

Transition

SBIR Topic Number:
AF01-119

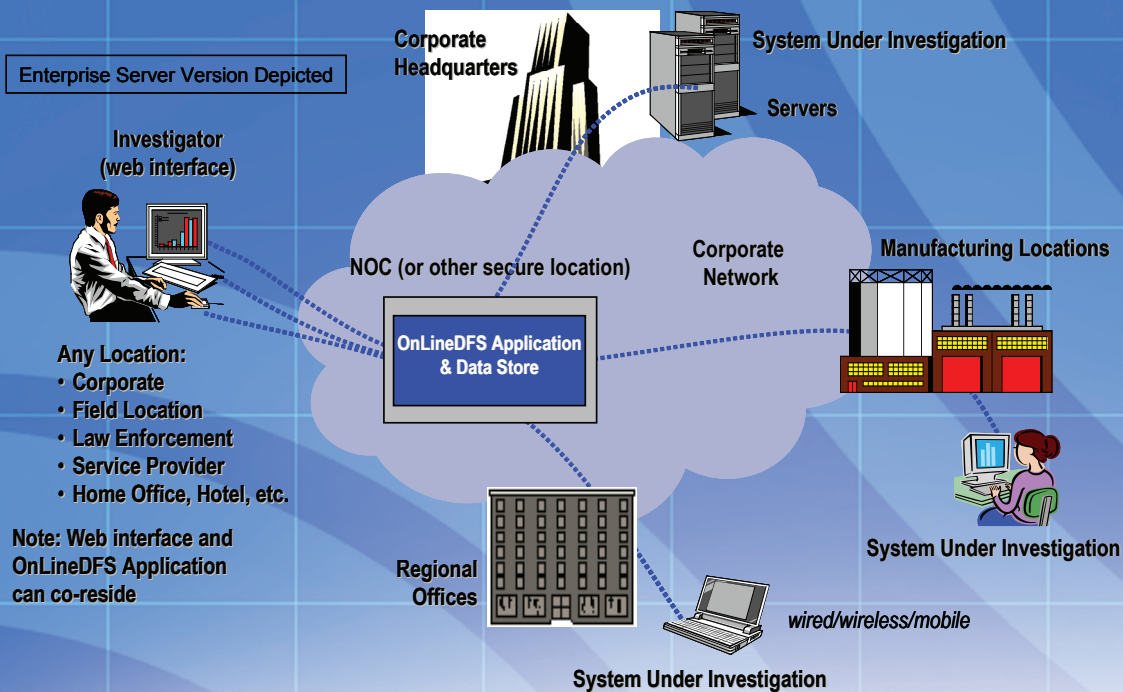
SBIR Title:
Mobile Platforms to
Support Network
Forensics

Contract Number:
F30602-02-C-0161

SBIR Company Name:
ATC-NY, Ithaca, NY

Technical Project Office:
AFRL Information
Directorate, Rome, NY

An example of Air Force supported SBIR/STTR technology that has been transitioned into an Air Force or other DoD system or subsystem or used by Air Force test ranges and facilities or maintenance depots.



Incident Response and Computer Forensics Product to Investigate Live Computers Enhances Enterprise Security

- With support from the Air Force SBIR program, a low-cost, low-infrastructure product for investigating security breaches in live computers in enterprise networks was developed and named the OnLine Digital Forensic Suite
- OnLineDFS is easy to deploy, maintain, and use
- Ideal for use by enterprise information technology (IT) security personnel and law enforcement agencies
- The patented OnLineDFS technology does not use pre-installed agents, making it ideal for use in network security environments where no additional infrastructure is desired

Commercialization Pilot
Program Series

20110517a

A

DISTRIBUTION A:
Approved for public
release; distribution
unlimited.

