WHITEPAPER

VERIFY0

SECURE USER VERIFICATION /SIMPLIFIED

Closing the authorization and authentication gap

in IT and customer support flows

An executive whitepaper on policy-driven user authorization and authentication for the human support channel.

AUDIENCE CIO, CISO, Head of IT, Head of Customer Operations

VERSION 1.0 / 2026-04-17

AUTHOR T34MS cybersecurity research team
Martin Adamsson
Erik Sturesson
Alexander Ostrow

CLASSIFICATION Public

TABLE OF CONTENTS

Contents

SECTION 01

Executive summary

The user authorization and authentication problem in IT and customer support is no longer an agent-script problem. It is a board-level risk topic, and it is growing. Threat actors have shifted their focus from technical exploits toward the human support channel, where an agent under time pressure can be persuaded to reset a second factor, change a registered device, or open access to a customer system without the trail of evidence that a modern control environment demands.

Verify0 Access and Verify0 Verified address this gap as two connected services. Verify0 Access is the user authorization service: it lets a support-giving organization create a clean, customer-specific support interface based on a contract that defines which customer Entra ID security group or groups contain the users entitled to receive support. The customer remains responsible for maintaining those groups through its IAM, onboarding, and offboarding processes. Verify0 Access reads eligibility live from the customer tenant and does not write to the customer tenant. Verify0 Verified is the user authentication service: it verifies an eligible user through Microsoft Entra ID authentication with MFA or SMS OTP before the support action proceeds.

The value shows up in two places a buyer can measure. First, every support-mediated action becomes a contract-defined, automatically enforced step that produces structured audit evidence, instead of an agent judgment recorded in scattered call notes. Second, because eligibility is read live from customer-managed Entra ID groups, an offboarded user loses support access the moment IAM removes them, which closes the stale-list gap that manual support contact lists leave open. The threat reporting below explains why this matters now.

This whitepaper addresses four executive questions:

- Why existing controls leave a verification gap in human support channels.
- How Verify0 closes that gap without disrupting the current operating model.
- What the deployment, integration, and compliance path looks like.
- Which outcomes a buyer should expect and how to measure them.

KEY TAKEAWAY

Manual verification scripts are difficult to prove. Generic multi-factor authentication protects the login, not every support-mediated action. Spreadsheet-based support lists drift as soon as onboarding or offboarding changes. Verify0 Access uses customer-managed Entra ID security groups to authorize who may receive support, and Verify0 Verified authenticates eligible users before sensitive support actions proceed.

SECTION 02

Why this paper now

Three forces have converged to move identity verification in support flows from a back-office concern to a strategic topic for IT and Security leadership.

Attackers target the human support channel

Public reporting and security advisories continue to show that social engineering remains a material route into organizations. The support desk is attractive because it combines identity, urgency, and delegated administrative power. Recent public reporting on UNC3944 / Scattered Spider, UNC6040-style voice phishing, and OAuth-token compromise through trusted SaaS integrations shows the same pattern: attackers exploit support processes, identity workflows, and delegated trust rather than relying only on technical exploits.

Public examples of the wider pattern:

The scenario narrative below is a composite. Named incidents are cited as public examples of the wider pattern, not as claims that Verify0 was involved in those incidents.

1) UNC3944 / Scattered Spider-style help desk social engineering, where attackers impersonate users or employees and pressure support teams into password resets, MFA changes, or other identity actions.

2) Qantas, 2025, where public reporting described a cybercriminal targeting a call center and gaining access to a third-party customer service platform containing customer records.

3) Salesloft Drift / Salesforce OAuth-token compromise, 2025, where a trusted SaaS integration exposed customer CRM and support-case data across downstream organizations. Publicly affected organizations included Cloudflare and other technology companies that disclosed Salesforce-related exposure.

4) MGM Resorts, 2023, where public reporting described a Scattered Spider actor using details from a public profile to impersonate an employee to the internal IT help desk and trigger a credential and MFA reset. The intrusion led to a ransomware attack that MGM disclosed as causing significant operational disruption and a financial impact of roughly USD 100 million.

Regulators now require demonstrable identity controls

Three European frameworks in particular raise the bar for verification controls in human channels. Each one translates into concrete technical and procedural requirements that a policy-as-code verification layer is uniquely positioned to satisfy.

- GDPR: lawful basis, proportionality, and evidence of consent for identity data.
- NIS2: identity and access management controls for essential and important entities.
- DORA: ICT operational resilience for financial services, including third-party risk.

Support cost pressure and CX expectations collide

At the same time, IT and customer operations leaders are under pressure to reduce average handling time (AHT), expand self-service, and improve customer satisfaction scores. Every manual verification step adds friction. A well-designed verification layer can resolve the apparent conflict: it raises the security bar while reducing the variance and duration of the verification step.

WHY NOW

The question is no longer whether to standardize support authorization and authentication. The question is whether to standardize it now, ahead of the next incident, or after it, under regulator and board scrutiny.

SECTION 03

The problem, in depth

Three mechanisms explain why verification gaps persist in even mature IT and support organizations. Each one is rational at the individual level, and collectively they produce an outcome that neither security nor operations leadership would choose on purpose.

Mechanism 1: verification as a script, not a control

Most organizations treat identity verification as a set of instructions in a knowledge base article. The quality of the outcome depends on the agent, the time of day, the complexity of the case, and the caller's emotional pressure. This is the textbook definition of a non-deterministic control.

Mechanism 2: the wrong question is asked

Knowledge-based authentication (date of birth, home address, last four digits of something) was built for an era before social media and before commercial data brokers. Most of this information is now cheap to acquire. Asking questions that a determined attacker can answer in 15 minutes of open-source research is not verification. It is theater.

Mechanism 3: no audit trail that the auditor accepts

Even when agents follow the script and ask the right questions, the evidence typically lives in call recordings, chat transcripts, or agent notes. These artifacts are difficult to correlate with a specific change, require manual labor to retrieve during an audit, and in many jurisdictions have retention rules that make them unsuitable as long-term compliance evidence.

