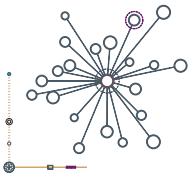
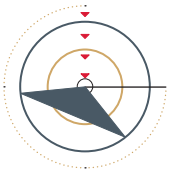
POSITIVE TECHNOLOGIES


CORE NETWORKS


POSITIVE RESEARCH

SAP SECURITY


PINPOINT ACCURACY

ALL-IN-ONE SOLUTION

# MaxPatrol:
## 기업용 취약점 및 컴플라이언스 관리 솔루션

해커들은 여러가지 다양하고 정교한 방식으로 기업의 애플리케이션, 데이터베이스, 네트워크, 운영체제 등을 공격합니다. 그러나 해커들의 방식에도 적어도 한 가지 공통점이 존재합니다. 바로, 취약점과 잘못된 시스템 설정을 악용한다는 점입니다.

전세계적으로 대부분의 보안 침해 사건들이 잘 알려진 취약점들과 잘못된 시스템 설정, 취약한 취약점 관리 등으로 인해 발생하고 있습니다. 2013년 Positive Technologies가 실시한 조사에 따르면, 외부 공격자의 경계 보안 우회 성공률이 90%에 달했습니다. 아울러, 조사 대상의 55%의 경우에 있어서 침입자가 공격 개발에 성공해 기업 전체의 인프라를 장악했습니다.

다양한 비즈니스, 운영, 정보 기술의 통합 역시 현대 기업의 공격 표면을 확대시켜 사이버 공격의 위험에 크게 노출시키고 있습니다. 취약한 ERP 시스템을 통해 스마트 그리드나 발전소를 원격으로 제어하거나 취약한 GSM-R 시스템의 초고속 열차를 하이재킹하는 일은 이제 더 이상 영화에서나 가능한 일이 아니라 더 이상 무시해서는 안 되는 현존하는 위험이 되었습니다.

그렇다면 취약점 및 컴플라이언스 관리에 있어서 왜 그렇게도 많은 기관들이 실패하는 것일까요?

바이러스 백신 프로그램, 방화벽, 침입 차단 시스템 등 기존 도구들은 문제의 원인을 제거하기보다는 문제가 발생한 사후를 처리하려고 합니다. 이 같은 보안 방식에만 의존한다면 보안 침해 사고는 시간 문제입니다. 이러한 상황에서 반드시 필요한 것은 시스템과 네트워크 전체에 걸쳐 취약점 탐지 및 분석, 침투테스트, 네트워크 및 데이터베이스 스캐닝, 시스템 및 애플리케이션 테스트, 설정 및 인벤토리 진단 및 상세 컴플라이언스 점검 등을 자동화한 프로세스이며, 이 모든 것이 가능한 솔루션이 바로 MaxPatrol™입니다.

**스마트한 해법**

여러 기업에서는 이미 기존 보안 방식을 보완하기 위해 연간 또는 분기별로 취약점 감사를 실시하고 있습니다. 하지만 시스템, 애플리케이션, 관련 설정들을 지속적으로 변경하면서 보안에 결함이 발생하고 있으며, 때문에 대부분의 기업들은 생각만큼 보안이 제대로 갖춰지지 않는다고 생각합니다.

보안 정책, 절차, 표준 등은 전혀 새로운 것들이 아니지만 대부분의 기업들에게는 이러한 지침들의 효과 및 적용 가능성을 측정할만한 적절한 도구가 부족합니다. 기업의 네트워크 및 전화 장비, 와이 파이, 데이터베이스, 운영체제, 웹 애플리케이션 등이 노출되어 있는 취약점에는 어떠한 것들이 있는지 파악하고 있습니까? **ERP와 같은 주요 비즈니스 애플리케이션과 SCADA와 같은 운영 기술은 또 어떠합니까?**

Positive Technologies의 MaxPatrol은 다양한 애플리케이션, 데이터베이스, 네트워크, 운영체제 등에 걸친 취약점 및 설정 결함을 식별하는 데 있어서 에이전트가 없는 낮은 권한의 블랙박스 및 화이트박스 기법을 제공함으로써 단편적인 보안 및 고가의 외부 컨설팅을 대체합니다

## 주요 기능:

**지능형 기법**

상세 보안 설정 파라미터 점검 등 블랙박스와 화이트박스 분석 기법을 모두 사용한 위협 분석을 통해 인프라의 전체 자산을 지속적으로 모니터링하고 진단합니다.

