

## Navy taps Securify to manage legacy apps risk

By [DAN VERTON](#)  
AUGUST 13, 2003

The U.S. Navy has awarded a \$5.8 million contract to Mountain View, Calif.-based Securify Inc. that's designed to help the service tackle one of its most pressing security challenges: integrating thousands of legacy applications into its multibillion-dollar Navy/Marine Corps Intranet (N/MCI) program.

The two-year deal, signed officially last month and announced Aug. 11, will give the Navy unlimited use of Securify's SecureVantage security management product. The goal is to ensure that all of the Navy's networks, including applications and shipboard networks, comply with the more robust security policies put in place by the N/MCI contract.

The Navy awarded the \$6.9 billion N/MCI contract in 2000 to Plano, Texas-based Electronic Data Systems Corp. Among the challenges that have at times threatened the health and stability of the contract has been the existence of tens of thousands of applications that, if moved into the Intranet, would expose the Navy to security vulnerabilities.

The total number of legacy applications now stands at 30,000, and of those, 12,000 have been either approved or approved with restrictions to operate in the N/MCI environment. The Navy hopes to get the total number of applications it uses down to 5,000 in the coming months, according to Capt. Chris Christopher, staff director at the N/MCI program office.

The deployment of the Securify product will help the Navy more quickly integrate existing applications -- the majority of which still sit on servers located outside of the N/MCI, he said. Starting on Oct. 1, all new applications deployed by Navy units must comply with stringent N/MCI security requirements.

"That's going to be a challenge," said Christopher. "There's probably going to be a lot of waivers put in to try to move the process along."

Steve Vetter, director of strategic planning for the N/MCI program at EDS, said the key issue facing the Navy -- and the driving factor behind the decision to purchase the Securify product -- is the need for enough information about the

security of various legacy networks and applications that good decisions can be made about which applications to allow inside the N/MCI environment.

"The Navy is much more comfortable with the decisions they're making about how legacy applications are connected," said Vetter. "We believe that Securify will be a very important step forward in allowing [the Navy] to more rapidly address the situation," said Vetter.

For now, the Navy is moving to deploy 65 enterprise SecureVantage monitoring points, which are PC-based platforms that run on Red Hat Linux, said Carl Wright, vice president of federal operations at Securify. The typical deployment location for the monitoring point is behind the firewall, he said.

"SecureVantage focuses on expected good behavior of network traffic" and enables rapid assessment of that traffic based on N/MCI security policy, said Wright. "It's not an intrusion-detection system or an anomaly detector," he said. The product, slated to be updated in October, uses role-based authentication and is expected to provide the Navy with important statistical information about which regions in its global network are integrating faster. It will also provide the Navy and its partner EDS with data on which applications are proving most difficult to integrate.

"Most government organizations today really don't understand what their [current] IT environment is like," said Wright. "And as they moved during the last two years from mainframe to distributed client/server architectures, they really lost control of that information architecture."

In addition to the N/MCI program, Securify has been doing a lot of work with the Defense Information Systems Agency and the U.S. Central Command in support of Operation Iraqi Freedom, validating the security configurations of Web sites and user traffic, said Wright.

Source: Computerworld