ThreatDown
Powered by Malwarebytes

22-Point Checklist for Ransomware Prevention

A successful ransomware attack can cost your company time, money, and its reputation. Create a prevention plan and understand the steps needed to mitigate an attack quickly with this checklist.

What you should do:	Breach	Infiltration	Attack	Restoration	Recovery
Create an inventory of assets including hardware, software and data	✓	✓			
Audit your network for unknown computers and services	✓	✓			
Disable Internet-facing systems, services, and ports you don't need	✓	✓			
Perform regular vulnerability scans	✓	✓			
Patch systems regularly, prioritizing the most vulnerable and critical	✓	✓			
Ensure systems are properly configured, and security features are enabled	✓	✓			
Harden remote access with MFA, password rate limits, and password lockouts	✓				
Deploy endpoint security software to all endpoints and servers	✓	✓	✓		
Provide staff with cybersecurity awareness training	✓	✓			
Implement a process for reporting and responding to suspicious activity	✓	✓	✓		
Document your network structure and data flows		✓			✓
Use network segmentation to subdivide your computer networks		✓			
Use least-privilege access for all systems and services	✓	✓			
Use allow listing to ensure that only authorized software can run		✓	✓		
Restrict the use of legitimate tools commonly used by attackers[1]		✓			
Harden domain controllers according to the latest best practice[2]		✓			
Monitor your network and endpoints using IDS, EDR and SIEM		✓	✓		✓
Make regular, comprehensive backups, keeping at least one copy offline				✓	
Have a process for restoring computers from clean system images				✓	
Practice restoring systems from backups, so you know they work				✓	
Create an incident response plan[3] that aligns with regulations			✓	✓	
Create a critical asset list so you know what you need to restore first				✓	

[1] This is known as "living off the land." The Living Off The Land Binaries and Scrip (LOLBAS) project maintains a list of legitimate software used by attackers at https://lolbas-project.github.io/
[2] Domain controllers are a prime target for attackers. Microsoft maintains a guide to securing domain controllers against attack at https://docs.microsoft.com/ven-us/windows-server/identity/ad-ds/plan/security-best-practices/securing-domain-controllers-against-attack
[3] You can find a response plan template at https://github.com/counteractive/incident-response-plan-template/blob/master/playbooks/playbook-ransomware.md