nodeware®
Built by IGI CyberLabs

5 Reasons to Implement Proactive Vulnerability Management

In today's fast-paced digital world, cybersecurity isn't just a buzzword; it's a crucial for every business. Executives everywhere are waking up to this reality, but there's a catch – with cyber threats continuously evolving, knowing what to protect against isn't always clear. That's where you come into play.

As an MSP, you don't just react to threats; you're always one step ahead. And with proactive vulnerability management, you're not just patching up holes; you're fortifying digital fortresses around the clock. It's this vigilant approach that's redefining how you help your clients stay safe.

Proactive vulnerability management is not just about detecting threats – it's about staying ahead of them. Here are five compelling reasons why implementing proactive vulnerability management is essential for you and your clients.

1 Amplifies Protection

- Provides continuous oversight for 24/7/365 protection.
- Prevents costly incidents more effectively than periodic tests.

$10.5 trillion
The predicted financial damages from cybercrime by 2025.[2]

2 Improves Efficiency

- Automates routine tasks, reducing manual labor.
- Lowers operational costs, especially in IT and cybersecurity.

47%
of DevSecOps pros cite prioritization issues as the main cause of vulnerability backlog.[3]

3 Addresses Compliance and Cyber Liability Requirements

- Maintains visibility and control in remote and hybrid work environments.
- Aids in meeting standards like NIST Data and CIS 18 Controls.

60%
of data breaches occur because organizations neglect to address vulnerabilities in their systems.[4]

4 Reduces Response Time

- Accelerates threat detection and remediation.
- Nodeware offers links to actionable resources for quick resolution.

21 minutes
that's how long it takes to manually detect and remediate each vulnerability.[5]

5 Enhances Client Visibility

- Provides you real-time reports and alerts you can share with clients or co-managed IT teams.
- Encourages proactive investment in cybersecurity tools and services.

62%
of executives reported recent security incidents impacting business operations.[1]

In today's high-stakes cyber environment, proactive vulnerability management is more than a necessity; it's a game-changer. It not only steps up cybersecurity efforts but also solidifies relationships between you and your clients. This is achieved through continuous protection and consistent, real-time updates, fostering deeper trust and engagement.

Enter Nodeware, a leading vulnerability management solution that exemplifies this approach. Its user-friendly SaaS platform not only aligns with compliance requirements, but also opens new avenues for MSPs. If you're ready to experience a better way to secure your clients' networks, let's talk.

Contact Us

nodeware.com

Sources:
[1] https://www.prnewswire.com/news-releases/cybersecurity-resilience-emerges-as-top-priority-as-62-percent-of-companies-say-security-incidents-impacted-business-operations-301696237.html
[2] https://www.forbes.com/sites/bernardmarr/2023/02/06/cyber-apocalypse-2023-is-the-world-heading-for-a-catastrophic-event/?sh=4268869c1070
[3] https://www.rezilion.com/wp-content/uploads/2022/09/Ponemon-Rezilion-Report-Final.pdf
[4] https://nsetcyber.com/vulnerability-management-guide/
[5] https://www.securityweek.com/vulnerability-management-fatigue-fueled-non-exploitable-bugs/