NEOPLEX 회사소개서

2017.08

NEOPLEX

1. 네오플렉스 개요


· 서울시 영등포구 여의도동 13-21 맨하탄21 516호
Address
· Tel : 02-783-0456
· Fax : 02-786-0456
· E-Mail : neoplex@neoplex.co.kr
Member
NEOPLEX
Contact
· 대표자 강동선
· 솔루션 사업부
· 기술 사업부
· 기술 지원팀
Start Up
· 2014년 11월 17일
· 임직원수 9명

2. 네오플렉스 조직도

네트워크 보안 전문기업
네오플렉스

3. 네오플렉스 연혁

2014

- 11월 - ㈜네오플렉스 법인 설립
- 11월 - 인하공업전문대학 PMS, 백신관리서버 구축
- 12월 - 인천NESThotel 통합 네트워크 및 보안시스템구축
- 12월 - 장수CC 통합 네트워크 및 보안시스템 구축
- 12월 - ㈜XNsystems Gold Partner 선정

2015

- 1월 - MG신용정보 AhnLab V3 및 APrM 구축 및 유지보수
- 3월 - 구주제약 본사-지사간 VPN, 방화벽 및 SSL VPN 구축
- 6월 - 국민대학교 교직원 홈페이지 유지보수
- 6월 - 세종대학교 서버가상화 유지보수
- 7월 - Sky72 방화벽 이중화 구축 및 유지보수
- 7월 - 한국자금중개 QoS 유지보수
- 8월 - 미래앤서해에너지 무선네트워크 구축
- 10월 - 국군기무사 디지털포렌식 수사 서버 및 방화벽 구축
- 12월 - 인하공업전문대학 웹보안시스템 구축

2016

- 1월 - 인천 NEST Hotel 통합보안 유지보수
- 1월 - 의약품안전원 백신관리서버 유지보수
- 2월 - 한국관광대학교 통합 네트워크 및 서버 보안시스템 구축
- 3월 - 내쇼날모터스 전 지점 및 A/S센터 네트워크 유지보수
- 5월 - JTB교육그룹 서버 IDC이전 및 보안시스템구축
- 9월 - 장수레져 모니터랩 DB접근제어, AhnLab 백신관리서버 구축
- 12월 - 내쇼날모터스 평택AS센터 – 각지점 - BMW코리아 네트워크구축
- 12월 - SGI서울보증 AhnLab 백신, PMS, 내PC지키미, 내, 외부망 관리 서버구축
- 12월 - 도이치 파이넨셜 모니터랩 웹방화벽 구축

2017

- 2월 - 항공대학교 L2 노후스위치 Piolink 보안스위치 교체
- 3월 - JTB교육그룹 HP HC250 서버 증설 및 지란지교 오피스 하드 구축
- 4월 - SAISEI Global Partner 선정
- 7월 - ㈜유니언스 L2 보안스위치 구축 및 지사 VPN 구축
- 7월 - 평창댐 수위계 CCTV관제 VPN구축

4. 네오플렉스 주요사업

Partner Business
SAISEI 총판 AhnLab, Monitorapp 파트너쉽

SI Business
네트워크 설계, 네트워크 보안 컨설팅, 신규 네트워크 구축

Network Maintenance
네트워크 유지보수 및 장애처리

5. 솔루션 - SAISEI

▪ **Flow Command(Network Performance Enforcement)**

네트워크 성능향상을 위한 All-In-One 솔루션

Control

- 플로우별 자동 트래픽 분배
- 사용자별 자동 트래픽 분배
- Flow 수 및 사용량에 따른 자동제어

Optimization

- 회선을 최적화 하여 관리
- 환정된 대역폭의 효율적 분배
- 과점유 사용자별 별도 관리 제어

Analytics

- 마이크로 플로운 분석
- Application 분석
- 국가별 분석
- BGP AS별 분석

Service Continuity

- 사용자간 지연시간 분배 및 관리
- 중요 서비스 우선 보장
- TCP/IP 프로토콜 기술적 한계 보완

5. 솔루션 - SAISEI

- **Flow Command(Next Gen QoS)**

최적의 서비스 품질관리

- 사업자의 효율적인 인터넷 망 운영
- 세션 멈춤 현상 제어로 인한 사용자의 VOC감소
- VoIP나 IPTV와 같이 지연에 민감한 데이터 및 주요서비스 유형에 대한 품질보장
- 인터넷 장애 위협요소 관리

