# Adlumin Exfiltration Prevention

## A New Frontier in Cyber Defense

Exfiltration and extortion-based attacks have emerged as a significant threat to enterprises worldwide. The sophistication and frequency of these attacks have surged, with cybercriminals employing advanced tactics to maximize their profits. Adlumin's Exfiltration Prevention expands on the Adlumin Ransomware Prevention capability and is designed to thwart these pre-ransomware activities and safeguard enterprise data.

## The Ransomware Threat Landscape

**11 Sec**[1]
Frequency of Ransomware Attacks

**$1.85 Mil**[2]
Total Cost of Recovery

**77%**[3]
Of Ransomware Attacks involved Data Exfiltration

## Exfiltration and Extortion Tactics

Ransomware attackers have evolved their strategies to include exfiltration and extortion as a precursor to deploying ransomware. This method involves several steps:

| | | |
|---|---|---|
| **Step 1** | Initial Compromise | Attackers gain access to the victim's network through phishing, exploiting vulnerabilities, or other means. |
| **Step 2** | Data Staging | Critical business files are moved into a consolidated directory in preparation for data exfiltration. |
| **Step 3** | Data Archiving | Files are moved into a single archive file to reduce the size and encrypt sensitive data leaving the network. |
| **Step 4** | Data Exfiltration | Sensitive data is identified and exfiltrated to an external location controlled by the attackers. |
| **Step 5** | Extortion Threat | The attackers threaten to publicly release the exfiltrated data unless a ransom is paid. |
| **Step 6** | Ransomware Deployment | Ransomware is often deployed and encrypts data, demanding additional payment, regardless of whether the ransom exfiltrated data is paid. |

This dual-threat model increases the pressure on victims, significantly enhancing the chances of ransom payment.

## Key Features of Exfiltration Prevention

**Monitoring Pre-set Markers and Files:** The system continuously monitors strategically placed markers and files acting as honeypots to attract malicious processes.

**Process Monitoring and Interaction Tracking:** Exfiltration Prevention monitors processes interacting with pre-set markers and files, triggering an alert if any attempt is made to move them.

**Archiving Detection:** The capability includes monitoring when these markers or files are archived, detecting file compression into formats like ZIP, RAR, 7Z, and others.

**Process Chain Termination:** Upon detecting these attacker activities, the process chains are terminated, disrupting attacks before ransomware deploys and prevents data exfiltration and extortion.

**Alerting and Reporting:** Administrators receive real-time alerts and detailed reports on the attempted exfiltration activities, enabling them to take further security measures and conduct forensic analysis.

## Advantages of Adlumin's Exfiltration Prevention

**Early Threat Detection:** By focusing on pre-ransomware activities, Exfiltration Prevention provides early warnings, allowing organizations to act before significant damage occurs.

**Process Chain Disruption:** Terminating the process chains involved in exfiltration activities halts the attack in its tracks, preventing both data theft and subsequent ransomware deployment.

**Comprehensive Coverage:** The capability covers a wide range of potential exfiltration methods, ensuring robust protection against diverse attack vectors.

**Ease of Integration:** Designed to integrate seamlessly with existing security infrastructure, Exfiltration Prevention enhances overall cybersecurity posture without disrupting operations.

Ransomware attacks continue to pose a grave threat to enterprises, with exfiltration and extortion tactics adding a new layer of complexity. Adlumin's Ransomware and Exfiltration Prevention capability offers a powerful solution to this challenge, providing early detection and disruption of malicious activities before they can escalate into full-blown ransomware attacks. By integrating this capability, organizations can significantly enhance their defenses and protect their sensitive data from the evolving threat landscape.

Adlumin Inc. provides an enterprise-grade security operations platform that keeps organizations secure regardless of size or budget. Its patented technology gives organizations and solution providers everything they need for effective security, including SIEM, threat hunting, incident response, penetration testing, vulnerability management, darknet exposure monitoring, compliance support, and more.

The Adlumin platform is feature-rich enough for organizations to operate on their own yet explicitly built to amplify the skills and capabilities of channel resellers.