SHORT VERSION

Non-deterministic control, wrong questions, and untraceable evidence. Any of the three is enough to fail an audit. Most organizations fail on all three.

Scenario: an attacker calls the help desk

A composite narrative, drawn from publicly reported incidents. Details changed to protect sources.

1) Attacker pretext and preparation. The attacker begins with research, not malware. They identify a large organization with a busy service desk, collect employee details from public profiles and prior breaches, and learn the vocabulary of the internal environment: the identity provider, remote access tool, ticketing system, and support escalation paths. Public reporting on UNC3944 and Scattered Spider describes this pattern: social engineering targets support teams that can modify identity settings or provide security information.

2) Initial contact and emotional pressure. The call sounds routine. The attacker claims to be an employee or contractor locked out during a business-critical activity. They add pressure: a customer escalation is waiting, a manager is chasing them, travel explains why the usual device is unavailable, and every minute of delay is costly. Weak knowledge-based questions are answered confidently because the data is already available from open sources, data brokers, or old records.

3) The exact moment the control failed. The failure occurs when the agent accepts a convincing story as evidence and performs the change without an independent verification event. The agent resets a password, adds a new MFA method, changes a recovery number, creates temporary access, or opens a live access path before the legitimate user has completed a policy-mandated verification through an approved channel.

4) What the attacker gained. The attacker now has a valid identity path. Depending on the environment, that can mean SSO access, an attacker-controlled MFA factor, access to collaboration tools, internal documentation, privileged workflows, customer records, or support-mediated access to customer systems. In extortion cases, this foothold can cause data theft, operational disruption, and ransomware pressure.

5) What standardized verification step would have changed. With Verify0 Verified, the agent does not decide whether the caller sounds credible. The workflow invokes the required verification policy and

records the result. The challenge is delivered to the legitimate user's registered Microsoft Entra ID account, so a caller impersonating that user but not in control of the account cannot complete it, and the support action does not proceed. With Verify0 Access, the downstream action or live link is permitted only after verification succeeds, is scoped to the ticket, expires according to policy, and leaves structured evidence of requester, target, method, timestamp, decision, and result. This logic holds when the genuine user can authenticate. The harder lost-device and account-recovery case is addressed separately (see the note in section 06).

SECTION 04

Why existing controls fall short

Most organizations have invested heavily in identity. The question is not whether controls exist, but whether they reach the support flow. Three common patterns illustrate the gap.

Comparative view

Control	What it protects	Where it fails
Manual scripts and KBAs	Nothing deterministically. Assumes the agent behaves consistently.	Agent variance, social pressure, data broker leakage, unprovable to the auditor.
Generic MFA on login	The moment the user signs in.	Not triggered on account recovery, MFA reset, device swap, or delegated actions.
Self-service portals with KBAs	The login step.	Does not protect sensitive post-login actions; portal KBAs share the same data-broker weakness.
Callback to a registered number	Low-risk identity confirmation.	Number is often the attack vector; offers no audit trail beyond the call log.
Verify0 Access + Verify0 Verified	The eligible support population and the verification step before support proceeds. Customer-managed Entra ID groups define who may receive support; Microsoft Entra ID authentication with MFA or SMS OTP verifies the eligible user.	Requires a customer contract defining the relevant Entra ID security groups; requires customer ownership of group membership and governance of verification methods.

THE GAP

Login-time controls and manual scripts were designed for a threat model in which the attacker is outside the front door. Today, the attacker is on the phone pretending to be the owner of the key.

SECTION 05

Introducing Verify0 Verified and Verify0 Access

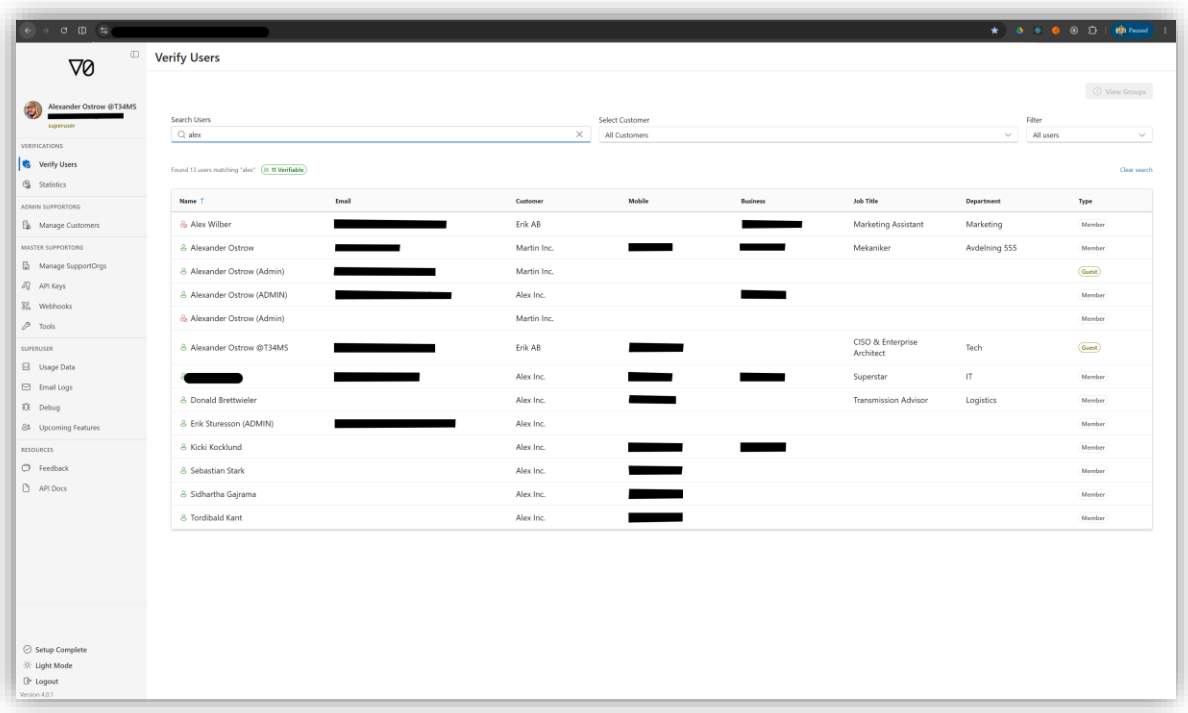


Figure 1 Verify0 web user interface

Category and positioning

Verify0 Access and Verify0 Verified form a policy-driven control layer for human support flows.

