

How an MSP Eliminated Standing Privileges & Reduced Attack Surface with Evo Security's Just-In-Time Access



Industry
SMB



Endpoints
1200



Evo Solution
Tech Elevation
& MFA

Challenges

- **Fragmented Access Management:** Scripts to manage local admin accounts synced to IT Glue worked separately and could not be easily monitored, creating visibility gaps
- **Retiring MFA Solution:** Passly had not been updated in years, with unreliable push notifications forcing a vendor replacement
- **Limited Audit Capabilities:** RMM could generate privileged account reports, but the process was inefficient for comprehensive security monitoring
- **Manual Account Management:** No centralized visibility into device status or automated workflows for managing JIT access

Results

- **Reduced Attack Surface:** Admin accounts now have restricted access when not in use, lowering attack vectors and overall risk
- **Improved Visibility:** Real-time device status monitoring and helpful audit logs provide transparency into privileged access activity
- **Consolidated IAM Platform:** Single dashboard for PAM and MFA replaced fragmented vendor solutions, with mobile app enabling efficient JIT access management
- **Cost-Effective MSP Scaling:** Per-technician pricing allows client growth without proportional cost increases

Executive Summary

Technology Advisory Group (TAG), a managed service provider serving Rhode Island and nearby areas for almost 30 years, needed a comprehensive solution to manage Just-In-Time (JIT) access to Office 365, client servers, and desktops. Their existing approach involved separate scripts and tools that lacked centralized monitoring, while their desktop MFA solution was being retired due to reliability issues.

After evaluating several vendors, TAG partnered with Evo Security approximately one year ago, selecting Evo for its unique combination of PAM, MFA, and mobile access capabilities. The implementation has delivered significant security improvements, enabling TAG to lower attack vectors and increase their overall security posture with clients.

President and founder Gary Harlam has already recommended the solution to others in his peer group, describing Evo in three words: "Simplified Privileged Access."

"We are very happy with the combination of features offered by the platform. I have already recommended EVO to others – especially those in our peer group."

About Technology Advisory Group

Technology Advisory Group is a Rhode Island-based managed service provider that has supported local businesses for nearly 30 years. Founded and led by Gary Harlam, TAG delivers comprehensive IT services to small and mid-sized organizations across Rhode Island and surrounding areas, helping them maintain secure, reliable, and efficient technology operations.

More than a traditional MSP, TAG partners closely with its clients to make technology work for the business—not against it. From cybersecurity and cloud strategy to proactive IT consulting and 24/7 support, the team combines deep technical expertise with a highly personalized approach, acting as both a trusted advisor and long-term technology partner.

The Challenge: Fragmented IAM and Outdated Access Controls

Before partnering with Evo Security, Technology Advisory Group faced several critical challenges with identity and access management that were impacting their security posture and operational efficiency.

Fragmented Just-In-Time Access Management

TAG required a vendor to manage JIT access to Office 365, client servers, and desktops. Their existing approach relied on scripts to manage local admin accounts synced to IT Glue, but these components worked separately without easy monitoring capabilities. The lack of centralized visibility made it difficult to see the status of devices across their client base.

Outdated Multi-Factor Authentication for MSPs

TAG was using Passly for desktop MFA, but the product was being retired. More critically, Passly had become increasingly unreliable over time. "We were not a big fan of the product - it had not been updated in years, and push notifications were not reliable," Harlam explained. This forced TAG to search for a replacement that could provide dependable multi-factor authentication for their technicians and clients.

Inefficient Privileged Account Auditing and Monitoring

While TAG's RMM could generate reports on privileged accounts, the process was not as efficient as needed. The lack of streamlined auditing capabilities made it challenging to maintain comprehensive visibility into admin accounts and ensure proper security monitoring across their client environments.

Need for Consolidated Identity Access Management

Managing multiple separate vendors and dashboards for different security functions created inefficiencies in TAG's operations. "Having MFA as an option with our PAM is definitely more convenient," Harlam later noted, highlighting the operational burden of their fragmented approach.



The Solution: Unified PAM and MFA Platform for MSPs

After evaluating several vendors approximately one year ago, TAG selected Evo Security because it offered the unique combination of services they were seeking. The implementation focused on several key components that addressed their specific challenges.

Just-In-Time Privileged Access Management

Evo's PAM solution, Technician Elevation, became TAG's primary tool for managing JIT access to admin accounts across Office 365, client servers, and desktops. The platform provides centralized visibility into the status of each device and enables management of local admin accounts with rotating passwords synced to IT Glue. "One of our primary goals was JIT access to admin accounts. We feel like this has increased our security posture with our clients," Harlam stated.

Mobile Access Management for MSP Technicians

The Evo mobile app was deployed to facilitate JIT access management across environments. "The mobile app works well with our JIT access," Harlam confirmed, providing technicians with flexible access capabilities from anywhere.

