Barracuda

Zero Trust Access migration checklist

PHASE	MILESTONE	TASK	TIMEFRAME	ACTIONS	PROGRESS
PHASE 1: ASSESSMENT AND PLANNING	Stakeholder engagement	Identify stakeholders and project teams/admins	1 week	Identify all key stakeholders and assign responsibilities for different aspects of the Zero Trust migration.	☐
		Communications/meetings plan for project team/ stakeholders	1 week	Develop a communication plan for stakeholders and schedule regular meetings.	☐
	Security and risk analysis	Conduct a comprehensive risk assessment	2 weeks	Identify potential threats, vulnerabilities, and risks.	☐
		Assess current state of applications	2 weeks	Conduct an inventory and analysis of your application landscape.	☐
		Identify security gaps and vulnerabilities	1 week	Review current security controls and identify areas for improvement.	☐
		Determine your Zero Trust maturity level	1 week	Assess the organization's current Zero Trust maturity level.	☐
	Project management	Quality management plan	1 week	Define quality standards and procedures for the migration project.	☐
		Risk management plan	1 week	Develop a plan to identify, assess, and mitigate potential risks.	☐
		Define roles and responsibilities	1 week	Clearly define roles, responsibilities, and accountability within the project team.	☐
		Identify pilot users	1 week	Select a group of users to participate in the pilot phase.	☐
PHASE 2: DESIGN AND ARCHITECTURE	Security architecture design	Design a Zero Trust security architecture	4 weeks	Develop a comprehensive architectural plan that aligns with Zero Trust principles.	☐
		Develop comprehensive security policies	3 weeks	Create detailed security policies addressing the core Zero Trust pillars.	☐
		Training plan for admin/support	2 weeks	Create a training plan for administrators and support staff.	☐

PHASE	MILESTONE	TASK	TIMEFRAME	ACTIONS	PROGRESS
PHASE 3: PILOT	Internal application migration	Internal application migration	4 weeks	Plan for migrating internal applications to align with Zero Trust principles.	☐
	SSO/SAML migration	SSO/SAML migration	4 weeks	Implement configurations to integrate applications and IdP with SSO and SAML protocols.	☐
	Enforcement design/testing	Enforcement design/testing	2 weeks	Design and test enforcement mechanisms for Zero Trust policies.	☐
	External application configuration	External application vendor configuration	2 weeks	Ensure external applications or SaaS platforms are configured to meet Zero Trust requirements.	☐
	Pre-launch testing	Pre-launch testing	2 weeks	Conduct comprehensive pre-launch testing of the Zero Trust implementation.	☐
	Enforcement	Configuration conditional access	2 weeks	Configure conditional access policies to enforce granular access control.	☐
		Document lessons learned	Ongoing	Emphasize documentation of lessons learned during the pilot phase for continuous improvement.	☐
PHASE 4: FULL DEPLOYMENT AND ENFORCEMENT	Communications	Draft communications templates/timing/channels	2 weeks	Develop communication templates to inform stakeholders about the migration.	☐
		Validate admin/support/ FAQ/wiki	1 week	Ensure support materials are updated to reflect the new Zero Trust environment.	☐
		Send initial communication for awareness and expectations	1 week	Send an initial communication to raise awareness about the implementation.	☐
	Deployment to endpoints	Deployment to endpoints (PC/Mac)	4 weeks	Deploy Zero Trust agents or software to all relevant endpoints.	☐
	Post-deployment support	Post-deployment support plans	Ongoing	Include post-deployment support plans to handle user feedback and issues.	☐
PHASE 5: MONITORING AND IMPROVEMENT	Monitoring	Metrics/results	2 weeks	Track key performance indicators (KPIs) and security metrics, such as blocked access attempts and incident response times.	☐
		Sundown	Ongoing	Develop a plan to decommission legacy systems and VPNs that are no longer necessary.	☐

Have questions? Join the over 200,000 organizations worldwide that trust Barracuda Networks to protect them.
For more information, visit barracuda.com.