# Ransomware Risk Assessment

## Your Ransomware Risk Assessment


You failed 7 out of 11 tests on your ransomware risk assessment. Your organization is at Critical risk of a ransomware attack. We encourage you to review the detailed results along with the recommendations to address this risk. For any questions on how to address this with a true Zero Trust Exchange, please contact us.

| Initial Compromise | Lateral Movement | Data Loss/Exfiltration |
|---|---|---|
| 4 Tests \| 3 Failed | 2 Tests \| 0 Failed | 5 Tests \| 4 Failed |

### Initial Compromise

| Test | Result | Recommendation |
|---|---|---|
| Simulated Malware Download | Passed | We strongly recommend that you use advanced malware prevention tools to detect and prevent malicious files from being downloaded. |
| Simulated Malware Download (encrypted) | Failed | We strongly recommend that you inspect all TLS traffic to prevent encrypted threats that have become very common. Zscaler analyzed over 6.6 billion encrypted threats in 2020 alone. |
| Command and Control | Failed | You should block all known command and control traffic as it is a common vector used by most ransomware to receive additional malicious instructions. |
| Credential Theft/Phishing | Failed | We strongly recommend that you enable all anti-phishing capabilities in your existing security solution to stop credential theft to stop the attacker from stealing sensitive information. |

### Lateral Movement

| Test | Result | Recommendation |
|---|---|---|
| SMB to Internet | Passed | As part of cyber hygiene, you should block unfettered outbound access to the internet for protocols like SMB that are used by most ransomware families.<br>This web based test is non-invasive and does not directly evaluate lateral movement within your network. The best practice is to use a zero trust proxy-based architecture to connect users directly to the application they need without over-exposing your network with legacy VPN technologies. |
| RDP to Internet | Passed | As part of cyber hygiene, you should block uncontrolled outbound access to the Internet for protocols like RDP that are used by ransomware families to exfiltrate data and to compromise internet-facing systems. We recommend blocking direct or unauthenticated RDP access to or from any internet-facing systems.<br>This web based test is non-invasive and does not directly evaluate lateral movement within your network.The best practice is to use a zero trust proxy-based architecture to connect users directly to the application they need without over-exposing your network with legacy VPN technologies. |

### Data Loss/Exfiltration

| Test | Result | Recommendation |
|---|---|---|
| Credit Card/SSN Exfiltration | Failed | We strongly recommend that your security solution should block such data exfiltration attempts as financial and personally identifiable information (PII) are the most stolen data types in ransomware attacks. |
| Source Code Exfiltration | Failed | A leak of intellectual property can have profound consequences for your enterprise — from rewriting source code to re-issuing binaries. We strongly recommend that you use a data filtering solution to detect and block such attempts. |
| Encrypted File Upload | Failed | We recommend that you block uploads of password protected/encrypted files to any unsanctioned suspicious cloud storage services. |
| Access New Domains | Passed | We strongly recommend that you block, conditionally allow or isolate newly-observed and newly-registered domains in your current security solution as a large number of these domains are malicious. |
| Suspicious Cloud Services | Failed | We strongly recommend that you detect shadow IT application use and limit data movement to any high-risk cloud storage application. |