Netsurion

Managed Open XDR

Unify all your security telemetry to achieve wider attack surface coverage and deeper threat analytics resulting in faster incident response.

Wider Attack Surface Coverage

Protection of your critical devices like servers and firewalls are a great start, however, cybersecurity is only as effective as the coverage of your entire network. Blind spots in your coverage can be as risky as no security at all, leaving endpoints vulnerable to attacks that could then reach critical devices in your network. Netsurion's Managed XDR Solution protects your entire attack surface including endpoints and cloud infrastructure. Our lightweight agents and sensors monitor and protect devices even when not connected to a corporate network.

Deeper Threat Detection

Get wider attack surface coverage, deeper threat detection, and ultimately, faster incident response by integrating more of your data sources with our Open XDR platform. Netsurion offers a continuously growing library of hundreds of Data Source Integrations. Our open platform leveraging your current infrastructure and tools and does not require you to rip-and-replace.

Faster Incident Response

Successful Incident Response (IR) centers on our customers who know their business and cybersecurity posture best. We provide guided response and enlist partners for hands-on Digital Forensics and Incident Response (DFIR). As part of the cybersecurity threat model, Netsurion offers both automated response by our Open XDR platform and guided remediation by our 24×7 SOC.

SOLUTION SUMMARY

KEY BENEFITS

- **24x7 Alert Monitoring**
- **Actionable Threat Intelligence**
- **Threat Hunting**
- **Automated Incident Response**
- **Turnkey Implementation**
- **Log Collection and Correlation**
- **Compliance Reporting**

AWARD-WINNING SOLUTION

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2023

Managed Detection & Response
Extended Detection & Response
Threat Hunting

CERTIFIED SERVICE PROVIDER

ISO 27001

AICPA SOC aicpa.org/soc4so SOC for Service Organizations | Service Organizations

What You Get with Netsurion Managed Open XDR

24x7 SOC

Netsurion's SOC continuously monitors security alerts generated by our XDR platform and conducts threat hunting to detect, alert and respond to any Indicators of Compromise (IoCs) and Indicators of Attack (IoAs).

Security Information & Event Management (SIEM)

A foundational component to Netsurion Open XDR is SIEM. The platform collects, normalizes, and correlates telemetry and security events from a wide array of devices and cloud services to enable powerful threat detection and practical compliance reporting.

Security Orchestration and Automation

Netsurion Open XDR receives and processes high volumes data from your IT assets. Security incidents are automatically triaged through Workflow Automations. Data is orchestrated with your IT systems through Service Integrations.

Managed SIEM & Log Management

Security visibility and intelligence that only SIEM and proper log management can deliver, but without the headaches of self-hosting, data management, configuration, and tuning. Our Open XDR platform has robust security information and event management at its core.

Continuous Threat Detection & Response

Threat hunting is more than digging into a confirmed security breach. Threat Hunting is a proactive investigation for unknown Indicators of Attack (IoAs). Threat Hunting includes the application of data science, threat intelligence, indicators from the MITRE ATT&CK framework and the intuition of experienced threat hunters.

Flexible Cybersecurity-as-a-Service

As your business changes, easily scale your coverage by deploying or decommissioning sensors. As your risk tolerance changes, easily flex your defenses by adding optional capabilities like vulnerability management or endpoint security.

Compliance Reporting

Streamline regulatory compliance management with built-in reports for PCI DSS, HIPAA, GDPR and NIST 800-171. Our platform also provides 400-day log management which is exceeds most regulatory requirements. Also, Netsurion is SOC 2 Type 2, ISO/IEC 27001, ISO 20000, PCI DSS, and Privacy Shield certified.

Turnkey Deployment

Netsurion Managed XDR is designed for rapid activation. Perfect for any IT team to deploy, but this is particularly effective for Managed IT Service Providers (MSPs) that need to rapidly deploy security services to various small and medium-sized businesses.

Power-Packed for Common Environment

Take advantage of our extensive Data Source Integration library of *hundreds of supported telemetry sources. Our engineers continuously add new integrations to keep pace with your IT landscape.

* Data Source Integration availability depends on XDR package

Netsurion Managed Open XDR	Essentials	Enterprise
Core Services		
24×7 Security Monitoring	✓	✓
24x7 Support	✓	✓
Custom Selection of Priority-1 Alerts	**Fixed***	✓
Threat Hunting		✓
Threat Hunting Report		✓
Console Reporting Engine	✓	✓
Compliance Reports	**Standard***	**Full**
Monthly Services Review Meeting		✓
Technology		
Anomalous Login Detection	✓	✓
Centralized Log Management	✓	✓
Host-Based Intrusion Detection System (HIDS)	✓	✓
MITRE ATT&CK Integration	✓	✓
Security Orchestration & Automation	✓	✓
Security Information & Event Management (SIEM)	✓	✓
Threat Intelligence Platform (TIP)	✓	✓
User & Entity Behavior Analysis (UEBA)	✓	✓
Windows Application Control	✓	✓
Data Source Integrations	**Standard***	**Full**
Implementation & Customer Success		
Data Source & Notifications Tuning		✓
Live and On-Demand End-User Training	✓	✓
Log Retention – 400 Days	✓	✓
Platform Technical Support	✓	✓
Netsurion-Hosting & Health Check Available	✓	✓
Assigned Customer Success Team		✓
Implementation Project Management		✓
Available Options		
Managed Endpoint Protection Security	✓	✓
Vulnerability Management	✓	✓
Incident and Audit Support		✓
Log Extraction by Customer		✓
Log Retention - Extended		✓

* https://www.netsurion.com/service-description/mxdr/essentials