ARCTIQ

Strengthen Your Security to Conquer Advanced Cyber Threats

Managed Extended Detection & Response (MXDR) Service

☒ Enterprise Security

Empower Your Organization's Defense

Modern organizations face an ever-growing array of evolving security threats with significant consequences for finances, trust, and reputation. The key challenge is the ability to effectively monitor, identify, respond to, and remediate multiple simultaneous security threats.

Your 24/7 Shield Against Evolving Security Threats

Arctiq's Managed Extended Detection and Response (MXDR) service delivers expert, 24/7, year-round vigilance, providing comprehensive SIEM operations and threat detection coverage. This fully managed service automates security detection and response to safeguard IT infrastructure, systems, data, and more.

- Highly certified and accredited team: CISSP, CISM, GSEC, OSCP, and many more
- 99% managed security services client retention rate
- Ranked 60th globally by msspalert.com
- Elite 150 on CRN MSP500

Our comprehensive cybersecurity strategy combines advanced technology, real-time threat prevention, and historical data analysis. We prioritize awareness, promptly reporting incidents and trends, and collaborate effectively. In incidents, we swiftly deploy resources and countermeasures. Our analysis includes vulnerability scanning, awareness initiatives, and expertise in security architecture and offensive services.

Security Operations Centers

Arctiq operates three Security Operations Centers strategically located across North America, ensuring comprehensive coverage and timely threat response. We offer a robust suite of services designed to fortify your cybersecurity defenses, including:

Advanced Threat Intelligence

Our experts constantly monitor the threat landscape to provide you with up-to-date intelligence on emerging threats and vulnerabilities.

Threat Hunting

We proactively seek out potential threats within your environment, going beyond traditional monitoring to actively identify and neutralize risks.

Analytics

Our analytics capabilities provide in-depth insights into security incidents, offering granular context for each threat detected.
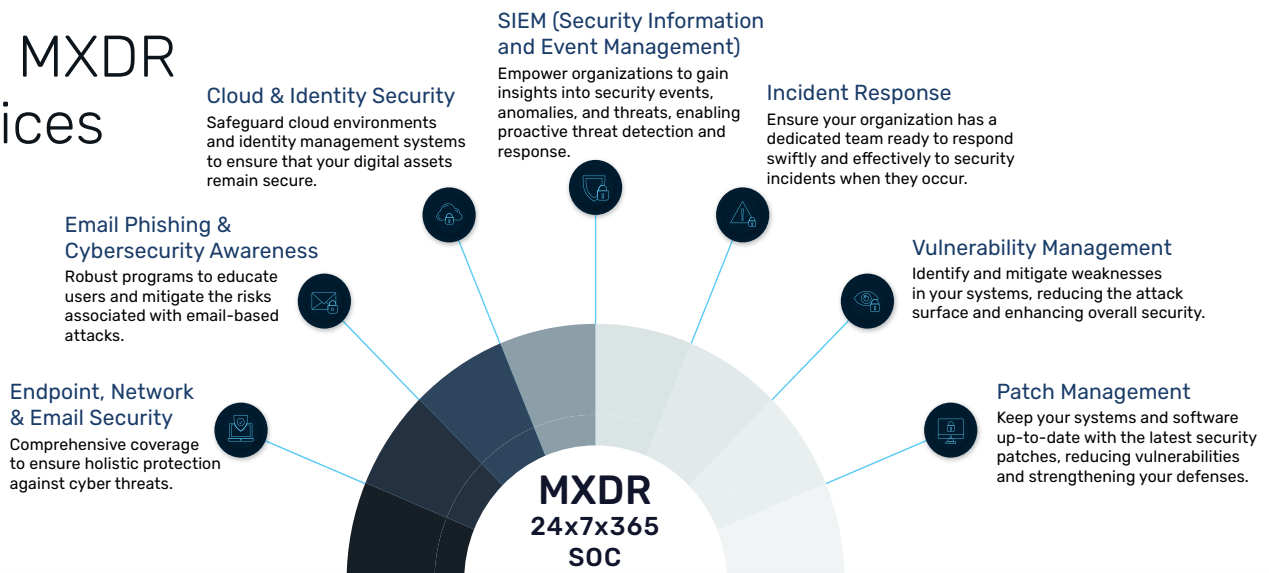
Monitoring and Alerting

With round-the-clock 'eyes on glass' coverage, we swiftly identify critical threats in near real-time, converting alerts into actionable intelligence.

