structured
bridging people, business & technology™

Ransomware Prevention Services

Shrink attack surfaces, identify and analyze possible threats, modernize tools, assess policies and procedures, and test, test, test.

Ransomware is one of the most persistent and relevant cybersecurity concerns of 2021. While ransomware is not new, tactics are shifting. Formerly, threat actors would lock up data, making it inaccessible to victims unless a ransom was paid. Some chose to pay. Many didn't, relying either on good backups or the belief that retrieving the hostage data wasn't worth the risk of dealing with cybercriminals.

Today's more targeted attacks exfiltrate data and leverage extortion techniques, increasing the pressure to pay ransoms. Victims often are left with the odious choice between paying – further increasing the adversary's resources – or having their sensitive and precious data disclosed to the world.

At the same time, the ransomware-as-a-service market continues lowering the barrier to entry for less sophisticated actors while providing another revenue stream for ransomware authors. In this environment, protecting against ransomware means updating your protection strategies to meet the evolving threat. Start with Structured, and with these four key elements of security:

Email Security: More than 90 percent of companies report ransomware delivered via email is their single largest attack vector. Leveraging the cloud's scale and advanced email security provides protection from spam, malware, viruses, phishing and other emerging threats. (But don't forget to conduct user education and training!)

Next-Generation Firewall: Providing enhanced visibility and advanced awareness of applications and users, NGFWs stop ransomware infections over the network, prevent command and control communication, and prevent data exfiltration.

Next-Generation Endpoint Protection: Leveraging artificial intelligence and machine learning, next-gen endpoint protection stops ransomware infections on the endpoint, prevents file encryption, and provides a forensic level of information about endpoint activity.

Backup and Recovery: Modern storage and backup solutions that provide constant monitoring and immutable backups allow for prevention of data encryption or allow for quick restoration of data encrypted by ransomware.

structured.com

p 800.881.0962

a 12901 SE 97th Ave., Ste. 400, Clackamas, OR

e info@structured.com

structured
bridging people, business & technology™

Test Your Best

Preparation and planning. Testing, measuring, re-testing, re-tooling. Avoiding security breaches is the result of careful work and good oversight. For organizations that want to put their meticulous planning through the paces, Structured offers **Incident Resilience Assessments.**

IRAs gauge your readiness to withstand cyber attack, providing executive and board-level risk findings that can be used to make critical decisions about cybersecurity spending, workforce levels, and other areas of impact.

Structured's IRAs are modeled after Cyber Resilience Review (CRR) guidance from the Department of Homeland Security, but are truly mature services. We systematically review overall system readiness, including policies, procedures and notification checklists. We also review critical systems such as backup and restore platforms, data immutability and storage systems, and other security mechanisms such as intrusion detection and protection.

Incident Resilience Assessment

Structured uses the categories below as a framework.

- Inventory
- Security controls
- Vulnerability management
- Configuration management
- Incident management processes
- Risk management
- Training
- Monitoring

Track the Hack

You know the names: REvil, Ryuk, Stop, Cryptolocker, Dharma, LockerGoga, SamSam, Snatch, Phobos and WannaCry. And there's more. The list of well-known ransomware variants is getting so long that it truly does make one want to stop and cry. But there is hope. And help.

Ransomware Penetration Test

Structured includes the following areas of testing.

- Phishing
- Powershell execution
- PsExec
- SMB weaknesses
- Remote Desktop Protocol
- Active Directory login scripts
- Cloud applications
- Backup systems

You can harden your systems against these common hacks with a **Ransomware Penetration Test** from Structured.

This helpful test is a shorter version of a full penetration test, specifically directed at your organizational exposure to a wide variety of common ransomware attacks -- including those named above. Additionally, Emotet and TrickBot exploits are tested as primary infection vectors.

The Ransomware Penetration Test includes direct technical feedback and recommended remediation to all exploitable vulnerabilities Structured discovers.

THE CHANNEL CO. CRN SOLUTION PROVIDER 500 2011-2021

THE CHANNEL CO. CRN MSP 500 2016-2021

THE CHANNEL CO. CRN TECH ELITE 250 2011-2021

About Structured

Structured is an award-winning solution provider delivering secure, cloud-connected digital infrastructure.

For nearly 30 years, we've helped clients through all phases of digital transformation by securely bridging people, business and technology. We provide design guidance, engineering assistance, and product recommendations that adhere to best practices, boost ROI, and -- most importantly -- maximize information security.

structured.com

p 800.881.0962

a 12901 SE 97th Ave., Ste. 400, Clackamas, OR

e info@structured.com