WINMAGIC

Authenticate. Encrypt. **Achieve.**

MagicEndpoint: Nine Core Principles

WinMagic Authentication Suite

Table of Contents

MagicEndpoint in the WinMagic Authentication Suite 3

Value Statement. 4

Dear Reader. 5

What to Expect in This Paper 6

9 Core Principles. 7

- Principle #1: Eliminate User Interaction—Securely and Completely. 7
- Principle #2: Make the Endpoint the Identity Machine. 9
- Principle #3: Achieve Maximum Trust With a Persistent Trusted Channel Between Endpoint and IdP. 11
- Principle #4: Authentication Is More Accurate and Resilient With Time as a Factor. 13
- Principle #5: Replace Static Tokens With Continuous Post-Login Validation 15
- Principle #6: Real-Time, Event-Driven Updates—Because Cybersecurity Demands Instant Reaction . . 17
- Principle #7: Provide IAM Coverage Across Cloud, On-Prem, and Legacy Systems. 19
- Principle #8: Unify IAM and Password Management Where It Belongs—at the Endpoint 21
- Principle #9: Ensure Recovery Is Passwordless and Policy-Driven 25

Looking Ahead: Live Key and the Secure Internet. 27

MagicEndpoint in the WinMagic Authentication Suite

MagicEndpoint is WinMagic's solution for **secure, seamless online access**—and it's part of a comprehensive authentication portfolio that includes:

1. **Pre-Boot Authentication with Full Disk Encryption**
2. **Windows Login (OS-level authentication)**
3. **Online Authentication through MagicEndpoint**

Together, these solutions cover every stage of identity verification—from powering on the device to accessing cloud and on-prem applications.

This document focuses on **MagicEndpoint and online access**, which can be deployed as a standalone solution. However, the ideal approach is to integrate all three for an **identity-first** security model that starts at pre-boot, flows through OS login, and extends to every application and service—delivering **continuous trust without user friction**.

Value Statement

MagicEndpoint **redefines workforce identity** by making authentication **invisible, continuous, and endpoint-driven**. Instead of relying on passwords, prompts, or fragile session tokens, MagicEndpoint transforms the endpoint into a **trusted identity machine**—verifying user presence, device integrity, and security posture from power-on to power-off.

This persistent, event-driven trust channel:

- Eliminates MFA fatigue
- Stops polling and session vulnerabilities
- Removes costly password resets through policy-based recovery

The result: **stronger security, zero user friction, and dramatically lower operational risk and cost**.

The Nine Core Principles—outlined below—define how MagicEndpoint delivers identity-first security without friction. They are not radical; they are grounded in clarity and logic. They reflect what security should have always been: **simple, consistent, and enforced where it's most effective**. By leveraging the endpoint—the device every user depends on—MagicEndpoint achieves results that may seem novel, yet are rooted in common sense.

Dear Reader

Thank you for taking the time to explore **MagicEndpoint**—a new approach to online authentication. MagicEndpoint is unlike anything you've seen before, and to fully appreciate its impact, we invite you to set aside everything you think you know about authentication.

For over two decades, the industry has invested enormous resources in cybersecurity. Yet, despite MFA, passwordless strategies, Zero Trust, and an alphabet soup of frameworks—IAM, PAM, IGA, EDR, ITDR, CAEP—the results remain questionable. Breaches continue. Attacks grow more sophisticated. Even as the industry celebrates progress with Passkeys and Zero Trust, it experiments with new ideas like continuous access evaluation, token binding, and now channel binding—signs that no one has truly solved the problem.

The uncomfortable truth? **The root cause of cybersecurity brittleness remains misunderstood**. Perhaps it's because we are still new to the online world and have yet to realize this:

The most secure form of online authentication is… no authentication at all.

At WinMagic, we understand this—and MagicEndpoint is built on that principle.

What to Expect in This Paper

This document introduces the concepts behind MagicEndpoint and explains why it represents a fundamental shift in how we think about identity and access. While we will reference MagicEndpoint features where helpful, our focus is on the principles that make this approach possible. We will also compare MagicEndpoint to traditional solutions, highlight key takeaways, and share the philosophical shifts required to embrace this model.

To guide you through this journey, we've organized the discussion around nine principles, grouped as follows:

- **Human Experience** – Principle 1
- **Security** – Principles 2, 3, 4, 5, and 6
- **Coverage and Manageability** – Principles 7 and 8
- **Fallback, Operations, and Business Outcomes** – Principle 9

Although security is the ultimate goal, we begin with **Human Experience**—because the most transformative benefit of MagicEndpoint is also the hardest to imagine: a world where users take no action at all to authenticate beyond logging into their endpoint.

Before we dive in, there's one universal concept you need to understand.

