WINMAGIC

Authenticate. Encrypt. **Achieve.**

# No Prompt. Always-On Security!

## The Endpoint as the Foundation for Online Access

Introduction

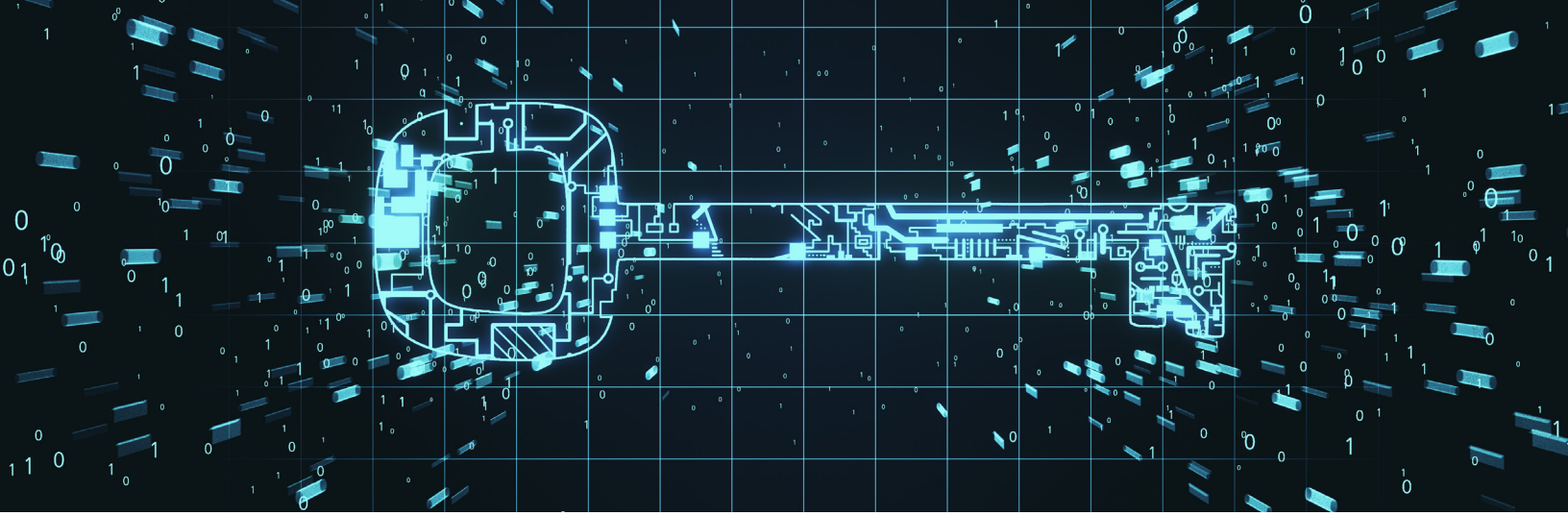
# Rethinking Identity Through the Endpoint

In today's enterprise landscape, Identity and Access Management (IAM) remains a critical yet cumbersome challenge. Traditional IAM systems rely heavily on server-side verification, user interaction, and fragile session tokens—creating friction for users and vulnerabilities for organizations.

MagicEndpoint introduces a paradigm shift: identity is no longer verified at the server, but asserted from the endpoint itself. MagicEndpoint establishes a persistent, policy-bound trusted channel between the endpoint and the Identity Provider (IdP), using Live Key-based mutual TLS (mTLS) to continuously assert verified user presence and device integrity.

This trusted channel transforms the endpoint into a Lived Identity Machine—a dynamic, policy-aware agent that governs access from power-on to power-off. MagicEndpoint eliminates passwords, MFA prompts, and session hijacking risks, while enabling seamless access to applications, infrastructure, and data.

MagicEndpoint is not just a product—it's a new category of identity architecture. It is deployable today, and it lays the foundation for the broader vision of the Secure Internet, where transport-layer trust becomes universal.



