 익스플로잇 그리고 멀웨어를 무력화합니다.

효과 성과 속도가 뛰어난 아키텍처

Forcepoint는 단순한 패킷 검사가 아닌 동적 스트림기반 접근법을 채택하고 있습니다. 이는 실제의 페이로드를 재구성하고 검사해 익스플로잇과 멀웨어를 위장하는 회피기법들을 무력화합니다.

또한, 고속의 세분된 복호화기능으로 SSL/TLS 트래픽내에 숨겨진 공격을 검출합니다. Forcepoint는 각각의 페이로드스트림을 분석해 비정상적이거나 형태가 올바르지 못한 프로토콜 설정, 메타데이터 그리고 헤더를 검사하기 위해 프로토콜들의 각계층을 디코딩합니다.

장황한 패턴 기반의 시그니처메커니즘과 달리 Forcepoint의 보다 정교한 접근법은 단일의 간결한 핑거프린트를 이용하여 이와같은 공격들을 식별할 수 있도록 합니다. 핑거프린트는 각각의 프로토콜 상황 정보에 최적화된 고속의 결정적 유한오토마타(DFA)를 이용하여 매칭되어, CPU 자원에 대한 영향이 거의 없이 신규의 핑거프린트를 적용할 수 있습니다.

공격자들보다 앞서가는 지속적인 업데이트

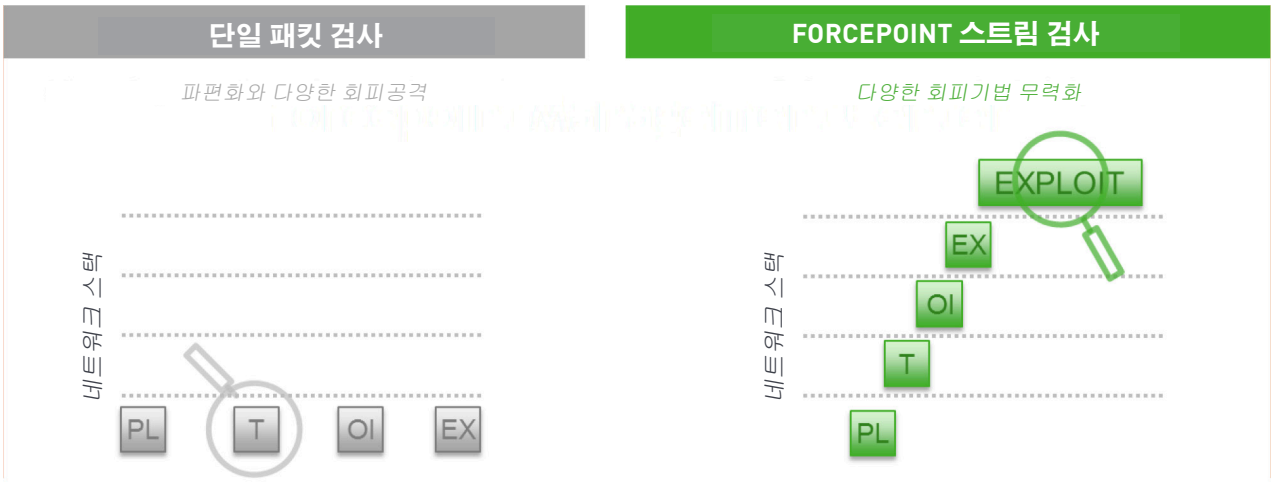
Forcepoint의 글로벌 연구팀은 위협관련 정보피드, 다양한 출처의 취약점보고서, 그리고 다양한 테스트 시스템들을 지속해서 검사함으로써 취약점을 분석하고 있습니다. 새롭게 발견된 핑거프린트들은 필요에 따라 당사의 클라우드 서비스를 통하여 배포되어 Forcepoint의 네트워크 보안시스템에 의해 자동으로 내려받게 됩니다. 이러한 선제적 접근법은 IT 팀들이 즉각적 공격에 노출되는 위험없이 신규 발표패치들을 분석하며, 취약점에 대한 대책을 구현하기 위한 시간을 확보할 수 있도록 합니다.

제로 데이공격과 유해 콘텐츠의 차단

Forcepoint의 네트워크 보안 제품들은 이전에는 알려지지 않았던 공격 유형과 유해 콘텐츠에 대한 다층적 방어 기능도 제공합니다. 송신 파일들은 철저한 평판과 멀웨어스캐닝을 거치며, 제로데이 공격과 같은 신규 위협들은 당사의 지능형 샌드박스 기술을 이용하여 색출 가능합니다. Forcepoint는 웹사이트와 콘텐츠의 분류와 필터링에 있어 업계 선도 기업으로, 당사의 IPS 장치와 방화벽을 이용해 조직들은 사업장 관련 규정을 더욱 쉽게 준수할 수 있습니다. 또한, 개인정보의 노출을 제한하며, 사용자들이 위험한 콘텐츠를 보유한 웹사이트를 방문하는 것 자체를 방지할 수 있습니다

장애 시개 방복원성

Forcepoint의 어플라이언스들은 IPS 또는 NGFW의 전원 이상실 되더라도 트래픽을 계속 유지하는 장애 시개 방인터페이스를 포함한, 일련의 모듈형 네트워크 카드들을 지원합니다.