SBIR Requirement

In a large computer network, a sophisticated and coordinated attack can have a devastating impact. To thwart the effectiveness of such an attack, investigators and administrators must be able to quickly understand which resources were affected and how they were affected. Complicating this task is the fact that few large facilities, either commercial or military, have sufficient expert personnel to physically examine each network segment that was attacked, as often these networks will be hundreds, if not thousands, of miles apart.

SBIR Technology

Mobile Forensic Platforms (MFPs) are a tool to aid investigators with the computer network forensic task. MFPs are computers that are quickly deployed on any network to perform remote forensic investigation with very high assurance security. The MFPs contain a number of extensible forensic tools to allow an investigator to quickly and securely examine network resources remotely.

MFPs give incident responders the ability to quickly respond to coordinated computer attacks. Because of the limited number of expert personnel who can perform forensics live over a network in any organization, MFPs provide an edge in defending against such attacks by giving investigators direct, low-level access to many geographically diverse networks. This increases the effectiveness of the experts by allowing them to conduct investigations without requiring them to travel to the sites, which in turn creates a stronger defense against coordinated attacks. The mobile platforms provide remote access without further risk to the security of the installation.

Transition Impact

ATC-NY used the MFP SBIR technology to develop its OnLine Digital Forensic Suite™ (OnLineDFS; www.OnlineDFS.com). OnLineDFS aids investigators and administrators with the forensic task of system assessment following a suspected intrusion or internal security issue and the potential compromise of a host. It can be quickly deployed on any network to perform remote forensic investigation of a running system with very high assurance of security.

No software needs to be preloaded on the target machines. A web-based interface allows the investigator to connect to OnLineDFS and manage an investigation from anywhere using a wide variety of web browsers and operating system

(OS) platforms. The connection, which does not need to be high speed, is encrypted via the Secure Sockets Layer (SSL) protocol.

Analysis with OnLineDFS is forensically sound—employing accepted best practices to document all actions, preserve the integrity of evidence, and maintain the chain of custody. Data is stored in non-proprietary formats, making OnLineDFS work easily with third-party tools.

Company Impact

After completion of Phase II, ATC-NY and its parent company, Architecture Technology Corporation, formed a new company named Cyber Security Technologies (CST) Corporation to launch the OnLine Digital Forensic Suite into the commercial market. Both Architecture Technology and CST have invested significant financial resources in marketing OnLineDFS and further enhancing it. It is now on its fourth major release. OnLineDFS is in use in federal, state, and local law enforcement agencies in the United States and internationally, and in public and private sector enterprise security operations. It has been recognized in the industry analyst community, most notably by Frost & Sullivan which awarded it the 2009 North American Computer Forensics Product Innovation Award.

OnLineDFS is a low-cost alternative for information technology (IT) security organizations that need to conduct investigations of live computers over their internal networks. It is also an ideal product to integrate with other security technologies, such as firewalls, intrusion detection systems, security information and event management products and the like, to automatically initiate investigations of suspect computers when possible security breaches are detected. Because OnLineDFS does not rely on pre-installed agents, it is very simple and inexpensive to deploy, maintain and use in response to an incident, on new networks/machines, and on a wide variety of target operating systems.

OnLineDFS was the first product commercialized by ATC-NY in computer forensics/incident response. Since this first project, ATC-NY has successfully bid on, won, and developed several additional products in computer forensics and incident response funded by Federal R&D programs. These products are in use by thousands of law enforcement investigators and private sector IT security personnel world-wide. As a result, ATC-NY and CST are now also engaged in a training business domestically and internationally supporting the effective use of these products.



SBIR/STTR

Air Force SBIR Program
AFRL/XP
1864 4th Street
Wright-Patterson AFB OH 45433

AF SBIR/STTR Program Manager: Augustine Vu
AF CPP Program Manager: Richard Flake
Website: www.afsbirsttr.com
Comm: (800) 222-0336
Fax: (937) 255-2219
e-mail: afrl.xppn.dl.sbir.hq@wpafb.af.mil

