Kaseya

Secure your Microsoft environment

A five-step checklist

Microsoft provides the foundation for modern business productivity, but every new identity, cloud application, shared file and administrative privilege expands your attack surface. Today's attackers target users, identities, email and trusted cloud services to gain access and move through Microsoft environments.

While Microsoft provides essential security capabilities, reducing modern cyber risk requires continuous visibility, behavioral detection, automated response and ongoing validation.

Use this checklist to strengthen your Microsoft security strategy and reduce risk across your environment.

1 Reduce identity risk

Reduce identity-based attacks by regularly reviewing and maintaining:

- [ ] Multifactor authentication for all users, especially privileged accounts.
- [ ] Legacy authentication and other outdated access methods.
- [ ] Privileged roles, administrative accounts and excessive permissions.
- [ ] Inactive users, guest accounts and unnecessary access.
- [ ] Conditional Access policies aligned to organizational risk.

2 Stop email-based attacks earlier

Strengthen your first line of defense by ensuring:

- [ ] GenAI-powered phishing protection is in place to defend against modern AI-generated attacks.
- [ ] Users receive clear guidance when suspicious messages reach their inboxes.
- [ ] Business email compromise, credential harvesting and account takeover attempts can be identified quickly.
- [ ] External senders, impersonation attempts and malicious links are clearly detected.
- [ ] Email protection extends beyond traditional signature-based filtering.

3 Detect threats before they become incidents

Continuously monitor your Microsoft environment for:

- [ ] Risky sign-ins and impossible travel activity.
- [ ] Privilege escalation and administrative changes.
- [ ] Suspicious mailbox rules and forwarding activity.
- [ ] Abnormal user behavior across Microsoft 365 applications.
- [ ] OAuth application consent, unusual access and identity abuse.
- [ ] Security settings that have changed from your approved configuration.

4 Respond faster and contain threats automatically

Reduce response time by ensuring your security processes can:

- [ ] Automatically contain compromised accounts before attacks spread.
- [ ] Revoke active sessions when suspicious activity is detected.
- [ ] Enforce password resets and MFA when user risk increases.
- [ ] Alert IT teams with actionable context instead of isolated events.
- [ ] Reduce manual investigation through intelligent automation.
- [ ] Capture response actions and security events as audit evidence.

5 Continuously strengthen your security posture

Regularly validate and improve your Microsoft security posture by reviewing:

- [ ] Security configurations that drift from organizational standards.
- [ ] Vulnerabilities and weaknesses before attackers exploit them.
- [ ] Microsoft Secure Score and other security posture recommendations.
- [ ] Security controls that support cyber insurance, customer security reviews and regulatory requirements.
- [ ] Emerging attack techniques and changes to your overall security posture.

A secure Microsoft environment requires continuous monitoring, proactive threat detection, automated response and ongoing security validation. By strengthening identity security, stopping email threats early, detecting suspicious activity, accelerating incident response and continuously improving your security posture, you can significantly reduce cyber risk and build greater resilience against evolving attacks.

Ready to take the next step?

Request a demo today

See how our advanced Microsoft security solutions can help you protect your users, identities and business with confidence.

Kaseya®