MAXPATROL™: ENTERPRISE VULNERABILITY AND COMPLIANCE MANAGEMENT

Hackers have many different and sophisticated ways to attack applications, databases, networks and operating systems. However, their techniques have at least one thing in common: they focus on exploiting vulnerabilities and misconfigured system settings.

Most security breaches and incidents around the world occur due to well-known vulnerabilities, misconfigured system settings and poor vulnerability management. Consider this: a 2013 study by Positive Technologies revealed that an external attacker could bypass the perimeter security in 9 out of 10 cases. Moreover, it was determined that in 55% of the cases, an intruder could successfully develop an attack and gain full control of a company's entire infrastructure.

The integration of various business, operational and information technologies has also dramatically increased the attack surface of any modern enterprise, putting it at high risk of cyber-attack. Taking control of a Smart Grid or a power plant remotely, through a vulnerable ERP system, or hijacking a high-speed train over a vulnerable GSM-R system used to be only possible in the movies. However, they are now real and present dangers that must not be ignored any longer.

So why are so many organizations failing when it comes to vulnerability and compliance management?

Traditional tools like antivirus, firewalls and intrusion prevention systems struggle with the problems aftermath, instead of trying to eliminate its root cause. If you solely rely on these security methods than it's not a question of if you will suffer a security breach, but rather a question of when. Alternatively, what you need is an automated process for vulnerability detection and analysis, penetration testing, network and database scanning, system and application testing, configuration and inventory assessments and detailed compliance checks, across all your systems and networks. What you need is MaxPatrol™.

A SMARTER ALTERNATIVE

Many companies already conduct annual or quarterly vulnerability audits to complement their existing security measures. However, frequent and continuous changes to systems, applications and associated configurations create cracks in their security, and is the leading reason why most companies are not as well protected as they think.

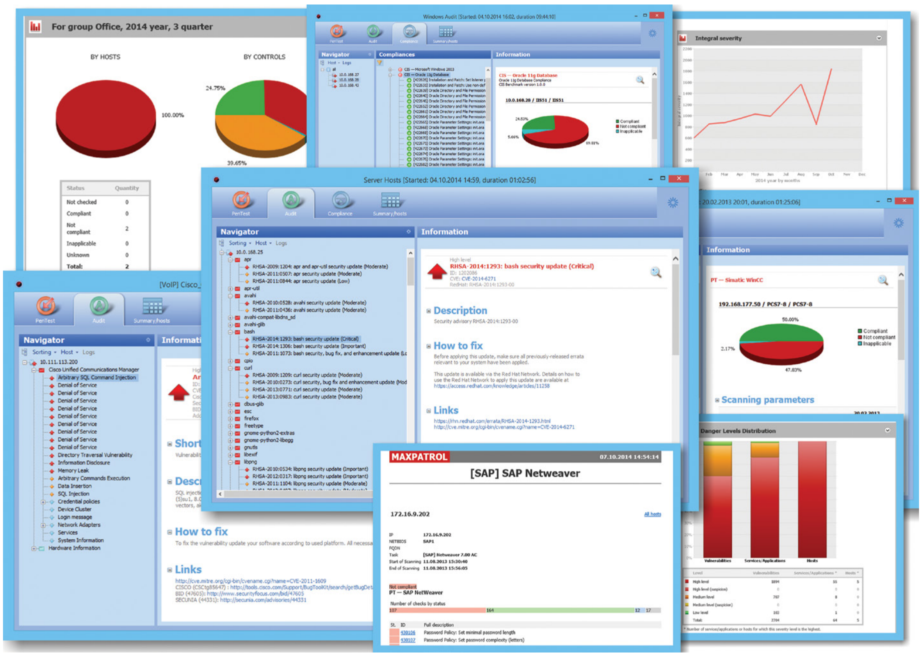
While security policies, procedures and standards are nothing new, most companies lack the tools to measure their effectiveness and applicability. Do you know **what your company's vulnerability exposure is for network & telephony equipment, Wi-Fi, databases, operating systems and web applications? What about your business critical applications like ERP or operational technologies like SCADA?**

Positive Technologies MaxPatrol™ replaces fragmented security and high priced consultants by providing agentless, low-privileged, black-box and white-box identification of vulnerabilities and configuration flaws across a variety of applications, databases, network and operating systems.