Verify0 Access answers the authorization question: which users are entitled to receive support under the customer contract? It retrieves the eligible support population from customer-managed Microsoft Entra ID security groups and presents that population to the support-giving organization through the Verify0 web interface or through API-based workflows.

Verify0 Verified answers the authentication question: can the eligible user complete the required verification step before the support action proceeds? Verification uses Microsoft Entra ID authentication and can be configured to require a specific Microsoft Entra authentication strength. Verify0 also adheres to the end customer's MFA and Conditional Access configuration. SMS OTP can be used where customer policy permits a lower-assurance fallback.

Access is the authorization foundation. Verified is the authentication layer. A user must be included in the contracted customer security group or groups before Verify0 Verified can authenticate that user for a support-mediated action.

Design principles

- Contract-driven access: support eligibility is defined through the customer contract and customer-managed Microsoft Entra ID security groups, not through manually exchanged spreadsheets or informal contact lists.
- Live eligibility: Verify0 Access checks eligibility against the customer tenant rather than relying on stale exports. When the customer removes a user from the relevant group, that user should no longer be eligible for support through Verify0 Access.
- Verification where it matters: Verify0 Verified introduces a policy-controlled verification step before sensitive support actions proceed.
- Authentication-strength aware: Verify0 can be configured to require a Microsoft Entra authentication strength, while also respecting the customer's own MFA and Conditional Access configuration.
- API first: Verify0 can be used standalone through the web interface, deep-linked from existing workflows, or integrated through API calls and webhook callbacks.
- Evidence by default: completed eligibility checks, verification attempts, outcomes, timestamps, requester context, and correlation identifiers are recorded as structured operational evidence.
- Low data collection: Verify0 does not collect government identity documents or biometrics in the standard Access and Verified flow. It uses the customer's existing Microsoft Entra ID context and configured verification methods.
- Operable in regulated environments: Verify0 is Azure-hosted. For Swedish customers, the default deployment region is Sweden Central. For German customers, deployments can be placed in Germany. Other Azure regions are available where commercially agreed. The preferred posture is to deploy close to the customer, with EU data residency as the primary default.

Microsoft Entra ID dependency

The current Verify0 Access and Verify0 Verified model depends on Microsoft Entra ID. Access uses customer-managed Entra ID security groups as the source of support eligibility. Verified uses Microsoft Entra ID authentication as the primary verification route and can be configured to require a specific Microsoft Entra authentication strength. Verify0 also adheres to the customer's MFA and Conditional Access configuration.

Organizations that do not use Microsoft Entra ID, or that need Okta, Google Workspace, on-premises Active Directory, national eID, biometric proofing, or document-based identity proofing, should treat those requirements as separate scope items until explicitly contracted and confirmed as supported. Google directory support is on the product roadmap, but it is not a current product claim in this version of the whitepaper.

Scope

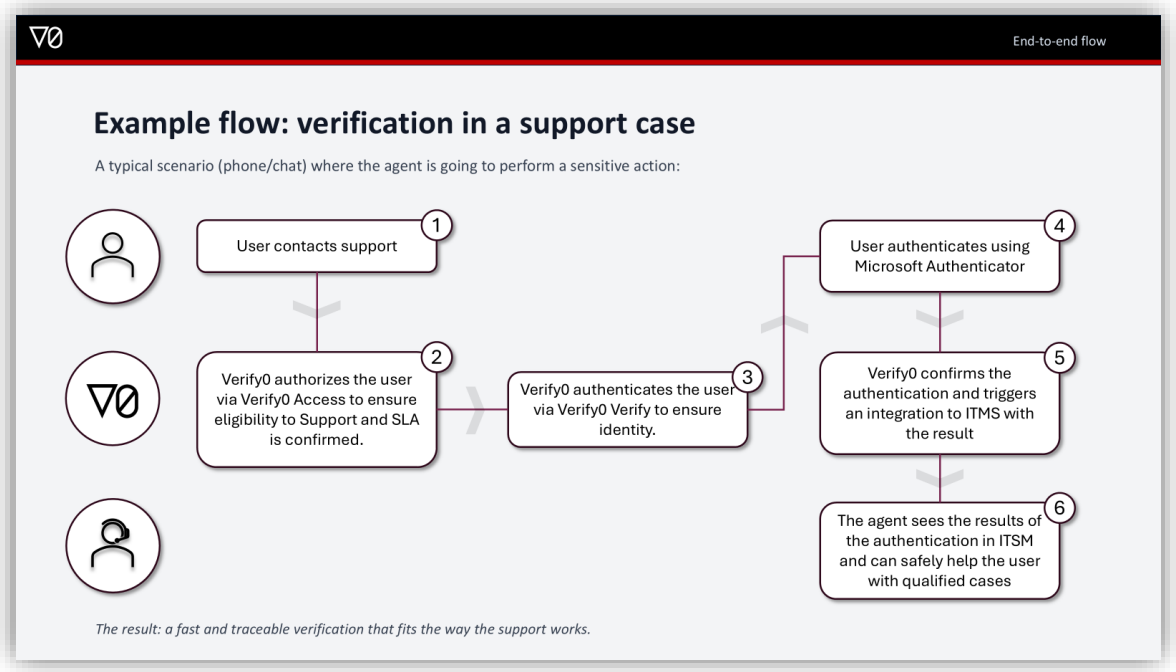
In scope for Verify0 Access: contract-based support eligibility using customer-managed Microsoft Entra ID security groups, live eligibility lookup, support-user search, administrator export where permitted, and structured evidence for authorization decisions.

In scope for Verify0 Verified: authentication of eligible users using Microsoft Entra ID authentication, optional Microsoft Entra authentication strength requirements, the customer's MFA and Conditional Access configuration, and SMS OTP where customer policy permits, with structured evidence attached to the support workflow.

