Terms and Conditions

Auto-Elevate (PAM) - Schedule CS-9

Effective Date: October 14, 2025 | Supersedes prior versions.

Service Summary
Service Provider will provide Privileged Access Management (PAM) services using the Auto-Elevate platform to control and secure local administrative privileges on endpoints.
This service is designed to minimize the risks of privilege misuse, unauthorized software installation, and elevation-based attacks by requiring users to request administrative actions through an approved workflow.

Auto-Elevate provides real-time approval, auditing, and policy enforcement for privilege elevations while maintaining user productivity.

Scope of Services

- Deployment and configuration of the Auto-Elevate agent on supported Windows endpoints.
- Integration with Service Provider's centralized management console and ticketing platform.
- Creation and maintenance of elevation policies based on best-practice least-privilege standards.
- Review and approval (manual or automated) of elevation requests within the Service Provider's standard support hours.
- Logging and reporting of all elevation activities for audit and compliance purposes.
- Coordination with other endpoint security tools (e.g., EDR, XDR, DNS filtering) where applicable.

Exclusions
- Configuration or troubleshooting of unsupported operating systems or third-party PAM tools.
- Coverage of unmanaged or unenrolled endpoints.
- Guarantee of full prevention of privilege-based threats; PAM reduces risk but does not eliminate it.
- Custom scripting, integration, or policy design outside Service Provider's standard policy set (treated as a separate project).

Client Responsibilities
- Provide a current and accurate list of covered endpoints and authorized users.
- Ensure endpoints remain online and reachable for policy updates and reporting.
- Inform Service Provider promptly when personnel changes require modification of privilege access.
- Cooperate in applying remediation actions for denied or escalated privilege events.
- Maintain internal security policies consistent with least-privilege principles.

General Terms
- PAM services are preventive controls intended to reduce the risk of unauthorized privilege use. They do not guarantee protection from all endpoint compromise.
- Service Provider may disable local admin rights on covered endpoints to enforce least-privilege operation.
- Service Provider recommends complementary safeguards such as EDR, DNS filtering, MFA, and XDR to achieve layered protection.
- Fees for this Schedule are billed in accordance with the Payment Terms of the Master Service Agreement.
- Additional costs (e.g., advanced analytics, custom integrations, or non-standard workflows) may apply and will be quoted separately.