InfoSight®
www.infosightinc.com

Attackers Don't Wait for Patch Tuesday

Patch & Vulnerability Management

Every Unpatched System Is an Open Door.
Cybercriminals target unpatched servers and workstations within hours of a public exploit release — and overloaded IT teams can't track, test, and deploy patches fast enough across every OS and application.

www.infosightinc.com | info@infosightinc.com | 305-828-1003

WHERE PATCHING BREAKS DOWN

- **Rising Vulnerability Exploits:** Cybercriminals target unpatched servers and workstations within hours of a public exploit release.
- **Resource Constraints:** Overloaded IT teams struggle to track, test, and deploy patches across diverse systems and applications.
- **Compliance Risks:** Missed security updates can trigger regulatory fines under HIPAA, PCI DSS, NERC, and GLBA.
- **Business Disruption:** Uncoordinated patch rollouts often lead to downtime, compatibility issues, and user complaints.

InfoSight's 24×7 Patch & Vulnerability Management automates security updates across Windows, Linux, and third-party applications — closing the gap before attackers find it, without disrupting your operations.

TURN PATCHING INTO PROTECTION

- ✓ **Zero-Downtime Patch Automation:** Windows, Linux, and third-party updates deployed off-peak, without disrupting operations.
- ✓ **Tested Before Deployed:** Every patch is evaluated for criticality and validated in staging before it touches production.
- ✓ **Broad Coverage:** Security updates, service packs, cumulative rollups, and third-party apps like Adobe, Java, and Chrome.
- ✓ **Audit-Ready Reporting:** Regulatory-grade patch reports built for auditors and the C-suite.

INFOSIGHT'S 24×7 PATCH & VULNERABILITY MANAGEMENT

1. **Continuous Vulnerability Scanning**
   Automated scans identify missing Windows/Linux security updates and third-party patch gaps.
2. **Prioritization & Approval Workflows**
   We evaluate criticality, test in staging environments, and get your sign-off before deployment.
3. **After-Hours Patch Deployment**
   U.S.-based engineers install updates off-peak (7 pm–7 am) to minimize operational impact.
4. **Comprehensive Remediation**
   We deploy service packs, update rollups, and hotfixes, then validate stability and performance.
5. **Detailed Compliance Reporting**
   Regulatory-grade patch reports for auditors, C-suite dashboards, and continuous improvement insights.

WHY CHOOSE INFOSIGHT

✓ **24×7×365 U.S.-Based SOC/NOC:** Staffed by SOC 2 Type II-certified analysts covering IT, cloud, and OT/ICS environments.	✓ **Flexible Engagement & Pricing:** 24×7, 8×5, or off-peak coverage, billed device-based or consumption-based.
✓ **25+ Years of Regulatory Expertise:** HIPAA, PCI, NERC, AWIA, and GLBA expertise built in.	✓ **Certified Security Experts:** CISSP, CISA, CEH, OSCP, AWS, and AWWA credentials across our team.

MITIGATOR®
CYBER RISK AND THREAT INTELLIGENCE PLATFORM

All results are delivered via our Mitigator™ Cyber Risk & Threat Intelligence Platform, with customizable exports for executives, auditors, and regulators.

TAKE THE NEXT STEP

Protect your network from exploit-driven attacks with InfoSight's Proactive Patch Management — request your assessment today. One expert call, zero obligation, no surprises.