## Key Performance Indicators

By bringing all these areas together, we can develop a compelling set of KPIs that can measure the identity security program over time.

These draw on all four pillars of identity security and map to clear cybersecurity and business outcomes.

| NIST CSF Stage | Identify Capability | Example KPIs | Cybersecurity Outcomes | Business Outcomes |
|---|---|---|---|---|
| **Identify** | User Inventory | # orphaned accounts<br># discrepancies with HRIS<br># of non-unique and/or shared IDs<br># of administrator accounts | Enable zero trust journey | Breach Prevention; Employee satisfaction; Improve compliance |
| | Machine Identities | # of service accounts with unknown owners<br># service accounts with default passwords or expired keys | Reduce unauthorized access | Breach Prevention and Brand Reputation |
| | Guest Accounts | # inactive guest accounts<br># guest accounts with excessive access<br># unmanaged devices with access | Reduce attack surface | Breach Prevention; Third Party Risk; Improve compliance and Reduce audit findings |
| **Protect** | Onboarding | Speed to onboard new employees rate<br># users with excessive access rights<br>% User account creation satisfaction rate | ATO prevention | Operational Efficiency; Breach Prevention |
| | De-provisioning | % Accounts disabled within SLA for terminated users<br>Speed to deprovision | Reduce unauthorized access and data loss | Operational Efficiency; Breach (ATO) Prevention |
| | SSO | % of business apps protected under SSO<br># apps with direct access<br>% password complexity rate<br># unused applications<br># of logins per day | ATO prevention | Breach Prevention, Employee Satisfaction |
| | MFA | % of user accounts configured to use Multi-factor Authentication<br>% of Guest Accounts with MFA<br>% of user accounts using strong forms of MFA (FIDO2, Passwordless, passkeys, number-matching) | ATO prevention | Breach Prevention; Improve Compliance; Third Party Risk |
| | Access Policy | % access coming from trusted or known locations or IPs<br>% access evaluated for risk at authentication time<br>% access coming from trusted devices | Limited access to critical data | Breach Prevention; Improve Compliance |
| **Detect** | Collection | # Unsuccessful logins (SOX)<br># Anomalous access events<br># User-reported suspicious activity<br># Unmanaged endpoints<br># Priviliged users without MFA | Develop "baseline behavior" and custom Risk Profile<br>Reduce unauthorized access | Improve Compliance and Reduce Audit Findings; Operational Efficiency |
| | Detection | # of parallel sessions<br># Impossible travel events<br># Suspicious IP addresses blocked<br>Average time to detect brute-forcing attempts and compromised users<br># Highlighted risky events raised per day | Quicker detection of compromised users and insider threats | Breach Prevention; Operational Efficiency |
| **Respond** | Response | Average time to perform a password reset<br>% False positive rate<br># authentication-related help desk tickets<br># OS/browser device update self-remediations performed<br># MITRE ATT&CK sub-techniques mitigated<br># Risky events triaged per day<br># Access policies improved | Improve Mean Time to Remediation<br>ATO prevention<br>Optimize and protect for current state of business | Operational Efficiency; Improve Compliance; Breach Prevention |