Comprehensive Audit Logging and Compliance

Evo's audit logging capabilities addressed TAG's need for improved visibility into access management activity. "The audit logs are helpful," Harlam noted, providing transparency regarding who had privileged access and for how long - a significant improvement over their previous reporting capabilities.

Multi-Factor Authentication for Enhanced Security

TAG replaced their retiring Passly solution with Evo's MFA capabilities, consolidating authentication with their privileged access management. "Having MFA as an option with our PAM is definitely more convenient," Harlam noted, appreciating the integration that eliminated the need for separate vendor relationships and dashboards.

"We feel like this has increased our security posture with our clients... with JIT, the Admin accounts have restricted access when not in use, so we have lowered our attack vectors and the risk."

The Results

The partnership with Evo Security delivered meaningful security and operational improvements for Technology Advisory Group. While stronger security requires some trade-offs, TAG found the added protection well worth the investment.

Beyond reducing risk, Evo helped TAG turn privileged access into a standardized, scalable process. By centralizing JIT access, MFA, and audit logging into a single workflow, TAG cut operational overhead and replaced one-off fixes with a consistent access model. The result is privileged access that's easier to manage, audit, and explain to clients—strengthening security without adding complexity as the business grows.

Operational Improvements

Streamlined Mobile Access Management:

The mobile app has proven effective for JIT access management, providing technicians with convenient access to critical systems when needed.

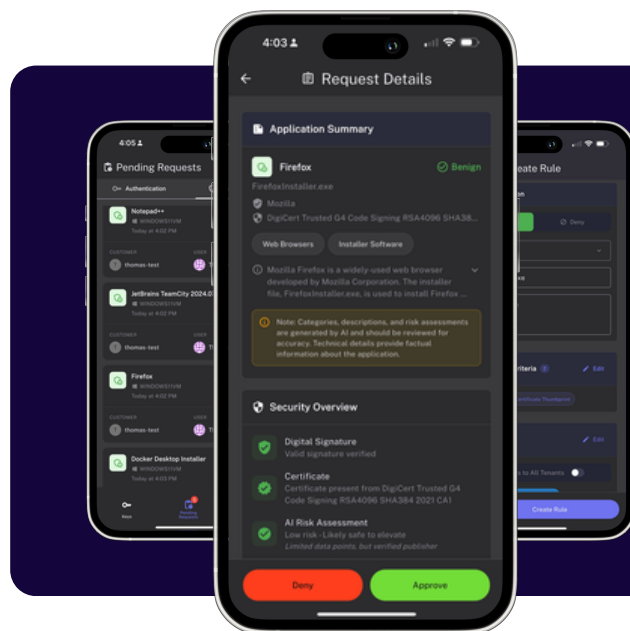
Scalable Pricing Model for Client Growth:

Evo's pricing structure, which charges per technician rather than per client, allows TAG to add new clients without increasing their security tool costs. "Pricing per tech allows us

to add clients without increasing our cost. Some of the other vendors charge by the client," Harlam noted, highlighting this competitive advantage that supports business growth.

Responsive MSP Partner Support:

TAG has worked closely with Evo's support team throughout their partnership. The team particularly appreciated the support team's responsiveness to their needs and questions.



Balancing Security and Convenience in IAM

TAG recognizes that enhanced security requires some adjustments to workflows. "Honestly, security often requires a trade-off with convenience. There are extra steps required, but we are more secure," Harlam explained. "In the case of JIT, we spend a bit more time gaining access to tenants or devices, but we are more secure!" This measured perspective reflects TAG's understanding that while it takes slightly more time to access systems, the risk reduction justifies the investment.

Looking Forward: Expanding IAM Capabilities

Technology Advisory Group continues to see meaningful opportunity to expand its use of Evo Security as part of its long-term security strategy. After successfully deploying Technician Elevation, TAG has identified End User Elevation and Help Desk Verification as logical next steps to further strengthen security and improve service delivery.

The strength of Evo's unified platform has already translated into real-world advocacy. Harlam has actively recommended Evo within his MSP peer group, citing the platform's ability to consolidate critical security functions into a single, manageable solution. For MSPs evaluating IAM and PAM tools, his guidance is straightforward: prioritize platforms that reduce complexity while delivering comprehensive security coverage. In TAG's experience, Evo strikes that balance, helping MSPs improve operational efficiency while raising the bar on identity security.

About Evo Security

Evo Security is the only IAM platform built for MSPs, consolidating six critical authentication and access tools into one multi-tenant solution. Designed to boost efficiency, margins, and security, Evo simplifies IAM for MSPs, MSSPs, and their SMB clients. Our unified platform integrates MFA, SSO, RADIUS, Help Desk Verification, and PAM, ensuring seamless, secure access. Evo empowers IT service providers with a purpose-built solution that streamlines security and operations. Learn more: <https://www.evosecurity.com/>