회선 증설 비용 및 운영비용 대폭 절감

- 서비스 제공자로 하여금 현재 사용되고 있는 회선 최적화를 통해, 추가 회선 증설 없이 최적의 성능 및 그에 따른 수익 창출을 가능케 함
- 기업의 비트당 비용을 대폭 줄이고 새로운 네트워크 대역폭 구매 시기를 연장 할 수 있음

감시

보고

분석

최적화

보안사고 위협관리

- 차세대 방화벽과 비교해 플로우 기반 보안을 위한 보다 나은, 보다 빠른, 보다 깊은, 보다 저렴한 새로운 모범사례 제공
- 문제 해결을 위해 실제 마이크로 플로우의 모든 측면에 대한 즉각적이고 심층적인 분석

업무생산성 향상

- Micro-flow 레벨의 분석을 통한 비 업무용/유해사이트 서비스 유형의 제한/차단
- 대역폭 과다 점유 서비스 유형에 대한 실시간 DPI 분석을 통한 트래픽 점유 제한
- 기존 WAN 최적화 압축과 패킷 쉐이핑은 더 이상 불필요함

5. 솔루션 - AhnLab

▪ AhnLab TrusGuard (네트워크 통합보안 솔루션)

AhnLab TrusGuard

- Firewall, IPS, VPN, Anti-Virus/Spam 등 다양한 보안 기능을 제공하는 통합 보안 시스템입니다.
- 31A부터 22000 등 Low-End 모델에서 데이터 센터급 모델까지 다양한 제품 라인업을 갖추고 있어 기업의 네트워크 규모에 따라 선택적으로 사용할 수 있습니다.
- **Advanced A-TEAM** 아키텍처 기반의 고성능 방화벽과 ※**ACCESS** 기반의 강력한 통합보안 기능을 제공합니다.
- 다양한 VPN 사업 구축 경험을 바탕으로 안정적이고 보안성이 뛰어난 고성능 VPN 기능을 제공합니다.

CC 인증 획득(EAL4)

IPv6 TTA 인증 획득

Advanced A-TEAM 구조
(멀티코어 최적 활용기술+ 소프트웨어 가속 처리 기술)

능동적/종합적 방어체계

광범위한 보안 위협 대응

Flexible & Secure VPN 네트워크 구성지원

※ACCESS AhnLab Cloud Computing E-Security Service
(Cloud 보안위협 수집 분석 시스템)

5. 솔루션 - AhnLab

▪ **MDS malware defence system (좀비PC 대응 솔루션)**

AhnLab Malware Defence System

- 웹, 이메일, 파일전송(FTP/SMB/NFS)을 통해 유입/전파되는 위협탐지 하는 제품입니다.
- 행위간 연관 분석 및 평판 분석 기반의 차세대 동적 행위 분석 기능을 제공합니다.
- **모든 탐지 및 분석대상의 악성 여부에 대한 명확한 가시성 제공하여 관리의 편의성을 극대화 하였습니다.**
- 탐지된 신종 악성코드에 대한 즉각적인 제거 및 포렌식 분석 수행.

Technology
APT공격 대응기술

- 멀티레이어드 분석 엔진 사용
- 화이트리스트보유를 통한 오진률 최소화
- 알려지지 않은 악성코드 탐지 가능
- 수집-분석-모니터링-대응의 프로세스 관점의 솔루션

Synergy
도입 효과

Ahnlab MDS는 네트워크로 유입되는 위협의 최초 감염 단계부터 감염이후 C&C 서버와의 통신을 통한 2차 감염, 내부전파, 정보 유출 등 악의적인 행위, 잠복 단계까지 지능형 위협의 라이프사이클을 중심으로 위협에 대한 가시성과 실질적인 대응 체계를 제공합니다.

5. 솔루션 - AhnLab

- **EndPoint Security 9.0(엔드포인트 통합 관리 솔루션)**

AhnLab EndPoint Security 9.0

- AhnLab V3 EndPoint Security 9.0은 **매체제어 기능**을 제공하여 PC의 다양한 경로를 통해 유입되는 악성코드를 **원천 차단**합니다.
- 강력하고 다양한 보안기능인 **매체제어, 웹 보안, Active Defense 등** 보안 기능을 제공합니다.
- 기존에 알려진 악성코드를 **빠르고 정확하게 분석**하며, **알려지지 않은 신•변종** 악성코드를 **진단**합니다.

