Messageware Z-Day Guard

for Microsoft Servers

Microsoft Windows Servers are constantly under attack. Messageware Z-Day MDR server protection detects changes indicating attacks by zero-day, webshell, and other exploits. Security technology that cannot be turned off by malicious software.

TRUSTED SECURITY
EXCHANGE SERVERS | WINDOWS SERVERS | AZURE SERVERS

- ✓ Zero-Day Detection
- ✓ Catch Exploits
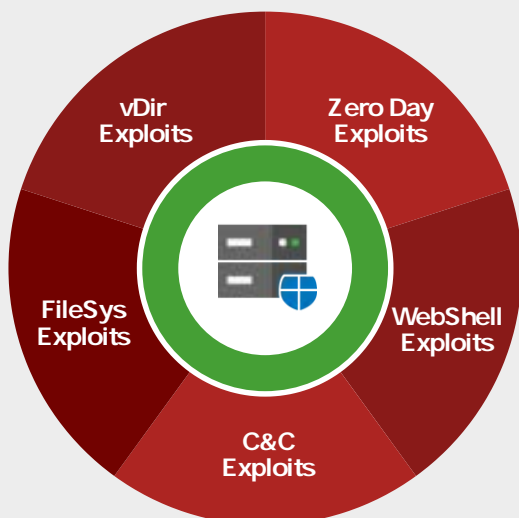- ✓ Managed Detection (MDR)
- ✓ Post-Incident Forensics
- ✓ SIEM/SYSLOG and Email Alerting
- ✓ Always-on, Cannot be Disabled

vDir Exploits
Zero Day Exploits
WebShell Exploits
C&C Exploits
FileSys Exploits

Next-Generation Threat Detection

Exploits prey on unpatched Servers and vulnerabilities not yet known to the public. Next-generation protection starts with understanding the server's purpose and establishing a trusted system state.

Start Free Trial

messageware

FEATURE HIGHLIGHTS

Time to React

Compromised servers are leveraged in under 90 minutes. Z-Day catches threats and sends alerts to respond long before this threat window closes.

File Integrity Monitoring (FIM)

Track unexpected changes to the file system and trigger threat alerts categorized by severity.

vDir Integrity Monitoring

Instantly detect changes to Virtual Directories that can compromise Microsoft Servers.

Task Scheduler Monitoring

Cybercriminals often abuse Windows Task Scheduler to hide and run malware. Z-Day detects abnormal Task Scheduler activity, warning security teams of potential threats.

Ready-to-Use Templates

Quickly deploy Z-Day with pre-built templates for various Windows servers. Easy to customize and tailored for protection.

Maintenance Mode

Z-Day can be put in maintenance mode to quickly update, then re-establish a trusted baseline.

Notifications & Daily Digests

Receive real time threat alerts and notifications, and daily Server health summaries.

Detailed Data Visualizations

Easily identify hot spots and trends by displaying historical threat data in a bubble chart, or drill into detailed incidents over time using tree view.

SYSLOG & SIEM Integration

Send alert events and threat data to existing SIEM and SYSLOG servers using standardized RFC 3164 and RFC 5424 messages.

Certified PPL ELAM Mode

Z-Day is a certified PPL ELAM driver, ensuring that it is monitoring your system from startup to shutdown.

Messageware Z-Day Guard

for Microsoft Servers

TRUSTED SECURITY
EXCHANGE SERVERS | WINDOWS SERVERS | AZURE SERVERS

Server Baseline Change → Risk Analysis → SYSLOG & SIEM Notifications → View Detailed Threat Data → Remediation → Analytics & Reporting

Use Messageware EPG to prevent logon attacks and AD lockouts. Add Z-Day to monitor for other threats and security incidents.

★★★★★

Stop looking for an MDR solution. Messageware Z-Day is easy to install and won't break the bank.

★★★★★

Z-Day saves hundreds of hours spent checking system health. It vastly reduces efforts monitoring servers and provides confidence that servers have not been compromised.

★★★★★

ABOUT MESSAGEWARE

Founded in 1993, Messageware has been a trusted Microsoft Certified Partner and a Global Microsoft Exchange Server ISV for over 20 years. Messageware products are used in all major verticals by over 2,500 enterprises, including the Fortune 100. As a world leader in advanced server security, our solutions protect organizations of all sizes from today's most persistent cyber threats.

Messageware

www.messageware.com/z-day