Out of scope unless separately contracted: primary authentication, IAM lifecycle ownership, account proofing for users who cannot access any registered factor, privileged access management, remote monitoring and management, contact-center replacement, ITSM replacement, CRM replacement, SIEM replacement, and ownership of the customer's Entra ID group governance.

SECTION 06

How Verify0 works



End-to-end flow

01 Trigger

A user contacts support. The agent opens Verify0, or an integrated support workflow, to check whether the requester belongs to the customer's contracted support population.

02 Access eligibility

Verify0 Access checks the relevant customer contract and retrieves eligibility from the customer's Microsoft Entra ID security group or groups. The customer remains responsible for group membership through its IAM, onboarding, and offboarding processes.

03 Eligibility decision

If the user is enabled in the customer tenant and present in at least one contracted security group, the user is marked eligible for the configured support flow. If the user is disabled or outside the contracted groups, the user is marked un-verifiable and the support action should be denied or escalated according to customer policy.

04 Verification challenge

If the user is eligible, Verify0 Verified initiates the configured verification method. The primary route is Microsoft Entra ID authentication. Verify0 can be configured to require a specific Microsoft Entra

authentication strength, and it adheres to the end customer's MFA and Conditional Access configuration. SMS OTP may be used as a lower-assurance fallback only where the customer policy permits and a phone number is present.

05 User response

The user completes the Microsoft Entra ID authentication flow, including the required authentication strength where configured, or enters the SMS OTP where SMS fallback is permitted. Verify0 validates the result and updates the session status with timestamp, method identifier, requester context, ticket or case reference where provided, and outcome.

06 Result & Audit

Verify0 returns a structured response to the calling system, including eligibility outcome, verification result, and verification ID. The calling system can attach the verification ID to the ticket, case, or support record.

Verify0 records structured operational evidence, including eligibility checks, verification outcomes, webhook delivery records, timestamps, requester context, and PII-minimized analytics. Session records retain PII for 10 minutes and are then stripped of PII. PII-stripped webhook delivery logs and analytics/statistics are retained for eight years. Application logs are retained for 30 days. In this public version, audit logs are described as structured operational evidence, not as immutable, signed, or hash-chained records.

Lost-device and account-recovery handling

The highest-risk support scenario is the case where a user claims to have lost access to their registered device, MFA method, phone number, or account. Verify0 should not be positioned as a complete standalone account-recovery proofing service unless that capability is separately contracted.

For the standard Verify0 Access and Verify0 Verified flow, the policy should be:

1. If the eligible user can complete Microsoft Entra ID authentication with the required authentication strength and the customer's Conditional Access policy permits the session, the verification may proceed.
2. If SMS OTP is allowed by customer policy and the user can complete the SMS OTP challenge, the support action may proceed only within the assurance level and risk boundary agreed with the customer.
3. If the eligible user cannot complete the configured Entra authentication or approved SMS OTP fallback, Verify0 should return a failed or incomplete verification result.
4. The support action should not proceed on agent judgment alone.
5. The case should be escalated to the recovery process agreed in the contract between the support-giving organization and the customer organization. That process may include manager

approval, customer security-team approval, existing IAM recovery workflow, in-person verification, or another contractually approved proofing step.

6. The escalation decision, failed verification result, requester context, and ticket or case reference should be recorded as evidence.

This design prevents Verify0 from becoming a shortcut around the customer's own account-recovery controls. It also makes the boundary clear: Verify0 standardizes support authorization and authentication for eligible users who can complete an approved verification method. Full account recovery for users with no working factor follows the agreed contractual recovery process between the support-giving organization and the customer.

Policy model

Verify0 enforces eligibility before verification. The current Access model is contract-driven: the support-giving organization defines, per customer contract, which customer Microsoft Entra ID security group or groups contain users entitled to receive support. The customer is responsible for keeping that population current through IAM, onboarding, and offboarding.

Verify0 resolves eligibility live against the customer tenant to reduce stale-list risk. Verify0 Verified can authenticate only users who are included in the contracted groups and are not disabled.

Support-giving administrators can export the eligible list where permitted. Support-giving users can search the customer population and check eligibility. Users outside the contracted groups, disabled users, and users who cannot complete an approved verification method are marked un-verifiable and should be denied or escalated according to policy.

Example contract and verification policy

Example contract and verification policy

Customer	Support-giving organization
ACME Nordic AB	Managed Services Partner AB

Contracted Microsoft Entra ID security groups	ACME-Support-Eligible-Users ACME-VIP-Support-Eligible-Users
Authorization rule	A user must be enabled in the customer tenant and present in at least one contracted security group.
Primary authentication method	Microsoft Entra ID authentication.
Authentication strength	Required where configured by the customer or support-giving organization.
Fallback authentication method	SMS OTP, only where customer policy permits and a phone number is present in the customer Entra ID account.
Lost-device behavior	Failed or incomplete verification, followed by escalation to the recovery process agreed in the contract between the support-giving organization and the customer.
Decision behavior	users outside the contracted groups, disabled users, and users who cannot complete verification are marked un-verifiable. Recommended action is deny or escalate.
Logging	session records retain PII for 10 minutes and are then PII-stripped. PII-stripped delivery and analytics records are retained for eight years.

SECTION 07

Channel landscape

Verify0 Verified currently focuses on two verification routes: Microsoft Entra ID authentication and SMS OTP. The right choice depends on assurance requirements, user availability, customer policy, and the risk of the support action.

Supported channels

Microsoft Entra ID authentication

This is the preferred route where the customer environment supports Microsoft-based verification. Verify0 can be configured to require a specific Microsoft Entra authentication strength and also adheres to the customer's MFA and Conditional Access configuration. For higher-risk support actions, customers should use stronger Entra authentication methods and should consider enforcing phishing-resistant authentication where available.

SMS OTP

SMS OTP is widely available and operationally useful, but it is a lower-assurance method. SMS is not phishing-resistant and is exposed to SIM swap, interception, number-porting, and social-engineering risks. SMS OTP should be treated as a convenience fallback, gated by customer policy, not as the primary control for high-risk support actions.

