Resilience checklist for 2026

Building on the findings of the Expel 2026 Annual Threat Report, these concrete steps can help you better protect your environment in the year ahead.

IDENTITY

- ☐ Strengthen protection for the most-critical and highly privileged accounts through conditional access policies for authentication.
- ☐ Reduce the risk of phishing with policies and tools such as:
  - Secure email gateways
  - Authentication audits and assessments
  - MFA based on the FIDO2 standard
- ☐ Task red teams with auditing your identity security controls to identify weaknesses and reveal the blast radius of a compromised account.
- ☐ **For Expel customers:** Enable account disablement as an auto remediation action to help us quickly contain identity-based incidents.

ENDPOINT

- ☐ Disable the use of the Windows Run hot key (Windows + R), which is used in the majority of ClickFix attacks.
- ☐ Ensure employees have official means for downloading approved applications to prevent fraudulent downloads.
- ☐ Block unwanted applications with whitelisting and Application Control for Windows.
- ☐ Block remote management tools that aren't expected in your environment.
- ☐ **For Expel customers:** Enable the "contain host" auto remediation for a faster response to endpoint incidents.

CLOUD INFRASTRUCTURE

- ☐ When using package managers, such as NPM, control and monitor what happens in this environment by:
  - Disabling lifecycle scripts
  - Implementing version pinning
  - Requiring MFA for the deployment of your own NPM packages
- ☐ Use tools like TruffleHog or GitHub Secret Scanning in CI/CD pipelines to implement proactive secret key security and monitoring.
- ☐ Transition from long-term IAM access keys to IAM roles and OIDC for automated workflows to enforce short-lived credentials.
- ☐ Use a secrets manager to automatically rotate keys every 30 to 90 days. Create a predefined automated script to immediately revoke and rotate any key identified as exposed.
- ☐ Enforce least privilege access policies to ensure all API keys have restricted permissions. Never use `AdministratorAccess` for integration keys.
- ☐ Harden AWS instance metadata service (IMDS) settings and require IMDSv2 for new instances.
- ☐ Guard against cryptomining installations with AWS GuardDuty, Runtime Monitoring, Kubernetes pod security policies, and outbound connection monitoring.
- ☐ **For Expel customers:** Enable the disable access key auto remediation so our SOC can quickly shut down a compromised long-term AWS IAM access key.

Know your enemy

Effective threat defense begins with understanding your adversaries and their tactics. Learn more about the latest cybersecurity trends across identity, endpoint, and cloud in the full Expel 2026 Annual Threat Report: **expel.com/2026atr**