Verified Trust at Scale

Modern Identity Recovery, Helpdesk Defence & Workforce Assurance in the Age of AI-Driven Social Engineering

trevonix

Executive Summary

Identity is now the most critical security control in the modern enterprise. While MFA, SSO, and adaptive access have strengthened login defences, attackers have shifted to a softer target: **identity recovery, helpdesk processes, and the human layer of trust.**

- Attackers increasingly bypass login security by compromising helpdesks, recovery workflows, and human operators.
- AI-generated deepfake voices and multi-channel impersonation attacks have reduced the cost and effort of targeted social engineering by up to 99%.
- MFA fatigue, SIM swapping, and vishing allow attackers to trick support staff into resetting credentials or disabling MFA.
- Even the strongest MFA is irrelevant if helpdesks and recovery processes can be socially engineered.

This white paper outlines a blueprint for securing identity across the full lifecycle from onboarding to recovery, privileged access, and continuous monitoring, integrating:

- Ping Identity's Verified Recovery Playbook, helpdesk security research, verifiable credentials, identity orchestration, and ITDR capabilities, and
- Trevonix's role as a Ping Identity Elite Delivery Partner, with:

  1 - 100+ Ping Identity certifications

  2 - Hundreds of successful Ping Identity deployments delivered

  3 - Accelerators developed for faster time-to-value

  4 - End-to-end lifecycle support through the Trevonix IMPACT Programme

Together, Ping Identity + Trevonix provide organisations with a comprehensive, scalable identity-centric defence model.

trevonix

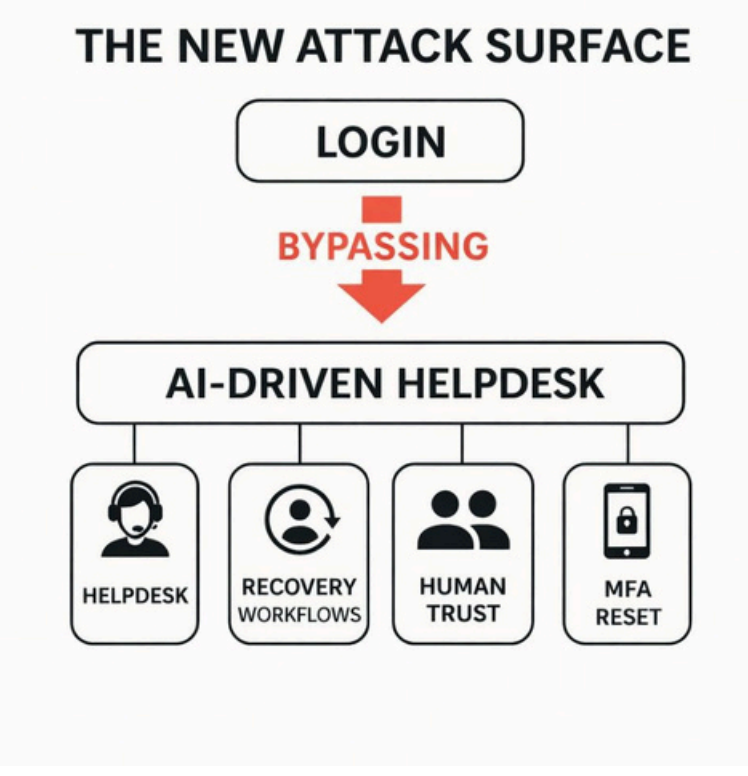
1. The New Attack Surface: Helpdesk, Recovery & Human Trust

1.1 Why Attackers Now Target Recovery

Ping Identity's research shows that helpdesks have become the front door for attackers. As authentication hardens, adversaries pivot to recovery workflows that rely on:

- Human verification
- Manual decision-making
- Inconsistent operational processes
- Weak signals like SMS OTP or directory lookups
- Outsourced support teams without contextual knowledge

This "trust gap" has fuelled a surge in high-impact breaches initiated by impersonation, urgent pretexts, and deepfake voices.



trevonix

1.2 Deepfakes and Multi-Vector Social Engineering

Attackers blend communication channels: email, chat, phone, and video, while using AI to clone voices, generate synthetic identities, and spoof high-trust individuals.

Ping Identity research calls this multi-vector deception, drastically lowering the cost of personalised attacks.

AI-DRIVEN SOCIAL ENGINEERING LIFECYCLE

1.3 Why Helpdesk Agents Are Vulnerable

From Ping Identity Securing the Human Perimeter brief:

- High workload and speed-focused metrics
- Lack of personal familiarity with end-users
- Distributed/remote support centers
- Burnout and alert fatigue
- Training gaps around social engineering and deepfakes

These conditions create an ideal environment for exploitation.

2. Ping Identity's Six Principles of Verified Recovery — Activated by Trevonix

Ping Identity's Verified Recovery & Re-Onboarding Playbook provides a modern blueprint for secure recovery processes. Trevonix operationalises and deploys these principles across large-scale enterprise environments.

2.1 No Verification, No Reset

High-assurance verification (government ID, biometric, liveness) must be mandatory before any MFA reset or account recovery.

