



# The Adlumin Difference

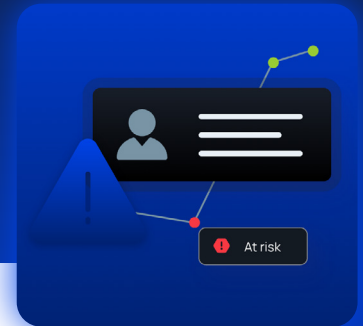
## Security Operations Platform

Extended Detection and Response (XDR), Managed Detection and Response (MDR), and Managed Security Services



# Table of Contents

|                                    |   |
|------------------------------------|---|
| What Makes Adlumin Different ..... | 2 |
| Features of Adlumin XDR .....      | 2 |
| Compliance Automation Tools .....  | 4 |
| Darknet Monitoring .....           | 5 |
| Compliance Reporting .....         | 5 |
| Adlumin MDR .....                  | 6 |



## What Makes Adlumin Different?

### We won't let your business get caught in the dark.

Adlumin provides the premier command center for security operations. We stop advanced cyber threats, eliminate vulnerabilities, and take command of sprawling IT Operations with Adlumin's Security Operations Platform. You can manage Adlumin Extended Detection and Response (XDR) SaaS product yourself, through a trusted Partner, or engage the Adlumin 24x7 Manage Detection and Response (MDR) team to protect your business.

Adlumin offers world-class analytics, compliance reporting, automation and remediation tools, integrated threat intelligence, 24x7 search for leaked accounts on the darknet, on-demand customer support, implementation in 90 minutes, and more.








Adlumin is a cost-effective and attainable solution for small, medium, or large organizations. Customers can monitor and defend their networks locally, in the cloud, and across the globe.

## Features of Adlumin XDR

### Illuminate Threats. Eliminate Risks. Command Authority.

What you can't see poses the greatest risk. Your exposures lurk amongst your employees and vendors, your hybrid environments, cloud services, and the darknet. There are countless gaps where threats can hide before they lead to business disrupting events like ransomware shutdowns or massive data breaches.

Adlumin XDR illuminates threats that would have otherwise gone unseen in the lead up to a massive attack. Our cloud-native security operations platform leverages powerful machine learning to identify critical threats, automates remediation rules and system updates, and provides continuous compliance reporting. Our platform is backed by a team of experts delivering 24x7 human insights, threat hunting, and trusted support.

|   |   |
|---|---|
|    | <p><b>Compliance Reporting</b></p> <p>The regulatory landscapes are constantly shifting. With Adlumin's One-Touch Compliance Reporting, you can snapshot reports, framework verification, and executive reports to eliminate uncertainty and streamline your compliance efforts.</p>  |
|    | <p><b>Darknet Monitoring</b></p> <p>Far too many cyberattacks rely on stolen credentials for sales on a booming darknet economy. Identifying darknet compromise before your own data is used to exploit you can be the difference between a minor nuisance and a major incident. Adlumin's darknet monitoring finds your confidential information before it falls into the wrong hands.</p> |
|    | <p><b>Honeypots</b></p> <p>Building on Adlumin's multi-layered security approach, this feature offers customers another way to detect threat actors already in their environment to quickly stop them before they access critical systems or data.</p>  |
|    | <p><b>Prevent Privilege Abuse &amp; Account Takeover</b></p> <p>Adlumin uses artificial intelligence to detect known and unknown threats—specifically when determining an insider threat, account takeover, and privilege abuse or misuse.</p>  |
|    | <p><b>Ransomware Prevention</b></p> <p>Identify and prevent malicious encryption at the earliest stage, minimizing the impact on your file system. (Only available with Adlumin MDR).</p>   |
|   | <p><b>Security Information and Event Management (SIEM)</b></p> <p>Our vendor-agnostic approach means you can ingest data across your enterprise. Adlumin correlates and prioritizes alerts from network traffic to web servers to SaaS applications.</p>  |
|  | <p><b>User &amp; Entity Behavior Analytics (UEBA)</b></p> <p>Using proprietary artificial intelligence and machine learning algorithms we analyze account-based threats. Our UEBA develops baselines in your environment to help identify, detect, analyze, and prioritize anomalous behavior in real-time.</p>   |

## Managed Security Services\* \*Please note that managed security services are offered at an additional cost to Adlumin XDR.