The Universal Concept of MagicEndpoint Authentication

MagicEndpoint operates on two distinct authentication scopes:

1. **Endpoint Authentication** – The only time the user interacts (e.g., MFA, Pre-Boot Authentication).
2. **Application Authentication** – Everything else (apps, servers, SaaS) happens silently, handled by the verified endpoint where **identity = user + device under policy**.

Furthermore, it's important to understand what makes MagicEndpoint fundamentally possible.

Two Foundations: Cryptography and the Endpoint

MagicEndpoint is built on two foundations: **cryptography** and the **endpoint**.

- **Cryptography** because in an online world, the only proven way to bring trust into data is through strong cryptographic assurance.
- **The Endpoint** because it is the user's constant companion—the one place where identity, intent, and context converge. As the companion users cannot go without to access the online world, the endpoint is uniquely positioned to help users navigate it securely and seamlessly.

Most solutions avoid these foundations. Why?

- **Endpoints** are complex and time-consuming compared to server-side approaches.
- **Applied cryptography** requires rare expertise—skilled engineers who understand that the best security paths are the hardest to attack, while shortcuts leave gaps for adversaries.

At WinMagic, we believe the best software engineers should work on security software—because in security, the path matters as much as the destination. MagicEndpoint reflects that belief.

Principle #1

Eliminate User Interaction—Securely and Completely

Tagline: Zero prompts. Zero friction. Stronger than SSO.

Goal: Deliver zero-prompt access with always-on, invisible security.

Traditionally…

SSO was designed to reduce friction: log in once, and access multiple apps without re-entering credentials. But it has become increasingly vulnerable to sophisticated attacks.

As a result, businesses are now disabling SSO for sensitive apps, leading to frequent interruptions that force users to stop what they're doing to complete an MFA challenge.

Even when SSO is enabled, it still requires user interaction: MFA at initial login and re-authentication when sessions expire.

A Better Way…

MagicEndpoint eliminates repeated logins without relying on SSO tokens.

Once the user signs in to their endpoint, MagicEndpoint becomes the trusted identity source for all apps—injecting credentials, enforcing MFA silently, and navigating access flows automatically.

Unlike SSO, MagicEndpoint requires no user action at all, not even for the initial login or token renewal.

The endpoint performs all authentication on behalf of the user—representing both user and device.

The industry's biggest blind spot? It assumes the user should perform authentication. That's friction for them—and a gift for attackers. MagicEndpoint flips the model: the endpoint does the work, silently and accurately.

Why It's Better

- **No Interaction at Any Stage**
  SSO still requires MFA at first login and re-prompts later. MagicEndpoint eliminates all prompts—users authenticate once at the endpoint, and can access everything else without friction.
  Even when the system re-authenticates (e.g., after screen lock or token expiry), MagicEndpoint handles it silently—no user action required.

- **No Credentials, No Devices, Nothing to Forget**
  Users don't forget what they never had to remember or carry. MagicEndpoint removes passwords, MFA apps, and physical tokens from the experience.
  No need to bring a phone, open an app, or enter a code.

- **No Phishing Surface**
  No login screens, no MFA codes, no bait. MagicEndpoint eliminates the entire interaction layer that phishing and AI threats exploit.

- **No UX Disruption**
  SSO breaks when sessions expire or when access policies change. MagicEndpoint works across SaaS, on-prem, SSH, RDP—without fallback chaos.

- **No Password Resets or Helpdesk Calls**
  MagicEndpoint doesn't rely on user memory. There's nothing to reset—because there's nothing to forget.
  Fallbacks (via phone or manager approval) are available, but only for endpoint login—not for app access.

- **No Dependency on SSO Availability**
  MagicEndpoint works even when SSO is disabled for sensitive apps. It's not just a convenience layer—it's a full access engine.

Use Case

A user signs in to their laptop in the morning. Throughout the day, they access SaaS apps, on-prem apps, SSH sessions, and RDP—all without entering credentials again. MagicEndpoint injects credentials and enforces MFA silently, delivering a better experience than SSO with stronger security.

Key Takeaway: Zero interaction with stronger, always-on security is here today. End MFA fatigue—deploy MagicEndpoint now.

Principle #2

Make the Endpoint the Identity Machine

Tagline: Verification at the source – beyond the cloud.

Goal: Verify user and device locally with MFA and posture checks for unmatched accuracy and resilience.

Traditionally…

Identity decisions live in the cloud. IdPs authenticate users and issue tokens, while Service Providers trust those tokens. But this model is blind to real-time conditions: it can't see if the device is encrypted, if the screen is locked, or if the user is still present. It assumes static trust based on a single login event—leaving gaps attackers exploit.

