Infrascale™

TOP 6 RANSOMWARE DEFENSE STRATEGIES

Ransomware is the costliest cyber threat your organization faces today, and the global losses due to ransomware run into the hundreds of millions of dollars. Thousands of new malware variants are being reported each year and cyber criminals are becoming more sophisticated each day. Here are 6 strategies that will lower your risk profile and help you defend your company's data and business.

01 Train your Users and Test their Knowledge

Since ransomware infections often come through links and attachments inside emails, or from a website or web application, train your users how to recognize phishing attacks and suspicious links and attachments. Training is only part of the story. Admins must also make sure to regularly test their users with simulated phishing attacks to ensure that your users have been properly conditioned to resist these attacks.

02 Monitor your Network

Diligently monitor your network by analyzing your logs, clearing out alerts, and processing potential threat feeds. If the infection is detected quickly and the workstation is disabled immediately, you can recover the data within 24 hours, and often in as quickly as five minutes. Organizations should constantly update the operating system and other software on their systems with the latest patches. Unpatched vulnerabilities in operating systems and software are a common entry point for malware.

03 Maintain Robust Backup and Disaster Recovery

The ultimate safety net for ransomware defense is a robust data protection and disaster recovery solution. Implement a backup strategy that fully supports organizations with multiple types of data, files, and systems to protect. Not all solutions are created equal, but enterprise-grade backup and disaster recovery solutions preserve a complete version history, which is crucial to being able to recover from any attack.

04 Commercial Grade Anti-Virus Protection

The best way to steer clear of viruses and malware is to use an industry-leading anti-virus software solution. There are many types out there, and they don't have to break the bank, but having a superior level of defense will go a long way. On your anti-virus software, enable the auto update, auto-protect, and personal firewall features to ensure you always have protection in the background that is continually updated.

05 Lock Down Suspicious Email Attachments

Organizations may also want to install advanced email spam filtering which will block email messages with attachments from suspicious sources. Admins can filter executable attachments in emails based on the file extensions (e.g., block emails sent with ".EXE" attachments). Admins should also disable macros embedded within attachments and re-enable the display to full file extensions which makes it way easier to spot suspicious files.

06 Have an Incident Response Plan

How you've prepared will determine how quickly you are able to restore your company's data and get systems functioning again. This starts with a well-designed plan that is understood by the entire team. Practice executing the plan to ensure you are able to get systems back online in the expected timeframe. The practice will also give your team the confidence to perform flawlessly when the need arises.

Infrascale™

Infrascale providers the most powerful disaster recovery solution in the world. Founded in 2006, the company aims to give every organization the ability to recover from a disaster- quickly, easily, and affordably. Combining intelligent software with the power of the cloud. Infrascale cracks the disaster recovery cost barrier without complex, expensive hardware, enabling any company to restore operations in minutes with a push of a button. Infrascale equips businesses with the confidence to handle the unexpected by providing less downtime, greater security, and always-on availability.