PROTECT THE DATA THAT POWERS YOUR BUSINESS FROM RANSOMWARE

Adopt this three-pronged strategy for complete ransomware protection

Cybercriminals and organizations like yours are engaged in an arms race. You adopt stricter security measures, they develop more sophisticated ransomware vectors and wage battles on new fronts.

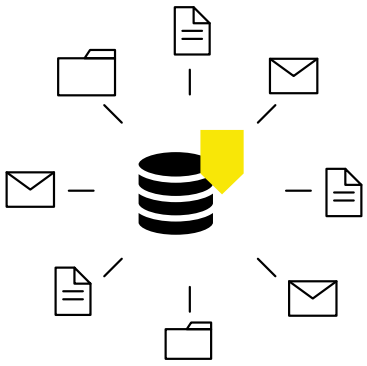
And, these ransomware attacks can decimate your bottom line. In fact, consumers are so protective of their personal data that a single attack in the past year will keep nearly 60% of them from doing business with you.

Are you prepared to protect, defend, and recover?

Arm your first line of defense—your end-users

Awareness breeds caution. Empower your end-users to act as a human firewall through regular cybersecurity training and testing.

- Implement data security training and ensure your end-users can spot phishing attacks, create strong passwords, secure their laptops and mobile devices, and connect securely on public WiFi
- Make your data security training sessions recurring and mandatory—even for leadership
- Schedule annual refresher sessions—or, even better, conduct them every six months
- Incorporate data security training into your new employee onboarding process
- Test end-user awareness and identify vulnerable employees with phishing testing
- Ensure end-users know who they should contact if they spot something suspicious



Secure your endpoints—and keep cybercriminals at bay

Ransomware is becoming increasingly sophisticated. Leverage cutting-edge cybersecurity technologies and best practices to deny cybercriminals the access they are after.

- Rigorously apply the "principle of least privilege"—giving employees only the access necessary to do their jobs—and regularly review that access
- Implement browser security and web filtering to block phishing attempts
- Vet third parties with remote access to ensure they are applying rigorous cybersecurity
- Implement secure password and multifactor authentication policies, and mandate the use of password managers
- Restrict corporate access to personal email accounts and social media sites
- Scan email content, and filter phishing attempts and executable files
- Implement a backup-only account and use it solely for backup tasks to deny ransomware viruses access to your most sensitive files
- Immediately install security patches across all operating systems, software, applications, mobile devices, cloud locations, and IoT

Deny cybercriminals their payday with backup and disaster recovery

Hackers require leverage to demand a ransom. When you're equipped to rapidly restore clean copies of your data, systems, and applications, you undercut their power.

- Fully-document your entire infrastructure, including systems leveraging Remote Desktop Protocol, application dependencies, data flows, SLAs, and downtime costs
- Implement a 3-2-1 backup strategy—creating three backups, with two stored locally on different media—virtual and tape, for example—and one offsite
- Backup your backup to protect yourself against multiple points of failure
- Implement data protection for on-premises and cloud workloads—delivering rapid disaster recovery (DR) and application availability
- Integrate virtualization into your DR strategy—enabling you to instantly stand up virtual machines and restore services
- Implement automated testing and non-disruptive disaster recovery testing to ensure you can deliver against your RPOs and RTOs
- Regularly test backups to ensure systems and data are fully recoverable
- Validate your solutions and processes to uncover—and resolve—any vulnerabilities

Tap into our ransomware prevention expertise

We're here to help. Let us show you how you can efficiently and effectively protect your critical systems, applications, and data.

+1 844 639-6792
arcserve.com