Trevonix accelerator:
Pre-built PingOne DaVinci flows ensure no helpdesk agent can bypass verification.

2.2 Proof Before Privilege

Privileged account recovery requires both system assurance and human approval.

Trevonix accelerator:
Dual-control privilege recovery workflows, including manager attestation.

2.3 Automation Over Discretion

Helpdesk discretion is eliminated by orchestration-driven playbooks.

Trevonix accelerator:
ITSM gating patterns that trigger verified Ping Identity flows automatically.

2.4 Issue and Reuse Trust (Verifiable Credentials)

After verification, a verifiable credential can be issued and reused for future re-verification.

Trevonix accelerator:
VC lifecycle management integrated with HRIS and enterprise apps.

2.5 Vendor Parity

MSPs and external helpdesk teams must follow the same verification controls as internal teams.

Trevonix accelerator:
Contractual and technical enforcement across multiple support partners.

2.6 Detect Risky Sequences

Monitor sequences such as reset MFA enrolment device registration for signs of takeover.

Trevonix accelerator:
Identity Threat Detection & Response (ITDR) rules integrated into SIEM.

trevonix

3. Trevonix IMPACT Programme — Strategy to Operations

Trevonix delivers end-to-end identity transformation aligned with Ping Identity verified trust model.

3.1 Strategy & Architecture

- Identity maturity assessments
- IAM roadmap development
- Zero Trust & future-state architectures
- AI for Identity / Identity for AI

3.2 Solution Delivery (Ping Identity Elite Partner)

- 100+ Ping Identity certifications
- 100s of deployments across enterprise IAM
- DaVinci orchestration patterns
- Pre-built accelerators for onboarding, recovery, and re-verification
- Change management & enterprise rollout programmes

3.3 Managed Services

- Cloud & hybrid identity operations
- DevSecOps-enabled IAM engineering
- Application Onboarding Factory
- Upgrades, enhancements & continuous improvement

This complete lifecycle approach ensures sustainable identity operations, not just initial deployment.

trevonix

4. Joint Ping Identity + Trevonix Identity-Centric Defence Model

Aligned with Ping Identity's identity-centric, layered defence architecture.

Layer 1 — Verification & Assurance

- Biometric/liveness verification
- Government ID verification
- Trusted device checks
- Passkey and verifiable credential enrolment

Layer 2 — Controlled Identity Workflows

- Peer-based recovery
- Dual-control mechanisms
- Privilege re-verification flows
- Automated fallback escalation

Layer 3 — Monitoring, Detection, and Response

- ITDR rules for anomaly detection
- Sequence-based detection
- Impossible travel and device risk signals
- Automated step-up authentication

trevonix

5. Enterprise Playbooks: Proactive and Reactive

5.1 Proactive Identity Re-Onboarding

Ping Identity's recovery playbook outlines enterprise-wide re-verification in cohesive waves after risk events or major upgrades. Trevonix operationalises this with:

- Cohort-based workforce re-verification
- Passkey and verifiable credential distribution
- Recovery flow upgrades & automation

5.2 Reactive Post-Incident Recovery

Joint Ping Identity + Trevonix approach:

- Rapid zero-trust lockdown
- 0–6–24–72-hour re-verification sequence
- Rebinding devices and MFA factors
- SIEM correlation & forensic evidence capture

6. Governance, Compliance & Auditability

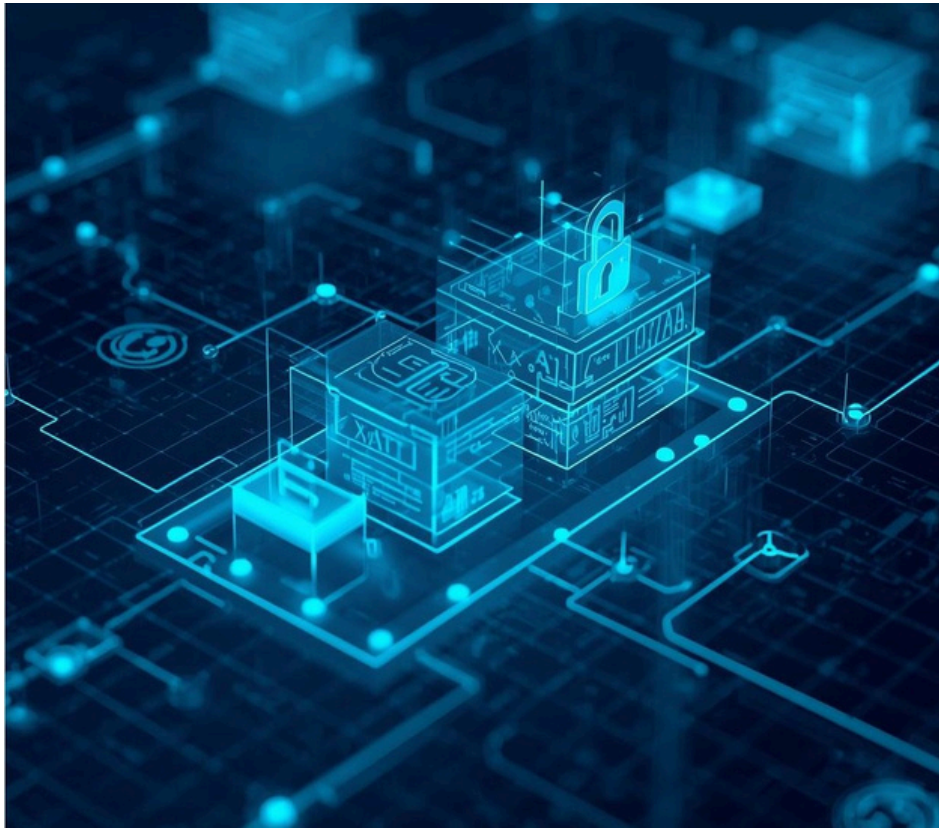
Ping Identity provides the verification and orchestration capability; Trevonix ensures organisational adoption and auditability.

