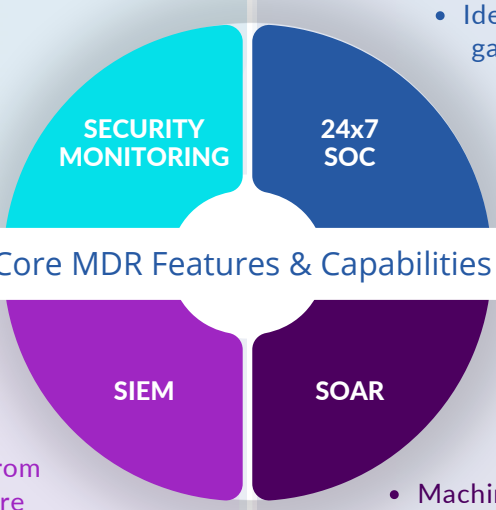
Smart Guard

Managed Detection & Response (MDR)

Take charge of your cybersecurity defense strategy with advanced 24x7 threat monitoring, analysis and incident response for real-time security protection against today's most malicious threats.

Omega's managed detection & response (MDR) service, Smart Guard, delivers the 24x7 security monitoring, integrated threat hunting and analysis, and rapid incident response services companies need to combat today's rising security threats.

With a view of your entire cybersecurity environment – including users, workstations, and cloud applications – Smart Guard acts as a single source of truth for threat intelligence and insight, helping you identify and mitigate risks, reduce your cybersecurity overhead and improve your overall security posture.



Core MDR Features & Capabilities

- Monitors users and endpoints across your network as well as SaaS applications
- Reports on at-risk users, groups, systems and behavior
- Profiles user behavior to identify behavioral patterns and report anomalies
- Perimeter defense performs external attack surface review
- Dark web monitoring scans dark net for data breaches

- 24x7 security monitoring & response from SOC analysts ensures real-time prevention & detection
- Trained analysts prioritize and remediate anomalous behavior
- Identify root cause of incidents and gather evidence for analysis
- Threat intelligence feeds link detected security events to known vulnerabilities

- Ingests logs and events from network servers, devices, workstations, etc.
- Cloud-to-cloud API collects logs from Azure, AWS, Google, and other core applications
- Central data storage (US) correlation & analysis
- 1-year log retention to meet routine security and compliance standards
- Supports SYSLOG data ingestion

- Uses templated playbooks and automated workflows to accelerate incident response & reduce time to remediation
- Machine-learning capabilities complement human analysis
- Ensures consistency and allows SOC analysts to better allocate time and resources to priority alerts

omega systems
technology managed

MDR Security Reporting & Compliance Insights

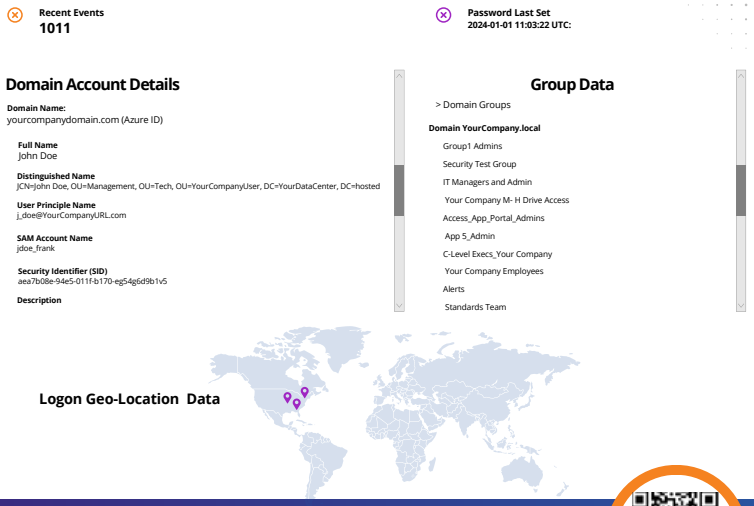
With Smart Guard, you'll have access to a wealth of security reporting (as well as custom templates) to leverage for strategic IT planning, executive board review and regulatory compliance support. Sample reports include:

- Executive Summary/Board and IT Steering Committee
- Detection Analysis
- Network Health Overview
- Dark Net Exposure
- Privileged Account Activity
- Perimeter Defense Port Scan

Integrate MDR with Cloud & SaaS Applicatons *including:*

Microsoft 365, mimecast, Acronis, SOPHOS, okta, Microsoft Entra ID, solarwinds, ORACLE, Cisco Umbrella, Cisco Meraki, JumpCloud, DUO, HUNTRESS, proofpoint, CONNECTWISE, salesforce, TREND MICRO, SentinelOne, paloalto NETWORKS, KnowBe4 Human error. Conquered., Google, aws, Bitdefender

User-Friendly Dashboards



Key Benefits of Managed Detection & Response (MDR)

Access to dedicated security team

without the expertise or overhead needed to hire, train and retain an internal security staff

