



CASE STUDY

FINANCIAL SERVICES FIRM



This is a blind case study. This is an actual PortSys customer. For legal reasons, security practices or privacy concerns, customers sometimes prefer not to make all of their security and company information public in case studies.

Total Access Control Provides Zero Trust Application Access for Financial Services Firm



Security is a must for any company in the financial services industry. This PortSys customer provides portfolio management tools along with IT infrastructure development and services.

“For most of our clients, we are their IT infrastructure,” said the senior systems engineer for this firm.

The company had an important decision to make when Microsoft announced it was ending support

for its Unified Access Gateway (UAG). The IT team set out to find a replacement that would enable and improve upon the secure remote access and endpoint security features found in UAG.

After an extensive review, the team found that Total Access Control (TAC) from PortSys offered even more features and functions than UAG, on a Zero Trust Access platform that was immediately familiar. “The console is similar to UAG, but more streamlined and modern,” the senior systems engineer says.

“ THE CONSOLE IS SIMILAR TO UAG, BUT MORE STREAMLINED AND MODERN. THERE WAS NO OTHER PRODUCT ON THE MARKET THAT GAVE US THE ENHANCED FEATURE SET WE REQUIRED WITH THAT FAMILIAR LOOK AND FEEL.”



“There was no other product on the market that gave us the enhanced feature set we required with that familiar look and feel.”

PORTSYS TAC: SECURITY MADE SIMPLE

TAC provides secure access to any application from any device, using a reverse proxy approach to protect applications. Rather than log in directly to an application, users log in to the TAC gateway, which applies predefined policies to determine whether the user should be allowed access to the requested application.

Importantly for this financial services firm, TAC also provides Single Sign-On (SSO). Users authenticate just once to the TAC gateway and then can access any application for which they are authorized.

That feature allows users to log in from a home laptop, authenticate to the TAC gateway, and see the same menu of applications they would as if they were in the office. “We have more users who are able to work from home than we ever did in UAG,” the senior systems engineer says.

Previously, setting up an employee or client to work from home required a hardware-based virtual private network (VPN) device, which was complex and expensive. Each device cost more than \$1,000 and had to be shipped to the employee’s home, along with a company-approved laptop at a cost of about \$2,500. The IT team had to put labels on the VPN device denoting which port connected to the router and computer, and how to configure it. The process proved difficult and laborious, resulting in excessive amounts of support calls and hand-holding. What’s more, the VPN worked only with Microsoft operating systems.

With TAC, the company's employees, clients and even partners can now use their own devices, no matter what operating system they use. TAC runs a security check to ensure the device is configured with proper antivirus and firewall software, and that it is up to date on security patches and the like. Users employ an RSA SecurID token to provide multi-factor authentication, which costs only about \$100 for 3 years.

"TAC is very simple," the senior systems engineer says. "Users get a one-page instruction sheet that shows how to connect through a URL to us. They enter their username and password, input the code from the RSA SecurID token and, once authenticated, that's it. They see their usual desktop layout and can immediately access any application."

EASY IMPLEMENTATION

TAC was also easy for the company's own IT team to deploy. "It was extremely easy to migrate from UAG to TAC," the senior systems engineer says. "PortSys

has some really good engineers I've worked with over the years." In many instances, if the financial services firm had a suggestion for a customization or found something wasn't working as intended, PortSys would have a new software build available later on the same day.

The IT team also found TAC to be more stable and easier to manage than UAG. The company has two data centers, one for its headquarters in Pennsylvania and another at a colocation facility in a neighboring state. With UAG, the two were completely separate and it was difficult to keep them in sync. Any change implemented on one would have to be manually entered on the other. If they fell out of sync, it could result in users being denied access.

By contrast, the IT team implemented its two TAC instances in a cluster such that when they make a policy change in one, it automatically replicates to the other. "It's a massive improvement," the senior systems engineer says.

“TAC IS EASIER, MORE SECURE AND MUCH MORE COST-EFFECTIVE COMPARED TO ALTERNATIVE SOLUTIONS ON THE MARKET TODAY.”



“ THE PORTSYS SUPPORT TEAM IS GREAT, AND OUR OVERALL EXPERIENCE SINCE MOVING TO TAC HAS BEEN FANTASTIC.”

COUNTING UP THE TAC BENEFITS

“TAC is easier, more secure and much more cost-effective compared to alternative solutions on the market today,” the senior systems engineer said.

By eliminating the need for a hardware-based VPN, the company now fields far fewer support calls from employees and clients, while also generating annual savings of more than \$100,000 compared to the cost of competitive solutions. Those benefits are enabling the IT team to justify an increase in the number of users who now have access from home.

Prior to rolling out TAC, the financial services firm had only about 15 of its 50 employees set up with the VPN in the headquarters. It now has about 35 set up to log in from home with TAC. In all, about 160 employees, customers and partners use TAC –

and all of them can potentially take advantage of the remote log-in features of TAC, making them more productive.

Most importantly, TAC provides the security that the financial services firm needs, ensuring only authorized users can access its systems. It even integrates with the company’s security information and event management (SIEM) platform, providing potentially valuable information on who accessed what resources, and when. Such details are important to help the company meet regulatory requirements.

“TAC provides the robust security layer that we require to protect our enterprise resources, and then backs it up with great reporting that helps us to stay on top of any issues in real time,” the senior systems engineer says. “The PortSys support team is great, and our overall experience since moving to TAC has been fantastic.”



Learn more about how PortSys and TAC can secure access to all of your applications, from any device.

Visit: www.portsys.com.

+ 1 781 996 4900 (North America)

+ 44 208 196 2420 (International)

sales@portsys.com / www.portsys.com