Cygilant Unified Vulnerability and Patch Management

Reduce security vulnerabilities and enforce change control

Benefits

- Unify vulnerability scanning and patch management in one service

- Co-managed Qualys, Rapid7, or Tenable technology

- See adversary's view of internal and external vulnerabilities

- Uncover common flaws like misconfigured firewalls

- Automatically fetches available patches

- Deploy patches to multiple systems in one clear workflow

- Automatically verify patches are installed

- Obtain an auditable change management and rollback process

- Generate executive scorecards for management reporting

"Security and risk management leaders responsible for vulnerability management should implement a vulnerability management program that includes discovery, prioritzation and then treatment."

- Gartner*

Sophisticated attackers exploit unpatched and misconfigured software every day. But, while the rate patches need to be applied is increasing, lack of time and staff, as well as technical, organizational and process control challenges all contribute to why IT teams don't continuously scan for vulnerabilities and regularly patch systems.

This is where Cygilant comes in.

Cygilant's mission is to help resource-constrained organizations of all sizes build an affordable enterprise-class security program.
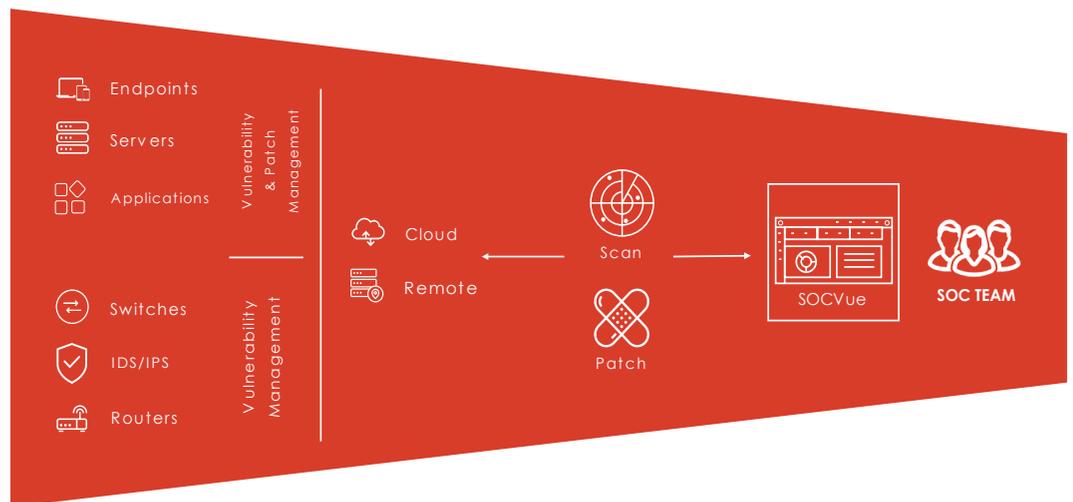
Scan, Locate, Prioritize, Deploy

Cygilant's Unified Vulnerability and Patch Management is a subscription-based service to find and fix unpatched servers, desktops and laptops on, or off, a network. It is unique and integrates four main capabilities:

1. **Scheduling recurring scanning** using popular technology such as Rapid7's Insight VM or Nexpose, Tenable Nessus, or Qualys to systematically uncover unpatched or misconfigured systems and vulnerabilities.

2. **Locating needed patches** for operating systems including Windows, Linux, MacOS and dozens of third-party applications.

3. **Risk prioritization** ranking systems based on asset value, vulnerability exploitability and business impact.

4. **Patch deployment** using an integrated workflow with change control processes to review, approve, schedule, apply, validate, and, if needed, rollback.

Cygilant's Unified Vulnerability and Patch Management service saves you time by automatically correlating identified vulnerabilities with missing patches. Instead of manually locating required patch updates, Cygilant's Unified Vulnerability and Patch Management service will assess vulnerabilities and deploy the patches in one integrated workflow.

How It Works

Each customer is assigned a dedicated Cybersecurity Advisor, who becomes familiar with their client's systems, processes, compliance requirements and security goals. The Cybersecurity Advisor provides technology management assistance, security best practices and works with you to find and fix vulnerabilities, misconfigured and unpatched systems.

Your dedicated Cybersecurity Advisor helps to deploy your chosen scanner technology and patch agents across the network, workstations and servers

We schedule recommended scans (internal, external, authenticated and non-authenticated, etc.) to uncover vulnerabilities and needed updates

We provide you the relevant patches and best-practice change controls, so you can progressively apply, and if desired, roll-back, patches to update systems and address vulnerabilities

We work with you to continuously scan systems and help prepare documents and artifacts to satisfy your compliance mandates

Features

–   Dedicated Cybersecurity Advisor

–   Integrated vulnerability and patch management

–   Scheduled vulnerability scanning

–   Risk-based prioritization of vulnerabilities

–   Auditable change management

–   Remote deployment

–   Executive scorecards and reports

Empower Your Security with Cygilant

Acting as an extension of your IT team, Cygilant frees you of laborious time consuming tasks while protecting against known vulnerabilities, misconfigured and unpatched systems. We empower IT and security teams to leverage scarce resources and improve their effectiveness, all at a reasonable total cost of ownership.

Protect the organization

Safeguard against cyber-attacks with an effective vulnerability patching process that protects the organization.

Leverage vulnerability management investments

Cygilant will remotely manage or co-manage your Qualys, Rapid7, or Tenable solutions yielding better ROI and security results.

Easy, fast and reliable updates

Cygilant's unified vulnerability and patch management service replaces error-prone manual processes.

Regulatory compliance and reporting

Meet vulnerability and patching requirements of regulations including PCI DSS, HIPAA, FFIEC, GLBA, SOX, FERPA, NERC-CIP, NIST and others.

*Gartner, Implement a Risk-Based Approach to Vulnerability Management, Prateek Bhajanka, Craig Lawson, 21 August 2018

AICPA SOC
aicpa.org/soc4so

Cygilant, Inc.
60 State Street, Boston, MA 02109
www.cygilant.com