Architect Security

Ransomware Strategies

End-to-End Security, Automation, and 24/7 Monitoring

Delivering Comprehensive Ransomware Prevention and Recovery Solutions

Our expertise extends to optimizing cyber insurance coverage, enabling you to fortify your security posture to minimize premiums. With extensive network and storage infrastructure knowledge, we bolster your defense against ransomware and ensure robust recovery capabilities. With three Security Operations Centers strategically located throughout North America, we offer 'Eyes on Glass' Threat Hunting and Threat Intelligence Correlation for unparalleled protection. By combining our specialized services with the proactive measures, your organization can significantly reduce the risk of falling victim to ransomware attacks.

Password Reset

- Enforce a policy that mandates IT staff with admin privileges to reset their passwords only through direct approval from IT management.
- Identity verification such as employee number, birthday, calling a person back on a known phone number, in-person visits, etc.
- Establish a cybersecurity training program for employees—especially those with the ability to reset passwords such as help desk staff—to recognize and report phishing and social engineering attempts.

Microsoft Endpoint / Server / Cloud Security

- Enforce multi-factor authentication (MFA) for all user accounts to prevent unauthorized access.
- Implement Just-In-Time (JIT) administration for administrative tasks.
- Implement least privilege access control policies to limit admin account privileges and reduce the attack surface.

Secure Data Center Virtualization / Storage / Backup

- Regularly back up virtualized data to immutable, secure storage to ensure data recovery options in case of an attack.
- Maintain and test offline, immutable backups of critical data, ensuring they are not accessible to ransomware.
- Maintain a physical and virtual instance for essential IT services such as domain controllers, DNS, and DHCP to ensure redundancy and minimize disruption in the event of a virtualization system compromise.

24/7 Monitoring / Security Operations Center (SOC)

- Implement intrusion detection systems (IDS) and intrusion prevention systems (IPS) to block potential threats proactively.
- Continuously monitor and audit your network, systems, and cloud environment for any unusual behavior such as IT global admin password resets.

Organizational Policy

- Maintain backup local admin accounts (non-AD reliant) for your key IT systems such as hypervisors, network management systems, systems visibility, and IT provisioning tools. These backup local admin accounts should be as complex as possible and stored in either an out-of-band password manager or off-line vault that are only available in a 'break glass' scenario.
- Develop an incident response plan that clearly defines roles and responsibilities in the event of a ransomware incident. This incident response plan should identify escalation paths for all technology recovery support in your environment as well as internal/external staffing requirements for recovery work in the event of a cyber incident.

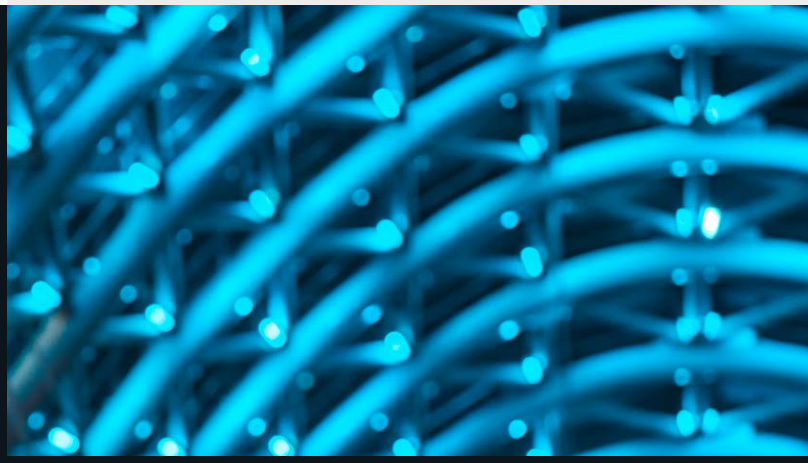
Network Security

- Segment your virtualized network to limit lateral movement for potential attackers.
- Regularly update and patch all network devices and systems to mitigate known vulnerabilities.

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.



Business Drivers and Challenges

We're here to align your IT strategy with your business objectives and tackle the challenges that matter most to you.

- Ransomware Attacks
- Data Breaches
- Insider Threats
- Phishing and Social Engineering
- Patch Management
- Cloud Security
- Security Skills Shortage
- Compliance and Regulatory Requirements
- Infrastructure Recoverability

Contact Arctiq Today

At Arctiq, we are dedicated to ensuring the highest level of cybersecurity for your organization. Our tailored solutions, combined with our commitment to innovation, empower you to navigate the digital landscape securely, confidently, and with resilience.

Review your current prevention and recovery strategies with Arctiq's cyber specialists today!

Book a consultation