**Incident Response** Adlumin's Incident Response provides lean teams with the expertise necessary to understand the full scope of a breach, remove the threat, and provide actions to strengthen security. When faced with a security breach, gain the confidence of knowing you are covered every step of the way.

**Penetration Testing** Adlumin Penetration Testing offers progressive assessments to meet every customer's risk tolerance. Our tests can simulate different vantage points, from limiting the scope and seeing what an attacker could exploit from inside a defined range to an "outside-in" perspective to see if an attacker could access critical data and assets inside a specific scope.

**Security Awareness Training** Adlumin's Security Awareness Training empowers employees with the skills to identify and report suspicious activity, which is the best defense against cyber adversaries delivering attacks through convincing campaigns and phishing lures.

**Total Ransomware Defense** Total Ransomware Defense compliments your existing security solutions by recognizing when ransomware is in your environment. Adlumin takes a layered approach to identify and stop ransomware before it completes its tasks and includes a recovery as the last layer, so you can access any encrypted files.

**Vulnerability Management** Criminals leverage system exploits and poison code at the sources, which means vendors are constantly publishing patches and updates. Vulnerability Management enables you to identify and prioritize critical vulnerabilities and reduce the likelihood of a criminal exploiting your business through a known vulnerability.

## Compliance Automation Tools

### Simplify Your Compliance Requirements

Adlumin XDR is designed for businesses that care about security and compliance. Therefore, we have automated PCI DSS, NIST, and HIPAA compliance, which includes the following actions:



Automatically tracks and records all access and combines compliance details across the entire enterprise



Investigates anomalous activity on your network quickly and easily using Adlumin's Investigation Tool



Continuously implements PCI DSS best practices



PCI DSS device log management



Determines and views all privileged accounts at local and domain levels quickly and easily



Reviews logs daily and retains log monitoring audit trail for one-year making you fully PCI compliant



Graphically visualizes active directory groups, accounts, members, and memberships identifies PCI DSS violations across log analysis, account management, and GPO audit policies



Reviews your Active Directory GPO policies for PCI violations and bad security practices



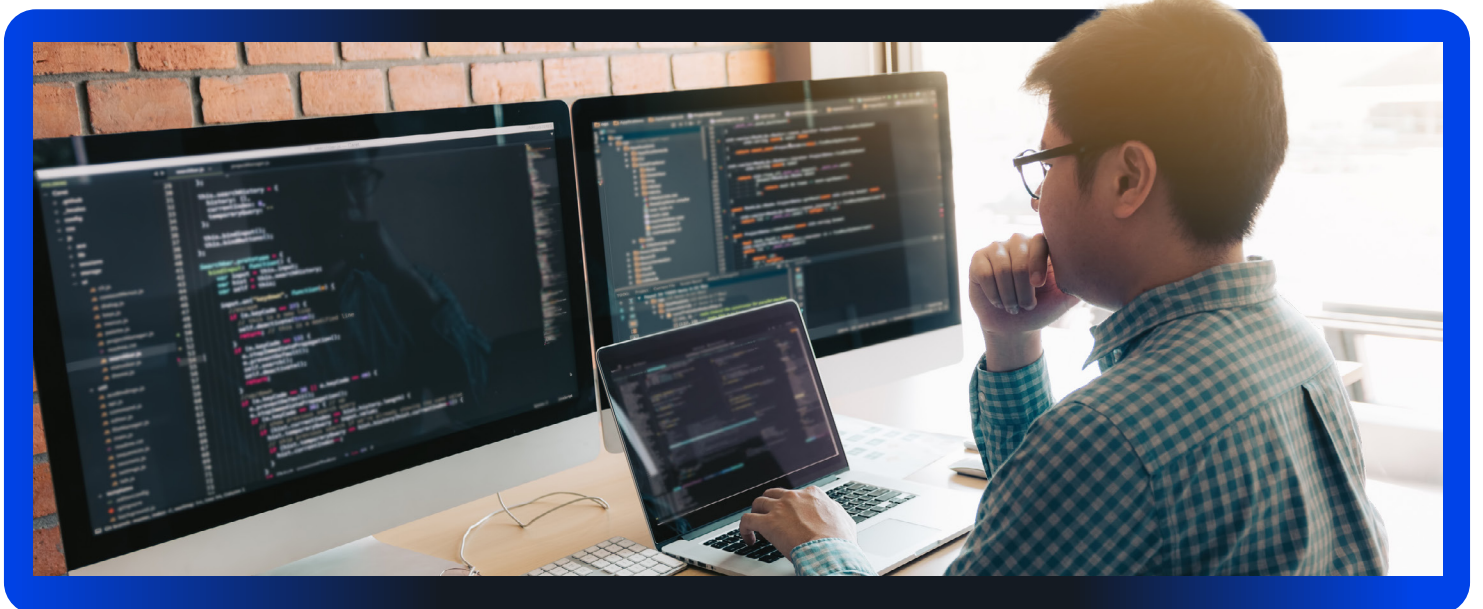
Satisfies Tier 1 PCI attestation compliance



