

Protecting more than just pipelines

Natural-gas service provider improves IT security, staff efficiency and regulatory compliance by taking an automated, enterprisewide approach to IAM with One Identity

Key Facts

Company

Natural gas operations service provider

Industry

Oil and gas

Country

United States

Employees

5,000

Challenges

A top operations service provider for gas companies needed to increase identity-and-access-management (IAM) insight, control and efficiency — consistently, across its enterprise.

Results

- Improves security and IAM insight
- Increases efficiency and cuts risk with automation
- Boosts ROI and minimizes IT complexity
- Creates one source of user profile data from disparate repositories
- Provides a flexible platform for customization

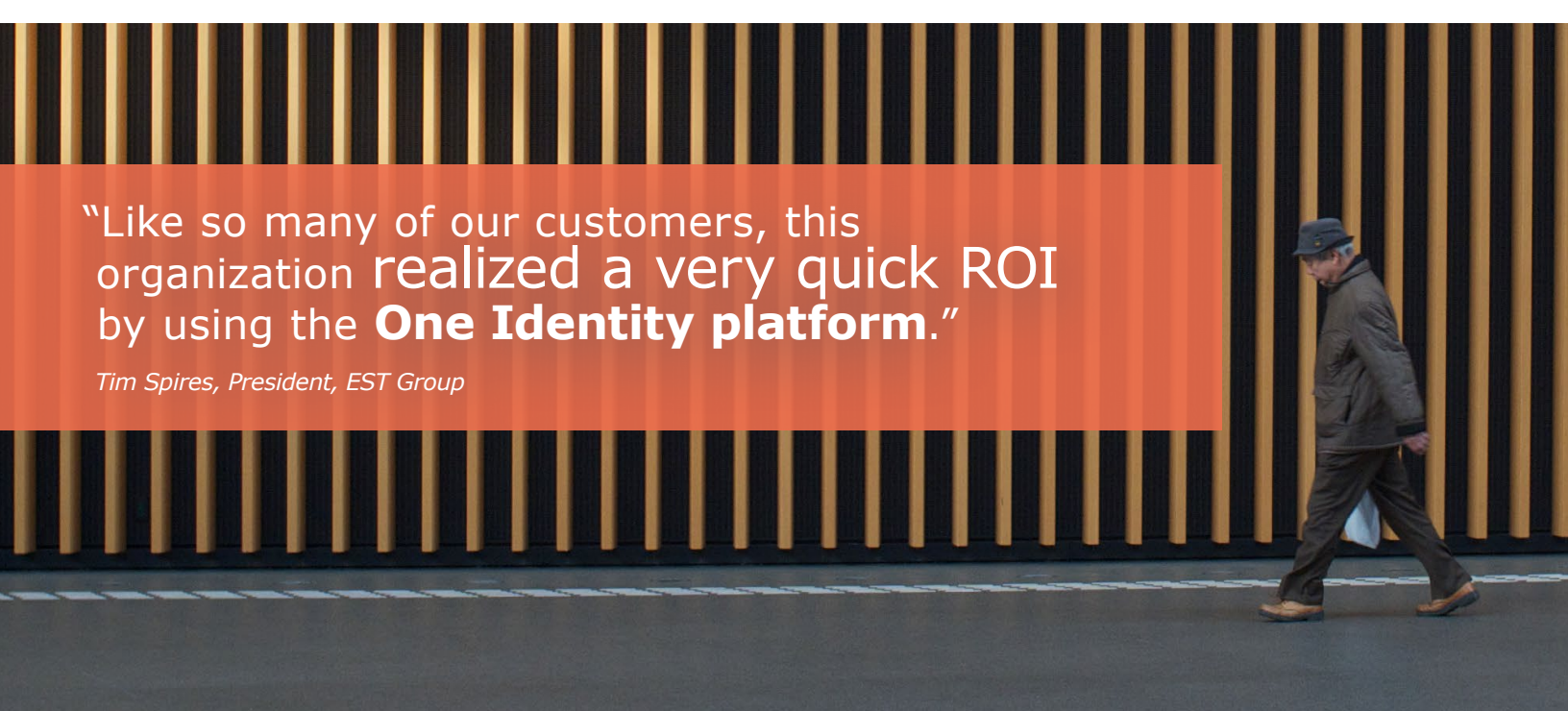
Products

[One Identity Manager](#)

[Password Manager](#)

To improve security, many organizations no longer allow IT employees to directly access Active Directory. They have also empowered managers to decide which resources their staff can access. And many companies allow only help-desk staff to issue new passwords. Unfortunately, these approaches can result in security, compliance and efficiency problems.

