CONNECTWISE

Cybersecurity Checklist for the AI Era

Exploits now happen in minutes. This checklist helps defenders prioritize risk mitigation, speed, and pre positioned response agility over single-layer prevention.

1 Identity and Access Management

Primary Control Plane

- [ ] Enforce multi-factor authentication (MFA) everywhere (email, RMM, VPN, admin accounts, backups)
- [ ] Create a unique account for every user and admin (no shared accounts)
- [ ] Eliminate standing admin rights
- [ ] Use just in time (JIT) admin access where supported
- [ ] Remove inactive and stale accounts monthly

2 Establish a Baseline Configuration

High Blast Radius Risk

- [ ] Lock down RMM tools
  - Use centralized IDPs/SSO and avoid local accounts
  - Use a least privileged approach to roles and permissions
  - Ensure audit coverage of all RMM tools
  - Use tools that enforce zero trust by default (MFA, IP restrictions, alert on scripts/mass changes)
- [ ] Separate MSP internal systems from client environments
- [ ] Use dedicated admin workstations (PAWs)
- [ ] Segment vendor and third party access

3 Endpoint and Email Hardening

Assume Patch Lag

- [ ] Deploy EDR/XDR on all endpoints and servers
- [ ] Ensure tamper protection is enabled
- [ ] Block execution from AppData, Temp, and Downloads folders
- [ ] Restrict PowerShell, macros, and scripting for non admins
- [ ] Use application allowlisting where feasible
- [ ] Enable advanced phishing protection
- [ ] Enforce DMARC, DKIM, and SPF on all domains
- [ ] Disable auto forwarding to external addresses
- [ ] Deploy one click "report phish" with fast triage

4 Patch and Vulnerability Response

Speed Over SLAs

- [ ] Maintain an inventory of internet facing assets
- [ ] Patch critical/high vulnerabilities within 24 to -72 hours
- [ ] Same day or next day patching for exposed systems when feasible
- [ ] Prioritize vulnerabilities assuming time to exploit = hours or minutes
- [ ] Predefine emergency zero day remediation workflows
- [ ] Maintain a tested rollback plan
- [ ] Apply compensating controls for unpatchable systems (segmentation, WAF/IPS, allow listing, privilege reduction)

5 Network and Exposure Reduction

Contain the Inevitable

- [ ] Segment user, server, backup, and management networks
- [ ] Disable or tightly restrict RDP (VPN and MFA minimum)
- [ ] Use firewalls with IDS/IPS enabled
- [ ] Enforce egress filtering to limit C2 and exfiltration
- [ ] Monitor for lateral movement (east west traffic)
- [ ] Reduce unnecessary internet exposure

6 Backup and Ransomware Resilience

Backups Are a Target

- [ ] Use immutable or offline backups (3 2 1 minimum)
- [ ] Separate backup credentials from domain access
- [ ] Monitor for backup tampering or mass deletion
- [ ] Test restores quarterly (not just backup success)

7 Detection and Response Readiness

Machine Speed Defense

- [ ] Have observability in all business systems of record, not just EPP (SIEM capabilities)
- [ ] Alert on behavior, not just signatures
- [ ] Ensure 24/7 alert triage with an SLA that meets your goals (SOC or trusted partner)
- [ ] Pre stage containment actions:
  - Isolate host
  - Disable accounts
  - Revoke tokens
- [ ] Track and reduce MTTD and MTTR, but recognize these are "look backward" metrics

8 People, Process, and Surge Readiness

- [ ] Maintain a simple documented incident response plan
- [ ] Establish a "report fast, no blame" culture
- [ ] Run tabletop exercises for vulnerability storm scenarios
- [ ] Prepare customer communication templates in advance
- [ ] Maintain trusted paths with vendors, ISACs, CERTs

Bottom Line Priority Reminder

Identity failures turn bugs into breaches

Vulnerabilities become far more dangerous when attackers can pair them with stolen, weak, or overprivileged credentials. Strengthen identity controls with MFA, least-privilege access, conditional access policies, and continuous monitoring to reduce the risk of a single exploit becoming a larger compromise.

RMM and shared tooling protective measures are key

RMM solutions are critical for preventative management and response. These same capabilities can make them a target for bad actors, which is why using secure, zero-trust-based tools and additional security controls, such as MFA and role-based access, are essential to maintain security and access.

Teams must balance patch speed with patch quality

Effective patch management is about balancing speed and risk. Organizations need the ability to quickly address critical vulnerabilities and zero-day threats while validating updates before broad deployment. Identify high-impact machines, use staged rollouts, test groups, and risk-based prioritization to ensure high-impact patches reach vulnerable systems quickly without introducing unnecessary business disruption.

Segmentation limits damage when exploits succeed

Even strong defenses can fail, so organizations need controls that contain attacker movement. Segment networks, restrict lateral access, and isolate critical systems to limit the blast radius of a successful exploit and protect business-critical operations.

Backups must survive attacker pressure

Backups are only effective if they remain available and recoverable during an active attack. Use immutable, isolated, and regularly tested backups to ensure organizations can restore operations even if attackers target production systems, credentials, or backup infrastructure.

Visit connectwise.com/solutions/security-management to see how ConnectWise solutions can help you stay ahead of cyberthreats in the AI era.