매체제어 기능 제공
(APC/APC Appliance 연동)

USB 제어	네트워크 제어
드라이브 제어	기타 장치 제어

5. 솔루션 - AhnLab

▪ V3 Net for Windows Server 9.0(서버운용 보안 솔루션)

AhnLab V3 Net for Windows Server 9.0

- AhnLab V3 Net for Windows Server 9.0은 기업의 정보자산을 **보호**하고, **안정적인 서버운영을 제공**합니다.
- **정확한 악성코드 진단/치료**는 물론 **서버 방역 및 다양한 기능을 제공**해 기업의 **비즈니스 연속성 확보에 기여**합니다.
- 다차원 분석 플랫폼 기반의 **차별적인 사전 방역** 및 클라우드 기반의 **ASD를 통한 정확한 진단 및 실시간 치료**하며, **능동적인 대응 서비스를 지원**합니다.
- 다양한 환경에 최적화하여 **안정적으로 제품을 제공**하며, **편의성이 증대**된 다양한 기능을 제공합니다 .

Support
다양한 Windows버전 지원

- Windows Server 2003 / 2008 / 2012
- 모든 32bit CPU와 64bit CPU를 지원
  (IA 64계열 제외)

Synergy
도입 효과

서버 방역을 통한 기업 자산 보호 및 비즈니스 연속성에 기여

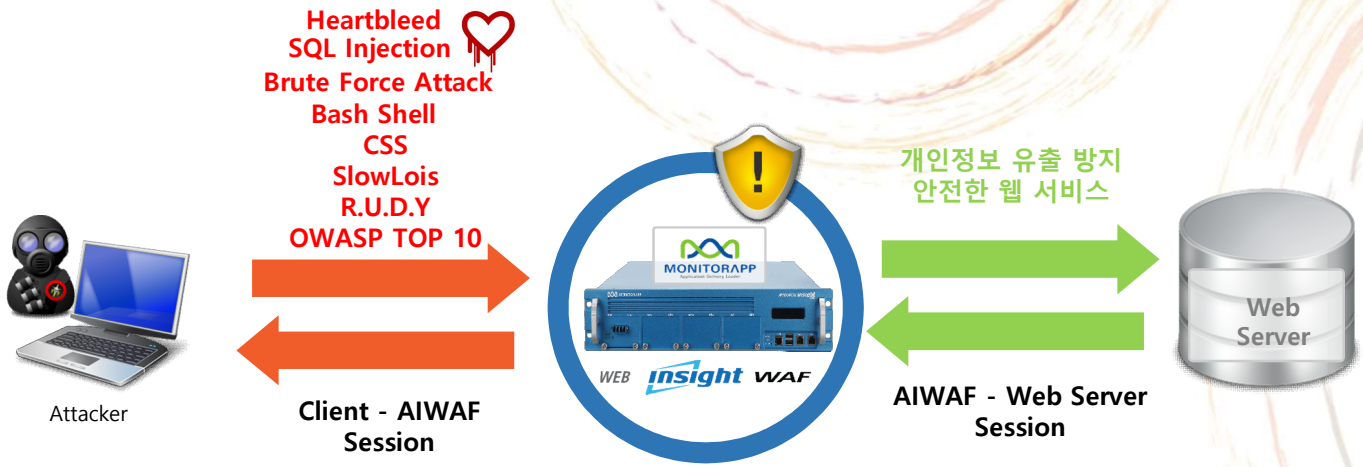
- 안전한 업무 환경 조성 및 업무 생산성 향상
- 보안 관리 및 운영 부담 최소화
- 보안성 증대

제품 인증

- **2013. 07 V3 Net for Windows Server 9.0 출시, CC인증 및 GS 인증 진행 중**
- 2004. 11 V3 Net for Windows Server 6.0 출시, CC 인증 획득

5. 솔루션 - Monitorapp

- **Application Insight WAF**



도입 전

- 기본 웹 취약성을 이용한 공격(SQL Injection) 노출
- 취약한 웹 서비스 등을 통한 개인정보 유출 가능성
- Openssl 등 취약점으로 인한 추가 공격 가능성
- HTTP 기반 DOS 공격 등 이상 트래픽으로 인한 서비스 지연
- 서비스 대표 홈페이지 변조 등을 통한 기업 신뢰도 저하 가능성

도입 후 기대 효과

- 기본 취약성을 이용한 공격(SQL Injection) 공격 차단
- 웹 서비스를 통한 개인정보 유출 방지
- Openssl 등의 취약점에 대해 사전 대응
- HTTP에 특화된 DOS 트래픽 차단으로 서비스 가용성 확보
- 홈 페이지 위변조 방지

5. 솔루션 - Monitorapp

▪ **DB Insight SG - 고성능 Network 기반 전용 장비**

➢ **DB INSIGHT SG**는 완전한 Query 분석을 기반으로 사용자 기반의 **강력한 권한제어** 및 **접근제어**, **Profile** 기반의 자동화된 보안 정책을 제공함으로서 **외부로부터의 비정상적인 DB 접근을 통제**하고, **접근 이력 관리를 통한 사후 감사기능**으로 주요 내부 정보 자산을 보호해주는 **전용 DB 접근제어 제품**입니다.