A leading operational service provider for natural gas companies was struggling with these very issues around identity and access management (IAM). Managers decided who could access which systems on a case-by-case basis, so permissions varied greatly across the organization. Manual provisioning and deprovisioning workflows meant people had to wait for system access, and when they switched roles or left the company, they might have access to systems longer than they should. IT staff didn't have an enterprisewide view of user profiles and it was very time-consuming to see system-access histories. That's because they had to obtain this insight



“Like so many of our customers, this organization realized a very quick ROI by using the **One Identity platform.**”

Tim Spires, President, EST Group

from individual system log files, and text files downloaded from the company’s disparate Active Directory, Azure Active Directory and Active Directory Lightweight Directory Services (AD LDS). In addition, help-desk staff knew people’s passwords and they spent too much time managing them.

To overcome these challenges, the organization engaged third-party EST Group for help in designing and deploying an IAM solution. It needed to work with existing investments including the different user repositories. And, the organization wanted to be able to define its own user roles and IAM workflows instead of using preset templates. After evaluating leading IAM technologies, EST Group proposed a solution based on the One Identity platform. Nathan Wiehe, vice president of identity and security services at EST Group, says, “What stood out to me was that we could customize Identity Manager and Password Manager to meet the organization’s very specific needs.”

A flexible framework that simplifies role and privilege mapping

Working with business and IT employees, EST Group helped define every possible user role and the digital tools each one requires. They also categorized all corporate data. Tim Spires, the president of EST Group, says, “Once we classified their data into what is public, what is private and what might be secret or intellectual property, we were then able to correlate access to each type of data with specific user roles in Identity Manager.”

Improving protection and increasing efficiency with automation

Employees and contractors now get faster access to the tools they need and the company has improved security. That’s because it worked with EST Group to establish consistent and automated IAM processes. So today, when an employee changes someone’s role in the human resources system, Identity Manager automatically initiates


the appropriate provisioning or deprovisioning workflows.

Faster operational insight and regulatory audits

From the Identity Manager dashboard, IT staff can immediately see user profile information including who can access what — and they can see access histories for systems, data and users. This insight and the ability to instantly generate IAM audit reports have simplified and improved both security and regulatory compliance. As an added precautionary measure, EST Group implemented extra monitoring via Identity Manager for employees who can access sensitive data and those who have administrative privileges.

Greater efficiency, security and ROI

People can now reset their own passwords instantly from a portal. This saves time for employees and reduces risk because only one person knows each password. With its One Identity technologies, the company can



“We could customize Identity Manager and Password Manager to meet the organization’s **very specific needs.**”

Nathan Wiehe, Vice President of Identity and Security Services, EST Group

also use two-factor authentication to protect sensitive information. “One Identity has a tremendous solution for automating the governance around both access and data,” says Spires. “Like so many of our customers, this organization realized a very quick ROI by using the One Identity platform.”

About EST Group

EST Group is an IT solutions company, with a strong focus in providing integration and consulting services tailored around automating, managing and securing organizations’ IT environments. Our goal is for our clients to achieve maximum efficiency and productivity.

About One Identity

The One Identity family of identity and access management (IAM) solutions, offers IAM for the real world including business-centric, modular and integrated, and future-ready solutions for identity governance, access management, and privileged management.

[Learn more at OneIdentity.com](https://www.oneidentity.com)

The One Identity logo is a trademark of One Identity LLC and/or its affiliates. Other trademarks are property of their respective owners. Availability and terms of our solutions and services vary by region. This case study is for informational purposes only. One Identity LLC and/or its affiliates make no warranties — express or implied — in this case study. ©2018 Quest Software Inc. All Rights Reserved.

 **ONE IDENTITY**