QUISTOR

An ITG Company

Patch Management Service

QUISTOR
An ITG Company

Managed Operational Security

As part of Quistor's Managed Services, the Managed Operational Security (MOS) department is responsible for mitigating technical risks associated with your company's security vulnerabilities. The MOS team protects valuable assets through security patching, vulnerability assessments, incident handling, and 3rd party security product implementation, ensuring that all systems are fortified against security threats.

Benefits

Patch Management - Trusted Approach

Recurring security patching follows a mutual pre-aligned schedule. Critical patches are applied ad hoc upon release and in alignment. Additionally, there's a guarantee of patch compatibility with applications within the scope of support.

Clear Reporting

MOS reports are meticulously designed to meet auditing requirements and compliancy standards. Security statistics are seamlessly integrated into existing monthly and quarterly reports. Furthermore, vulnerability assessments provide valuable insights into your system's security posture.

Dedicated Team of Experts

Our team comprises of dedicated consultants with technical application and cyber security knowledge. They ensure correct patch levels, prioritize patches effectively, and conduct thorough testing. Their expertise extends to 3rd party security products, tailored precisely to your needs.

Patch Management Services

Patch Management involves identifying vulnerabilities and then acquiring, testing, and applying updates (patches) to the relevant software. By applying these updates and fixes to software, operating systems, and devices, you can effectively protect against potential cyber threats. This reduces the risk of data breaches, unauthorized access, and system compromises. Security patching also helps enhance system performance and stability, ensuring your digital infrastructure operates smoothly.

The MOS team provides a comprehensive approach that enhances security while also reducing downtime and ensuring compliance with industry standards. Whether are dealing with routine patches or emergency updates for critical vulnerabilities, Quistor's ongoing dedication ensures the highest level of operational security and reliability for its customers in this Patch Management process.

Features

Protection against Vulnerabilities

Security patches play a vital role in protecting computer systems from vulnerabilities. These are weaknesses in software code that hackers or malicious actors can exploit to gain unauthorized access or control over a system. By applying patches, organisations can effectively mitigate these vulnerabilities and reduce the risk of exploitation.

Prevention of Exploits

Exploits are techniques or tools used by attackers to benefit from known vulnerabilities in software. Organisations can prevent these exploits from successfully compromising their systems by promptly applying security patches. This keeps the attackers at bay by ensuring known vulnerabilities are fixed before exploits become widely available.

Ensuring Data Confidentiality

Patching is crucial for maintaining the confidentiality of sensitive data. Many security patches address vulnerabilities that could lead to data breaches or unauthorized access to confidential information. Organisations can protect their data and maintain the trust of their customers and partners by rapidly applying these patches.

Maintaining System Integrity

Security patches are essential for maintaining the integrity of computer systems. The integrity of a system refers to its ability to function as intended without any unauthorized modifications or tampering. By patching vulnerabilities, organisations can prevent unauthorized changes to system files, configurations, or settings, ensuring the system remains secure and reliable.

Compliance with Regulations

Security patching is often required to comply with regulations and standards, as some industries have stringent requirements for protecting sensitive data. Non-compliance can lead to severe consequences, including legal penalties, reputational damage, and loss of business. By regularly patching systems, organisations demonstrate their commitment to security and compliance.

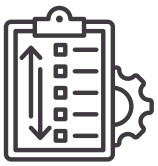
MOS Patch Management Catalog

Security Patch Management (continuous, recurring process)

- Windows Operating System (monthly / at chosen interval*).
- Linux Operating System (monthly / at chosen interval*).
- Oracle Weblogic Server / Fusion Middleware (quarterly*).
- Oracle Java (quarterly*).
- Oracle Database Client & Oracle Database (quarterly*).

*Ideal moment, but can also be patched at other intervals.

Benefits



Prioritization

With the security Patch Management services, the MOS team takes responsibility for prioritizing and applying the latest security patches, for systems and software in the scope of our support.

Trusted Approach

Recurring security patching follows a mutual pre-aligned schedule, applied ad-hoc, upon release and aligned with the customer.

When Patch Management is included in your SLA, MOS will drive the process from A to Z . It includes timely communication, testing, phased implementation of patches, and additionally taking care of issue handling related to patching.

Compatibility Check

Additionally, there is guaranteed patch compatibility for applications within the Quistor scope of support. As our MOS team already has the relevant in-house knowledge about these products, we will integrate this seamlessly and adopt that for patch eligibility and compatibility checks.

Signaling End-of-life Software

In some cases, vendors will discontinue support for a software program/operating system, also known as end-of-life software. The continued use of EOL software poses a consequential risk to your system, as it allows an attacker to exploit security vulnerabilities. Therefore, it is recommended that users and administrators retire all EOL products.

Quistor MOS will signal any (due) EOL products and timely communicate about end-of-support dates, in addition to recommending an update or upgrade to supported versions. Where applicable, these can be directly arranged via the Quistor Managed Services departments.

QUISTOR

An ITG Company

info@quistor.com

+31 164 213 300

www.quistor.com