

Built by a MSP for MSPs

Help Desks Are Under Attack

Password resets, MFA changes, and approvals are prime attack vectors for impersonation

Manual caller ID checks and callbacks are slow, unreliable, and leave no audit trail

Plaintext passwords and API keys in tickets create long-term breach exposure

TRACELESS

Traceless stops help desk phishing attacks and prevents exfiltration of sensitive information.

TRACELESS

Confirm customer identity:

in seconds (text code, phone call, or authenticator)

Ephemeral by default:

passwords and files go out as one time links that auto expire after opened

Integrated:

Use Slack, Teams or your ticketing system; no new portal required

L**ogs:**

Records directly into ticket for auditing

The Traceless Advantage

Verify Identity in the ticket

- Trigger MFA directly
- ConnectWise, MS Authenticator, Duo, Okta, SMA, Email or automated callback

Share information safely

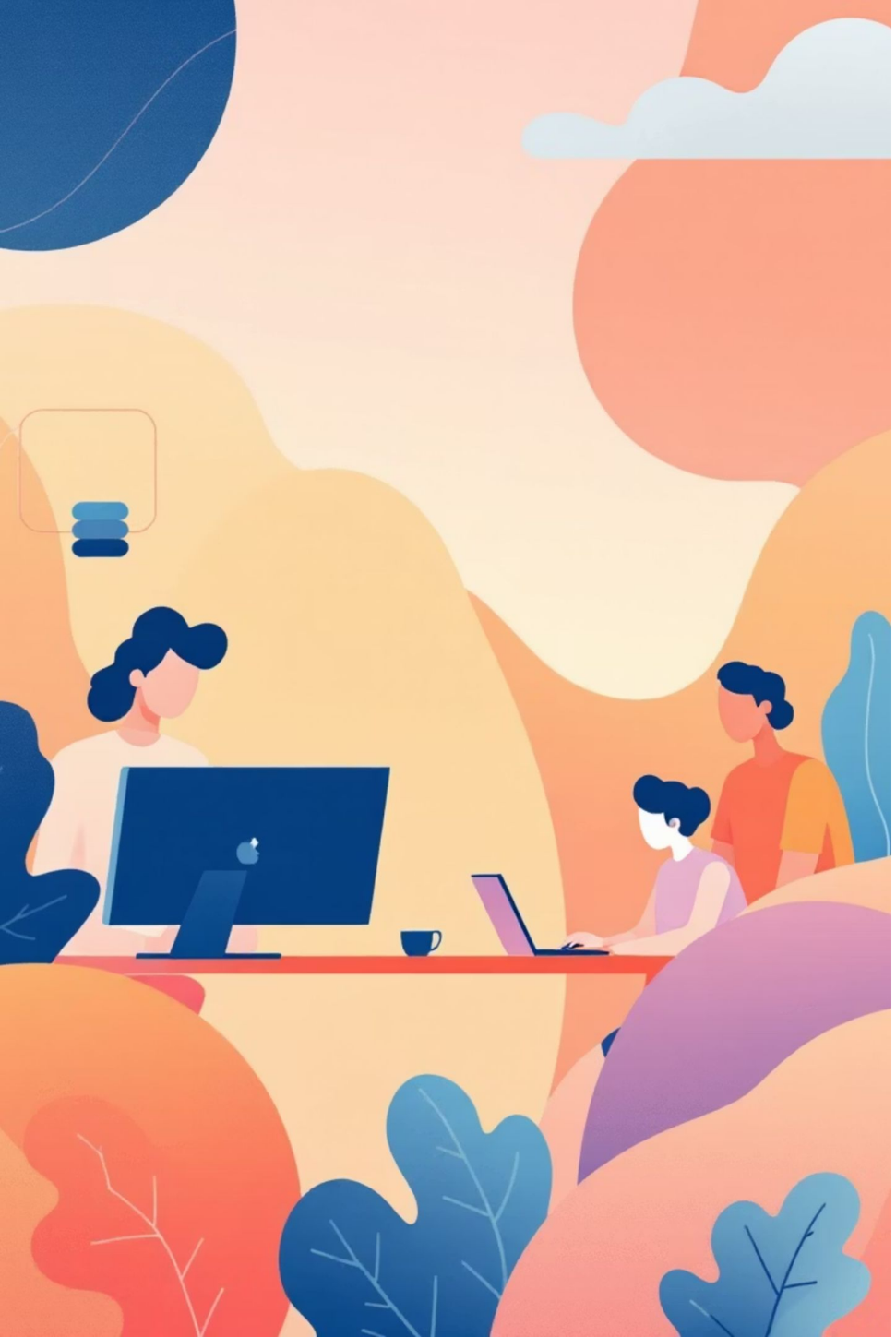
- One-time expiring links
- Auto-purge after viewing.
- Ram only – no data at rest

