

# 5 Key Use Cases for SSCP

## SaaS Security Control Plane (SSCP)

An identity-based architectural element commonly leveraged to discover SaaS services and user-SaaS relationships, identifying risky access controls, malicious or abandoned SaaS services, and credential exposures throughout the SaaS service layer. SSCP orchestrates remediation and workflows to enforce security policy or offboard users in just a few clicks.

### Safeguard the SaaS service layer –past, present, and future

01



#### SaaS Discovery

Grip SaaS Security Control Plane (SSCP) is identity-based, enabling security and risk teams to fingerprint user-SaaS connections and relationships across their global SaaS service layer, including historic SaaS services and apps with dangling access or abandoned accounts.

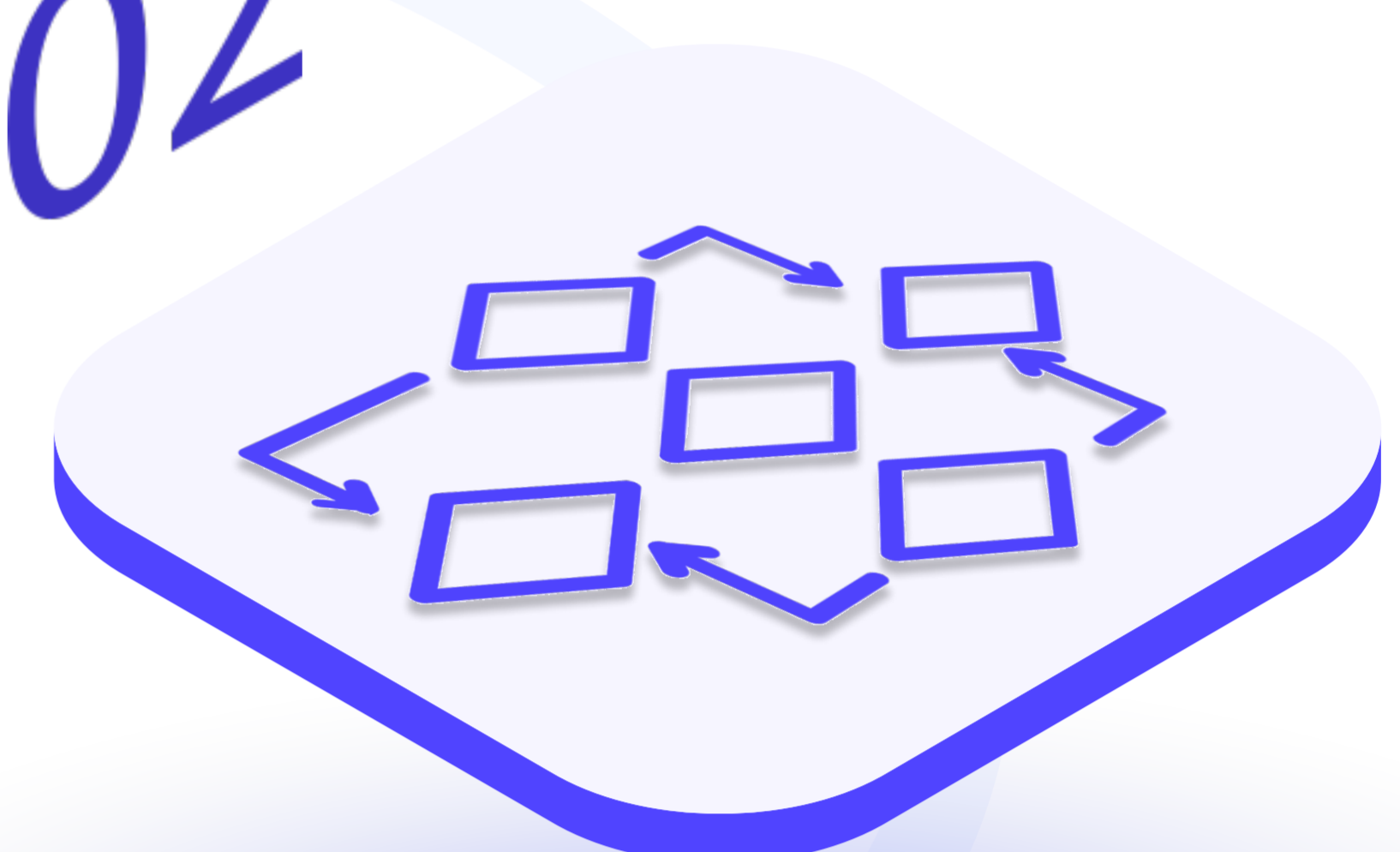
**Key capability:** Identity-based, AI-enabled SaaS discovery with observed risks and threats

#### SaaS Risk Indexing

Grip SSCP extracts SaaS intelligence from billions of SaaS signals and AI-enabled scanning, delivering dynamic SaaS risk indexing to prioritize mitigation and remediation, including accumulated risk from unguarded SaaS for 10+ years.

**Key capability:** Continuous AI-powered SaaS mapping and SaaS risk indexing (SRI)

02



03



#### Secure Access and Offboarding

Grip SSCP detects and monitors SaaS access controls, missing SSO, policy dodging and changes to SaaS authentication. Security teams can destroy weak and duplicate passwords, automate offboarding for users and SaaS out of reach for IAM and CASB.

**Key capability:** Robotic process automation (RPA) and justification-based access control

#### Credential Security

Enforce authentication and credential policy, password strength, and analyze telemetry from user-SaaS connection events. Users get the ease and confidence of single sign-on, on-demand across SaaS services and apps—security gets universal credential security by destroying weak passwords, revoking risky access, and automating offboarding for users, SaaS, or both.

**Key capability:** Strong password generator, double-blinded credential vaulting with continuous rotation

04



05



#### Orchestrate and Enforce

Realize identity-based SaaS security and mitigate risks and threats across the enterprise SaaS layer without agents, proxies, or dependencies. Integrate SaaS insights and intelligence with existing control points via SaaS detection rules and policy enforcement. Scale through time by removing built up SaaS risk from the past, closing access control gaps in the present, and adapting controls for SaaS yet to be discovered (future).

**Key capability:** Agentless, identity-based SaaS intelligence and open integrations to existing security tools

