Ransomware Assessment

EVOTEK's Ransomware Assessment takes a holistic, whole-of-enterprise review of an organization's ability to address the risks associated with ransomware.

In collaboration with various levels of your team and colleagues, we evaluate the ability of your organization to prevent, detect, and respond to ransomware compromises. Specifically, our team examines data protection and backup environments, network topology, endpoint protection, and broader incident response preparedness as part of the comprehensive evaluation.

Business Challenge

It is easy to be blindsided by ransomware and other forms of cyber risk. Too frequently, organizations are caught flat-footed and largely unprepared to address the myriad impacts that a ransomware incident entails. The impacts are often not limited to a singular aspect of business operations but extend to organizational distraction, mandated disclosures, and risks to the organization's reputation.

Organizations that take the time to evaluate their preparedness are far more likely to reduce the impact of a cyber incident caused by ransomware. Moreover, for many organizations, there's an expectation that risk assessments and reasonable security practices are in place.

A Proven Solution

Our team brings a multi-disciplinary approach to ransomware assessments. With our expertise in enterprise architecture, security best practices, and data protection we evaluate ransomware risks from multiple perspectives. Your organization gains a comprehensive review versus a more narrowly defined assessment, which leads to a higher fidelity response to identified risks.

With security architects, engineers, analysts, business information security officers, and chief information security officers, our team incorporates a broad mix of functional expertise coupled with executive oversight.
This analysis identifies guidance that prioritizes changes to security functions and solidifies the resilience of enterprise architecture.

Credit Union Solves Ransomware Problem

A Southern California-based credit union was seeking a solution to address the end-to-end nature of ransomware attacks. Our team of experts developed an internal framework, aligned with industry best practices, to address ransomware risks at each stage of its deployment and propagation. We identified areas where the business was strong and where improvement was needed. While robust security tools were in place, the security team lacked additional SME coverage within the organization. We also found that a significant core business application lacked a solid monitoring solution outside of the manufacturer's operational deployment. The client worked through a prioritized remediation exercise to strengthen the overall security program and now is prepared to respond proactively and effectively to the latest ransomware threats.