Audit-Ready by Default

- Every verification and retrieval action is automatically logged to the ticket

Setup in seconds

- integration with existing systems



Why MSPs Choose Traceless

TRACELESS

Stops Vishing Attacks

Eliminates social engineering at the exact moment of risk during help desk interactions

Removes Plaintext Exposure

No more sensitive data lingering in tickets, emails, or chat systems

Saves Time

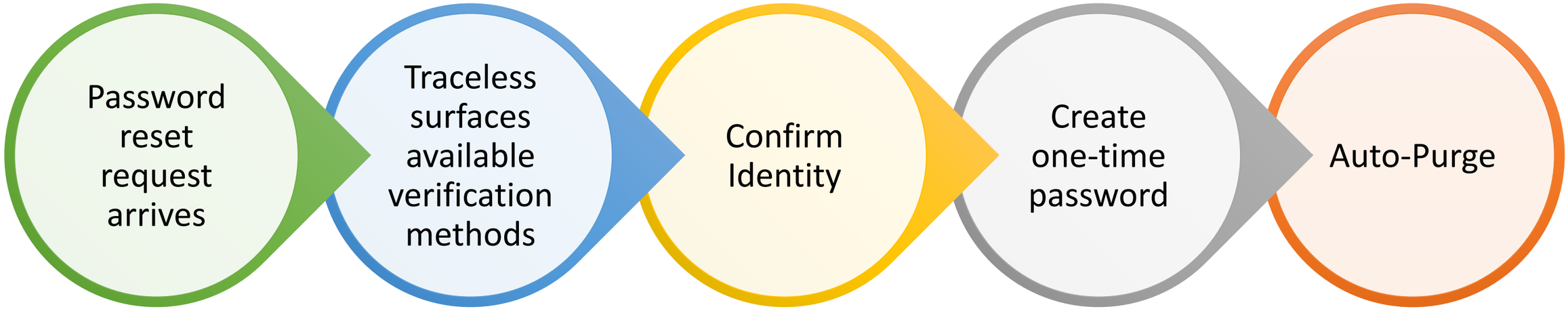
Early partner feedback shows ~90 seconds saved per ticket with REWST automation

Automation-Ready

API integration plus Roost automations for streamlined workflows

5 Simple Steps

TRACELESS



- Open ConnectWise Ticket
- Open MFA Tab
- Push Authenticator (or other) validation, confirm and log
- One time link shared via SMS/email
- Link expires after use, reterival logged

One click to verify, two clicks to share—always logged

Identity Verification: In-Workflow Security

Multiple MFA Options

- MS Authenticator, DUO, OKTA, SMS, email or through the ticket.

Policy Controls

Enable/disable methods and enforce strongest available authentication

Directory Integration

365/Azure integration automatically surfaces best-fit MFA methods

If customer’s authenticator isn’t available, Traceless lets you verify with another approved channel—all logged.

TRACELESS

Ephemeral Sharing

One time links

- Share any text such as passwords, API Keys and files up to 200GB with expiring links (30 mins to 7 days)

White-Label Experience

- Your MSP branding and contact details in all communications

Bi-Directional Security

- Request data/files from end users with automatic MFA gating

No data storage

- After retrieval, only a dead-link remains – no data stored at rest

Seamless Integration & Automation

PSA integration in minutes w/API credentials

Works with:

- ServiceNow, Zendesk, Halo PSA, Autotask, Jira, ConnectWise Manage, Slack and Teams

Rich reporting data to help MSPs enforce verification for sensitive tickets



TRACELESS

Enterprise-Grade Security

SOC2 Type2

As a Cyber Security company and we take our own security seriously.

Zero-Trust Aligned

Zero trust communication for your help desk, data and identity.

Competitive Advantage

Show your customers how serious you take today’s most prevalent threats.

TRACELESS

14

Day Free Trial

Unlimited access, no contracts required

$15

Per User/Month

Minimum 5 users, volume pricing available

2

Weeks to Value

Pilot proves ROI, adoption is immediate