Roadmap channels

Google directory support is on the product roadmap. It should not be presented as a current production capability in this version of the whitepaper. Other identity providers, national eID methods, biometric proofing, document-based identity proofing, and non-Entra directory sources should be treated as roadmap or separately contracted scope unless explicitly confirmed.

Selecting the right channel

Channel selection should follow four rules:

1. Proportional to the risk of the support action.
2. Available to the eligible user.
3. Approved in the customer configuration.
4. Recorded in the audit evidence.

For identity-sensitive or higher-risk actions, Microsoft Entra ID authentication with an appropriate authentication strength should be the default. For the highest-risk actions, customers should prefer phishing-resistant methods where available. SMS OTP should be reserved for lower-risk actions or exceptional fallback cases, and the lower assurance level should be visible in the evidence record.

Operational note

SMS OTP remains operationally important because it is broadly available. It should not be oversold. The commercial message is stronger when Verify0 is explicit: Microsoft Entra ID authentication is the preferred route, authentication strength can be required where configured, SMS OTP is a controlled fallback and lost-device recovery must follow the contractually agreed process between the support-giving organization and the customer.

OPERATIONAL NOTE

SMS OTP remains operationally important because it is broadly available. It should not be oversold. The commercial message is stronger when Verify0 is explicit: Microsoft Entra ID authentication is the preferred route, authentication strength can be required where configured, SMS OTP is a controlled fallback and lost-device recovery must follow the contractually agreed process between the support-giving organization and the customer.

SECTION 08

Integration model

Verify0 is designed to give the support-giving organization a clean interface to each customer's eligible support population, while still fitting into the systems support teams already run.

Integration points

- ITSM integration: Verify0 exposes API endpoints and webhook callbacks that can be invoked from any system able to call APIs. The agent can check Access eligibility and launch Verified from the support workflow. Verify0 can also be used standalone through the web UI, through deep links from another platform, through webhook writeback, or through API integration with webhook writeback.
- CRM integration: the same API and webhook pattern applies to CRM platforms when customer support or case management workflows need eligibility checks and verification evidence. The integration principle is platform-neutral: any system that can access APIs can invoke Verify0.
- Identity provider: Microsoft Entra ID is the source for customer security groups used by Verify0 Access. The customer owns group population through IAM, onboarding, and offboarding. Verify0 Verified uses Microsoft Entra ID authentication with MFA where configured.
- SIEM and observability: Verify0 writes structured operational logs, webhook delivery records, and PII-stripped analytics. SIEM integration should be handled through the agreed deployment and integration pattern for the customer environment.
- Autotask is supported in live deployments, but this public paper positions Verify0 primarily as API-first and webhook-first rather than listing packaged connectors as the main value proposition.

Typical integration pattern

The default pattern is a synchronous API call to create the verification or access session and an asynchronous webhook result when the user completes, fails, abandons, times out, or when an authorization decision expires. The calling system can attach the Verify0 session ID to a ticket or case. If the customer passes a ticket ID or case ID as an allowed incoming parameter, the webhook payload can carry that value back to the calling system.

Time to first integration

Standalone Verify0 web UI: setup can be completed in hours and often during a 30-minute onboarding call, assuming Entra consent and customer group selection are ready.

API and webhook integration: typically, around two weeks when technical resources are available.

ITSM integration: typically, around two weeks when the support workflow, API access, and webhook writeback requirements are clear.

Fast-path deployment: a prepared organization can go live in 24 hours. A more typical organization goes live in two to three weeks when the required customer and support-giving resources are available.

SECTION 09

Security architecture

Confidentiality

- **TLS 1.2 minimum for all external traffic.**
- Secrets are stored through Azure Key Vault references and environment-specific vaults. Cosmos DB uses Microsoft-managed encryption at rest. T34MS maintains a key rotation process.
- Tenant IDs are explicitly separated in the backend design; Cosmos DB containers are partitioned by tenant-relevant keys. Single-tenant deployments are available when commercially agreed.
- No HSM-backed customer key claim is made in this public whitepaper. Key rotation is handled through an internal T34MS process.

Integrity

- Structured audit events are written to Cosmos DB and Application Insights. The public product claim is structured operational evidence, not immutable, signed, or hash-chained logging.
- **Webhook delivery records stored for operational evidence. Statistics records are written through a whitelist model that excludes PII-heavy fields.**
- Retention model: verification session records are retained for 10 minutes and then stripped of PII; Access eligibility checks are performed on demand and are not retained as PII-bearing records; PII-stripped webhook delivery records and analytics/statistics are retained for eight years; application logs are retained for 30 days.

Availability and resilience

- Backend Container Apps are configured with minimum and maximum replicas, with startup, readiness, and liveness probes. Azure region is deployment-specific: Sweden Central is the default for Swedish customers, Germany can be used for German customers, and other Azure regions are available when agreed. No public SLA, RTO, or RPO commitment is stated in this version.
- Microsoft Entra ID authentication with MFA is promoted as the primary verification method. SMS OTP is available as fallback when policy permits and when the user has a phone number provisioned in the customer Entra ID account.
- Each customer deployment has its own status page. Incident communication is handled through contractual notification, email, and the relevant deployment status page.

Identity and access control within Verify0

- Role-based access for agents, administrators, auditors, and read-only observers.
- The Verify0 admin UI supports SAML SSO and Microsoft Entra ID login. API credentials are scoped and can be used for programmatic access.

- MFA enforcement for the support-giving organization depends on that organization's identity policies. Verify0 supports SSO-based administration but does not claim to override the support-giving organization's MFA policy in this public paper.
- Current roles are support-giving admin, support-giving user, and API credentials. Segregation of duties for configuration changes is not claimed in this version.

SECTION 10

Compliance alignment

The value of Verify0 to a CISO, DPO, or auditor is not only the authorization or authentication decision itself. The value is the evidence trail around that decision: who requested support, which customer contract applied, whether the user was part of the contracted support population, which verification method was used, what the result was, when it happened, and which ticket or case it related to.

This section is a practical control-alignment summary, not a legal opinion.