**보안 사각지대 차단**

인프라의 전체 자산과 ICS/SCADA, 코어 텔레콤, 코어 뱅킹 시스템 등 운영 기술들을 지속적으로 모니터링하고 진단하며, 위험 제어를 KPI에 연계시켜 비즈니스 보호 수준을 측정합니다.

**신속한 컴플라이언스**

MaxPatrol은 하이레벨의 컴플라이언스 표준을 운영상 보안 규제에 적용시켜 문서기반의 수동정책 점검을 자동화된 점검방식으로 변경합니다.

**사용자 지정 보고서 작성**

비즈니스 고유의 특성에 맞는 보고서를 작성합니다. MaxPatrol은 수 백 개에 달하는 개별 데이터 필드를 제공하여 비즈니스에 가장 중요한 세부사항을 선택할 수 있도록 합니다.

**공격 차단**

200 여 명의 보안 전문가들이 연간 20회 이상의 대규모 침투테스트와 200회 이상의 애플리케이션 보안 진단을 실시하여 150개 이상의 제로데이 취약점을 발견하고 있으며, 이러한 결과가 바탕이 된 지식이 MaxPatrol에 적용되고 있습니다.

MaxPatrol (SAP 보안진단 인증 솔루션)은 SAP 인증 ERP, ICS/SCADA, 모바일 코어 및 뱅킹 시스템에 대한 심도 깊은 보안 진단을 실시하는 통합형 취약점 관리 솔루션으로, 전세계 1천 여 기업들이 실질적인 공격 모델을 생성하고, 비즈니스상의 위험 요소를 업데이트하며, 보안 및 컴플라이언스를 유지하는 데 사용되고 있습니다.