Ping Identity Enables

- Verification logs
- Sequence telemetry
- Verifiable credentials
- Orchestration policy enforcement

Trevonix Adds

- RACI structures
- Identity governance forums
- Policy, process, and operational alignment
- Quarterly control validation



trevonix

7. Business Outcomes

Security Outcomes

- Reduced helpdesk compromise
- Verified recovery across all workflows
- Continuous detection of identity threat patterns

Operational Outcomes

- Automated, scalable recovery
- Lower ticket volume and handle time
- Strong, repeatable workflows for operators

Financial Outcomes

- Reduced breach likelihood
- Lower TCO via reusable credentials
- Faster time-to-value with Trevonix accelerators

User Experience Outcomes

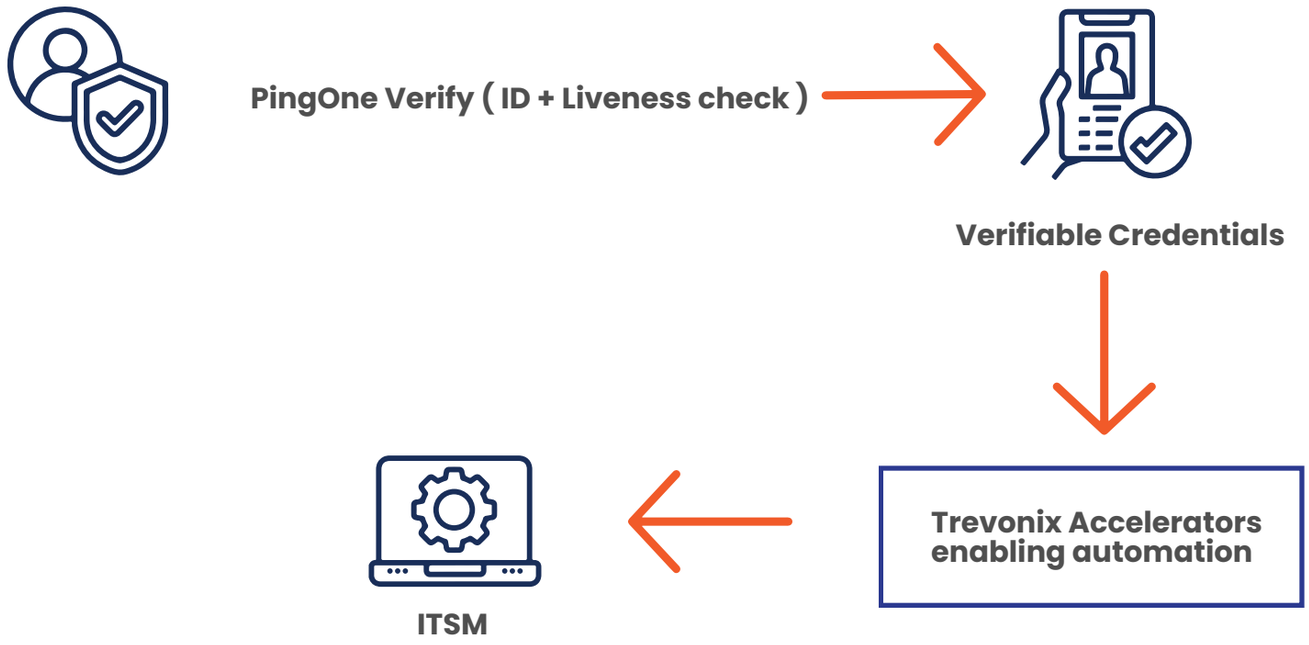
- Passwordless & frictionless workforce access
- Modern, intuitive recovery and onboarding
- Elimination of legacy OTP and knowledge-based verification

trevonix

Conclusion

- Ping Identity provides the platform to secure identity across every touchpoint where trust must be re-established.
- Trevonix delivers the strategic frameworks, accelerators, and operational depth required to deploy this at enterprise scale.

Modern Identity Recovery Workflow (PingOne DaVinci)



Together, Ping Identity + Trevonix enable organisations to:

- Eliminate recovery and helpdesk-based attack vectors
- Achieve continuous, verifiable trust
- Modernise identity operations end-to-end
- Build resilience against AI-enabled impersonation and social engineering

This partnership ensures that identity becomes the foundation of secure, seamless, and future-ready enterprise operations.

trevonix