Forcepoint는 풀스트림 복원 기법과 고속 익스플로잇 핑거프린팅을 조합하였습니다.

사업의 지속성 유지를 위한 보호기능

엔터프라이즈 네트워크, 애플리케이션, 데이터센터 그리고 엔드포인트에 대한 공격자들의 침투 능력은 매일같이 향상되고 있습니다. 이들은 일단 침투한 후에는 지적 재산, 고객정보, 그외 다양한 중요 데이터를 탈취하여 사업과 평판에 대해 재기 불가능한 피해를 일으킵니다.

인터넷 공격은 단순히 취약점에 대한 익스플로잇을 전파하는 수준을 능가하고 있습니다. 이러한 기법들은 여러 유명 제품 방화벽을 포함한 기존의 네트워크 보안장치들에 의한 탐지를 회피하는데 사용되고 있는 경우가 증가하고 있습니다.

이러한 회피 기법들은 여러 계층에서 동작하여 익스플로잇와 멀웨어드를 위장하여, 기존의 시그니처 기반의 패킷 검사 기법으로서는 탐지할 수 없습니다. 회피 기법을 이용할 경우 이미 수년전에 차단 되었던 구식의 공격도 내부 시스템의 무력화에 갑자기 사용될 수 있습니다.

Forcepoint는 다른 접근법을 채택했습니다. 당사의 업계 최고 IPS 엔진은 네트워크 방어의 세단계인 회피 기법의 무력화, 취약점에 대한 익스플로잇 탐지 그리고 멀웨어차단을 모두 지원하도록 개발 되었습니다. 이는 중단없이 보호 기능을 추가할 수 있도록 기존 방화벽 뒤에서 투명하게 또는 만능 보안을 지원하도록 모든 기능을 지원하는 NGFW의 일부로서 적용할 수 있습니다

Forcepoint의 모든 네트워크 보안 제품들은 지속해서 업데이트 되며, 중앙에서 관리 되고 귀사 네트워크 전반에 걸쳐 보안정책과 대시보드를 원활하게 공유할 수 있습니다. Forcepoint를 통하여 귀사의 데이터센터, 오피스 네트워크, 지사위치 또는 클라우드 환경에 걸쳐 신뢰성, 일관성 그리고 효율성을 실현하면서 귀사의 사업을 안전하게 유지할 수 있습니다.

www.forcepoint.com

비즈니스 장점

- **침해 감소**
- **중단없는 보안수준 향상**
- **IT 팀이 신규 패치를 적용하는 동안 새로운 취약점의 노출 감소**
- **지사, 클라우드 또는 데이터센터의 더욱 안전한 적용**
- **네트워크 인프라와 보안에 대한 TCO 감소**

주요 특징

- **레이어2 IPS 또는 레이어3 NGFW로 적용치**
- **실제 페이로드를 검사하는 스트림 검사 기능**
- **선구적인 회피기법 방어**
- **세분화 프라이버시 제어기능을 지원하는 고속 복호화**
- **프로토콜 이상 및 부정사용 탐지기능**
- **고속 DFA를 통한 익스플로잇과 멀웨어 탐지기능**
- **서비스 거부 공격(DoS) 탐지기능**
- **봇공격 방어**
- **클라우드 또는 온프레미스어 플라이언스를 통한 제로데이 샌드박스 기능**
- **업계 최고의 URL 필터링**
- **어플라이언스의 모듈형 고장시 개방 네트워크 인터페이스**
- **장비간의 통합 기능과 성능**
- **정책 기반 중앙 집중관리**
- **가동 중단없는 신속한 업데이트**

Forcepoint침입 방지시스템(IPS) 사양

지원 플랫폼	
어플라이언스	데이터센터, 네트워크에지와 지사에 적용 가능한 다수의 모듈형 어플라이언스 시리즈
클라우드인프라	Amazon Web Services, Microsoft Azure
가상 어플라이언스	x86 64비트 기반 시스템: VMware ESXi, VMware NSX, Microsoft Hyper-V 그리고 KVM 가상화 환경
적용 모드	독립형 IPS(레이어2, 고장시 개방 네트워크 인터페이스 모듈 선택사양) ,NGFW(레이어 3)의 일부
가상 컨텍스트	논리적 컨텍스트를 별도의 인터페이스와 정책으로 분리하기 위한 가상화