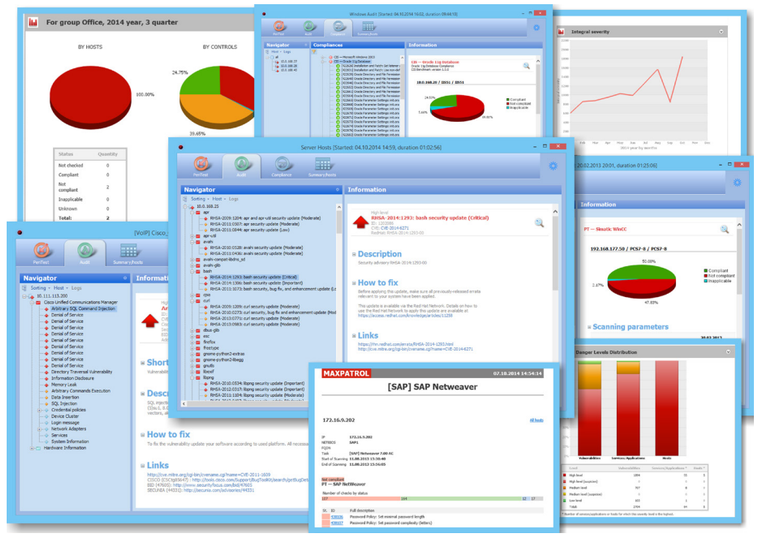



**Figure 1: MaxPatrol**
Greater visability into security across a wide range of systems.

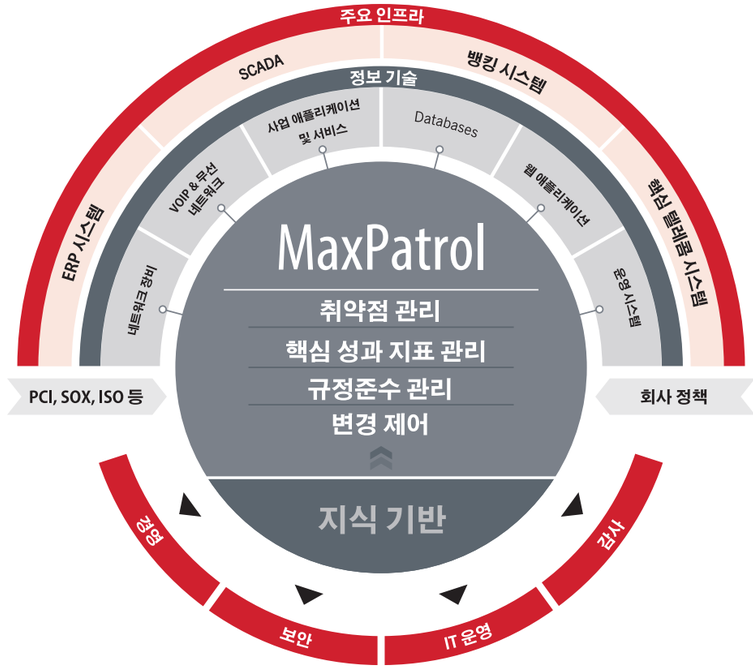



**Figure 2: MaxPatrol**
Main diagram

## Positive Research:
## MaxPatrol을 뒷받침하는 브레인

MaxPatrol에는 연간 20회 이상의 대규모 침투테스트와 200회 이상의 애플리케이션 보안 진단을 실시하여 150개 이상의 제로 데이 취약점을 발견하고 있는 보안 전문가 200여 명의 지식이 축적되어 있습니다. Positive Research의 전문가들은 PHDays, Black Hat, Defcon 등 유명 국제 보안 회의에 정기적으로 참석하여 연구 결과들을 발표하고 있습니다. 이 같은 독자적 지식들이 다양한 보안 점검과 벤치마크를 포함하는 방대한 취약점 데이터베이스의 형태로 MaxPatrol에 통합되어, 급속도로 변화하는 위협에 대한 보호막이 되고 있습니다.

**철저한 시스템 분석**
취약점 탐지 및 분석, 침투테스트, 네트워크 및 데이터베이스 스캐닝, 시스템 및 애플리케이션 테스트, 설정 및 인벤토리 진단, 상세 컴플라이언스 점검 기능 등이 모두 통합된 MaxPatrol은 현존하는 가장 포괄적인 취약점 및 컴플라이언스 관리 솔루션입니다. 또한, 네트워크, 와이 파이 장비, ERP 시스템, 데이터베이스, 웹 애플리케이션, ICS/SCADA, 모바일 코어, 뱅킹 시스템, ERP 등과 같은 운영 기술(OT) 등 기존의 모든 IT 시스템을 위한 단일 솔루션입니다.

**강력하고 유연한 컴플라이언스**
네트워크 보안의 글로벌 리더로서, Positive Technologies는 SOX, ISO, PCI-DSS, 3GPP, NIST, NERC, HIPAA 등의 데이터 보안 규격을 준수하는 데 필요한 요구사항들을 파악하고 있습니다.
아울러, 기업에게는 글로벌 또는 업계 규정 외에도 지역 또는 기업 내부 표준과의 컴플라이언스도 요구된다는 사실 또한 인지하고 있습니다.

MaxPatrol은 벤치마크들을 통합하여 5천 개 이상의 규제 사항들을 제공함으로써 기업의 하이레벨 컴플라이언스 표준이 운영상 보안 규제에 신속히 적용될 수 있도록 합니다.

"VimpelCom에 있어서 전사적인 IT 시스템의 보안 규정 준수를 전적으로 관리하는 능력이 중요합니다. MaxPatrol은 VimpelCom의 글로벌 오퍼레이션 전체에 보안 취약점 및 컴플라이언스의 스캔, 감사, 우선순위 설정, 검증, 보고서 작성 기능 등을 제공하는 유일하고도 완벽한 솔루션입니다."

Dmitry Ustyuzhanin
(VimpelCom 정보 보안 매니저)

**POSITIVE TRUSTED BY:**

ING, SAMSUNG, INTESA SANPAOLO, SOCIETE GENERALE, Allianz, VimpelCom

### 그 외의 기능들

**주요 IT 솔루션과 통합**
MaxPatrol의 탁월한 취약점 및 컴플라이언스 기능은 Best Practical Request Tracker, BlackStratus SIEM Storm, CyberArk Enterprise Password Vault, HP ArcSight ESM, IBM® Security QRadar® SIEM, RSA enVision and RSA Security Analytics, NetWeaver® 7.0 SAP® certified, SkyBox View Enterprise, Symantec SIM 등 주요 IT 솔루션들과 통합되었습니다.

