OTAVA

DATA SHEET

VULNERABILITY SCANNING

Proactively prevent exploitations: Do you know if your security posture is free from gaps and shortfalls?

Data explosion, rapid growth in IT infrastructure, cloud computing and the Internet of Things are creating larger attack surfaces for cybercriminals and increased complexity for organizations. The potential for cybercrime is greater than ever, and continues to grow, which is why fortifying your defense and recovery strategies is vital to business continuity in today's world. But how do you know where your defenses fall short? Otava can scan your business critical systems and applications to expose vulnerabilities and help you understand what could happen if attackers were to exploit these weaknesses.

Vulnerability Scanning is a vital piece of protecting sensitive data and is emphasized by many compliances, including PCI DSS [Sec. 11.2.3], and HIPAA [Included in 164.308(a)(1)]. It is a big step towards proactively shoring up gaps in your defenses before an attack occurs. These scans can uncover important patches and updates that need to be made, and also highlight shortfalls in security services so that you can take proper action in reducing and eliminating potential attack vectors.

Key Features of Otava Vulnerability Scanning and Compliance Kit

- Auto-Scheduled vulnerability scans
- Meets internal and external scanning requirements for PCI
- Scan up to 10 IP addresses, 12 times per year
- Easily track resolution and compliance in the OTportal
- Includes an interactive PCI Self-Assessment Questionaire (SAQ)
- Initial configuration assistance and SAQ from Otava's 3rd party security consultant

Why Otava Vulnerability Scanning?

Required for PCI DSS compliance

If you are a merchant that needs to meet PCI DSS compliance (Payment Card Industry Data Security Standards) because you collect, store or process credit cardholder data, then you need to perform routine vulnerability scans each year, as well as after an incident occurs.

Bolsters HIPAA compliance

For healthcare, healthcare support, or insurance organizations that collect, store or transmit electronic protected health information (ePHI) and are required to meet HIPAA compliance, routine vulnerability scans are highly emphasized, and inform the necessary risk analysis and management plans.

A proactive defense approach

Protect yourself from cybercrime before an attack occurs by scanning for vulnerable patches and updates, and eliminating potential attack vectors.