Net at Work®

Data Sheet

Managed XDR Premium

Experience true peace of mind with a modern Managed Detection and Response solution protecting you on the endpoint and beyond.

Powered by:

Barracuda
Your journey, secured.

With the growing challenge of persistent cross-domain threats, companies need comprehensively managed solutions that provide reliable, more effective detection and response coverage across their environment.

Net at Work's Managed Detection and Response (MDR) is an expert-led 24x7x365 managed security service providing comprehensive coverage across endpoints, identities, cloud workloads, network devices, and more. Our most layered and comprehensive security offering, *Managed XDR Premium*, includes AI-powered EDR and XDR platforms coupled with a managed Security Operations Center (SOC).

End-to-End Coverage

A security-first Managed Services Provider (MSP), Net at Work's AI-powered MDR ensures that clients stop threats across their IT stack and with greater speed, scale, and accuracy than humanly possible.

Managed EDR

Net at Work's comprehensive cybersecurity solution delivers round-the-clock monitoring, threat detection, and incident response capabilities, ensuring the utmost protection for your digital assets and data.

- Focused on endpoint threats (workstations and servers) including Windows, Linux, Mac, and cloud workloads
- Automatically block or quarantine malware leveraging the MITRE ATT&CK framework
- Visibility and self-service functionality available for IT staff
- 24x7 SOC monitoring and remediation guidance
- Security expertise to leverage sophisticated features of EDR
- Ongoing maintenance and support of the endpoint protection platform.

Cloud Protection

- Monitors malicious activity in the cloud to find identity, asset, and privilege risks such as unauthorized access to cloud mailboxes, admin changes, impossible logins, and brute force attacks
- Protect Microsoft 365, Google Workspace, and other cloud environments through comprehensive integrations.
- Security Orchestration, Automation, and Response (SOAR) capabilities such as automatically blocking logins to users' mailboxes if a threat is detected
- Threat correlation between Endpoints and Cloud environments

Server Security

- Protects Windows and Linux Server Operating Systems
- Monitors for malicious activity on servers that may go undetected by EDR, including changes to Active Directory, Privilege Escalation, Password Spray Attempts, abnormal logins, and more

Network Security

- Protects network infrastructure, including firewalls, routers, and switches
- Monitors for malicious activity such as unauthorized device changes, attempts to bypass authentication, suspicious connections, data exfiltration, denial of service attacks, and more
- Intrusion Detection System (IDS) - Inspect network traffic for malicious activity undetected by a firewall

Email Security

- Monitor for malicious activity at the mailbox level, including credential stealing, mailbox rule creation, invoking a sense of urgency, brand impersonation, and more
- Includes Email Protection solutions, including Email Gateway Defense, Impersonation Protection, Incident Response, Cloud Backup, and Security Awareness End-User Training

DNS / Web Filtering

- Protects DNS, which is inherently insecure, even though it's the bedrock of the internet and how networks communicate
- Protects against tactics such as DNS tunneling and beaconing
- Preventative protection – blocks threats in the cloud before they reach your network or endpoint
- Web Content Filtering
  - Robust default policies
  - Customizable policies

24/7/365 Security Operations Center (SOC)-backed SIEM

With our SOC-backed security, information, and event management (SIEM) solution, individual events are auto-correlated into an attack sequence, to streamline investigation and response. Our analysts can automatically resolve threats by executing actions in a single step, including network quarantine, auto-deploy agents on unprotected workstations, or automate policy enforcement across cloud environments. Per identified threat, Net at Work's SOC analysts immediately respond to ensure that the situation is isolated and stopped with remedies like Account Disable, IP Block, Password Reset, Host Quarantine, Instance Re-deploy, and Message Block.

End-user and Administrator Support

+ Unlimited multi-channel support (email, phone, and chat)
+ Incident report and review

This service is priced per user and covers up to three workstations for each.

With Net at Work as your IT partner, you can leverage our expertise and cutting-edge solutions to streamline your IT operations, enhance productivity, and fortify your cybersecurity posture. Whether supporting a single IT project, managing IT, or delivering fully managed infrastructure, Net at Work has you covered.

Contact us for a no-obligation IT consultation.

About Net at Work

Founded in 1996, Net at Work is one of North America's largest technology advisors and solution providers for small and mid-size businesses. Our award-winning consultancy offers a rich portfolio of next-generation technology, industry expertise, implementation and managed services to help organizations derive value from the transformative benefits of technology. Through the integration of ERP, HCM and/or CRM solutions, Net at Work offers unique, industry-specific solutions and operation platforms that enable companies to compete more effectively in today's digital economy. For more information, visit www.netatwork.com.