The ShinyHunters Checklist

Are your security controls properly configured to stop modern attacks?

ShinyHunters is the name associated with a shifting set of financially motivated data theft and extortion operations. Across separate campaigns, attackers repeatedly found openings created by security controls that were missing, overly permissive, weakly enforced, or exposed to the wrong users and networks.

ShinyHunters didn't break in. They walked through doors that were already unlocked.

DIFFERENT CAMPAIGNS. REPEATED CONTROL FAILURES.

MISSING MFA AND NETWORK RESTRICTIONS

Attackers used previously stolen credentials to access Snowflake customer instances. Successful compromises involved accounts without MFA, credentials that remained valid for years, and environments without network allowlists.

The opening: Password-only authentication, stale credentials, and unrestricted network access.

EXCESSIVE CONNECTED-APP PRIVILEGES

Employees were persuaded to authorize malicious Salesforce connected applications that could query and export sensitive data.

The opening: Excessive API privileges and insufficient connected-app guardrails.

PHISHABLE MFA AND WEAK ENROLLMENT CONTROLS

Attackers stole SSO credentials and MFA codes, registered their own authentication methods, and accessed SaaS applications available to the compromised user.

The opening: Phishable MFA, weak enrollment controls, and broad SaaS access.

OVERLY PERMISSIVE GUEST ACCESS

Public-facing Salesforce Experience Cloud sites exposed data through guest profiles and APIs configured with more access than intended.

The opening: Excessive guest permissions and publicly accessible data interfaces.

THE RECURRING PATTERN

- Missing MFA
- Stale credentials
- Excessive guest access
- Unrestricted applications
- Broad SaaS permissions
- Publicly reachable management endpoints

Whether the insecure state came from the original setup, an approved exception, or configuration drift, attackers found and exploited the live misconfigured security control.

Score your security controls

Check each box only if the statement is true and enforced in your production environment today.

IDENTITY AND MFA HARDENING

- [ ] Administrative and sensitive accounts require phishing-resistant MFA.
- [ ] Enrolling a new MFA factor requires strong identity verification.
- [ ] MFA resets cannot be approved through an unverified phone call.
- [ ] Password-only, dormant, contractor, and unnecessary local accounts are regularly removed.

SAAS AND CLOUD ACCESS

- [ ] Guest and external users have only the access they require.
- [ ] OAuth and connected applications require administrator approval and least-privilege scopes.
- [ ] API tokens, sessions, and credentials expire or are rotated, with stale grants revoked.
- [ ] Bulk exports and unusual downloads can be detected, investigated, and blocked.

NETWORK AND APPLICATION EXPOSURE

- [ ] Sensitive platforms are restricted to trusted networks, devices, or private endpoints.
- [ ] Internet-facing administrative and management interfaces are continuously inventoried.
- [ ] Firewall, WAF, and access policies block unnecessary inbound paths and risky outbound traffic.
- [ ] Changes that broaden network access are reviewed before reaching production.

CONTROL VALIDATION AND DRIFT

- [ ] Changes to MFA, permissions, guest access, APIs, network policies, and connected apps generate alerts.
- [ ] Actual configurations are compared with an approved security baseline everyday.
- [ ] Temporary exceptions have owners, expiration dates, and documented justification.
- [ ] Control gaps have a named owner and remediation deadline.

YOUR SCORE

0–5 CHECKED

You are significantly exposed. Multiple attack paths remain open.

6–11 CHECKED

You may stop a few attacks, but many attack paths still remain open.

12–16 CHECKED

Your controls are configured well. Continuously validate them as environments change.

Continuous assurance across every security control



Security controls change constantly. Permissions expand, exceptions remain in place, capabilities get disabled, and policies drift away from the design security teams intended.

Reach gives security teams continuous visibility into how their controls are actually configured and whether those controls remain aligned, enforced, and ready.

By analyzing the tools already deployed across your environment, Reach uncovers misconfigurations, identifies underused protections, detects configuration drift, and guides teams through the changes needed to close each gap.

01

FIND THE GAPS THAT CREATE EXPOSURE

Identify missing protections, overly permissive policies, ineffective enforcement, and configurations that have drifted from their approved state.

02

PRIORITIZE WHAT TO FIX FIRST

Focus remediation on the gaps that create meaningful exposure based on your environment, active threats, and the controls available to you.

03

AUTOMATICALLY REMEDIATE

Give teams clear, step-by-step guidance to correct each issue and bring controls back into alignment with security policy.

04

CONTINUOUSLY VALIDATE

Continuously monitor configurations to detect drift the moment it happens and validate that controls are working as intended.

Security controls only protect you when they are properly configured.

See how Reach helps continuously find and fix security control gaps.

Request a Demo

reach.security

Research sources: U.S. Department of Justice; Mandiant and Google Threat Intelligence Group reporting on UNC5537, UNC6040, ShinyHunters-branded SaaS operations, and UNC6240; FINRA's Salesforce Experience Cloud alert.