A Better Way…

MagicEndpoint moves identity to where it belongs: the endpoint. The endpoint is closest to the user and can verify them with local MFA, enforce posture checks, and act instantly when conditions change. Once the user signs in, MagicEndpoint continuously enforces policy, injects credentials, and navigates access flows silently—without extra prompts.

Critically, MagicEndpoint verifies both the user and the device together. This redefines the trust model: instead of asking "Who is the user?", MagicEndpoint asks "Is this trusted user on a trusted device?". This dual verification enables non-interactive access and naturally aligns with Zero Trust principles—continuous verification and context-aware access—without requiring extra infrastructure.

When most people think authentication, they think yes/no—did the user pass the check? But attackers exploit the gaps between those checks. How accurate is that decision? How resilient is it against real-world attacks? These questions rarely get asked, yet they define true security. MagicEndpoint answers them by verifying at the source, where reality lives—delivering **accuracy and resilience** that cloud-only models can't match.

Attackers can plan for months, but breaking strong cryptography would take longer than humanity has existed—even with all the world's computing power. That's the strength of anchoring identity in the endpoint with cryptographic keys: it's security at a scale humans can't match.

Why It's Better

- **Full Context**: The endpoint knows what the cloud can't—boot integrity, encryption state, user presence, and posture.
- **Instant Decisions**: No round trips to the IdP for every change; MagicEndpoint enforces policy locally in real time.
- **Dual Verification**: Identity = user + device, verified together.
- **Seamless UX**: Users authenticate once at the endpoint; MagicEndpoint handles app access silently.
- **Resilient Recovery**: Lost device? MagicEndpoint supports fallback via phone or manager approval—without password resets.
- **ZT-Aligned, But Endpoint-Driven**: Every access decision is grounded in verified device and user state—not just a token.

Use Case

A user signs in to their laptop in the morning. MagicEndpoint becomes the trusted identity source for all apps—injecting credentials, enforcing MFA silently, and revoking access instantly if posture changes. If the device loses encryption or enters a risky location, MagicEndpoint cuts off access immediately—without waiting for the IdP or requiring user action.

Key Takeaway: Verification at the source delivers unmatched accuracy and resilience. Deploy MagicEndpoint as a delegated IdP and strengthen security in under a month.

Principle #3

Achieve Maximum Trust With a Persistent Trusted Channel Between Endpoint and IdP

Tagline: If banks need a trusted line, so do you.

Goal: Establish a persistent, trusted channel for real-time, context-rich decisions.

Traditionally…

Most systems only check the client when it requests a service—and only for a few seconds. MFA or even FIDO can block some attacks, but as adversaries grow more sophisticated, this short-lived check is no longer enough. The SolarWinds breach showed how attackers can chain dozens of techniques across multiple stages, bypassing traditional defenses.

A Better Way…

Banks solved this problem years ago. They don't rely on random calls for sensitive actions—they give you a trusted phone number on the back of your card. Why? Because a **persistent**, **authenticated channel** is the only way to guarantee you're talking to the right party.

MagicEndpoint applies the same principle to identity. It establishes a separate, persistent, trusted channel between the endpoint and the IdP—a channel that is locally verified and continuously monitored. Think of it as the phone number on the back of your bank card: a direct, authenticated line that can't be spoofed.

If this makes so much sense, why hasn't it been done? Because most vendors avoid the endpoint—it's hard. But that's exactly where real security lives. **Banks figured this out years ago. Applying the same logic to identity isn't innovation—it's overdue common sense**.

This channel is event-driven, not static. If posture degrades, the channel signals the IdP instantly, and access is revoked—even mid-session. And because the endpoint typically belongs to the organization, it becomes the logical anchor for trust—not just for device login, but for every online account.

Why It's Better

1. **Direct, Trusted Line**: No reliance on assumptions; the IdP always knows the real state of the endpoint.
2. **Continuous Assurance**: The channel reflects real-time trust, not a past login event.
3. **Event-Driven**: Immediate response to posture changes—no polling delays.
4. **Local Verification**: The endpoint enforces trust conditions before signaling the IdP.
5. **Built for Advanced Threats**: To combat attacks as sophisticated as SolarWinds, you need more than point-in-time checks—you need a channel attackers can't fake.
6. **Leverages What You Own**: The endpoint typically belongs to the organization. Why not use it as the anchor for online access security?
7. **A New Product Category**: MagicEndpoint unifies endpoint login and online account login under one logical model. The same system that secures the device now secures every app—creating a category that didn't exist before.
8. **Beyond Presence—Toward Intent**: MagicEndpoint can even verify that sensitive actions originate from the user's legitimate session—using browser flags and endpoint checks—making it harder for malware or injected scripts to impersonate the user. Planned features like a desktop portal will further ensure malware cannot invoke sensitive operations.