**우선순위 설정**
각기 다른 비즈니스에는 고유의 보고 기능이 필요합니다. MaxPatrol은 표준 보고서 외에도 BI 솔루션을 통해 수 백 개의 맞춤식 차등 동향 및 KPI 보고서와 대시보드를 제공하여 실시간 및 이력에 따른 데이터 분석과 의사 결정, 프로세스 컨트롤 등의 기능을 제공합니다. 이로써, 비즈니스에 가장 중요한 보안 정보에 대한 집중이 가능해 집니다.

**정확하고 정직한 보호**
어느 기업이나 보안과 관련하여 안정적인 결과를 원합니다. 오탐을 걸러내느라 또는 미탐과 관련된 결과를 처리하느라 며칠 혹은 몇 주나 되는 시간을 허비하고 싶은 기업은 없습니다. Positive Technologies의 숙련된 연구가들과 보안 전문가들에 의해 유지 보수되는 MaxPatrol은 다음과 같은 기능들을 제공합니다.

+ 배너 기반의 점검을 통해 오탐율을 낮추는 스크립트 점검
+ 휴리스틱 분석
+ 취약점 매핑에 대한 직접적인 OS가 아닌 서비스 및 시스템의 상태 점검으로 작동 중인 서비스 및 프로토콜에 대한 취약점 확인

이러한 고유의 방식으로 정확한 소프트웨어 ID 및 버전이 제공되어 업계 최저의 오탐율을 보장합니다.

**주요 인프라 보호**
주요 인프라라고 하면 ICS/SCADA만 해당될 뿐만 아니라 은행, 통신 등 사회적으로 중요한 비즈니스에 관련된 모든 기업이 될 수 있습니다. 비즈니스가 기존 IT 시스템이나 산업 기술에 의존하는지의 여부와 관계 없이 MaxPatrol은 기업 보안에 대한 깊이 있는 보안 진단을 실시하고, 위험성이 탐지되는 곳을 보여주는 실질적인 공격 모델을 생성하며, 공격 차단에 필요한 절차를 제공합니다.

**SAP 보안 자동화**
기존 SAP 인프라의 방대한 규모와 복잡성으로 인해 SAP 시스템의 보호와 시스템의 정확한 설정 보장이 어렵습니다. SAP 통합 인증을 받은 MaxPatrol은 업계를 선도하는 솔루션으로서 SAP 인프라의 모든 부분에 대하여 보안 자동화 기능을 제공합니다. MaxPatrol을 통해 다양한 SAP 인스턴스에 대한 신속하고 비침입적인 진단을 실시할 수 있습니다. 또한, "shadow SAP_ALL" 사용자, 취약한 암호, SOD 위반 등 SAP 보고서에서는 나타나지 않는 상세 정보를 제공합니다. 기업과 기업의 SAP 인프라는 지속적으로 변화합니다. 사용자 활동, 역할 및 프로파일, 환경 설정, 암호 정책 등을 정기적으로 모니터링 함으로써 이러한 변화가 기업의 보안 태세를 약화시키지 않도록 해야 합니다.

## MaxPatrol의 주요 기술적 특징

MaxPatrol은 하기 시스템에 대한 블랙박스 및 화이트박스 기반의 테스트와 보안 설정 진단이 가능합니다.