➢ 고성능 **Transparent Proxy**와 **Packet Sniffing Module**을 **동시 사용할 수 있도록 Hybrid mode를 지원**

고성능 Network 전용 장비

- Gigabit Performance 지원
- 기존 운영 시스템 성능에 영향 없음
- Fail Over (HA)

간편한 구성

- Proxy base Full Transparent Mode
- 효율적인 Hybrid 운영 방식
- 기존 인프라 환경 변경 없음
- 다양한 고객 네트워크 환경에 최적화 구성 지원

강력한 보안 기능

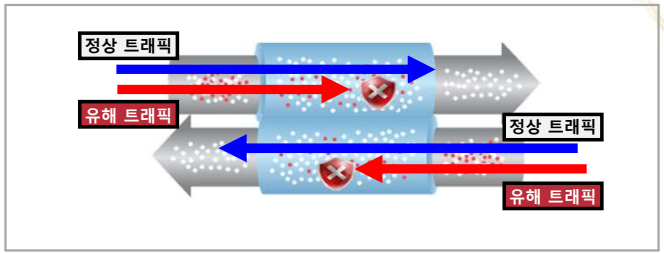
- 국내 최초 Positive Security Model 구현
- 강력한 접근 제어 및 권한 제어, 세션 제어
- Data Masking
- Virtual Patching

보다 편리한 설정과 운영

- 관리자 편이를 극대화한 직관적 GUI
- 대시보드 기반의 실시간 시스템 모니터링
- 시스템 통합 관리 기능

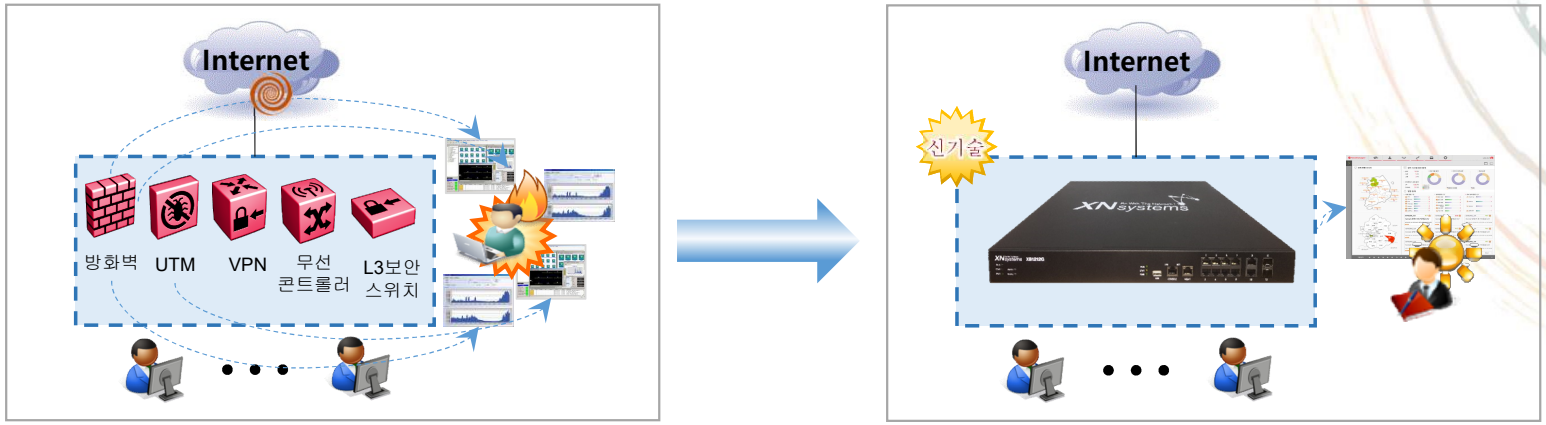
5. 솔루션 - XN systems

▪ **융합보안솔루션 XN-Box (L2 + UTM)**



XN-Box 는 외부로 부터 침입 차단 뿐만 아니라 내부의 이미 감염된 사용자로 인한 유해트래픽을 선별적으로 차단 및 확산 방지하는 양방향 보안으로 인한 **보안의 극대화**와 **서비스의 연속성**을 보장합니다.

XN-Box 는 각 모듈별 독립 하드웨어설계로 장애를 최소화하였고, 실시간 자가진단을 통해 이상작동시 모듈별 자동 전원 재인가로 **무중단 서비스**를 제공하며, **블랙박스** 메모리 탑재로 사후관리의 편의성을 제공합니다.



