BlackBerry

Case Study

How Strong Authentication and BES12 Help This Law Enforcement Agency to Protect and Serve New York

The Organization

First founded in 1960, the Suffolk County Police Department provides law enforcement services to five of the ten towns in Suffolk County, situated on Long Island, New York. With over 2,375 sworn members, 600 civilian members, and 400 school crossing guards, the organization operates out of seven precincts, making it one of the largest police agencies in the country. In addition to standard law enforcement, it provides a number of specialized services including marine patrols, airport operations, arson investigation, and search and rescue/medevac.

Industry Government/Public Sector
Location Long Island, New York
Employees 3000
Products Strong Authentication, BES12
http://apps.suffolkcounty.gov/police/index.htm

The Challenge

Like all law enforcement agencies, the Suffolk County Police Department needed to provide its field officers – intelligence officers in particular – with quick, seamless access to its central database through a VPN connection. For such officers, the ability to quickly obtain information on a suspect or developing situation can be the difference between a successful arrest and a failed one, or even between life and death. Therein lay the problem: in order to comply with strict IT security regulations, any device that connects to a police database must use two-factor authentication; a username and password simply aren't enough.

Traditionally, this meant equipping its field officers with physical RSA SecurID® Hardware Tokens.

"We'd been using RSA tokens for years, but there are a few problems with them in our line of work," explained Suffolk County PD Office Systems Analyst Alfred Odierno. "They're a bit confusing for non-IT people – you put in a username and password, then you need to input a code on another screen; it's a training issue. And not everyone will always carry their tokens with them. An officer in the field at night isn't going to be able to fumble around looking at a token in the dark, for example."

In addition to complexity, there was also the issue of cost. Every three years, expired tokens need to be replaced. Factor in that these tokens are easily lost or damaged, and the expenditures associated with purchasing replacements added up very quickly.

Security proved challenging, as well. Given the sensitive nature of the information police departments frequently work with, any solutions they chose would have to be compliant with the highest regulations.

"We take a layered approach to cybersecurity," said Odierno. "We have a number of different tools for monitoring and management – some are appliances, while others are just software that looks for suspicious activity. Any tools we chose to incorporate had to work with our existing solutions."

The Solution

The Suffolk County Police Department needed an affordable means of keeping their field officers connected whilst still complying with government regulations. More importantly, this solution had to be easy to use for both officers and administrators, integrating readily with existing infrastructure. Having already had several positive experiences with BlackBerry, they turned to the enterprise mobility leader to help them address the challenge of remote connectivity.

"We discussed things with our sales representative, and he got involved with setting a demo up for us," said Odierno. "It worked really well, and he helped us get our other onsite solutions working alongside BlackBerry's. After running a trial period with the demo, we purchased a hundred licenses, and have been running ever since."

With a growing fleet of Android and iOS phones coming into use alongside organization-owned BlackBerry 10 devices, Suffolk County PD also needed a cross-platform solution capable of seamlessly managing multiple mobile devices and operating systems. BES12.4, with its single-screen management, was an optimal choice, as it allowed them, through enabling a wider range of mobile devices, to better protect their VPN with BlackBerry's Strong Authentication. Rather than forcing officers to carry around a hard token or memorize a PIN, Strong Authentication allows them to authenticate with critical systems using only their device.

“There’s a government mandate that says any device that will access the law enforcement database needs to have two-factor authentication. A password just isn’t good enough anymore. We feel that between BlackBerry’s Strong Authentication and BES12, we’re now in compliance…[and] we’re in a place where we could allow our users access to national information from their mobile devices using BES security.”

- Sergeant William Okula, Executive Officer,
Suffolk County Police Department Technology Bureau

"We had a lot of officers call in saying they didn't have their token but they needed to work, which resulted in a lot of wasted man-hours," said Odierno. "But people tend not to forget their phone – and if they do, they tend to go home and get it right away."

The initial rollout, which took place approximately a year ago, was targeted at the mobile workers who needed VPN connectivity the most – field officers and intelligence command. These were also the workers for whom ease of use was the most essential. The rollout was seamless, and the results were almost immediate.

The Results

Since rolling out Strong Authentication and BES12, The Suffolk County Police Department has lowered its security costs and gained greater control over its mobile fleet. Officers in the field are able to more readily connect to the department's database in order to obtain critical information, and the IT department can spend less time on helpdesk requests and more time ensuring critical systems are kept running. Currently, administrators are discussing the possibility of enabling BYOD, leveraging Strong Authentication's capacity to support unmanaged mobile devices.

They are also looking to eventually roll out BlackBerry's Good Collaboration services, alongside several applications developed in cooperation with BlackBerry; these can be run securely on both managed and unmanaged iOS and Android devices.

Simple Implementation and Configuration

Many software security companies have multiple installations, configurations, and upgrades to sift through when a business moves from the demo phase to implementation. According to Odierno, BlackBerry's process, by contrast, was relatively painless. With the assistance of a BlackBerry representative, they were able to incorporate both Strong Authentication and BES12 with ease. Setting up employees with access to the police department's VPN is equally as simple, and reception to Strong Authentication has been excellent.

"I set one user up, and the next day I had everybody in my office wanting to convert, to hand in their token and switch over to the phone," explained Odierno. "Configuration is a lot easier as well, because we're basically deploying a device – I set it up, my Active Directory guys throw the user in the right group, and everything's good to go. The user's up and running in a few minutes."

Quick-and-Easy Training

Because Strong Authentication is so much more intuitive than an RSA token, the time and budget spent on training has also decreased significantly. Administrators have yet to have an officer request their help in figuring things out, and they've had very few returns. What little training officers do require can be completed in a matter of seconds.

"We give them a phone, set up access, show them how to work data, and send them out the door," said Odierno. "We literally only need to give them a 45 second tutorial, and they're good to go."

No-Fuss Connectivity

High-availability and quick connectivity are critical for field officers – and BlackBerry provides Suffolk County Police Department with both. Odierno recounted at least one instance where an officer was able to act quickly and effectively thanks to BlackBerry. He was able to get out his laptop, immediately connect to the network, and gather the information he needed to identify the suspect and make an arrest – the suspect, said Odierno, would likely have escaped had the officer had to fumble with or forgotten, the token.

Sgt. William Okula, Executive Officer of Suffolk County PD's Technology Bureau, had a similar story to tell.

"When Al set me up with my VPN, I connected to the network and entered my name and password," said Sgt. Okula. "The instant I hit 'enter,' my phone dinged – it was the VPN client asking me if I was trying to log in. I was surprised at how quickly everything happened; it only took a second or two before I was authenticated. I don't think my finger was even off the enter key before BlackBerry asked me if I was trying to VPN in."

Easier Administration

In addition to greater ease of configuration, Strong Authentication significantly reduces the resource load on IT. Phones are less likely to be lost, stolen, or hacked, and they never fall out of sync with the police department's servers. What's more, users can be granted access to the system without requiring Odierno's presence.

"In the past, if Al wasn't here to physically hand out the token and set up everything with RSA, the user had to wait for access until he arrived," explained Sgt. Okula. "Now, we're able to delegate a simpler setup to IT, and just hand the user their device. After that, they're up and running."

Disabling connectivity for a user that's left the department is also a seamless process – a single click prevents them from logging in remotely, a process that can even be tied to Active Directory group membership.

This new process allows officers to take to the field much quicker, and operate with much greater efficiency. It also allows Suffolk County PD's IT professionals to put more emphasis on maintaining critical systems, securing sensitive data, and seeking new and innovative ways to empower and enable their organization.