With a unique ability to provide in-depth security assessments of ERP (SAP-certified), ICS/SCADA, Mobile Core and Banking Systems, MaxPatrol™ is an all-in-one vulnerability management solution trusted by over 1,000 enterprises to create practical attack models, update and verify business risks and maintain security and compliance.

HIGHLIGHTS

- **Work Smarter Not Harder** Continually monitor and assess the complete scope of infrastructure assets through analysis of the threat-scape by employing both blackbox and white-box methods including detailed security configuration parameter checks.
- **Avoid Blind Spots in Your** Security Continually monitor and assess the complete scope of infrastructure assets and operational technologies, including ICS/SCADA, Core Telecom and Core Banking Systems. Connect risk controls to KPIs to measure how well they are protecting the business.
- **Speedy Compliance** MaxPatrol translates highlevel compliance standards into operational security controls, turning paper-based policies into automated checklists.
- **Reports Just the Way You** Like Them Your business is unique — which means your reporting needs are too. That's why MaxPatrol supplies hundreds of individual data fields giving you the freedom to select the details that matter most to your business.
- **Stop Being an Easy Target** Leverage the knowledge of 200 security experts who perform more than 20 large-scale penetration tests, over 200 application security assessments and discover more than 150 zero-day vulnerabilities each year.


For group Office, 2014 year, 3 quarter
BY HOSTS
BY CONTROLS
Integral severity
Windows Audit
Server Hosts [Started: 04.10.2014 14:59, duration 01:02:56]
Navigator
Information
Compliance
Summary/hosts
Danger Levels Distribution
Scanning parameters

High level
RHSA-2014:1293: bash security update (Critical)
ID: 1202086
CVE: CVE-2014-6271
RedHat: RHSA-2014:1293-00

Description
Security advisory RHSA-2014:1293-00

How to fix
Before applying this update, make sure all previously-released errata relevant to your system have been applied.

This update is available via the Red Hat Network. Details on how to use the Red Hat Network to apply this update are available at https://access.redhat.com/knowledge/articles/11258

Links
https://rhn.redhat.com/errata/RHSA-2014-1293.html
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271

MAXPATROL 07.10.2014 14:54:14
[SAP] SAP Netweaver

172.16.9.202 All hosts

IP	172.16.9.202
NETBIOS	SAP1
FQDN	
Task	[SAP] Netweaver 7.00 AC
Start of Scanning	11.08.2013 15:30:40
End of Scanning	11.08.2013 15:56:05

Not compliant
PT — SAP NetWeaver

Number of checks by status
107 164 12 17

St.	ID	Full description
	430106	Password Policy: Set minimal password length
	430107	Password Policy: Set password complexity (letters)

MaxPatrol™
Greater visibility into security across a wide range of systems

POSITIVE RESEARCH

With MaxPatrol™ you get the knowledge of 200 security experts, from Positive Research, who perform more than 20 large-scale penetration tests, over 200 application security assessments and discover more than 150 zero-day vulnerabilities each year. Our experts regularly present their findings at highly respected international security conferences such as PHDays, Black Hat and Defcon. All this proprietary knowledge is incorporated into MaxPatrol™ in the form of an enormous vulnerability database with numerous security checks and benchmarks providing protection in fast-paced and continuously changing threatscape.

IN-DEPTH ANALYSIS OF ALL YOUR SYSTEMS

MaxPatrol's combination of vulnerability detection and analysis, penetration testing, network and database scanning, system and application testing, configuration and inventory assessments and detailed compliance checks delivers the most comprehensive vulnerability and compliance management solution available. In addition, MaxPatrol™ is a single solution for all your traditional IT systems such as network and Wi-Fi equipment, ERP systems, Databases, Web applications and Operational Technologies (OT) like ICS/SCADA, Mobile Core, Banking systems and ERP.