XN-Box 는 중복투자를 방지하며, 관리포인트를 감소할 뿐만 아니라 장애로 인한 손실비용을 절감해줍니다. 또한, 그린IT 및 전원관리와 통합관제를 통하여 최대 70%이상의 TCO 절감효과를 기대할 수 있습니다.

5. 솔루션 - PioLink

- **L2 보안스위치 - TiFront**

Piolink Tifront Series

- **L2/3 스위칭+보안** - 사용자 단말에서 발생하는 유해 트래픽을 자동 탐지/차단하여, DoS 발생 방지, Protocol Anomaly, 인증, ARP 공격 방어, IP 관리 등의 다양한 액세스 네트워크 보안기능이 결합되어 있습니다.
- **하드웨어 기반 보안 엔진** - TiMatrix 보안 엔진을 내장하고 있어 타사 대비 차별화 되는 보안성을 갖고 있습니다. TiMatrix를 통해 고성능 멀티코어 CPU기반의 효율적인 태스크를 관리하고 최대 보안 성능을 제공할 수 있습니다.
- **비인가 공유기 탐지** - TiFRONT는 내부망에 위치한 NAT 장치 리스트를 작성하여 인가되지 않은 NAT 장치를 관리자가 인지할 수 있어 안전합니다
- **중앙 관제 시스템**- 쉽고 편리하게 네트워크 상태를 모니터링 하고, 즉각적으로 보안 위협에 대응할 수 있습니다. 수백대의 장비를 통합으로 관리할 수 있어 운영자의 업무 부담을 크게 줄여 주며 별도 라이선스 구매없이 사용 가능합니다.

5. 솔루션 - PioLink

▪ VDS(Vormetric Data Security)

▪ Data암호화 및 상황 기반의 접근제어를 통해 중요 DB Data의 유출을 차단하고 System의 무결성을 **보호하는 통합데이터 보안 솔루션 입니다**

1. 기업 IT 환경안에서 손쉽게 적용됨: OS, DB, 어플리케이션, 데이터 저장소에 변경이 필요하지 않음. (DB & Application 어떠한 수정 및 변경이 없음)

2. 빠른 성능 암호화 전후 속도차이 없음

3. 안전한 키관리 서버 제공 (전용 Appliance 장비 제공)

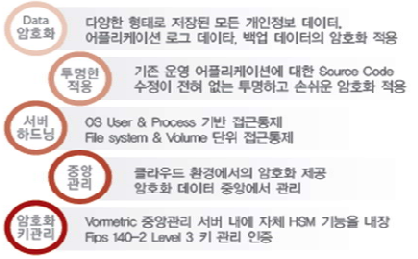
4. 모든 DB에 적용 가능한 시스템 kernel level의 TDE 암호화 제공

5. 암호화 된 모든 DB / System 중앙 관리 제공 (단일 web 메니지먼트 제공)

*** FIPS 140-2 level 2 (키관리 Level3) 인증**

* VDS 주요기능

- 고객 데이터(개인정보)를 포함한 주요 데이터 암호화
- OS 사용자 및 프로세스 단위 권한 및 접근 제어
- 주요 데이타 및 파일 엑세스 시 상세 감사 로그 생성
- 환경 설정 파일 및 컨트롤 파일에 대한 무결성 보장
- 암호화 Key에 대한 안전한 생성 및 관리
  (안전한 Master Key 관리)



* VDS 기대효과

- 기밀 데이터 및 개인정보가 포함된 시스템 파일에 대한 완벽한 보호
- 운영환경 변화 없이 간단히 구축함으로써 시스템의 무결성 유지 (구축 기간 최소화)
- 암호화 이후에도 서비스 성능 저하가 거의 없는 고성능 암호화 구현
- 사용자 행위기반 접근제어 정책을 통한 고객정보 보호
- 국내 개인정보보호법을 포함한 HIPPA, PCI등의 규제 및 감사 대응

* VDS 적용 가능한 개인정보 처리 시스템

- Vormetric 솔루션은 개인정보를 포함한 다양한 데이터 폼을 처리하는 개인정보처리시스템에 적용됩니다.
- 개인정보처리 시스템 종류
  : DB 서버, 파일서버, 스토리지, 백업미디어, 녹취 서버, 개인 PC, 특수성을 띤 어플리케이션 DB 등

감사합니다.

서울특별시 영등포구 여의도동 13-21 맨하탄21 516호 Tel : 02-783-0456 Fax : 02-786-0456 http://www.neoplex.co.kr

NEOPLEX