Architecture Overview

# The Trusted Channel and Live Key

At the heart of MagicEndpoint is its trusted channel, a persistent connection between the endpoint and the IdP that uses Live Key-based mTLS. This channel is not merely encrypted—it is authenticated by policy-bound cryptographic keys anchored in TPM hardware (or software fallback), available only when organizational trust conditions are met.

## Key Components:

- Live Key: A dynamic cryptographic key that behaves as a signal—available only when the user is present and the device meets policy-defined conditions. It is anchored in TPM and used to establish mTLS with the IdP.
- Trusted Channel: A persistent, authenticated connection that continuously communicates identity, posture, and context. It replaces fragile session tokens and enables real-time trust enforcement.
- Posture Evaluation: MagicEndpoint continuously evaluates endpoint conditions including:
  - GPS-based geolocation
  - Screen lock status
  - Patch level and security posture
  - Full Disk Encryption status
  - User activity and intent signals
- Delegated IdP Integration: MagicEndpoint acts as a delegated identity provider, integrating with existing IAM systems (e.g., Okta, Entra ID) and injecting credentials into applications without user interaction.
- Access Orchestration: MagicEndpoint handles SSH, RDP, and application access seamlessly, using the trusted channel to assert identity and inject credentials securely.

This architecture ensures that access decisions are made at the endpoint, based on real-time conditions, rather than relying on static server-side checks or user-entered credentials.


Core Capabilities

# Identity Without Interaction

MagicEndpoint redefines what identity and access management can achieve by leveraging the endpoint as a continuous, policy-aware identity engine. Its capabilities go far beyond traditional IAM, offering a seamless experience for users and a robust security model for organizations.

## 1. Non-Interactive Authentication

MagicEndpoint eliminates the need for passwords, MFA prompts, and manual login steps. Once the user logs into the endpoint, MagicEndpoint handles all downstream authentication silently and securely. This includes:

- Application access via credential injection
- SSH and RDP sessions initiated without user action
- Step-up MFA for sensitive resources, triggered by policy

## 2. Live Key-Based Trust Enforcement

MagicEndpoint uses Live Key, a cryptographic key anchored in TPM (or software fallback), to assert identity and device integrity. Live Key is only available when trust conditions are met, making it a dynamic signal rather than a static credential.

- Live Key is used to establish mTLS with the IdP
- It is policy-bound, ensuring availability only under verified conditions
- It supports multiple keys per user and per endpoint, enabling granular trust

## 3. Persistent Trusted Channel

MagicEndpoint maintains a persistent mTLS connection with the IdP, forming a trusted channel that continuously communicates:

- User identity and presence
- Screen lock status
- Security posture and patch level

- Full Disk Encryption status
- GPS-based geolocation
- Behavioral signals and user intent

This channel replaces fragile session tokens and enables real-time access decisions based on live context.

## 4. Delegated IdP Integration

MagicEndpoint integrates with existing IAM systems as a delegated identity provider, allowing organizations to retain their current infrastructure while upgrading their security posture.

- Supports Okta, Entra ID, and custom SSO
- Injects credentials into web apps and native applications
- Enables seamless access orchestration across environments

## 5. Endpoint MFA and Access Control

MagicEndpoint enforces multi-factor authentication at the endpoint, not just at the application level. Supported methods include:

- TPM PIN
- Smartcard
- USB token
- Phone app (via BLE or network)
- Password (as fallback or combined factor)
- Manager approval for bypass scenarios

This model ensures that access begins at the endpoint, governed by organizational policy and real-time conditions.

## 6. Continuous Verification

Unlike traditional IAM systems that authenticate once and assume trust, MagicEndpoint performs continuous verification from power-on to power-off—even without online access. This includes:

- Offline policy enforcement
- Pre-boot authentication (PBA)
- Real-time posture evaluation
- Event-driven updates to the IdP

Security Model

# Trust Begins at the Endpoint

MagicEndpoint introduces a security model that is fundamentally different from traditional IAM and Zero Trust architectures. Instead of relying on server-side authentication and network-layer controls, MagicEndpoint enforces trust at the endpoint, before any connection is made.