Use Case

A user logs in and opens sensitive apps. Later, the device posture fails a security check. MagicEndpoint signals the IdP through the trusted channel, and access is revoked instantly—without waiting for session expiry or periodic checks.

Key Takeaway: Bring a proven concept—trusted channels—to IAM. Always-on verification is no longer optional.

Principle #4

Authentication Is More Accurate and Resilient With Time as a Factor

Tagline: Time is a security factor—longer observation, stronger trust.

Supporting line: You can fool a system once—but not across hours of verified trust.

Goal: Strengthen initial authentication by leveraging signals accumulated over time—starting from power-on

Traditionally…

Authentication is treated as a snapshot—a few seconds of checks at login. Add MFA, add biometrics, even add conditional access signals… but it's still a single point of failure. If an attacker compromises that brief moment, they're in.

These systems have no memory. They don't care how the device booted, whether encryption was enforced, or if posture was healthy five minutes ago. They only care about now—and "now" can be faked.

Industry Blind Spot

Why MFA and Conditional Access Still Miss the Point

MFA, biometrics, and conditional access policies add layers, but all within the same tiny time window. They verify who you are right now—not how you got here. Without a trust history, the first authentication event remains fragile.

A Better Way…

MagicEndpoint turns authentication into a timeline of trust. From power-on, MagicEndpoint starts building assurance:

- Verifying boot integrity
- Enforcing disk encryption
- Checking OS posture
- Confirming user presence

By the time the user reaches the login screen, MagicEndpoint has accumulated hours of verified trust signals—not seconds. This isn't about re-authentication or CAEP after login. It's about making the **first authentication decision exponentially harder to attack** by basing it on a chain of verified conditions, not a single moment.

Why It's Better

- **Initial Authentication, Reinvented**: The first login decision is backed by a trust history, not a quick check.
- **Harder to Attack**: An attacker can fool a system once, but not repeatedly across multiple checkpoints.
- **Rich Intelligence Beyond User Presence**: Device health, encryption state, geolocation, behavioral signals—far beyond what MFA or Live Key alone can capture.
- **Resilient by Design**: Trust is cumulative and adaptive. If posture degrades at any point before login, the chain breaks and authentication fails.

Use Case

A device boots at 8:00 AM. MagicEndpoint verifies secure boot, confirms disk encryption, checks patch level, and monitors user login. By 9:00 AM, when the user authenticates, MagicEndpoint has an hour of verified trust history—making that initial decision exponentially stronger than a 5-second MFA check.

Key Takeaway: MagicEndpoint evaluates the entire journey—from power-on to sign-on—building deeper, more resilient trust. MFA alone can't match this. Ignore time, and you ignore risk.

Principle #5

Replace Static Tokens With Continuous Post-Login Validation

Tagline: Stop trusting copiable static tokens.

Supporting line: Because attackers love long-lived tokens.

Goal: Replace vulnerable bearer tokens with active cryptographic operations and real-time updates.

Traditionally…

Web and app sessions optimize for convenience: authenticate once, then trust for hours or even days. Identity providers issue tokens, apps create sessions, and neither checks the user again until the token expires. If a token or cookie is stolen, the attacker rides that session—unnoticed.

Industry Blind Spot

Why Session Tokens Are a Weak Link

Bearer tokens and cookies assume static trust. They don't know if the user walked away, if the device posture changed, or if the session was hijacked. Once issued, they live blind—until they expire.

A Better Way…

MagicEndpoint replaces static trust with continuous, event-driven verification. Instead of granting permanent trust at login, MagicEndpoint maintains a persistent trust channel from power-on to power-off. Every authentication event is silent, policy-bound, and evaluated fresh against the current user, device, and posture state.

This means apps can shrink token lifetimes to minutes and re-authenticate frequently—without prompting users. If posture drops, the screen locks, or location changes, MagicEndpoint revokes access instantly.

Why It's Better

- **Static Sessions Are Over**: MagicEndpoint eliminates the risk of stolen tokens by making trust dynamic.
- **Beyond IdP and App**: IdPs see logins; MagicEndpoint sees everything—boot integrity, posture, user presence—throughout the session.
- **Dynamic Revocation**: Trust isn't static. If conditions fail, access is revoked—even mid-session.
- **Silent UX**: Frequent re-authentication happens invisibly, preserving a seamless experience.

Use Case

A user logs in and opens a sensitive app. Later, they walk away and the screen locks. MagicEndpoint detects the lock event and revokes access instantly—long before any token expires or the app notices inactivity.

Key Takeaway: Static tokens can be stolen. MagicEndpoint enforces dynamic, event-driven trust—eliminate token replay risk today.

