

# 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 2020. 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.

[www.structured.com](http://www.structured.com)

**p**

800.881.0962

**a**

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

**e**

info@structured.com