GDPR

Verify0 is designed for a processor-based operating model.

In the relationship between T34MS and the support-giving organization, the support-giving organization is normally the controller and T34MS is normally the processor.

In flows where the supported customer's user data is processed, the supported customer may be the controller, the support-giving organization may be the processor, and T34MS may act as sub-processor. The exact role allocation should be confirmed in the contract, DPA, and customer-specific data-flow documentation.

Personal data categories may include user profile data, email address, phone number where present, tenant and organization identifiers, group membership information, eligibility result, authentication method, authentication strength requirement where configured, timestamp, ticket or case reference where provided, and result status.

T34MS maintains a DPA template, a sub-processor list, and a data subject request process. Session records retain PII for 10 minutes and are then stripped of PII. Longer-term operational records are retained only in PII-stripped form.

Microsoft Graph permissions and data minimization

Verify0 requires the following Microsoft Graph permissions from the end customer.

Backend App, application permissions:

- Group.Read.All
- GroupMember.Read.All
- Mail.Send
- User.Read.All

SPA SSO App, delegated permissions:

- email
- offline_access

- openid
- profile

These permissions allow Verify0 to read the customer directory information needed to determine support eligibility, read group membership, support the sign-in experience, and send required mail where applicable. Verify0 should request only the permissions required for the agreed deployment and should describe those permissions clearly in customer-facing security documentation.

The commercial message should be least-privilege by design: Verify0 reads the data required to determine support eligibility and verification status. It does not own customer IAM lifecycle processes and does not write group membership back to the customer tenant in the standard Access model.

NIS2 and DORA

NIS2, Article 21, cybersecurity risk-management measures: Verify0 supports access control, identity verification, incident evidence, and secure support processes by replacing manual lists and scripts with live Entra-based authorization and structured authentication records.

NIS2, Article 21, access control and asset management: Verify0 Access ties support eligibility to customer-managed Microsoft Entra ID security groups, so onboarding and offboarding changes are reflected through the customer IAM process.

DORA, ICT risk management: Verify0 provides a repeatable control for support-mediated actions, including structured evidence, role-based access, scoped API credentials, and deployment-specific monitoring.

DORA, third-party ICT risk: Verify0 reduces out-of-band spreadsheet transfer and clarifies responsibility between supported customer, support-giving organization, and T34MS.

ISO 27001, SOC 2, TISAX

T34MS does not claim ISO 27001, SOC 2, or TISAX certification in this version of the whitepaper. ISO 27001 is on the roadmap for the 2026/2027 period. The product is designed to support customer control mapping through structured authorization, authentication, and audit evidence, but certification claims should only be made when an attestation is available.

SECTION 11

Deployment options

SaaS

Verify0 is offered as a SaaS service. Deployments run on Azure and can be placed in the Azure region agreed with the customer. Sweden Central is the default for Swedish customers, German customers can be deployed in Germany, and the preferred posture is to deploy close to the customer with EU data residency as the primary default.

SaaS deployment and regional coverage

Verify0 is currently offered as SaaS. Each customer has its own deployment, and each deployment has its own status page. Swedish customers default to Azure Sweden Central. German customers can be deployed in Germany. Other Azure regions are available when commercially agreed, although the primary data residency posture is EU-first. No public SLA, RTO, or RPO commitment is stated in this version.

SECTION 12

Implementation methodology

Verify0 deployments follow a three-phase approach. The objective is to de-risk the investment by proving value in a narrow scope before expanding.

Phase 1: discovery workshop

Goal: identify one or two high-value support actions, confirm user population and identity provider context, agree supported verification channels, define webhook/ticket correlation needs, and set pilot metrics. Typical duration: approximately one hour.

Phase 2: pilot

Goal: deploy Verify0 for a narrow support workflow, integrate through API and webhook where needed, verify Entra lookup and eligibility behavior, test selected channels, and capture baseline metrics. Typical duration: approximately one week.

Phase 3: rollout

Goal: expand by action and support team, operationalize webhook monitoring, review audit evidence, and establish a regular review cadence for verification coverage and outcomes. Typical duration: approximately one month.

Indicative RACI

Activity	R / A owner	Consulted
Use-case selection	Support-giving org	Supported customer, T34MS
Entra group population	Supported customer	Support-giving org, T34MS
Contract configuration	Support-giving org	Supported customer, T34MS
Policy design	Support-giving org, T34MS	Supported customer
Technical integration	Support-giving org, T34MS	Supported customer
Pilot execution	Support-giving org	Supported customer, T34MS
Audit evidence reviews	Supported customer, support-giving org	T34MS
Production ops	T34MS (SaaS)	Support-giving org, supported customer

SECTION 13

Measuring outcomes

Measure Verify0 the same way you measure the rest of the IT portfolio: risk, efficiency, compliance, and experience. Define the targets in the discovery workshop, measure during the pilot, and hold them against the baseline at rollout.

Suggested KPI framework

Dimension	Metric	Target / benchmark
Risk	Incidents involving support-mediated account takeover	Measured during pilot. Use incident trend and blocked or escalated attempts as the baseline, not an invented benchmark.
Efficiency	Average handling time on sensitive actions	Measured during pilot. Compare sensitive-action handling time before and after Verify0.
Compliance	Evidence gathering effort per audit cycle	Measured during pilot. Track time to retrieve structured evidence compared with call recordings, notes, or manual ticket review.
Experience	Customer satisfaction with verified flows	Measured during pilot. Track completion rate, abandonment, and support feedback.
Adoption	Share of sensitive actions covered by policy	Measured during pilot. Target coverage should be agreed per support action and customer risk tier.

ROI framing for the business case

Because pricing and support volumes vary by customer, this paper uses a variable-based ROI model rather than published prices.

Baseline inputs: number of supported customers, number of eligible users, monthly sensitive support actions, manual eligibility-list maintenance effort, average handling time for identity-sensitive actions, audit evidence retrieval effort, and estimated exposure from support-mediated account takeover.

Investment inputs: Verify0 service fee, onboarding effort, integration effort if API/webhook or ITSM writeback is used, and internal process-change effort.

