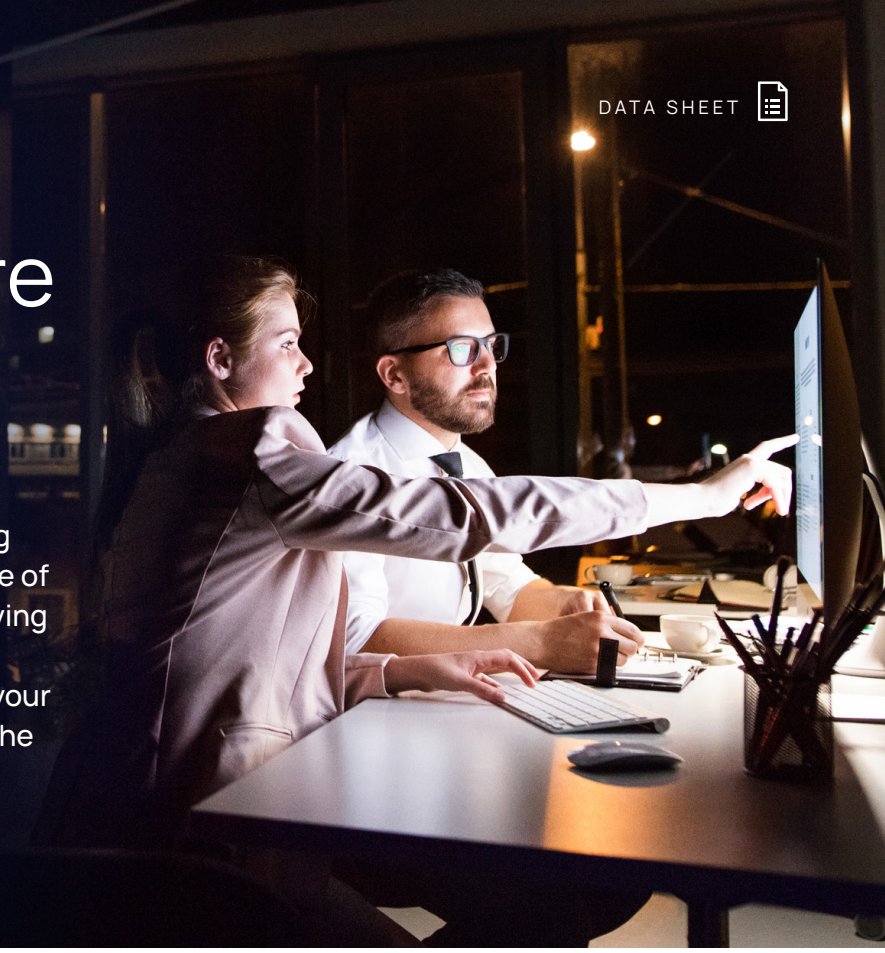
adlumin™

DATA SHEET

Total Ransomware Defense

Multi-Layer Ransomware Protection



Ransomware is one of the biggest threats facing the cybersecurity industry today. The magnitude of its danger continues to increase by the day, leaving organizations around the country vulnerable. Adlumin's Total Ransomware Defense provides your network with multi-layer protection to prevent the success of a ransomware attack at each layer.

How it Works

The first layer uses several external threat feeds, proprietary data feeds, and machine learning to instantly block known ransomware. Suspicious processes that are not "known bad" are passed to the additional layers for further analysis.

LAYER 1 Pre-Execution

The first layer uses several external threat feeds, proprietary data feeds, and machine learning to instantly block known ransomware. Suspicious processes that are not "known bad" are passed to the additional layers for further analysis.

LAYER 2 Entrapment

Ransomware operates within the confines of a ruleset to prevent it from being detected. The entrapment layer focuses on triggering this ruleset through deception techniques to prevent detonation. This layer enables the endpoint to hide files from encryption, laces the endpoint with artifacts to deceive the ransomware's internal execution rules, and adds bait files to amplify the ability to detect malicious behavior.

LAYER 3 Behavioral

Ransomware that is not blocked through the previous layers will trigger the next level. The behavioral layer employs an industry-first micro-model architecture designed on the principle of capsule network-based machine learning. that enables broad benefits over previous behavioral analysis methods. It works together across endpoints and the entire organization to make decisions on suspicious processes in real-time.

LAYER 4 Resiliency

Total Ransomware Defense has built-in resiliency and isolation to protect against the overall impact of a ransomware event if all other protection layers fail. The multiple layers of protection are further backed by multiple levels of resiliency specifically built to stop ransomware from spreading and mitigate the damage as much as possible. Should this occur, automated host isolation modifies firewall rules to quarantine an infected host. Additionally, the encryption key is captured so you can recover your files.

About Adlumin

Adlumin Inc. provides the enterprise-grade security operations platform and managed detection and response (MDR) services that keep mid-market organizations secure. With one license and one platform, its patented technology gives organizations and solution providers everything they need for effective threat hunting, incident response, vulnerability management, darknet exposure monitoring, compliance support and much more.

The Adlumin platform is feature-rich enough for organizations to operate on their own yet built specifically to amplify the skills and capabilities of managed service providers who use it to deliver cutting-edge security that can scale to meet the needs of any operating environment. With full access to the platform regardless of whether they are running it themselves or relying on Adlumin's MDR services or expert partners, Adlumin gives organizations unparalleled visibility into their security posture through access to alerts, investigation data, threat intelligence, compliance reporting and everything else – all in real time.

Illuminate Threats, Eliminate Risks, and Command Authority with Adlumin. www.adlumin.com