Ransomware Preparedness Assessment

DATASHEET

The Threat of Ransomware

Ransomware has been one of the biggest threats to information security for over a decade, and it's only getting worse. Ransomware, or malware designed to encrypt your data and files, is used by bad actors to deny access and hold your company systems hostage. These attacks continue to be successful, meaning companies are either agreeing to pay the ransom, or accepting that their data has been lost forever.

TraceSecurity developed our proprietary Ransomware Preparedness Assessment to determine your organization's readiness to handle a ransomware attack. The goal is to confirm security controls are in place to protect your data, as well as confirm data backups and recovery procedures should information be stolen or locked.

Our Assessment

TraceSecurity information security experts compiled best practice controls directly tied to ransomware preparedness to be included in this assessment. The controls are to be assessed through a ransomware control audit, followed by a Qualys-powered host configuration review.

The audit portion of the assessment includes collection of evidence of each control, with a focus on Prevention, Detection, and Response & Recovery functions in your organization. We also perform a system configurations best practices scan to provide areas that an attacker could use to gain unauthorized access to company systems and private data. Scan results also include security measures that should be taken to remediate the misconfigurations so that they cannot be exploited in a real-world attack.

With this approach, we can verify your control implementation related to ransomware preparedness and identify improvements that can be made to your security configurations.

Frequently Asked Questions

How is this service priced?
Our Ransomware Preparedness Assessment is priced based on the number of active devices on your network(s).

What's the difference between scans run during a Ransomware Preparedness Assessment and scans run during a Vulnerability Assessment?
The Ransomware Preparedness Assessment includes configuration scans of your Windows operating system devices. TraceSecurity has customized this control set to cover ransomware-related best practices and report back the most urgent device misconfigurations. The Vulnerability Assessment includes credentialed or non-credentialed vulnerability scans based on the broader library of vulnerability signatures which include a wide array of commonly reported vulnerabilities across operating systems and device types.

How often should we perform this type of assessment?
With ransomware continuing to be a threat to business worldwide, we recommend that a Ransomware Preparedness Assessment is performed with the frequency best suited for your organization.
At a minimum, a Ransomware Preparedness Assessment should be performed upon any major changes to your information systems and processes, especially those related to ransomware protection.

What if we don't have documentation you are requesting or don't know where to find it?
We send out a sheet that lists what documentation we need. If you don't know where to find something, you can ask us. If a piece of information is missing, the control will be marked "unimplemented" or "unverified" depending on the situation.

Assessment Methodology:

- Ransomware Control Audit
  - ✓ Prevention
  - ✓ Detection
  - ✓ Response & Recovery
- Qualys-Powered Host Configuration Review
  - ✓ Qualys Configuration Review
  - ✓ Configuration Best Practice Recommendations