THREATDOWN™

Ransomware Prevention Checklist for MSPs

A practical, no-nonsense checklist MSPs can use to reduce ransomware risk, limit blast radius, and recover quickly when incidents occur.

☐ **Harden the Initial Attack Surface**

- Enforce MFA everywhere (RMM, M365, VPN, admin accounts)
- Lock down RDP and remove unnecessary exposure
- Eliminate standing admin rights; use least privilege
- Patch OS, browsers, and common attack apps weekly

☐ **Deploy Modern Endpoint Protection**

- Use EDR with behavioral detection
- Enable anti-tamper and ransomware rollback
- Block unknown or untrusted applications
- Standardize policies across all customers

☐ **Ensure Backups That Survive an Attack**

- Follow the 3-2-1 backup rule with immutable storage
- Separate backup credentials from domain admin
- Test restores quarterly
- Include SaaS backups (M365, Google Workspace)

☐ **Detect Lateral Movement & Privilege Abuse**

- Monitor for credential misuse and admin escalation
- Alert on mass file changes or abnormal behavior
- Review RMM, M365, firewall, and endpoint logs
- Use 24×7 monitoring or MDR where possible

☐ **Document & Rehearse Incident Response**

- Maintain a written ransomware response playbook
- Define isolation, communication, and escalation steps
- Pre-assign roles (MSP, client, legal, insurance)
- Store response documentation offline

☐ **Train Humans (The #1 Entry Point)**

- Run regular phishing simulations
- Deliver short, repeatable security awareness training
- Provide a clear process to report suspicious activity
- Train MSP staff the same way as clients