Barracuda

PARTNER LOGO

Is Data Backup Really Backing You Up Against Ransomware Attacks?

Ransomware protection is a primary concern for organizations today. It is believed that the best defense is on one hand protecting your email system and web applications, and on the other hand backing up your data to ensure full recovery without paying the ransom. But unfortunately, attackers are staying one step ahead to target backup storage!

There were cases in which hackers took control of the backup application to disable all users in the organization from logging in their accounts and erase all data! Paying the ransom will not solve the problem. A recent research shows that 80% of companies that paid a ransom were attacked again. **It's time to go for a secure backup solution** to stop attackers from compromising valuable data. We need the following capabilities.

1. **Immutable storage —** Prevent attackers from modifying data in the backups.
2. **Multi-factor authentication —** Secure the accounts used for accessing backups.
3. **Role-based access control —** Follow the principle of least privilege for all users with access to the backup system.
4. **Air-gapped cloud —** Keep a backup copy in a secure cloud on an isolated network.
5. **Multiple backups —** Replicate your on-premises and cloud backups to another location.

All these are made possible by Barracuda Networks with the following offerings.

- Barracuda backup server is a hardened, air-gapped device that prevents network lurkers from finding your backup data during pre-attack reconnaissance.
- Barracuda Cloud-to-Cloud Backup supports Office 365 deployments to enable data protection and recovery from Microsoft SharePoint, Teams, Exchange, and OneDrive.
- Barracuda support eases your pain in deployment and configuration while providing recovery assistance to ransomware victims.

Use the right tool for the job. Contact us today for a demonstration and free consultation.

Contact Us

Forward this to a colleague

f G+ in

Privacy Policy I Unsubscribe