POWERFUL AND FLEXIBLE COMPLIANCE

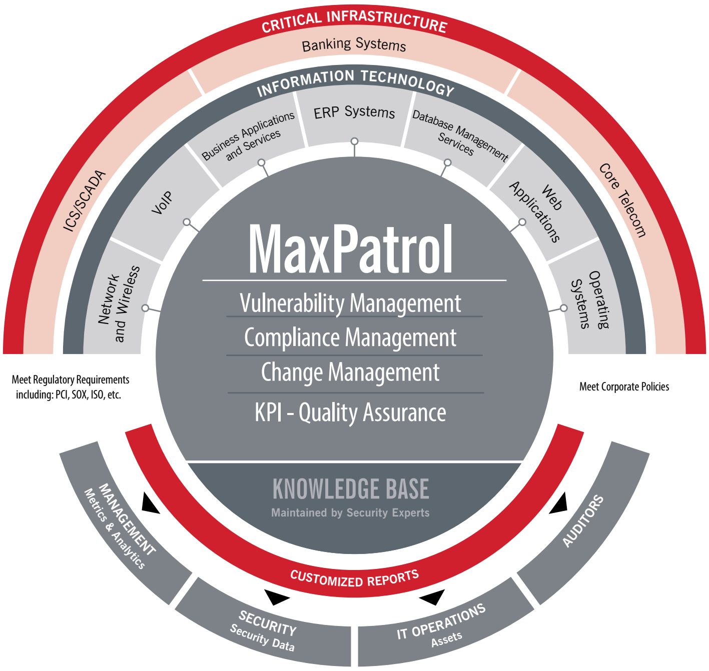
As a global authority on network security, Positive Technologies knows what it takes to comply with data security guidelines including SOX, ISO, PCI-DSS, 3GPP, NIST, NERC, HIPAA and many more. We understand that in addition to global or industry-wide regulations, often companies must also comply with regional or internal corporate standards.

MaxPatrol's combined set of benchmarks provides more than 5,000 controls that gives you the flexibility to quickly translate your high-level compliance standards into operational security controls.

> *"It's important for us to have full control of security compliance for all our IT systems. MaxPatrol is the only solution needed to scan, audit, prioritize, verify and report on security vulnerabilities and compliance across an entire global operation. MaxPatrol provides us with the complete solution to these challenges."*
>
> **Dmitry Ustyuzhanin, Head of Information Security, VimpelCom**

POSITIVE TRUSTED BY:

ING SAMSUNG
INTESA SANPAOLO SOCIETE GENERALE
Allianz VimpelCom



PINPOINT ACCURACY, HONEST PROTECTION

In terms of security, companies need reliable results that don't generate false positives, resulting in time spent sorting through necessary data, or dealing with the consequences of false negatives. Maintained by Positive Technologies experienced researchers and security experts, MaxPatrol™ provides:

- Script checks that reduce the level of false positives in banner-based checks
- Heuristic analysis
- Service and system state checks, instead of direct OS-to-vulnerability mapping — verifying vulnerabilities against active services and protocols

These unique methods deliver precise software IDs and versions, guaranteeing the lowest false-positive rate in the industry.

PROTECTING CRITICAL INFRASTRUCTURE

Critical infrastructure is no longer just ICS/SCADA, it can be a bank, a telecom, or pretty much any other company involved in key infrastructure business. No matter whether your business relies on traditional IT systems or industrial technologies, MaxPatrol™ can provide an in-depth security assessment of your enterprise landscape, create a practical attack model to illustrate where your business is at risk and outline the steps you should take to protect it.

AUTOMATING SAP SECURITY

Securing SAP systems and ensuring they are configured correctly is difficult due to the vast scale and complexity of a typical SAP infrastructure. MaxPatrol™ is certified for integration with SAP and provides industry-leading coverage of SAP by automating security for all parts of your SAP infrastructure. With MaxPatrol™ you can perform quick and non-intrusive assessments of multiple SAP instances. You will also get detailed information that SAP reports don't show like "shadow SAP_ALL" users, weak passwords and SOD violations. Your company and your SAP infrastructure are continuously changing. Be sure these changes are not weakening your security posture by regularly monitoring user activity, roles and profiles, configuration settings, password policies and more.