Future Vision

"Looking ahead, Secure Internet builds on the same principles to eliminate sessions entirely—trust becomes inherent in every connection."

Aspect	MagicEndpoint (ME)	Secure Internet
Session Model	Dynamic sessions via persistent trust channel	No sessions—trust is built into the channel
Revocation	Event-driven, instant revocation mid-session	Not needed—every packet is authenticated
Dependency	Requires IdP + ME agent	No IdP dependency after handshake
User Experience	Silent, frequent re-auth without prompts	Invisible—no concept of re-authentication

"This is the natural evolution of identity-first security: from fixing token risk to removing tokens altogether."

Caption: ME fixes today's token problem. Secure Internet eliminates it enti

Principle #6

Real-Time, Event-Driven Updates—Because Cybersecurity Demands Instant Reaction

Tagline: Interrupt beats polling—instant reaction wins.

Supporting line: Polling leaves blind spots; event-driven reacts instantly.

Goal: Ensure Zero Trust decisions use fresh, accurate data.

Why This Deserves Its Own Principle

Zero Trust demands **continuous verification**—but most systems still rely on **polling**, checking every few minutes or hours whether something has changed. That's not continuous. That's scheduled guessing.

MagicEndpoint takes a different approach: it listens. It maintains a **real-time, event-driven connection** that transmits updates the moment something changes. This isn't just more efficient—it's common sense.

Think about it:

- You don't ask a coworker every 10 minutes if they've finished a task—you expect them to notify you.
- CPUs don't poll peripherals—they use interrupts to respond instantly.
- So why are identity systems still polling?

The Industry Blind Spot

Most "continuous" verification is anything but. Polling every 30 minutes—or even every 5—is still reactive. It creates blind spots between checks, wasting resources and leaving systems vulnerable to changes that go unnoticed until the next cycle.

A Better Way

MagicEndpoint eliminates polling by maintaining a persistent, intelligent connection to the device. It listens for real-time events like:

- Screen lock
- Network anomalies
- Encryption state changes
- Posture degradation
- User intent signals

These updates are transmitted instantly—no waiting, no guessing.

Why It's Better

- **Instant Response**: Trust decisions are updated the moment something changes.
- **Lower Overhead**: Listening uses fewer resources than constant polling.
- **Smarter Signals**: Rich context—device health, geolocation, behavioral patterns—not just binary status.
- **No Blind Spots**: Eliminates the gaps attackers exploit between polling cycles.
- **Built for Zero Trust**: Real-time trust is the only kind that works.

Use Case

A user steps away from their laptop and locks the screen. With polling, the system might not notice for several minutes—leaving sensitive apps exposed. With MagicEndpoint, the lock event is transmitted instantly, and access to critical resources is revoked in real time.

Key Takeaway: Polling leaves blind spots. MagicEndpoint reacts in real time—enforce Zero Trust the moment risk changes.

Principle #7

Provide IAM Coverage Across Cloud, On-Prem, and Legacy Systems

Tagline: One IAM engine that spans cloud and on-prem—without the browser blind spot.

Goal: Provide full IAM coverage for SaaS, on-prem, LDAP, Radius, and federated flows.

Why This Deserves Its Own Principle

Most IAM platforms stop at the browser. They excel at SaaS SSO but leave gaps for on-prem apps, legacy protocols, and non-web systems. Those gaps get patched with bolt-ons—VPNs, jump hosts, and plugins—creating complexity and risk.

MagicEndpoint eliminates those blind spots. It acts as a **full IAM platform** that governs **SaaS, on-prem, LDAP, Radius**, and federated flows under one policy engine. Once the user and device meet policy, MagicEndpoint enforces trust across **all access paths**, not just the browser.

Traditionally…

- IAM platforms focused on **SAML/OIDC** for SaaS apps.
- On-prem apps and legacy systems required **separate tools**.
- Policies fragmented across systems; posture signals rarely applied beyond the browser.
- Result: **tool sprawl**, inconsistent enforcement, and attack surfaces IAM couldn't see.

A Better Way (What MagicEndpoint Does)

1. **Unified IAM Coverage**
   - **SaaS & Web Apps**: Full SAML/OIDC support with continuous posture enforcement.
   - **On-Prem Apps**: Integrated via LDAP, Radius, and Kerberos—no VPN dependency.
   - **Legacy Protocols**: Governed under the same Zero Trust policies.
2. **Consistent Policy Everywhere**
   - Posture, geolocation, and risk signals apply across **cloud and on-prem**.
   - **Step-up MFA** triggered by policy—not just at login, but dynamically.
3. **Trusted Channel**
   - Persistent, verified connection between endpoint and MagicEndpoint IdP ensures **real-time enforcement** and **session binding**.
4. **Future-Ready**
   - CAEP-ready for continuous access evaluation.
   - Integrates with **Live Key** for Secure Internet scenarios (mTLS without extra user steps).

