POSITIVE TECHNOLOGIES

"As attackers compromise the ever-expanding sections of organizations' networks, retain long-term access, and venture deeper into corporate IT resources, the attacks on ERP systems are anticipated to increase."

Anton Chuvakin, Research VP, Gartner

Source: Gartner, G00255885, Vulnerability Assessment Technology and Vulnerability Management Practices, February 2014

What MaxPatrol can do for you

+ Cut costs by reducing reliance on expensive external consultants
+ Automate control of security for all parts of your SAP software deployment from network infrastructure, business modules and SAP Notes to SoD analysis
+ Provide visibility of vulnerabilities in SAP software before attackers can exploit them
+ Improve visibility with automated inventory of SAP components
+ Demonstrate due diligence and compliance with configuration assessments and SoD control

Certified Integration with SAP NetWeaver®
You cannot afford to trust your SAP system security to just anyone. MaxPatrol has been SAP-certified for integration with SAP NetWeaver 7.0 and is certified CVE-Compatibility by MITRE. It has also achieved CIS Security Software Certification.

SAP® Certified
Integration with SAP NetWeaver®

TAKE CONTROL OF YOUR SAP® SYSTEM SECURITY WITH MAXPATROL™

By facilitating real-time information flow between all core business functions, enterprise resource planning (ERP) systems can save organizations both time and money. But with direct connections to critical technologies such as Industrial Control Systems (ICS) or core banking software, they also present an attractive target for both outside hackers and insider threats. Regardless of who is behind the breach, the danger of fraud, data theft and reduced system availability that disrupts every part of your operations is real and present.

Security Challenges with SAP ERP

For most organizations, rolling out ERP software, like the SAP® ERP application, is a continuous, long-term process. Securing these systems and ensuring they are configured correctly is a significant undertaking because of the vast scale and complexity of a typical SAP infrastructure, not to mention the need to consider around 3,000 updates (SAP Notes) and 500+ controls and settings that are recommended in SAP security guides.

The pivotal business role of the SAP system and its connections to multiple operational technologies can discourage organizations from making any changes that might impact its functionality and availability. As a consequence, security for SAP systems, and particularly SAP business components, isn't always given the focus it deserves.

But with increased use of new technologies such as SAP HANA® Cloud Portal, to facilitate external access for staff and contractors, the risk of an SAP system attack is higher than ever. And the burden of compliance, including Segregation of Duties (SoD) analysis required by SOX, continues to grow.

Maintaining Control at Massive Scale

Many organizations rely on expensive external consultants to develop, deploy and maintain their SAP infrastructure but also to carry out security, compliance and SoD audits. They believe that with hundreds of SAP software instances and thousands of users, keeping track of their own inventory, vulnerabilities, compliance and configuration settings including access rights and password policies is an impossible task. But effective control can be achieved with automation. MaxPatrol, from Positive Technologies, is the only automated solution that provides combined support for all these features across all layers of your SAP infrastructure.

With MaxPatrol's multilayer analysis, certified to interoperate with the SAP NetWeaver® technology platform, you can take back control of your security. Our white-box assessments give you visibility and oversight of all SAP components at the network, operating system, database and application layers, for even the largest-scale systems. Data from our regular audits and configuration analysis will inform change control decisions and provide a historical reference for elements like Account Privileges and SAP Notes.

Black-box and white-box assessments are used to check SAP software installations and infrastructure components against MaxPatrol's database of more than 45,000 known vulnerabilities which is continuously updated by our team of security experts. With rapid, early detection of flaws in your network, you can work to close the gaps before attackers can exploit them.

A TOTAL SECURITY SOLUTION FOR YOUR SAP SYSTEM

MaxPatrol gives you visibility and control over the following elements of your SAP infrastructure:

+ System parameters
+ SAP services
+ Vulnerabilities in SAP software and SAP Notes
+ SAProuter configuration
+ Component version control
+ Authorization profiles
+ User groups
+ Accounts with critical privileges
+ Data and object access rights
+ Segregation of Duties
+ Password policy (online and offline bruteforce)
+ Audit settings
+ Backup settings
+ Encryption settings
+ RFC connections
+ OS and database settings

And because MaxPatrol is an agentless technology, you can enhance your security without creating deployment headaches, even if you have hundreds of SAP software instances. No code changes are required; just create a read-only user account in each SAP system (or a single account in SAP central user administration) and let MaxPatrol get to work.

Compliance Certified

Security standards provide only high-level guidance, without detailing the practical controls you need to implement to achieve compliance. MaxPatrol is pre-configured to conduct the specific technical checks that will provide visibility of your performance against SAP security guides, ISACA controls and technical aspects of international standards such as ISO and SOX. Custom security controls can also be easily created to automate assessments of compliance with your own unique corporate guidelines or those specified by authorities in individual countries.

MaxPatrol: Multilayer Analysis for SAP Software

MaxPatrol supports SAP system components including SAP NetWeaver for ABAP®, SAP NetWeaver for Java, SAP GUI client applications and SAProuter. In addition to performing automated SoD audits on most SAP components, MaxPatrol features built-in security and compliance checks for the following:

+ Basis
+ SAP ERP
+ SAP ERP Human Capital Management solution

But SAP ERP is a multi-layered application, and that means you need control at every layer or you'll leave gaps for attackers to crawl through. That's why MaxPatrol also supports inventory, change control, security audit, compliance and vulnerability assessments for components such as operating systems, network hardware, database management systems and terminal and virtual infrastructures. So it will uncover, for example, an incorrect configuration in an Oracle DBMS that could give hackers direct access to the SAP database and the ability to bypass security settings.

Why Positive?

Positive Technologies is recognized as a global authority on ERP security, in particular with SAP software–based infrastructures. Experts from Positive Technologies routinely conduct security assessments of SAP systems, and over the years have worked with SAP to eliminate vulnerabilities.

In addition to hands-on research, MaxPatrol has been proven successful in protecting many customers' SAP systems, including one installation with more than 700 SAP software instances that serves over 40,000 users.

About Positive Technologies

Positive Technologies is a leading provider of vulnerability assessment, compliance management and threat analysis solutions to more than 1,000 global enterprise clients. Our solutions work seamlessly across your entire business: securing applications in development; assessing your network and application vulnerabilities; assuring compliance with regulatory requirements; and blocking real-time attacks. Our commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on SCADA, Banking, Telecom, Web Application and ERP security, and distinction as the #1 fastest growing Security and Vulnerability Management firm in 2012, as shown in an IDC report*. To learn more about Positive Technologies please visit www.ptsecurity.com.

*Source: IDC Worldwide Security and Vulnerability Management 2013-2017 Forecast and 2012 Vendor Shares, doc #242465, August 2013. Based on year-over-year revenue growth in 2012 for vendors with revenues of $20M+.

POSITIVE TECHNOLOGIES