Real-time SOC security monitoring

enables 24x7 risk mitigation and keeps your sensitive data and assets protected from malicious intrusion or suspicious behavior

Proactive threat hunting & remediation

stops attacks before they ever reach your endpoints

Automation & machine learning

accelerates response times to ensure rapid incident response

Threat intelligence

capabilities ingest data from global industry feeds and scan across customer environments to help identify and correlate emerging threats

Platform transparency

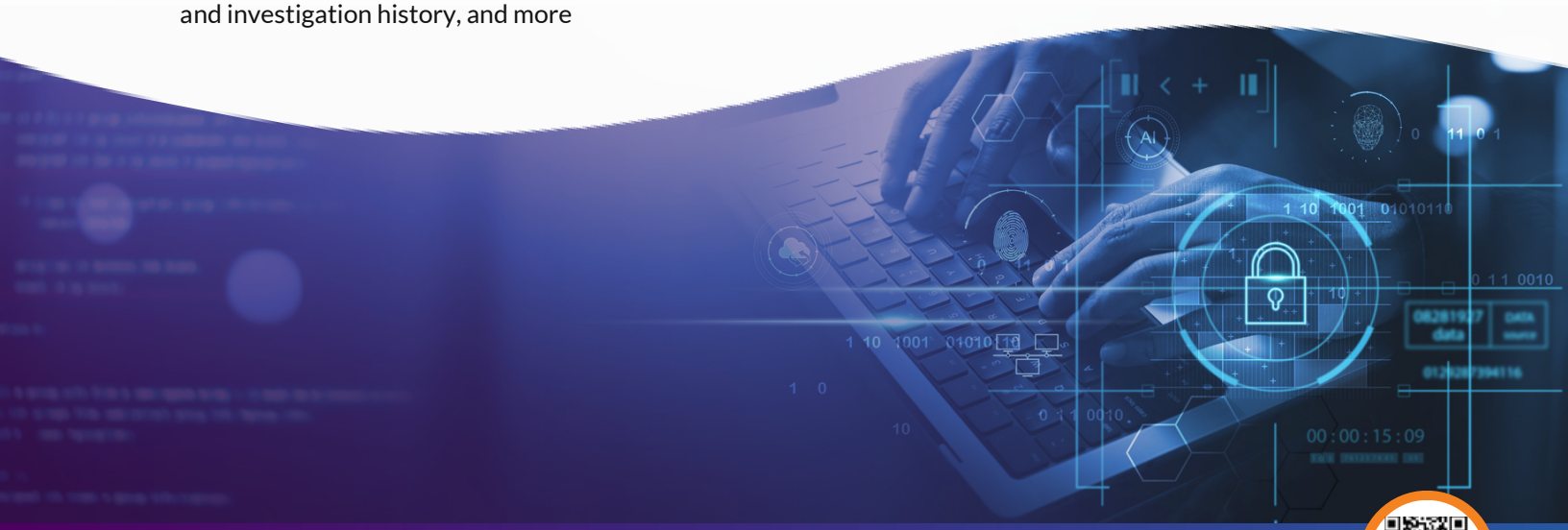
gives customers access to the same platform as Omega's SOC analysts with clear visibility into at-risk systems, privileged accounts, alert and investigation history, and more

Compliance reporting

aligns with security standards from various regulatory bodies (HIPAA, CJIS, PCI DSS, etc.) and streamlines reporting for boards, auditors, insurance providers and other stakeholders

Rapid deployment

capabilities outpace traditional managed SIEM tools and technologies



omega systems
technology managed

Smart Guard (MDR) Package Comparison

Regardless of your unique budget, compliance requirements, and internal team bandwidth, Omega Systems has an MDR security solution package to fit your needs. We offer three customizable packages to give you the appropriate security detection & response capabilities to meet your objectives.

	Basic	Alto	EXO
Security Operations Center (SOC) services with 24x7 monitoring and investigation		+	+
SIEM logging with 1-year retention	+	+	+
Log ingestion and correlation with SaaS applications (e.g. Microsoft 365, EDR+, MFA+)	+	+	+
Security orchestration, automation and response (SOAR) runbooks with incident automation	+	+	+
Local workstations and servers included (1 agent per user + 10%)	+	+	+
User and entity behavior analysis (UEBA)	+	+	+
Detection and protection for: • Dark web monitoring • External attack surface monitoring • Identity and application monitoring • Ransomware & malware infection • Lateral movement • Command & control • Data exfiltration • Privilege escalation • Impossible travel • Account takeover • Compliance Insights • Network Health Index	+	+	+
Threat Intel Feeds with SOAR automation to firewall	+	+	+
Local network honeypots			+
Local log collector for SYSLOG ingestion: • Firewalls • VPN • Network switches • Wireless access points & controllers • Additional log sources that support SYSLOG format			+

Get In Touch:
omegasystemscorp.com | connect@omegasystemscorp.com | (610) 678-7002