Why It's Better

- **One IAM for All Access**: SaaS, on-prem, LDAP, Radius—no blind spots.
- **No Tool Sprawl**: Eliminates VPNs, jump hosts, and plugins for most use cases.
- **Consistent Zero Trust**: Same signals and policies everywhere.
- **Dynamic Enforcement**: Continuous posture checks, not just point-in-time MFA.
- **Future-Proof**: Ready for CAEP and certificate-less mTLS.

Use Case

A financial analyst needs to:

- Access **Salesforce (SaaS)**,
- Log into an **on-prem ERP system**, and
- Connect to a **legacy app via LDAP**.

With MagicEndpoint:

- One login at the endpoint unlocks all three.
- Posture and geolocation policies apply consistently.
- If posture degrades mid-session, MagicEndpoint enforces **step-up MFA** or revokes access instantly.

Key Takeaway: IAM should unlock not only web apps but also Radius and LDAP—because customers need more than browser-based SSO. MagicEndpoint delivers full coverage under one Zero Trust model.

Principle #8

Unify IAM and Password Management Where It Belongs—at the Endpoint

Tagline: One control plane for identity, secrets, keys, and resilient access.

Goal: Combine IAM and password management at the source—the endpoint—for maximum security and simplicity.

Why This Deserves Its Own Principle

For two decades, enterprises have juggled two brains:

- **IAM** for federated authentication and SSO (server-side, token-centric)
- **Password Managers** for secrets (client-side, browser-centric)

But online authentication **begins on the endpoint**—where user presence is verified, device integrity is known, and secrets/keys are actually **used**.

If the endpoint is the foundation of trust, then **IAM should have absorbed password management from the start**—and applied the same IAM-grade controls to how passwords and keys are used.

MagicEndpoint does exactly that. It unifies IAM + Password Management and executes authentication **locally** with continuous assurance, so access is **silent when safe** and **stronger when needed**—across web and non web, online and offline.

Traditionally…

- **Two silos became "normal".**
  IAM handled SAML/OIDC tokens in the cloud; PMs autofilled secrets in the browser.
- **IAM couldn't govern local execution.**
  It lacked signals like **OS login state, screen lock, device posture, geolocation**, and couldn't enforce them before a password/key was used.

- **PMs didn't govern access.**
  They managed secrets but not **RDP, SSH, thick clients**, or **network-level** access policies.
- **Patchwork add ons proliferated.**
  Browser extensions, SSH key managers, jump hosts—each partial, none a single **policy brain**.
- **Resilience was an afterthought.**
  If the IdP was down, business stopped. If tokens were abused (e.g., Golden SAML), there was no **local verification** to resist misuse.

A Better Way (What MagicEndpoint Does)

MagicEndpoint applies IAM-grade trust to passwords and keys—and executes authentication at the endpoint.

1. **IAM Grade Controls for Passwords (and All Secrets)**
   - **Policy bound availability**: Secrets are usable only when **user + device** meet policy (login state, posture, geolocation, time, approvals).
   - **Continuous assurance**: Re-evaluate conditions throughout the session; revoke or step up dynamically (CAEP ready for future continuous access signals).
   - **Trusted channel**: Use a **persistent, verified channel** between endpoint and MagicEndpoint's control plane; bind secret use to live endpoint state.
   - **Silent orchestration**: **No extra prompts** when conditions are met; step up only when risk changes.
   - **Zero sprawl**: No scattered plugins or copy/paste; MagicEndpoint injects credentials directly into **web and thick apps**.
2. **FIDO Authenticators—For Resilience and Choice**
   - **Local fallback**: If the **IdP is offline**, MagicEndpoint can still enforce trust using **FIDO authenticators** (USB, BLE, platform) governed by local policy.
   - **Golden SAML mitigation**: Even if server tokens are abused, MagicEndpoint **won't release secrets or keys** unless local conditions and FIDO checks pass.
   - **Direct SP authentication**: Support for **Passkey/WebAuthn style** direct app authentication for customers who prefer IdP less flows in certain contexts—aligned with the industry's direction but **managed by MagicEndpoint policies**.
3. **SSH and RDP—Endpoint Based, Without Key Chaos**
   - **SSH**: MagicEndpoint derives/issues **per service keys** locally, **policy bound** and optional **step up** for sensitive targets; no roaming private keys, no unmanaged files; **misuse detectable counters** available.
   - **RDP / Windows**: MagicEndpoint integrates with **OS Credential Providers** to handle Windows login/unlock and RDP with the **same posture + MFA rules** as endpoint login—turning RDP from a loophole into a governed path.
4. **Access Matrix Governance (User × Endpoint × Resource)**
   - Define exactly **who** may use **which endpoint** to reach **which resource** (SaaS apps, thick clients, SSH hosts, RDP servers), under **which conditions** (posture, geo, time, approvals).
     This closes gaps that **server-only** IAM and **vault-only** PMs cannot address.

