



Regional Police Force Alerts Peers Nationwide of Wartime Threats

→ One of the largest police forces in England and Wales, the **Avon and Somerset Constabulary** has roots in the 18th century. In modern times, it has pioneered practices that have been adopted across the U.K. It was the first to photograph prisoners and to recruit female cadets. Now, in the Internet Age, the constabulary is the first to use ActiveScout Site to protect its network from attackers.

About the Customer



- One of the U.K.'s largest regional police forces with jurisdiction covering 1,856 square city and country miles and 1.5 million residents
- More than 5,000 law-enforcement and support employees
- Award-winning online police services

Most of the operating budget for the Avon and Somerset Constabulary goes to fighting crime. The force's jurisdiction covers 1.5 million residents spread across 1,856 square miles, from the industrial city of Bristol to the historic town of Bath, from wild moors to dense forests, from holiday resorts to quaint villages. Its approximately 5,000 employees have access to the full range of sophisticated law-enforcement technology. But the force's rich online police services are a particular source of pride and essential communication tools.

Protecting the Protectors

"There's no direct connection to our law-enforcement data via the Internet," says Rik Kershaw-Moore, the constabulary's information security administrator, "but hackers don't know that. Like any police force, we're an attractive target."

Kershaw-Moore was receiving security alerts from 300 to 500 individual IP addresses each week. "We needed an extra level of protection," he says "something we could trust to reduce the number of people getting through."

The constabulary's existing security system consisted of a firewall, a free-ware intrusion detection system (IDS), and an intrusion prevention system (IPS) that Kershaw-Moore had developed himself. "As a government agency, we are audited regularly for performance to standards," he says. "I needed to replace the home-grown IPS with something more professional. But I didn't have much money to spend."

Working alone, Kershaw-Moore also sought a proactive solution that was accurate and automated. His current security setup required him to spend time each day monitoring firewall logs for suspicious activity and responding to false positives from his IDS and IPS.

Elegant Appeal, Rapid Results

Kershaw-Moore read a review of ActiveScout in *Information Security* magazine, could see that the product was unique, and requested an evaluation. "I was absolutely fascinated with ActiveScout," he says. "The elegance with which it works appealed to me straight off."

Over the years, Kershaw-Moore had become accustomed to firewall and IDS implementations lasting three to six months. "It takes lots of effort to get good results," he says. "ActiveScout, on the other hand, is an uncomplicated,

one-stop operation. It took less than an hour not only to get the evaluation up and running but also to start instantly receiving real-time reports."

The results were immediate. Just one day after installing ActiveScout—just two days after the launch of Operation Iraqi Freedom—Kershaw-Moore saw a spike in attacks on his network from IP addresses in Egypt. "We received 35 attacks in 15 minutes, when we had received just two total since January," he says. "Was someone trying to access our network maliciously? Infect us with a worm? Regardless, we warned other police forces across the U.K. to check their systems. Our ActiveScout Site installation helped to protect law-enforcement networks nationwide."

ActiveScout gets the job done by using its patented ActiveResponse technology to recognize pre-attack reconnaissance activity, engage the suspicious parties in a counterfeit dialogue, and track their subsequent behavior. If they later attempt to access the fictitious resources provided by ActiveScout, they "prove their intent" to attack and trigger an automatic block. Identification is 100-percent accurate. Meanwhile, legitimate traffic moves freely.

“When we received 35 attacks from Egypt in 15 minutes, we warned other police forces across the U.K. Our ActiveScout Site installation helped to protect law-enforcement networks nationwide.”

Rik Kershaw-Moore, Information Security Administrator, Avon and Somerset Constabulary

Benefits Summary

- With ActiveScout, the Avon and Somerset Constabulary replaces a home-grown IPS with more professional, proactive attacker prevention.
- As the first U.K. police force with ActiveScout, the constabulary alerts other forces to potential network threats.
- The reasonable cost, easy management, and 100-percent accuracy of ActiveScout helps a government agency save human and financial resources needed for law enforcement.

“The automatic blocking function is just brilliant,” says Kershaw-Moore. “It gives me a warm fuzzy feeling inside.”

Icing on the Cake

One of Kershaw-Moore’s favorite aspects of the product—what he calls the “icing on the cake”—is the graphical user interface of ActiveScout Site Manager, which provides a geographical display of attacker activity in a series of charts, complete with animation options. “The Event Viewer enables me to see what’s happening around the world over time. I can create a ‘movie’ that shows which IP addresses are most targeted, which ports are being probed, and which countries are experiencing or launching the most attacks, day and night. It’s quite mesmerizing.”

It’s also quite a powerful sales tool. Kershaw-Moore used the Event Viewer to demonstrate the effectiveness of ActiveScout for his IT director when it came time to ask for the funds to buy the product. “It was very easy to get the purchase approved,” he says.

In addition to improved reporting tools, Kershaw-Moore prefers the proactive way that ActiveScout works, telling him that it has handled the problem, rather than alerting him that he needs to handle it himself. “The firewall will give me a text file, send me an e-mail, or—worst-case—page me in the middle of the night to tell me that something is wrong,” he says. “With ActiveScout, an alert simply pops up on my computer screen notifying me of a blocked attack. Moreover, it’s accurate and produces no false positives, which used to comprise about 30 percent of the alerts we received.”

Overall, says Kershaw-Moore, “ActiveScout lets me automatically block attackers in real time. It was easy to implement with no training. It functions successfully with our firewall and IDS. And it delivers meaningful results quickly.”

Moreover, ActiveScout is saving Kershaw-Moore four hours a week compared to managing his home-

grown IPS. That’s time he can devote to improving other areas of network security without adding staff. And money that can go to building the Avon and Somerset Constabulary’s crime-fighting resources.

About the Avon and Somerset Constabulary

The tenth largest of 53 regional police forces in England and Wales, the Avon and Somerset Constabulary employs 3,500 police officers and 1,500 support staff and hosts a training school that graduates approximately 40 officers every two months. Its jurisdiction serves a population of 1.5 million and is divided into eight districts covering 1,856 square miles, including the cities of Bristol and Bath, as well as the surrounding countryside. For more information, visit www.avonandsomerset.police.uk.



ForeScout Technologies, Inc.
2755 Campus Drive, Suite 115
San Mateo, CA 94403
USA

T 650.358.5580
F 650.358.5581

About ForeScout Technologies

ForeScout Technologies’ automatic Intrusion Prevention system is based on a simple philosophy: Identify and stop the attacker thereby preventing both known and unknown attacks. The patented ActiveScout solution provides “Protection by Proven Intent”, a methodology which identifies and blocks attackers with 100% accuracy, enabling the confidence to turn on automatic blocking. **For more information, please visit us at www.forescout.com.**