Key Benefits

- Comprehensive solutions aligned with core security controls to meet stringent compliance and cyber insurance requirements

- Ability to manage and support a broad range of SIEMs and ingest data from an extensive technology ecosystem

- Fast response times for security events with the ability to triage incidents

- Use of machine learning to increase efficacy of detection

- Reviews with security experts to analyze metrics, incidents, recommended security enhancements to existing toolset, and security best practices

- Access to technology experts in adjacent areas such as infrastructure, data center, storage, Microsoft platforms and more

- Customers maintain full custodianship and control of their data

- Enhanced visibility into the security of users and systems including analysis of user and entity behavior analytics

Core MXDR Services

Cloud & Identity Security
Safeguard cloud environments and identity management systems to ensure that your digital assets remain secure.

SIEM (Security Information and Event Management)
Empower organizations to gain insights into security events, anomalies, and threats, enabling proactive threat detection and response.

Incident Response
Ensure your organization has a dedicated team ready to respond swiftly and effectively to security incidents when they occur.

Email Phishing & Cybersecurity Awareness
Robust programs to educate users and mitigate the risks associated with email-based attacks.

Vulnerability Management
Identify and mitigate weaknesses in your systems, reducing the attack surface and enhancing overall security.

Endpoint, Network & Email Security
Comprehensive coverage to ensure holistic protection against cyber threats.

Patch Management
Keep your systems and software up-to-date with the latest security patches, reducing vulnerabilities and strengthening your defenses.

MXDR
24x7x365
SOC

Incident Response

Our incident response process follows a multi-phase approach focused on detecting, remedying, and preventing cybersecurity events swiftly. Key phases include:

1. **Monitor:** Our SOC analysts provide 24/7 monitoring, ensuring real-time threat vigilance.

2. **Triage:** We swiftly investigate alerts, determining if escalation is needed for further examination.

3. **Remediate:** Detailed incident reports and recommendations are provided for customer remediation, with our assistance available as required.

4. **Learn:** Post-incident reviews inform root cause analysis, knowledge base updates, and continuous improvement efforts.

Led by seasoned experts, our proactive consulting services prioritize continuous improvement and transparent collaboration with clients. Alongside core offerings, we provide specialized solutions:

- **Ransomware Prevention and Detection Strategies:** Equip organizations with effective measures against ransomware threats.

- **Infrastructure Recoverability Assessment:** Evaluate infrastructure recoverability to prepare for disruptions.

- **Incident Response Retainers:** Immediate access to expert response teams during security incidents.

- **Email Phishing Simulation & Cybersecurity Awareness Education:** Fortify defenses against phishing attacks through simulations and education.

- **Dark Web Monitoring:** Vigilantly monitor the dark web for potential threats.

- **Patch Management:** Timely and error-free deployment of patches to reduce risk and ensure compliance.

- **Vulnerability Management Services:** Identify and mitigate system weaknesses to reduce overall risk exposure.

- **Site Takedown and Brand Protection:** Take down malicious websites and protect brands from online threats.

- **Attack Surface Management:** Secure attack surfaces to minimize vulnerabilities and cyber threats.

- **Continuous Security Validation:** Ensure security measures remain effective over time against evolving threats.

- **Advanced Identity Protection:** Provide solutions to safeguard against identity-related cyber threats.

- **Security Assessments:** Evaluate current security posture and recommend improvements.

- **Penetration Testing:** Identify system vulnerabilities for proactive remediation.