## 1. Endpoint-Centric Trust Enforcement

MagicEndpoint treats the endpoint as the primary trust authority. It verifies user identity, device integrity, and posture before allowing access to any resource. This model ensures that:

- No access is granted unless the endpoint is trusted
- Trust is continuously evaluated, not assumed after login
- Security decisions are made locally, based on real-time conditions

This approach eliminates common attack vectors such as token hijacking, session replay, and adversary-in-the-middle exploits.

## 2. Live Key as a Dynamic Signal

The Live Key is central to MagicEndpoint's security model. Unlike static credentials or certificates, the Live Key:

- Is anchored in TPM hardware (or software fallback)
- Is policy-bound, available only when trust conditions are met
- Is used to establish mTLS with the IdP, forming a cryptographically authenticated channel
- This ensures that identity is asserted cryptographically, not just claimed via credentials.

## 3. Persistent Trusted Channel

MagicEndpoint maintains a persistent mTLS connection with the IdP, forming a trusted channel that:

- Continuously communicates posture, identity, and context
- Enables event-driven access control, reacting to changes in real time
- Replaces fragile session tokens with cryptographic trust

This channel is the backbone of MagicEndpoint's security model, enabling continuous verification and policy enforcement without user interaction.

## 4. Policy-Defined Trust Conditions

Access is governed by organizational policy, which can include:

- GPS-based geolocation (e.g., only allow access from approved regions)
- Screen lock status (e.g., deny access if screen is unlocked)
- Patch level and posture scores (e.g., require latest security updates)
- Full Disk Encryption status (e.g., deny access if FDE is disabled)
- User activity and intent signals (e.g., allow access only during work hours)
- These conditions are evaluated locally and enforced before any network connection is initiated.

## 5. Defense-in-Depth Without User Burden

- MagicEndpoint provides layered security without adding friction:
- MFA is enforced at the endpoint, not during app access
- Credential injection eliminates password reuse and phishing risk
- SSH and RDP access are handled silently and securely
- Offline access is governed by cached policy and pre-boot authentication
- This model offers stronger security than traditional IAM, while improving usability and reducing helpdesk burden.

Integration and Deployment

# Seamless Adoption, Immediate Impact

MagicEndpoint is designed for rapid enterprise adoption with minimal disruption to existing infrastructure. It integrates smoothly with current IAM systems, supports diverse environments, and delivers immediate security and usability benefits.

## 1. Delegated IdP Integration

MagicEndpoint functions as a delegated identity provider, allowing organizations to retain their existing IAM platforms while upgrading their authentication model. It integrates with:

- Okta, Entra ID, and other SAML/OIDC-based systems
- Custom SSO frameworks
- LDAP and Radius environments

MagicEndpoint injects credentials into applications and services without user interaction, enabling seamless access across web, desktop, and infrastructure layers.

## 2. Platform Support

MagicEndpoint is optimized for Windows environments, with full support for:

- TPM-based Live Key anchoring
- Full Disk Encryption and Pre-Boot Authentication (PBA)
- Credential injection for Windows login, RDP, and SSH

It also supports:

- Mac and mobile platforms, with no user interaction required
- Phone fallback for MFA and access recovery
- Linux support is planned, ensuring full cross-platform coverage

## 3. Deployment Model

MagicEndpoint is delivered as a lightweight endpoint agent, centrally managed and policy-driven. Deployment options include:

- Cloud-hosted IdP or on-premises integration
- Group policy or endpoint management tools for rollout
- Customizable policies for trust conditions and access control

MagicEndpoint is designed to scale across thousands of endpoints with minimal overhead, making it suitable for both SMBs and large enterprises.