ADDITIONAL BENEFITS:

- **Integrated with Leading IT Solutions.** MaxPatrol's superior vulnerability and compliance intelligence is integrated with leading IT solutions including 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 and Symantec SIM.
- **Focus on What Matters to You.** Your business is unique and in turn so are your reporting needs. In addition to standard reports, MaxPatrol's BI solution supplies hundreds of customizable differential, trend and KPI reports and dashboards for real-time and historical data analysis, decision making and process control. Letting you focus on the security information that is most critical to your business.

- **Agentless Network Integrity Monitoring** — built-in components help to detect incidents and unwanted changes throughout your network.
- **Sensitive Data Detection** — powerful search engine identifies data such as credit card and PIN numbers and card verification values (CVV) in files and databases.
- **Certified CVE-Compatible** — independently verified as supporting the universally-recognized CVE system for classifying vulnerabilities, simplifying integration with other IT security systems and tools.
- **XML-Based Integration API** — supports the creation of a unified information security framework across systems including Business Intelligence Portals, Asset Management, Help Desk Ticketing, Request Tracking, Risk Management, Patch Management, SIM/SIEM, IPS, NAC/NAP and WAF Penetration Testing.
- **Flexible Reporting System** — automatically generates reports for inventory and change management, compliance and IT performance management. MHT, PDF, XML translators ensure you can obtain reports in custom formats and designs.

MAXPATROL™ KEY TECHNICAL FEATURES

MaxPatrol™ performs black-box and white-box testing and security configuration assessments on the following systems:

- Network Equipment (including firewalls and IPSs) from Cisco, Check Point, Stonesoft, Juniper (JunOS, ScreenOS), etc.
- Telecom equipment from Alcatel, Huawei, Nortel, Ericsson as well as VoIP systems from Digium
- Operating Systems including Windows, MacOS X, Linux, AIX, HP-UX, Cisco IOS, Oracle Solaris, Fedora, Gentoo, Mandriva, Slackware, etc.
- Databases including Microsoft SQL, Oracle, IBM DB2, PostgreSQL, MySQL and Sybase
- Desktop Applications and Browsers including MS IE/Office, Firefox, Google Chrome, Safari, Opera, OpenOffice, Lotus, Acrobat Reader, Flash Player and Thunderbird
- Infrastructure Applications including Microsoft Active Directory, Exchange, Sharepoint and IIS, IBM Lotus, Netscape DS, LDAP-UX, Sendmail, PostFix, MDaemon, MailEnable, Exim SMPT Server, Apache and CommuniGatePro
- Virtualization and Terminal Platforms including VMWare vSphere/ESX, Microsoft Hyper-V, Citrix XenApp
- Security Systems including Personal IPSs, Firewalls and Antiviruses
- Business Systems including Oracle E-Business Suite, SAP R3/ECC and NetWeaver
- Various ICS/SCADA platforms from Siemens, Invensys, Schneider Electric, Rockwell Automation, etc.

Secure Communications — SSL/TLS encrypted channels to communicate between MaxPatrol™ components, along with local storage of all gathered information and advanced role-based access control mechanisms make sure that sensitive information about your vulnerabilities never leaves your premises.

Password Policy Audit — black-box and white-box auditing, including dictionary bruteforce for systems using the following protocols:

- Remote access: VPN, RDP, VNC, Radmin, Telnet, SSH, etc.
- Application protocols: SAP, Oracle, SQL, Sybase, SIP, VMWare, etc.
- Infrastructure protocols: SMTP, PoP3, SMB, FTP, HTTP, etc.

About Positive Technologies

Positive Technologies is a leading global provider of enterprise security solutions for vulnerability and compliance management, incident and threat analysis, and application protection. Commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on Industrial Control System, Banking, Telecom, Web Application, and ERP security, supported by recognition from the analyst community. Learn more about Positive Technologies at ptsecurity.com.

POSITIVE TECHNOLOGIES

info@ptsecurity.com ptsecurity.com