Integrates compliance (e.g., PCI DSS, NIST, and HIPAA)



Secures PCI DSS log audit trails in real-time



## Darknet Monitoring

### 24x7 Search for Leaked Accounts on the Darknet

Adlumin Darknet Monitoring extends defensive capabilities beyond your firewalls, endpoints, and security devices. Adlumin protects all domain accounts with automatic notifications and password resets if a business account is leaked.

#### Leaked Account Scanning

Adlumin measures risk associated with specified data breaches or credential leaks to help prevent account takeovers and credential stuffing attacks for critical (privileged accounts) and high (unprivileged accounts) severity breaches.

Adlumin can initiate an automated victim notification (to include the user and security team), and force a password reset of the business domain account that was leaked.

#### How Adlumin Protects Customers Against Breaches

Adlumin XDR knows the exact date and time that every account on your network last changed its password. Our security analytics platform enhances that data with information about if (and when) your account(s) were exposed on the internet. If an account was exposed and the last password change precedes the exposure date, it is at extreme risk for being used by an intruder to access your network.

## Compliance Reporting

### Compliance regulations and security professionals agree that log data should be retained for a minimum of one year



#### Satisfy Compliance Requirements

If you must comply with regulations (e.g., PCI DSS, NIST, HIPAA), you need reports that are designed to hand directly to financial auditors. Adlumin has PCI DSS and other compliance reports built into the platform, which can be downloaded in seconds.



#### Achieve Compliance and Regulatory Storage Requirements

Achieve compliance and regulatory requirements in seconds. PCI DSS requires that you keep your log data for one year to be compliant, while FINRA requires that you keep your data for seven years. Adlumin makes it simple to keep your data for as long as you need it.



#### Secure and Automatic Data Transfers

Adlumin XDR automatically backs up every single log that is ingested for your organization without any monitoring on your part.



#### Visualization in One Click

You can visually see that your data is backed for one year on the platform's dashboard. Don't worry about whether you captured it—the system does it automatically.



#### Better Informed Decision-Making

Decisions about your network should be driven by data. If data is needed to decide, it will be there. Remember, if you don't back up your data, it will be gone forever.

## Adlumin Managed Detection and Response (MDR)

### Adlumin XDR plus 24x7 Managed Detection and Response

Adlumin MDR provides 24x7 monitoring and response. Get all the capabilities of Adlumin XDR including SIEM, User & Entity Behavior Analytics (UEBA), Compliance Reporting and Threat Intelligence. Our transparent platform means you always have access to your data and visibility into your environment.



#### Monitoring, Detection, and Response in Real-Time

Real-time monitoring, detection, and response to potential intrusions through historical trending on relevant security data sources.



#### Analysis and Recommendations

Receive analysis and recommendations for confirmed incidents, including the use of timely and appropriate countermeasures.