## 4. Operational Benefits

Organizations deploying MagicEndpoint benefit from:

- Reduced helpdesk burden (no password resets, fewer MFA issues)
- Improved user experience (no login prompts or access delays)
- Stronger security posture (endpoint-driven trust, continuous verification)
- Future-proof architecture (ready for Secure Internet integration)

MagicEndpoint is not just a security upgrade—it's an operational transformation.

Strategic Positioning

# Foundation Today, Amplifier Tomorrow

MagicEndpoint is not just a product—it's a strategic foundation for the future of identity and access. It solves today's IAM challenges with unmatched usability and security, while preparing organizations for the next phase: transport-layer trust through the Secure Internet.

## 1. MagicEndpoint as the Core Identity Engine

MagicEndpoint governs identity at the endpoint, where trust can be most accurately enforced. It verifies user presence, device integrity, and policy compliance before any connection is made. This makes MagicEndpoint:

- Stronger than server-side IAM, which relies on static credentials and delayed posture checks
- More usable than Zero Trust, which often adds friction through repeated MFA and access prompts
- More precise than network-layer controls, which lack user context
- MagicEndpoint is deployable today and already in production, offering immediate value to enterprises.

## 2. Secure Internet as the Transport-Layer Amplifier

Secure Internet extends MagicEndpoint's trust model to the transport layer, enabling mutual TLS (mTLS) between endpoints and service providers. Secure Internet uses the same Live Key architecture to authenticate connections, replacing cookies, tokens, and fragile session mechanisms.

While MagicEndpoint governs who is accessing and from where, Secure Internet governs how that access is transported—ensuring cryptographic trust across the wire.

Together, MagicEndpoint and Secure Internet form a layered trust architecture:

- MagicEndpoint: Identity, posture, and access control at the endpoint
- Secure Internet: Transport-layer authentication and encryption across services

## 3. Future-Proofing Enterprise Security

By adopting MagicEndpoint today, organizations position themselves to seamlessly integrate Secure Internet tomorrow. MagicEndpoint already uses Live Key and mTLS for its trusted channel, making it natively compatible with Secure Internet's architecture.

This ensures:

- No rework or migration when Secure Internet becomes widely adopted
- Immediate security gains with long-term strategic alignment
- A unified trust model across identity, access, and transport
- MagicEndpoint is not a stepping stone—it is the foundation. Secure Internet is the natural extension.

Use Cases

# Real-World Impact Across the Enterprise

MagicEndpoint is designed to solve real-world identity and access challenges across diverse environments. Its unique architecture enables secure, seamless access in scenarios where traditional IAM solutions fall short.

## 1. Workforce Access Without Friction

MagicEndpoint enables employees to access applications, infrastructure, and data without passwords or MFA prompts. Once logged into their endpoint, users gain secure access to everything they need—reducing frustration and improving productivity.

- No login fatigue or password resets
- Step-up MFA for sensitive apps, triggered silently
- Credential injection for legacy systems

## 2. Remote Work with Real-Time Trust

MagicEndpoint ensures that remote access is governed by real-time posture and location data. GPS-based geolocation, patch status, and screen lock conditions are continuously evaluated, allowing organizations to enforce dynamic access policies.

- Allow access only from approved regions
- Deny access if device is unlocked or unpatched
- Support for offline access with cached policy

## 3. High-Security Environments

In regulated or sensitive industries, MagicEndpoint provides strong assurance of identity and device integrity. Its TPM-anchored Live Key and persistent trusted channel offer cryptographic guarantees that go beyond traditional MFA.

- Full Disk Encryption with Pre-Boot Authentication
- TPM PIN and smartcard support
- Continuous verification from power-on to power-off

## 4. Helpdesk Reduction and Operational Efficiency

By eliminating passwords and reducing MFA complexity, MagicEndpoint dramatically lowers helpdesk burden. Users no longer need to remember credentials or call support for access issues.