5. **Unified Lifecycle & Audit**
    - Secrets, keys, and sessions share **one policy engine** and **one audit trail**.
    - **Automated rotation** and **least-privilege access** for passwords and service keys.
    - **Break-glass** flows with **time-boxed approvals** and complete accountability.
6. **Secure Internet Ready (Future Proofing)**
    - When available, MagicEndpoint can assert identity using **Live Key** and enable **mTLS** so servers no longer need separate user auth.
    - **Certificate-based or certificate-less** options supported; MagicEndpoint keeps the user experience **non-interactive** when policy allows.

Why Others Don't Have Both (and Why MagicEndpoint Does)

- **Architectural gravity**: IAM is **browser/token centric**; PM is **endpoint/secret centric**. Neither spans both worlds.
- **Business model silos**: IAM sells "passwordless"; PMs monetize managing passwords. **Unifying** them breaks both narratives.
- **Missing trust fabric**: Safe automation needs **continuous user presence + device integrity + policy bound key use**—signals that cloud only IAM can't enforce and PMs don't govern across protocols.
- **Bolt-ons ≠ one brain**: Extensions, jump hosts, and key managers add features but **don't unify policy and execution** across web, thick apps, SSH, RDP, and **offline**.
- **Deep OS integration barrier**: MagicEndpoint sits **inside the OS trust path** (Credential Providers, local enforcement), enabling **IdP-outage resilience** and consistent policy everywhere.

MagicEndpoint breaks the split by running the **entire access lifecycle**—identity, posture, secrets, keys, and sessions—from **one policy engine** that spans web and non web, online and offline.

Why It's Better

- **One brain for IAM + Passwords + Keys** — A single control plane governs **how you authenticate** and **how secrets/keys are used**.
- **Silent by default** — No prompts when policy conditions are met; **step-up** only when needed.
- **Resilient trust** — **Keeps working** when your IdP doesn't; **stops working** the instant posture degrades.
- **End-to-end consistency** — The **same** real time signals (user presence, posture, geo) govern **web, thick apps, RDP, SSH**.
- **Reduced blast radius** — Secrets/keys are **encrypted, policy bound, and auto used**—never scattered across plugins or files.
- **Future-ready**—CAEP ready continuous assurance, Passkey alignment, and Secure Internet (mTLS) integration.

Use Case

A production engineer needs to launch a **legacy ERP client**, **RDP** into a jump host, and **SSH** to a prod cluster while HQ's IdP is experiencing an outage:

- MagicEndpoint **injects ERP credentials** silently—no vault login, no copy/paste.
- MagicEndpoint handles **RDP login** via OS Credential Provider with **local posture + MFA rules**.
- For **SSH**, MagicEndpoint uses a **per-service key** bound by policy; **step-up FIDO** required for prod.
- **Access Matrix**: Only **approved users** on **approved endpoints** can reach **prod SSH hosts**.
- The moment **disk encryption** is disabled or AV is stale, **all access halts** automatically.
- Despite the IdP outage, MagicEndpoint maintains **business continuity** with **FIDO fallback**—without compromising trust.

Key Takeaway: The endpoint is where identity can be verified best. MagicEndpoint uses its IdP and endpoint agent to handle IAM, password vaulting, and secure access (FIDO2, SSH, RDP)—all without user interaction.

Principle #9

Ensure Recovery Is Passwordless and Policy-Driven

Tagline: No credentials, no devices, nothing to forget—and no password reset.

Goal: Make recovery rare and passwordless, using phone fallback and manager approval instead of costly resets.

Traditionally…

When access breaks, organizations fall back to password resets—email links, security questions, helpdesk calls. It's slow, expensive, and easy to socially engineer.

- **20–50% of IT helpdesk calls** are for password resets.
- Each reset costs **$70 in labor**, not counting lost productivity.
- Reset channels (email/SMS links, phone verification) are prime targets for phishing and credential theft—the leading cause of breaches.

A Better Way…

MagicEndpoint makes recovery **passwordless by default—and in most cases, unnecessary**:

- If you're on your verified endpoint, you're in. There's nothing to forget and nothing to reset.
- When a true fallback is needed (e.g., endpoint unavailable), MagicEndpoint invokes **policy-governed recovery**: phone approval, manager/admin authorization, and device posture checks—not passwords.

