FOR SECURITY & IT LEADERS

How to protect yourself

The defenses are not mysterious. It is about getting the fundamentals right and taking them seriously. Most of these are things teams have on the roadmap and have not finished rolling out.

Now

This week

- [ ] Require phishing-resistant MFA (FIDO2 or passkeys) for IdP admins, SaaS admins for Salesforce, Workday, Snowflake, BigQuery, Google Workspace, helpdesk staff, and contractors with admin scope.
- [ ] Audit every account that holds Global Admin, Intune Admin, Salesforce Admin, or equivalent privileged roles across critical SaaS apps. See Lumos Identity Visibility.
- [ ] Inventory every OAuth app, refresh token, service account, API key, and vendor integration. Each one gets a named owner, a data scope, a last-used date, and an emergency revoke path. See Lumos NHI.
- [ ] Alert on bulk SaaS exports, unusual API reads, and dormant identities suddenly active.
- [ ] Run a 30-minute tabletop on what your team would do if a connected app like Salesforce were compromised tomorrow.

Next

This month

- [ ] Extend just-in-time access policies to every SaaS app with admin roles: Salesforce, Workday, AWS, ServiceNow, Snowflake, BigQuery, GitHub, Slack. Microsoft PIM only covers Microsoft. See Lumos JIT.
- [ ] Rotate API keys, refresh tokens, and cloud credentials, especially for any vendor whose breach has been publicly disclosed this year. Make frequent credential rotation mandatory.
- [ ] Review OAuth scopes for every connected app and remove broad permissions where narrower scopes work.
- [ ] Build and test an emergency revoke playbook for OAuth tokens, vendor access, and API keys across the critical SaaS apps. The Salesloft Drift response separated companies into two groups: those who could revoke in hours, and those who could not find the integrations for three weeks.
- [ ] Extend secret scanning beyond GitHub into Salesforce cases, ServiceNow records, Slack channels, Google Drive, Notion, support tickets, and call transcripts. The TELUS lesson is that secrets follow people, and people work in SaaS apps, not in source control.
- [ ] Classify entitlements across your software portfolio to identify admin-level and sensitive permissions. See Lumos Albus.

Ongoing

Continuous

- [ ] Conduct continuous access reviews of human and non-human identities, with priority on accounts that can export data or act offline. See Lumos UARs.
- [ ] Monitor for AiTM phishing indicators: token replay, sign-ins from new locations immediately after MFA completion, concurrent sessions with different device fingerprints.
- [ ] Train helpdesk teams on voice phishing escalation paths and verification scripts.
- [ ] Track every third-party SaaS vendor that holds credentials into your data warehouses, and require them to publish security postures and breach disclosure SLAs.
- [ ] Implement AI-driven entitlement classification so admin-tagged permissions get reviewed on a tighter cycle than standard access.