Adlumin

CONTINUOUS VULNERABILITY MANAGEMENT

Don’t just find vulnerabilities, fix them.

Organizations are constantly being challenged from attackers who are looking for vulnerabilities within their infrastructure to exploit and gain access. Organizations must have timely threat information available to them about: software updates, patches, and misconfigurations, open ports, unnecessary services running, etc., and they should regularly review their environment to identify these vulnerabilities before the attackers do. Understanding and managing vulnerabilities is a continuous activity, requiring focus of time, attention, and resources.

By moving towards continuous vulnerability management practices, organizations can close the gaps between security assessments and significantly reduce risk.

Adlumin’s cloud-based Continuous Vulnerability Management constantly assess and track vulnerabilities on all enterprise assets within the enterprise’s infrastructure, to remediate, and minimize, the window of opportunity for attackers.

The steps in the Vulnerability Management Life Cycle are described below:

1. **Discover**: Inventory all assets across the network and identify host details including operating system and open services to identify vulnerabilities. Identify security vulnerabilities on a regular automated schedule.
2. **Prioritize Assets**: Categorize assets into groups or business units.
3. **Assess**: Determine the risk profile, so you can eliminate risks based on vulnerability threat.
4. **Report**: Measure the level of business risk associated with your assets according to your security policies.
5. **Remediate**: Prioritize and fix vulnerabilities in order according to business risk.
6. **Verify**: Verify that threats have been eliminated through follow-up audits.

Adlumin

VULNERABILITY MANAGEMENT

Continuously detect and protect against attacks, anytime, anywhere.

Adlumin's Vulnerability Management Service is a cloud-based service that gives you immediate, global visibility into where your IT systems might be vulnerable to the latest internet threats and how to protect them. It helps you to continuously identify threats and monitor unexpected changes in your network before they turn into breaches.

Detailed Features	
Discover forgotten devices and organize your host assets. You can quickly determine what is running in the different parts of your network—from your perimeter and corporate network to virtualized machines and cloud services such as Amazon EC2. Uncover unexpected access points, web servers, and other devices that can leave your network open to attack.	• Visually map your network with our graphical host map. • Prioritize your remediation by assigning a business impact to each asset. • Identify which OS, ports, services, and certificates are on each device on your network. • Organize hosts to match the structure of your business—e.g., by location, region, and company department. • Control which hosts can be scanned by which users. • Dynamically tag assets to automatically categorize hosts by attributes like network address, open ports, OS, software installed, and vulnerabilities found.
Scan for vulnerabilities everywhere, accurately and efficiently. Scan systems anywhere from the same console: your perimeter, your internal network, and cloud environments (such as Amazon EC2). Since Adlumin separates scanning from reporting, you can scan deeply and then create custom reports showing each audience just the level of detail it needs to see.	• Select target hosts by IP address, asset group or asset tag. • Scan manually, on a schedule, or continuously. • Scan behind your firewall securely with Scanner Appliances, remotely managed by Adlumin 24/7/365. • Scan complex internal networks. • Securely use authentication credentials to log in to each host, database or web server. • Scan in Amazon EC2 without filling out request forms—Adlumin is pre-approved. • Store configuration information offsite with secure audit trails.

