InfoSight®
Bringing the Future into Focus®

877-577-9703
info@infosightinc.com
www.infosightinc.com

Patch & Vulnerability Management

InfoSight's Patch Management services are designed to address Windows, Linux and 3rd party applications. Our services reduce the risk around the exploitation of vulnerabilities by applying critical security patches within the shortest timeframe.

Overview - The Challenge

Today, most IT departments are stretched thin and keeping up with patches and vulnerabilities has become a full-time job. Adversaries utilizing attack vectors frequently seek to exploit vulnerabilities on systems that have not yet been patched against publicly available exploits. This leaves your organization at risk for a costly attack that could shut down business for good.

Key Features

- **Windows/Linux Server & Workstation Patches**
- **3rd Party Application Patches**
- **Security Updates**
- **Critical Updates**
- **Service Packs**
- **Update Rollups**
- **Patch Reports**

How We Solve It

InfoSight's proactive Patch & Vulnerability Management Services can act as an extension to your IT department to identify and, deploy critical patches 24x7. **Our US-based NOC operates 24x7, meaning our Network Engineers apply patches after work hours to minimize interruption and facilitate a stable and secure environment.**

We continuously scan devices and applications for missing required patches and from there, we test and determine which applications can be patched/updated and apply them for you.

The Outcome

With our patch management approval and rollout process, testing can occur prior to updating the entire population of servers and workstations. Additionally, our reporting is detailed and meets all regulatory requirements.

Why InfoSight

- Certified Experts (CISSP, CISA, CEH, CISSP, CPENT, CRISC, OSCP, AWWA, etc.)
- Complete Advisory Services that include Cybersecurity, Risk Management and Regulatory Compliance
- Experienced in both IT & OT ICS environments
- 22+ years of Regulatory Compliance experience (GLBA, PCI, HIPAA, NERC, AWIA, etc.)
- Offering comprehensive cybersecurity Awareness Training Solutions
- Virtual ISO Programs that bridge the communication gap between IT and OT networks
- 24x7x365 Emergency Incident Response Services
- Offering Network, Cloud, Application and Database Testing Services

Patch & Vulnerability Management

A Deeper Dive into InfoSight's Vulnerability & Cybersecurity Assessment Services

Social Engineering

- Patch updates/installation for manufacturer, critical and security patches, alerts, and status reports
- Supported 3rd party application patch updates
- Non-critical patch updates (available upon request)
- Preset patch implementation date/time (maintenance period)
- Reporting (installed, missing, reboot required, missed)
- Failed patch roll-back process (emergency roll-back requests)
- Collaborative management and reporting services

Microsoft Windows Patch Classifications

- Patch rollouts for “security” and “critical” operating system software patch updates (as defined by Microsoft terminology for software updates)
- Manage and deploy any Microsoft software update classification
- Expand software updates covering non-operating system Microsoft applications
- Determination of approved version updates, hot-fixes, rollups, and other application updates will be a collaborative process with the client.

Security Updates

- Widely released fix for a product-specific security-related vulnerability
- Security vulnerabilities are rated by their severity and the severity rating is indicated in the Microsoft security bulletin as critical, high, moderate, or low

Service Packs

- Tested, cumulative set of all hotfixes, security updates, critical updates, and non-emergency updates
- Contain additional fixes for problems that are found internally since the release of the product
- Contain a limited number of client-requested design changes or features
- Updates to utilities or features that helps complete a task or set of tasks
- Updates addressing critical, high, moderate, or low issues

Update Rollups

- Tested, cumulative set of hotfixes, security updates, critical updates, and updates that are packaged together for easy deployment.
- Targets a specific area, such as security, or a component of a product, such as Internet Information Services (IIS)

Patch Reports

- A generalized set of patch status reports are available and, in some cases, automatically generated/distributed to the client. Our standard patch status reports include the following information:
- Missing Patches Summary: Provides a graphical cross-customer summary of how many devices are monitored for patches per customer, and how many devices are missing security, critical and definition patches.
- Missing Patches Detail: Provides a breakdown of missing patches on one or more devices. It also indicates missing patches by workstation/ server and patch classification