Reduced cost categories: elimination of spreadsheet-based support population exchange, lower manual verification variance, faster evidence retrieval, fewer escalations caused by unclear eligibility, and reduced probability or impact of support-mediated identity compromise.

CFO model: calculate the 24-month net benefit as avoided manual effort plus avoided audit effort plus risk-adjusted avoided incident cost, minus service and implementation cost. Keep all assumptions visible so the model can be re-run with the customer's own figures.

Illustrative example (assumptions only, not a price list). Take a support-giving organization with 100 supported customers and 50 000 eligible users, handling 400 identity-sensitive support actions per month. Assume manual eligibility-list upkeep of 10 hours per month at EUR 60 per hour (about EUR 7 200 per year), and that structured evidence cuts audit-evidence retrieval by 40 hours per audit cycle (about EUR 2 400 per cycle). Assume Verify0 removes most of the manual upkeep and trims two minutes from each sensitive action. On the risk side, the IBM Cost of a Data Breach Report 2025 puts the global average breach at USD 4.44 million; if standardized verification lowers the annual probability of one support-mediated account-takeover incident by even two percentage points, the risk-adjusted avoided cost is roughly EUR 80 000 per year. Set those benefits against the Verify0 service fee, onboarding, and any integration effort. In a case like this the 24-month result is driven far more by the avoided-incident term than by the efficiency savings. Replace every figure here with the customer's own numbers before presenting.

SECTION 14

Typical deployment pattern

Anonymized deployment pattern

T34MS supports support-giving organizations that serve large customer portfolios. A typical support-giving organization may support between 50 and 200 customer organizations and a combined eligible-user population of around 50,000 users.

The common trigger is operational drift. Manually exchanged support contact lists become outdated, difficult to audit, and risky when onboarding, role changes, or offboarding happen faster than list maintenance. Verify0 Access replaces those static lists with live authorization against customer-managed Microsoft Entra ID security groups. Verify0 Verified then authenticates eligible users using Microsoft Entra ID authentication, including authentication strength requirements where configured, or SMS OTP where policy permits.

Typical starting scope

Most deployments should start with a narrow support flow rather than a broad platform rollout. Good first candidates include:

Password reset requests where the user still has an approved authentication method.

MFA-related support requests where the user can complete an approved verification step.

Customer support actions where the requester must be confirmed as part of the contracted support population.

High-value customer groups where manual support lists are currently exchanged by email or spreadsheet.

Deployment pattern

The initial deployment can start with the Verify0 web interface or a deep-linked support flow. API and webhook integration can then be added where the customer wants verification evidence attached directly to tickets or cases.

A prepared organization can complete an initial standalone deployment quickly when Entra consent, contracted groups, and support workflows are already defined. API or ITSM integration usually requires more coordination because webhook writeback, ticket correlation, operational monitoring, and error handling need to be agreed and tested.

Expected measurable outcomes

The deployment should be measured against a baseline, not against invented benchmarks. Useful pilot measures include:

- Reduction in manually exchanged support contact lists.
- Reduction in unclear eligibility escalations.
- Completion rate for verified support flows.
- Abandonment or timeout rate for verification sessions.
- Average handling time for selected sensitive support actions.
- Time required to retrieve evidence during audit or customer review.
- Number of denied, failed, or escalated attempts.

This section should be upgraded to a true case study only when T34MS can add one anonymized customer example with before-and-after metrics, deployment scope, timeframe, and an approved customer quote or attributed role.

SECTION 15

Build vs buy

Organizations with mature platform engineering sometimes consider building the verification layer in-house. The decision should be evaluated on three dimensions: differentiation, compliance, and total cost of ownership.

Differentiation

Identity verification for support flows is an undifferentiating capability. It is hygiene control, not a product feature that customers choose you for. Engineering capacity is better spent on services the customer sees.

Verify0 also sits in a different lane from identity-proofing vendors such as Nametag or Incode, and from Okta's identity-verification integrations, which confirm a person at the help desk by checking a government ID and a live biometric (selfie and liveness) and focus heavily on account recovery and self-service MFA reset. Verify0 does not collect government identity documents or biometrics. It ties eligibility to the customer's contracted Entra ID groups and reuses the user's existing Entra MFA, which keeps friction and data collection low and suits contracted B2B support populations where the user already has a working authenticator. The document-and-biometric approach is stronger for the cold account-recovery case where the user has lost access entirely; the Verify0 approach is lighter and faster for the common case where the eligible user can still authenticate. The two are better positioned as complementary than as identical.

Compliance

A home-grown verification service is subject to the same audit scrutiny as a vendor-provided one, but without the vendor's certification baseline. The compliance cost often exceeds the build cost within the first audit cycle.

Total cost of ownership

A build-versus-buy comparison should include more than application development. An internal build must cover Microsoft Graph integration, SAML SSO, role model, live eligibility lookup, MFA enforcement logic, SMS delivery, webhook delivery, audit records, PII stripping, retention logic, customer deployment operations, status communication, DPA and sub-processor documentation, support, and future authentication methods.

In-house build cost categories: product owner, backend engineering, frontend engineering, security engineering, cloud operations, compliance/legal review, SMS operations, monitoring, incident response, documentation, and ongoing maintenance.

Verify0 cost categories: service fee, onboarding, customer contract configuration, optional API/webhook or ITSM integration, and customer process rollout.

Sensitivity analysis: test the business case against delayed internal delivery, underestimated channel operations, compliance review effort, and the cost of maintaining authentication method changes over time. Without published pricing, use customer-specific variables rather than public price assumptions.

SECTION 16

Conclusion and call to action

The authorization and authentication gap in IT and customer support is real, measurable, and operationally important. It is not solved by login-time MFA alone. It is not reliably solved by manual scripts, callback routines, or spreadsheet-based customer contact lists.

Verify0 Access establishes the contracted support population directly from customer-managed Microsoft Entra ID groups. Verify0 Verified then verifies eligible users through Microsoft Entra ID authentication, including authentication strength requirements where configured, or SMS OTP where customer policy permits. Verify0 also adheres to the end customer's MFA and Conditional Access configuration and records structured evidence that can be attached to the originating workflow.

