Protect Against the Rising Ransomware Threat

Ransomware attacks of unprecedented scope are shaking organizations the world over. From healthcare systems and educational institutions to government agencies and the financial sector—cybercriminals now extort Bitcoin from organizations of every type, no matter how small or seemingly remote.

The simple fact is that, today, no one is immune.

How can you address your ransomware threat?

Immediately address data security vulnerabilities

Malicious actors have exploited end user naivité and endpoint vulnerabilities, underscoring the importance of ransomware education and data security.

As such, we recommend organizations:

- Invest in regular ransomware education and assessment
- Deploy robust, multi-layered endpoint security
- Promptly install new security patches
- Block legacy protocols to protect against malware evolution
- Upgrade software and operating systems to supported versions

Don't pay the ransom

You may not get your data back. In fact, only about half of all organizations do. Worse, your data may be incomplete or corrupted. Furthermore, attackers may up the ante—demanding a second ransom payment for the decryption key.

Ransomware attackers aren't recreational hackers, but organized criminals; don't count on responsive customer service.

Assess your backup and disaster recovery strategy

Recent global malware attacks have drawn the critical need for ransomware remediation into sharp focus. We recommend you:

- **Examine your RPOs and RTOs.**
  Ensure your critical systems are backed up as frequently as possible, and that system recovery will deliver against your business requirements.
- **Confirm all data sources are backed up.**
  Identify any servers or sources of data missing from your data protection plan and apply the correct level of data availability to ensure they're recoverable.

- **Protect the protector.**
  Make sure your backup files are stored on a secure server with access limited only to those that absolutely require it. These files are your best chance at remediation, so ensure they're secure.
- **Access the backup server as a user.**
  When logging into your secure server, make sure you're logging in as a user, not as an administrator. Never use your administrator account when opening email or searching the web.
- **Follow the 3-2-1 rule.**
  Store at least three different copies of your data on two different media, with at least one copy stored offsite. It's critical that your backup strategy features redundancies and leverages storage options not vulnerable to attack—like tape, offline disk, and cloud.
- **Practice the principle of least privilege.**
  When configuring accounts, only grant the degree of access privileges absolutely required by each role.

Real-world ransomware recovery

"The last ransomware attack was unbelievably major. It hit 45 different servers, spread itself, and just went crazy. The executive suite actually moved into my office for a period of time, if that tells you anything."

With Arcserve UDP, the IT network administrator was able to swiftly restore the backup from the previous evening, sidestepping a $30,000 ransom.

Circumvent ransom demands with Arcserve Unified Data Protection

Relied upon by 48,000+ customers in 150 countries, award-winning Arcserve UDP delivers the simplicity, flexibility, and enterprise-grade capabilities required by small and overstretched IT teams:

- Effortlessly deploy Arcserve as a software, appliance, or cloud solution
- Seamlessly scale your backup and recovery coverage as your organization grows—from 1TB to 1PB, and beyond
- Protect physical and virtual data, no matter where it lives—onsite, offsite, offline, and in the cloud
- Recover your data from file-based and image-based backups, or continuously available solutions
- Easily identify actual RPOs and RTOs, set-up automated testing, and identify unprotected machines with Assured Recovery capabilities
- Instantly stand-up critical applications with virtual standby or Instant Virtual Machine

And, do it all from a single, elegantly simple management console.

Ensure you're protected

Contact your Arcserve representative or call +1 844 639 6792 to get started today.

For more information on Arcserve, please visit **arcserve.com**