검사 기능	
복수 계층 트래픽 정규화/ 풀스팀 심층 검사	• 데이터스트림의 무결성을 보증하기 위한 실제 페이로드 재구성/ 분석 • 재구성 시 모호성을 일으킬 수 있는 중복된 하위 레벨 세그먼트 폐기
회피 차단 방어	비순서 프래그먼트, 중복 세그먼트, 프로토콜 조작, 난독화, 인코딩 속임 차단
동적 컨텍스트 탐지	프로토콜, 애플리케이션, 파일형식
프로토콜 특정의 트래픽취급/ 검사	이더넷, H.323, GRE, IPv4, IPv6, ICMP, IP-in-IP, IPv6 캡슐화, UDP, TCP, DNS, FTP, HTTP, HTTPS, IMAP, IMAPS, MGCP, MSRPC, NetBIOS 데이터그램, OPC Classic, OPC UA, 오라클 SQL.Net, POP3, POP3S, RSH, RSTP, SIP, SMTP, SSH, SunRPC, NBT, SCCP, SMB, SMB2, TCP 프록시, TFTP, Sidewinder Security Proxy를 이용한 통합 검사기능
SSL/TLS 트래픽의 세분 복호화	• HTTPS 클라이언트와 서버스 트림의 고성능 복호화 • 사용자 프라이버시의 보호와 개인데이터에 대한 조직의 노출을 제한하기 위한 정책기반 제어 • TLS 인증서 유효성 검사와 인증서 도메인명 기반 제외 목록
취약점 익스플로잇 탐지	• 프로토콜 비종속으로 모든 TCP/UDP 프로토콜에 대한 회피와 이상현상 로깅 • 클라이언트와 서버 양자의 CVE 취약점에 대해 가상패치 • 정교한 핑거 프린트 접근법으로 많은 시그니처의 불필요 • 고속의 결정적 유한 오토마타(DFA) 매칭엔진으로 새로운 핑거프린트의 빠른 관리 • Forcepoint에서 지속적인 핑거프린트 업데이트
사용자정의 핑거프린팅	• 프로토콜 비종속 핑거프린트 매칭 • 사용자정의 애플리케이션을 지원하는 정규 표현식 기반 핑거프린트 언어
정찰	IPv4와 IPv6에서의 TCP/UDP/ICMP 스캔, 스텔스와 저속 스캔탐지
봇넷차단기능	• 복호화 기반의 탐지와 메시지 길이 순서 분석 • 사용자들을 봇넷사이트들로 부터 차단 또는 경고하기 위한 자동 업데이트 URL 분류 기능
상관성	로컬 상관성, 로그 서버 상관성
DoS/DDoS 보호	• 동시 접속 제한을 포함한 SYN/UDP 플러드탐지, 인터페이스 기반 로그 압축기능 • 저속 HTTP 요청 기법에 대한 보호, 하프오픈(Half-open) 연결 제한 • 제어 영역과 데이터 영역의 분리
차단기법	직접차단, 연결 초기화, 블랙리스트(로컬및분산), HTML응답, HTTP 리다이렉트
트래픽 기록	부정 사용 상황에 대한 자동적 트래픽기록/ 발췌
자동 업데이트	• Forcepoint 보안 관리센터(SMC)로 부터의 지속적인 동적 업데이트 • 가상패치를 업데이트하며 신종 위협에 대한 탐지와 예방 기능제공

Forcepoint침입 방지시스템(IPS) 사양 (계속)

지능형 멀웨어 탐지와 파일 통제	
프로토콜	FTP, HTTP, HTTPS, POP3, IMAP, SMTP
파일필터링	효율적인 하향 선택 절차를 포함한, 정책기반 파일 필터링. 19개 파일 카테고리에서 200여개의 파일 형식 지원
파일평판	고성능 클라우드 기반의 멀우어평판 검사와 차단
백신	로컬 백신스캔엔진*
제로 데이샌드박스	Forcepoint Advanced Malware Detection은 클라우드와 온프레미스로 제공

URL 필터링	
URL 분류	Forcepoint Web Security와 Forcepoint Email Security 에서 사용되는 것과 같은 Forcepoint Threatseeker Intelligence로지원
자동 업데이트	신규사이트가분석됨에따라지속해서업데이트
카테고리 기반 접속 정책의 적용	Forcepoint NGFW URL 필터링은 추가 기능으로 제공

관리 및 모니터링	
관리 인터페이스	로그분석, 모니터링 및 보고 기능을 제공하는, 엔터프라이즈 수준 중앙 집중형 관리시스템 (상세정보는 Forcepoint Security Management Center 데이터시트 참조)
SNMP 모니터링	SNMPv1, SNMPv2c 그리고 SNMPv3
트래픽 캡처	콘솔 tcpdump, Forcepoint Security Management Center를 통한 원격 캡처기능
강력한 보안 관리 통신	엔진 관리 통신에 대해 256비트 암호화 사용
보안 인증	Extended Package Stateful Traffic Filter Firewall을 포함한 Common Criteria Network Devices Protection Profile, FISP 140-2 암호 인증, ANSSI 의 CSPN 인증, [First Level Security Certification USGv6]

*110/115 어플 라이언스는 로컬 멀웨어 방지 스캔을 지원하지 않음

연락처
www.forcepoint.com/contact

[DATASHEET_FORCEPOINT_TEMPLATE_EN] XXXXXX.062817