The practical value is straightforward:

- Support teams stop relying on stale lists and inconsistent identity checks.
- Customers keep ownership of their support-eligible population through their existing IAM processes.
- Security teams get a repeatable control for sensitive support actions.
- Auditors get structured evidence instead of scattered notes, call recordings, and manual reconstruction.

The recommended next step is a focused discovery workshop. The goal is to identify one or two high-value support actions, confirm the customer population and Entra group model, agree the verification policy, define pilot KPIs, and scope a narrow deployment with a measurable exit criterion.

THREE STEPS

1. Book a 45-minute discovery call.
2. Agree scope, customer groups, verification policy, and pilot KPIs.
3. Go live in a narrow pilot, then expand by support action and customer risk tier.

Contact

CONTACT

Kim Ericsson

Email: kim@t34ms.se

Phone: +46 87 6500 34

SECTION 17

About T34MS

T34MS builds security-focused services for organizations that need to make human support flows safer, cleaner, and easier to audit. Verify0 Access and Verify0 Verified help support-giving organizations replace manual customer lists and inconsistent identity checks with live Microsoft Entra-based authorization, strong user authentication, and structured evidence for support workflows. T34MS serves customers through secure Azure-based deployments and focuses on practical controls that reduce operational risk without forcing support teams to replace their existing tools.

SECTION 18

Glossary

AHT	Average Handling Time. The mean duration a support agent spends resolving a contact, from pickup to disposition.
Assurance level	A qualitative measure of how confident the system is that the user is who they claim to be. Common schemes include NIST SP 800-63 (IAL, AAL, FAL) and eIDAS (low, substantial, high).
Audit log	A structured, time-stamped event record used as operational and compliance evidence. In Verify0, structured audit events are written to Cosmos DB and Application Insights. This public version does not claim immutable, signed, or hash-chained logging.
Authentication strength	A Microsoft Entra ID control that allows an organization to define which authentication method combinations satisfy a given access requirement. In Verify0, authentication strength can be required where configured, while the end customer's MFA and Conditional Access policies continue to apply.
Conditional Access	Microsoft Entra ID policy framework used to control access based on signals such as user, device, location, risk, application, and authentication method. Verify0 adheres to the end customer's Conditional Access configuration for Microsoft Entra ID authentication flows.
DORA	Digital Operational Resilience Act, an EU regulation for ICT risk management in the financial sector.
eID	Electronic identity schemes are often issued or endorsed nationally BankID and other eID methods are roadmap items, not current product claims in this version.
Google directory support	Roadmap capability for directory-based eligibility outside Microsoft Entra ID. It is not a current production claim in this whitepaper version.
ITSM	IT Service Management. Systems used to manage IT tickets and workflows Verify0 integrates through API calls and configurable webhooks.
KBA	Knowledge-Based Authentication. Verification based on information the user is assumed to know, such as a date of birth or an address.
MFA	Multi-Factor Authentication. An authentication scheme combining two or more independent factors (something you know, have, or are).
NIS2	Network and Information Security Directive 2, an EU directive establishing cybersecurity obligations for essential and important entities.

SIEM	Security Information and Event Management. Systems such as Splunk, Microsoft Sentinel, or Elastic that aggregate and analyze security telemetry.
Step-up	The act of requiring a stronger verification factor for a higher-risk action, on top of an existing authenticated session.

SECTION 19

References and further reading

Public sources used for the scenario narrative and threat framing:

- Google Cloud / Mandiant, "Defending Against UNC3944: Cybercrime Hardening Guidance from the Frontlines," 7 May 2025. https://cloud.google.com/blog/topics/threat-intelligence/unc3944-proactive-hardening-recommendations Describes UNC3944 / Scattered Spider help-desk social engineering and recommends phishing-resistant identity controls for password resets and MFA registration.
- CISA, FBI and international partners, Joint Cybersecurity Advisory AA23-320A, "Scattered Spider," updated 29 July 2025. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a Documents social engineering against help desks and expanded targeting of the airline sector.
- Salesloft Drift / Salesforce OAuth-token compromise (tracked as UNC6395), August 2025. A compromised SaaS integration exposed Salesforce support-case and contact data across more than 700 organizations; Cloudflare publicly disclosed exposure of 104 API tokens. Cloudflare, "The impact of the Salesloft Drift incident on Cloudflare and our customers," https://blog.cloudflare.com/response-to-salesloft-drift-incident/
- Qantas contact-centre data incident, June 2025. Public reporting described a cybercriminal accessing a third-party customer-service platform holding records of roughly 5.7 million customers. https://www.qantas.com/au/en/support/information-for-customers-on-cyber-incident.html
- MGM Resorts help-desk social-engineering incident, 2023. A help-desk impersonation led to a credential reset and a ransomware attack that MGM disclosed with an estimated financial impact of roughly USD 100 million. Widely reported; see public reporting and MGM regulatory disclosures.
- Verizon, 2025 Data Breach Investigations Report. Analysed over 22 000 incidents and 12 195 confirmed breaches; the human element featured in around 60 percent of breaches and pretexting made up about 30 percent of social engineering. https://www.verizon.com/business/resources/reports/dbir/
- IBM, Cost of a Data Breach Report 2025. Global average breach cost of USD 4.44 million. https://www.ibm.com/reports/data-breach
- ENISA Threat Landscape 2024. Annual EU threat assessment covering social engineering and identity-based intrusion. https://www.enisa.europa.eu/
- NIST SP 800-63-4, Digital Identity Guidelines, finalised July 2025. Risk-based identity assurance and phishing-resistant authentication. https://csrc.nist.gov/projects/digital-identity-guidelines
- Regulatory texts: GDPR (Regulation (EU) 2016/679), NIS2 (Directive (EU) 2022/2555), DORA (Regulation (EU) 2022/2554), and ISO/IEC 27001:2022.
- T34MS product documentation for Verify0 Verified and Verify0 Access.

This whitepaper contains forward-looking statements about product capabilities. Specific feature availability and certifications are current as of the document version shown in the footer. Contact T34MS for the most recent information.