#### Achieve Compliance Requirements

Assists with automated compliance reporting (e.g., PCI DSS, NIST, and HIPAA)



#### Ransomware Prevention

Identifies and automatically stops malicious encryption process and contains the host to decrease business impact.



#### Vulnerability Network and Host Scans

Conducts regular vulnerability scans with reports for a clear view of your network (e.g., outdated software, weak passwords, dangerous open ports, etc.).



#### Privilege Analysis of Network Accounts, Systems, and Groups

Privilege analysis of every account, system, and group, so users know exactly who can access their most sensitive data.



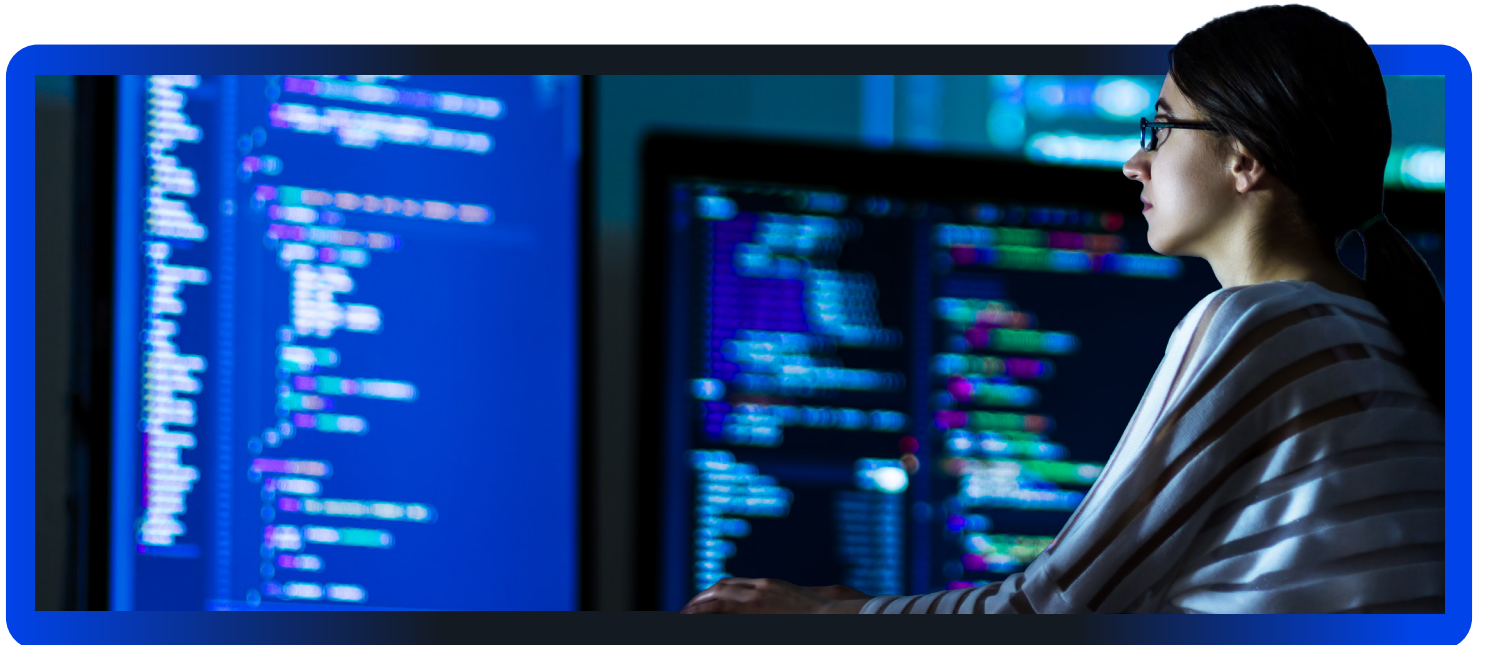
#### Situational Awareness and Reporting

Provides situational awareness and reporting on your organization's current cybersecurity posture, incidents, and trends.