Proactive
Security
Consulting

Partner Alignment

Arctiq partners with leading vendors to deliver stellar solutions in various domains, including:

Cisco	Google Mandiant	SyxSense
CrowdStrike	Microsoft	Tanium
CyberArk	Okta	Tenable
Cynomi	Qualys	Trellix
Delinea	SentinelOne	And More...
DTEX	Silverfort	
FraudWatch	Splunk	

Arctiq's Customer Experience

Our commitment to delivering an exceptional customer experience is at the heart of our services. We believe in providing you with a white-glove experience, accompanied by comprehensive metrics and reporting.

Rapid On-boarding

Our onboarding process is swift and hassle-free, with a dedicated success team and project management support to ensure a smooth transition.

Extensive Metrics & Reporting

Through regular cadence meetings between your team and our security experts, we provide robust metrics and reporting tools that offer deep insights into your security landscape. We provide clear, concise insights into your environment's security activity, as well as performance reporting on your existing cybersecurity toolset to ensure ongoing effectiveness and alignment with your goals.

Proactive Security Recommendations

We analyze data to offer proactive security recommendations, helping you stay ahead of potential threats.
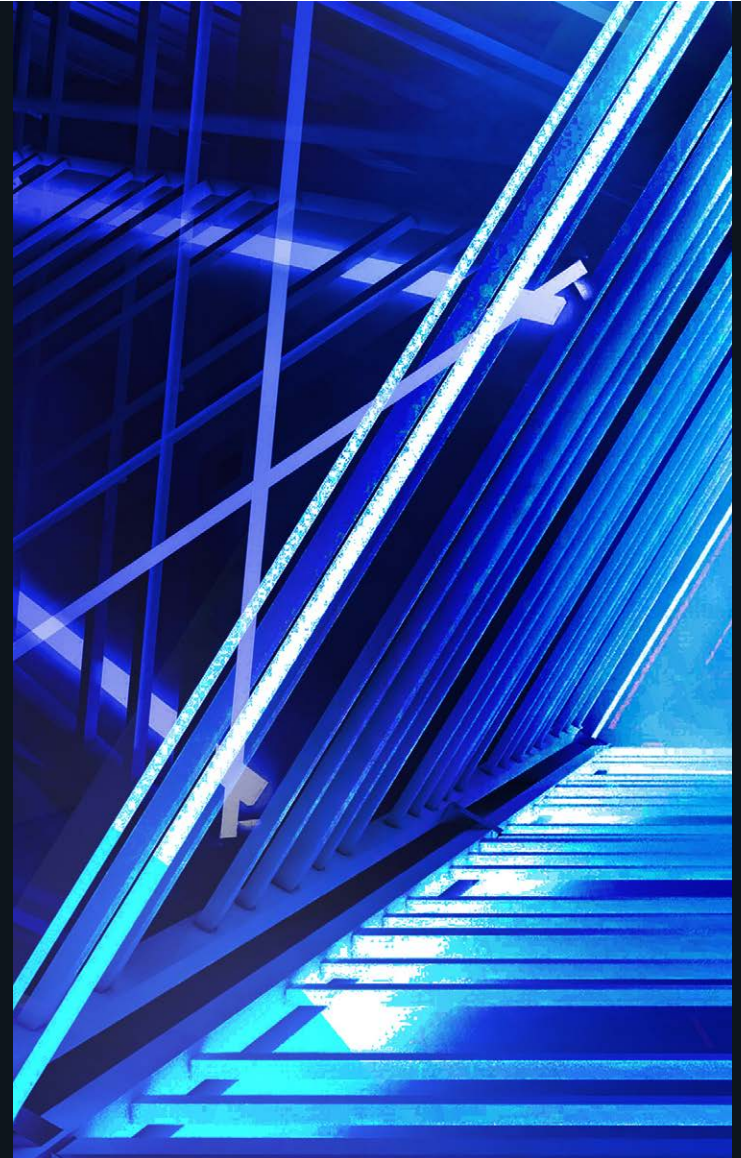
Contact Arctiq Today

Transform your security with Arctiq's MXDR and experience unrivaled protection by a highly certified team.

▶ Partner with Arctiq to elevate your defense with 24/7 vigilance, automated detection, and proven expertise.

Connect With Us