Detailed Features	
Identify and prioritize risks. Using Adlumin, you can identify the highest business risks using trend analysis, Zero-Day and Patch impact predictions.	• Track vulnerabilities over time; as they appear, are fixed or reappear. • Monitor certificates deployed throughout your network—see what's about to expire, which hosts they are used on, what their key size is, and whether they are associated with any vulnerabilities. • Put critical issues into context with the Adlumin's industry-leading, constantly updated Knowledgebase. • See which hosts need updates after Patch Tuesday every month. • Examine your network's vulnerabilities over time, at different levels of detail, instead of just single snapshots. • Predict which hosts are at risk for Zero-Day Attacks with the optional Adlumin Zero-Day Risk Analyzer.
Remediate vulnerabilities Adlumin's ability to track vulnerability data across hosts and time let you use reports interactively to better understand the security of your network. Use a library of built-in reports, change what's shown or choose different sets of assets—all without having to rescan. Reports can be generated on-demand or scheduled automatically and then shared with the appropriate recipients online in PDF or CSV.	• Automatically generate and assign remediation tickets whenever vulnerabilities are found. • Get consolidated reports of which hosts need which patches. • Integrate with third-party IT ticketing systems. • Manage exceptions when a vulnerability might be riskier to fix than to leave alone. • Exceptions can be set to automatically expire after a period for later review.
Custom reports anytime, anywhere—without rescanning. Adlumin's library of built-in templates allows you to generate reports showing vulnerability trending, that can be exported in a variety of formats (HTML, DocX, MHT, XML, PDF, CSV). With granular customization of report templates, you can add your logo and personalize reports with your organization's branding.	• Create different reports for different audiences—from scorecards for executives, to detailed drilldowns for IT teams. • Document that policies are followed and lapses get fixed. • Provide context and insight about each vulnerability, including trends, predictions, and potential solutions. • Track ongoing progress against vulnerability management objectives. • Management objectives. • Share up-to-the-minute data with GRC systems and other enterprise applications via XML-based APIs.

Adlumin

PATCH MANAGEMENT

Streamline and accelerate vulnerability remediation for all your IT assets.

Patch Management is a cloud service that helps security and IT professionals efficiently remediate vulnerabilities and patch their systems.

Adlumin is uniquely positioned to leverage both vulnerability and threat intelligence insights in its patching solution. Cleverly, Adlumin's approach of taking patch remediation a step further with the addition of zero-touch automation eliminates non-caustic threats like always patching Chrome or iTunes. It is a welcome addition that helps companies reduce their attack surface while also freeing up IT and Security resources to focus on more strategic areas.

Detailed Features	
A single solution to patch operating systems (OS), mobile devices and third-party applications.	Adlumin Patch Management can be used to patch and apply post-patch configuration changes to operating systems, mobile devices, and third-party applications from a large variety of vendors, all from a central dashboard. That way you don't have to manage patches in silos via multiple vendor-specific consoles.
Cloud-based solution that is easy to deploy and use.	No need to install software on premises or configure open ports and VPNs. Any on-premises workstation and server, or work-from-home (WFH) device with the Adlumin Cloud Agent installed can be immediately scanned for missing patches and patched. Anywhere you can put the Adlumin Cloud Agent, you can run Adlumin Patch Management. When Adlumin Patch Management is used with the Adlumin Cloud Agent Gateway Service, you can significantly optimize bandwidth usage by caching patches locally on your network.
Remote patching for corporate and personal devices (endpoint and mobile).	With remote work now the norm, many organizations struggle to deliver patches to corporate and personal devices when users are working from home or otherwise infrequently connected to the network. Adlumin Patch Management allows the patch team to deliver patches to these remote users within hours from the cloud, while avoiding the use of limited VPN bandwidth.

Detailed Features	
Automated correlation of vulnerabilities and patches.	Adlumin Patch Management lets you automatically correlate vulnerabilities with patches and required configuration changes, decreasing your remediation response time. Adlumin Patch Management efficiently maps vulnerabilities to patches and required configuration changes, and automatically creates ready-to-deploy “patch jobs” that can be scheduled and deployed automatically. A first-in-the-industry report lets security and IT teams define a single shared priority list of systems and applications to patch regularly, based on historical per-application vulnerability data, for increased productivity and cooperation between these two teams.
Zero-Touch Patch	Adlumin Patch Management gives the flexibility to automate patching based on prioritized vulnerability data that helps enterprises address the most critical threats like ransomware. Teams can automatically apply routine patches where risk of creating system instability is low, to reduce time to remediation and free up critical IT and Security resources to focus on strategic tasks. This helps security and IT teams reduce their attack surface, more easily meet SLAs, and reduce manual remediation efforts and costs.