How MagicEndpoint Makes It Work

1. **Identity Continuity via the Endpoint**
   The endpoint is the anchor. MagicEndpoint ties access to verified user presence + device integrity (disk encryption, secure boot, posture), so normal access rarely needs any reset.
2. **Policy-Driven Fallbacks**
   If recovery is required, policy can demand two independent approvals (e.g., phone + manager), location/network conditions, or time-boxed access—without ever reintroducing a password.
3. **Works Online and Offline**
   Approvals can flow over the network or via BLE (for pre-boot or locked-screen scenarios), so users aren't stranded when connectivity is limited.

4. **Scoped, Least-Privilege Recovery**
   Recovery can be just-in-time and scope-limited (e.g., temporary access to specific apps) until full assurance is restored.

5. **Auditability**
   Every recovery is an explicit, logged event—with approver identity, device posture, and reason—improving accountability and compliance.

Why It's Better

1. **Eliminates Most Resets by Design** – With no user action needed for routine access, users don't "forget the endpoint"—and without the endpoint, access is intentionally blocked.

2. **Cuts Cost and Downtime** – Removing password resets reduces a major helpdesk driver and the $70-per-reset burden—plus lost productivity.

3. **Resists Social Engineering** – No reset emails, no shared secrets, no "one-time bypass codes." Recovery uses policy-backed, multi-party approvals and device-bound trust.

4. **Higher Assurance During Recovery** – Recovery isn't a weak detour; it's a stronger path (device posture + approvers + context) that tightens access until full assurance is restored.

5. **User Experience That Scales** – Recovery is fast and silent when possible (endpoint present), and clear and policy-controlled when not.

Use Cases

1. **Endpoint Present, Password Forgotten**
   The user can't recall a directory password—but they're already logged into a verified laptop. MagicEndpoint leverages device-bound trust to re-establish identity without a password reset.

2. **Unmanaged Device, On the Road**
   The laptop is unavailable. The user requests scoped access from a personal device. MagicEndpoint enforces phone approval + manager authorization and issues time-boxed access—no password created or reset.

3. **Locked Screen / Offline Scenario**
   At pre-boot or during network loss, MagicEndpoint uses BLE-based approval from the phone to unlock the endpoint under policy (e.g., require proximity + recent manager approval). Once online, MagicEndpoint syncs trust state and audits the event.

Key Takeaway: Access recovery becomes rare with MagicEndpoint's zero-interaction model. When needed, it's passwordless—using phone fallback and manager approval instead of costly helpdesk resets.

Business Bottom Line

- **Fewer tickets, lower cost, higher productivity** – Removing password resets attacks a top helpdesk cost driver (20–50% of calls).

- **Lower breach risk from human-targeted attacks** – Eliminating reset links and shared secrets reduces phishing and credential theft exposure.

- **Happier users, less friction** – People keep working. Approvals happen behind the scenes or through simple, policy-driven prompts—no memorization, no resets.

Looking Ahead: Live Key and the Secure Internet

Live Key: The Next Layer of Trust

MagicEndpoint is just the beginning. At its core, MagicEndpoint introduces a powerful concept: **trust that is dynamic, continuous, and policy-bound**. The next step in this evolution is **Live Key**—a cryptographic identity that transforms how trust is enforced across the internet.

Live Key: A Dynamic Signal for Stronger Trust

Live Key is a **policy-bound cryptographic key anchored in hardware**, designed to be available only when specific trust conditions are met. Unlike traditional keys, Live Key behaves as a **dynamic signal**—asserting identity only when the endpoint and user meet organizational policies.

Why Live Key Matters

- Reinforces the trusted channel with **hardware-backed assurance**
- Enables **mutual authentication for advanced use cases**
- Provides **non-interactive, policy-driven authentication** beyond user presence

How It Complements MagicEndpoint

- Adds **cryptographic strength** to MagicEndpoint's persistent trust channel
- Supports advanced use cases like **mTLS without requiring new standards**
- Bridges today's endpoint security with tomorrow's **Secure Internet**

Live Key is **already part of MagicEndpoint**, but its full potential will be explored in the **Secure Internet vision**—a world where every connection is mutually authenticated, every packet is trusted, and the concept of sessions disappears entirely.

The Secure Internet: Eliminating Trust Gaps

Secure Internet builds on Live Key to deliver **end-to-end trust without passwords, tokens, or fragile session models**. Where MagicEndpoint fixes today's authentication and session weaknesses, Secure Internet **eliminates them entirely** by embedding trust into the transport layer itself—using mechanisms that work **with today's infrastructure**, without requiring disruptive standard changes.

This is the future of identity-first security:

- **No passwords. No prompts. No tokens.**
- **Every connection verified. Every packet authenticated.**

MagicEndpoint is your first step toward that future.

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