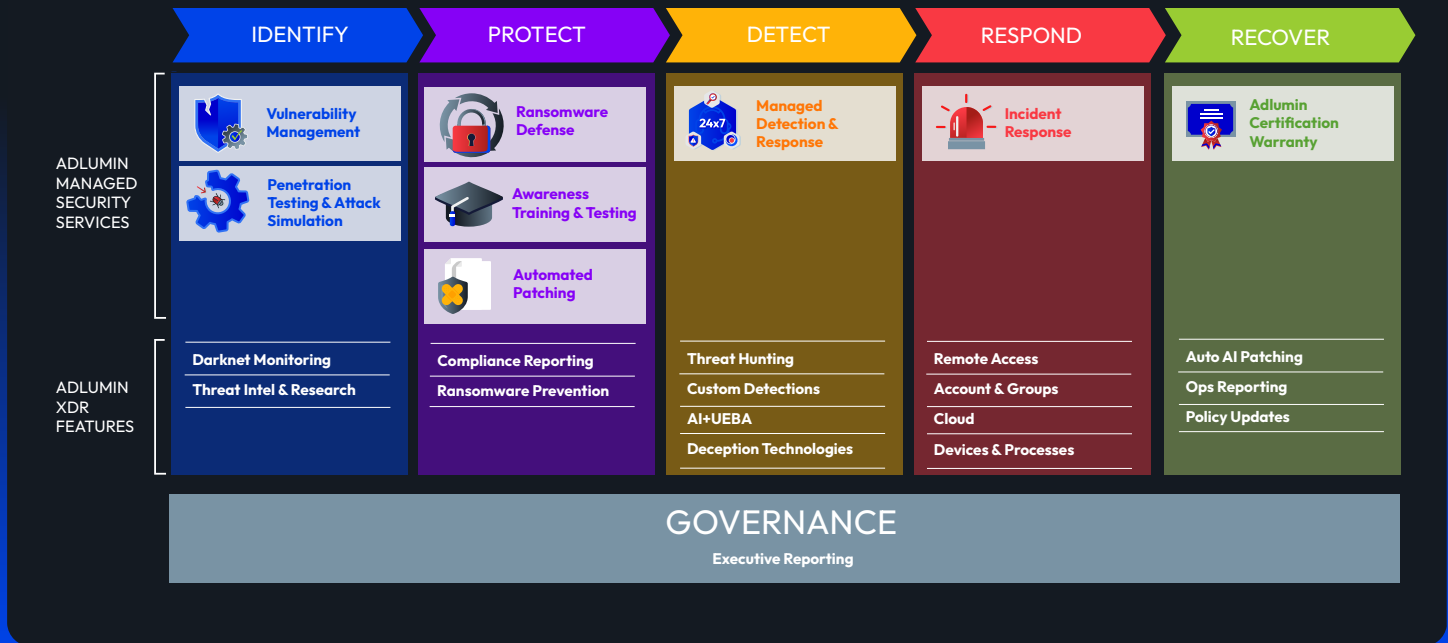
#### Single Point-of-Contact

All customers have a single point-of-contact for Adlumin Managed Detection and Response.



# Adlumin Security Operations Platform & the NIST Framework

Adlumin Extended Detection and Response (XDR), Adlumin Managed Detection and Response (MDR), and Managed Security Services



Adlumin is the security operations command center that simplifies complexity and keeps organizations of all sizes secure. Its innovative technology and seamless integrations create a feature-rich platform that includes everything a sophisticated security team needs, while empowering channel resellers, service providers and organizations of any size with the collaboration and transparency required to establish a coordinated and mature defense.

With a vendor-agnostic approach and preexisting integrations, Adlumin's Security Operations Platform obtains security telemetry from across an organization to provide greater insights into security alerts and streamline workflows. Organizations can use Adlumin's Security Operations Platform on their own or get full transparency and visibility while utilizing the 24/7 monitoring and response services provided by the Adlumin Managed Detection and Response (MDR) team. Whether organizations manage the platform on their own or with MDR, Adlumin consolidates all security needs for a unified experience.