- Fewer password resets
- No MFA troubleshooting
- Manager approval workflows for access recovery

## 5. Seamless Access Across Hybrid Environments

MagicEndpoint supports both cloud and on-premises systems, integrating with existing IAM platforms and infrastructure. It enables secure access to SaaS apps, internal systems, and remote desktops—all without user interaction.

- SSH and RDP access without manual login
- LDAP and Radius compatibility
- Support for Windows, Mac, and mobile


Conclusion

# A New Standard for Identity and Access

MagicEndpoint represents a fundamental shift in how identity and access are managed across the enterprise. By anchoring trust at the endpoint and establishing a persistent, policy-bound trusted channel, MagicEndpoint delivers stronger security, better usability, and lower operational overhead than any traditional IAM solution.

- It replaces passwords, MFA prompts, and fragile session tokens with Live Key-based authentication, governed by real-time posture and policy. MagicEndpoint is deployable today, already in production, and compatible with existing IAM systems—making it a practical and strategic upgrade for any organization.
- Looking ahead, the Secure Internet will extend MagicEndpoint's trust model to the transport layer, enabling universal mTLS and cryptographic trust across all services. MagicEndpoint is already built on the same Live Key foundation, making it natively compatible with Secure Internet and fully future-proof.
- Together, MagicEndpoint and Secure Internet form a cohesive architecture that secures identity, access, and communication—without user burden. MagicEndpoint is the foundation. Secure Internet is the amplifier. The future of cybersecurity begins at the endpoint.

---

***"We didn't build MagicEndpoint to chase compliance or follow frameworks. We built it to solve the core problems—identity fragmentation, session hijacking, and brittle trust assumptions. By starting from first principles and observing how identity breaks in the real world, we engineered a system that naturally meets or exceeds Zero Trust standards—not because we aimed for them, but because we did the right thing."***

Thi Nguyen-Huu, CEO and Founder

---

**Footnote**: While managed endpoints represent the best practice for enforcing Zero Trust—where device integrity and posture can be continuously verified—MagicEndpoint also supports unmanaged endpoints through **out-of-band (OOB) verification using the user's registered phone**, similar to leading IAM solutions. Unlike typical OOB-only approaches, MagicEndpoint still evaluates device context where possible, maintaining stronger alignment with Zero Trust principles. This ensures that even in BYOD or contractor scenarios, access is gated by a second, independent trust anchor—not just a browser prompt or network location.

## Zero Trust Alignment

MagicEndpoint wasn't built to tick boxes or follow trends. We built it to fix the root problems—session hijacking, token theft, and brittle trust assumptions.

By starting from first principles—verify the user, verify the device, enforce policy continuously—we ended up with a model that naturally embodies Zero Trust ideals:

- Never assume trust—MagicEndpoint enforces it at the endpoint before any connection.
- Verify continuously—from power-on to power-off, online or offline.
- Decide locally—based on real-time posture, not static claims.

For unmanaged endpoints, MagicEndpoint uses out-of-band (OOB) verification via the user's registered phone, similar to leading IAM solutions—but with stronger device context checks where possible. This ensures security even in BYOD or contractor scenarios, without compromising the principle of least privilege.

# About WinMagic

With over 25 years of continuous innovation, WinMagic's comprehensive full disk encryption controls user identities via MFA for endpoint access and continuously protects and monitors both endpoints and users from the moment the endpoint is powered on. For online access, embracing an identity-first approach and adhering to Zero Trust principles where the network lacks inherent trust, MagicEndpoint introduces uniquely verifiable identities, "user on device," utilizing TPM keys. MagicEndpoint IdP then provides best-in-class authentication services for all identities accessing online resources, and can be used as a delegated IdP for current IAM solutions.

Thanks to the secure channel continuously monitoring the device and user, MagicEndpoint is more resilient to attacks than current approaches. Perhaps more importantly for user adoption, this solution eliminates any burden on the user beyond endpoint login.

WINMAGIC®

For more information
winmagic.com/contact-sales