- Cisco, Check Point, Stonesoft, Juniper(JunOS, ScreenOS) 네트워크 장비(방화벽, IPS 포함)
- Alcatel, Huawei, Nortel, Ericsson 통신 장비 및 Digium VOIP 시스템
- Windows, MacOS X, Linux, AIX, HP-UX, Cisco IOS, Oracle Solaris, Fedora, Gentoo, Mandriva, Slackware 등 운영 체제
- Microsoft SQL, Oracle, IBM DB2, PostgreSQL, MySQL, Sybase 등 데이터베이스
- MS IE/Office, Firefox, Google Chrome, Safari, Opera, OpenOffice, Lotus, Acrobat, Reader, Flash Player, Thunderbird 등 데스크톱 애플리케이션 및 브라우저
- Microsoft Active Directory, Exchange, Sharepoint and IIS, IBM Lotus, Netscape DS, LDAP-UX, Sendmail, PostFix, MDaemon, MailEnable, Exim SMPT Server, Apache, CommuniGatePro 등 인프라 애플리케이션
- VMWare vSphere/ESX, Microsoft Hyper-V, Citrix XenApp 등 가상화 및 터미널 플랫폼
- 개인 IPS, 방화벽, 바이러스 백신 프로그램 등 보안 시스템
- Oracle E-Business Suite, SAP R3/ECC, NetWeaver 등 비즈니스 시스템
- Siemens, Invensys, Schneider Electric, Rockwell Automation 등 다양한 ICS/SCADA 플랫폼

**안전한 통신**- SSL/TLS 암호화 채널 기반의 MaxPatrol 컴포넌트 간 통신과, 수집된 모든 정보의 로컬 스토리지 및 역할 기반의 고급 액세스 제어 메커니즘이 취약점에 대한 민감한 정보의 유출을 예방합니다.

**암호 정책 감사** 하기 프로토콜을 사용하는 시스템에 대한 사전 브루트포스 등 블랙박스 및 화이트박스 감사:

- 원격 액세스 및 VPN, RDP, VNC, Radmin, Telnet, SSH 등
- 애플리케이션 프로토콜: SAP, Oracle, SQL, Sybase, SIP, VMWare 등
- 인프라 프로토콜: SMTP, PoP3, SMB, FTP, HTTP 등

**에이전트리스의 네트워크 무결성 모니터링** 내장형 컴포넌트가 네트워크 전체의 인시던트와 원하지 않는 변경 사항의 탐지를 돕습니다.

**민감한 데이터의 탐지** 강력한 검색 엔진으로 파일과 데이터베이스에 포함된 신용카드 및 PIN 번호, 카드 인증 값(CVV) 등의 데이터를 식별합니다.

**인증된 CVE와 호환 인증 솔루션** 취약점 분류와 IT 보안 시스템 및 도구와의 통합 간소화를 위한 보편적으로 인정되는 CVE 시스템 지원을 인증 받은 솔루션입니다.

**XML 기반의 통합 API** 비즈니스 정보 포털, 자산 관리, 헬프 데스크 티켓팅, 요청 추적, 위기 관리, 패치 관리, SIM/SIEM, IPS, NAC/NAP, WAF 침투테스트 등 시스템에서의 통합형 정보 보안 프레임워크의 생성을 지원합니다.

**유연한 보고 시스템** 인벤토리 및 변경 관리, 컴플라이언스, IT 성능 관리 등에 대하여 자동으로 보고서를 작성합니다 MHT, PDF, XML 번역기를 사용하여 사용자 지정 포맷과 디자인으로 보고서를 작성할 수 있습니다.

### Positive Technologies 소개

Positive Technologies는 취약점 진단, 컴플라이언스 관리, 위협 분석 솔루션 분야의 글로벌 리더로서, 전세계 1천 여 고객들에게 솔루션을 제공하고 있습니다. 개발 단계의 애플리케이션 보호, 네트워크 및 애플리케이션 취약점 진단, 규제 요구사항과의 컴플라이언스, 실시간 공격 차단 등 비즈니스와 관련된 모든 보안 문제에 완벽히 대처합니다. 고객 및 연구에 대한 헌신과 노력의 결과, SCADA, 금융, 통신, 웹 애플리케이션, ERP 보안 분야에서 최고의 권위를 가지고 있다는 평가를 얻고 있으며 2012년 IDC 보고서*에서는 가장 빠르게 성장하는 보안 및 취약점 관리 기업으로 선정되기도 했습니다.
Positive Technologies에 대한 보다 자세한 사항은 www.ptsecurity.com에서 확인할 수 있습니다.

*출처: Worldwide Security and Vulnerability Management 2013-2017 Forecast and 2012 Vendor Shares, doc #242465, August 2013. 매출 2천만 달러 이상 관련 분야 사업자의 2012년 전년대비 매출 성장률을 바탕으로 함.



POSITIVE TECHNOLOGIES