

Security in Full-Force

In the wake of September 11, 2001 and the ensuing demand for stringent homeland security measures, organizations worldwide are going to greater lengths to safeguard their business practices. While NASA is among the ranks of those constantly evaluating their security infrastructures, the Agency is firmly shielded by a gold-standard protection system, thanks to an ongoing relationship with Vanguard Integrity Professionals of Las Vegas, Nevada.

NASA teamed up with Vanguard shortly after the Chaos Computer Club of Hamburg, West Germany, hacked into the NASA Space Physics Analysis Network (SPAN) in early 1987. The unlawful intrusion was not discovered by NASA until 3 months later in July. In addition, NASA learned that the Space Shuttle's Primary Avionics Software System (PASS) flight software code had been compromised in November of that same year.

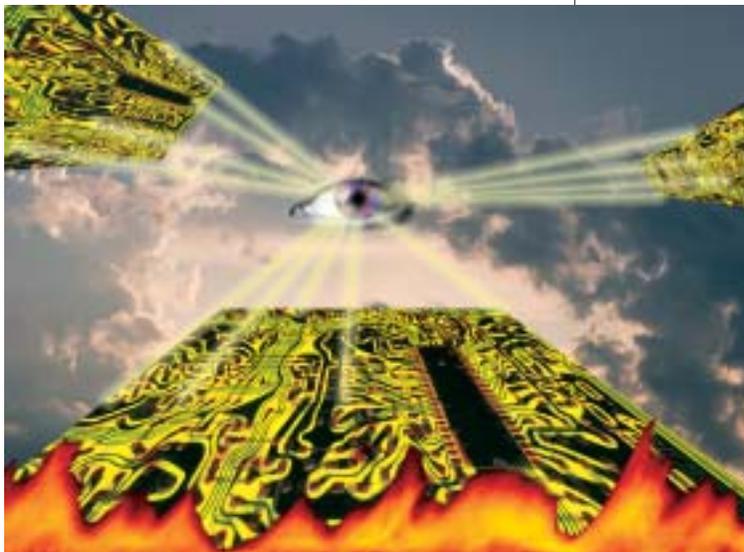
This led to the formation of the Joint Mission Operations Directorate/Mission Support Directorate Resource Access Control Facility Team in April of 1988. Tasked with performing a forensic investigation, the team unveiled that the security rules for the PASS data file were deleted on June 11, 1987, as a result of a human error made by an authorized security administrator. Essentially, the programs that NASA utilized to protect the lives of American astronauts and enable them to perform critical tasks of the Nation's space program had proven vulnerable to both malicious attack and human error.

In June of 1988, NASA recruited the IBM America Team to perform an assessment of the Software Development Facility (SDF). Within months of this date, the Mission Support Directorate (MSD) formed its own security committee to address specific issues within the SDF and other MSD-managed systems. The committee recommended that several actions be taken, including training and certification of security administrators. The thorough evaluation process concluded that the only way to provide fault tolerant security would be to implement a system that did not require human intervention. Subsequently, NASA's MSD/SDF approved the development of an automated security monitoring and enforcement system that would prevent human error and deliberate attacks. Work on a security software platform that would later become known as "Enforcer" began in March of 1989.

During that same year, a request for proposal was issued to create and implement the security administration certification program for NASA. Vanguard was awarded the contract, and subsequently, developed the NASA Security Administrator Certification Program. Vanguard also instructed, tested, and certified the Agency's security administrators.

Meanwhile, work continued on the development of Enforcer. Ronn Bailey, Vanguard's chief executive officer and chief technology officer, informally consulted with the makers on product design. When fully developed for NASA, the software system—which emulates the

Like the ever vigilant eye, Vanguard Enforcer™ monitors the constant stream of data in and out of the server system. As unauthorized attempts to access data are noticed by the system, it shuts down entry to the files before information can be copied, removed, or corrupted.



activities of highly technical security system programmers, auditors, and administrators—was among the first intrusion detection programs to restrict human errors from affecting security, and to ensure the integrity of a computer's operating systems, as well as the protection of mission critical resources. The first version of Enforcer, now known as the Vanguard Enforcer™, was delivered in 1991 to NASA's Johnson Space Center and has been protecting systems and critical data there ever since.

After a decade of successful implementation at Johnson and other NASA facilities, the Agency approached Vanguard to assume all product development, support, and commercialization of the Enforcer technology. In August of 1999, NASA granted Vanguard exclusive rights to commercialize the Enforcer system for the private sector. In return, Vanguard continues to supply NASA with ongoing research, development, and support of Enforcer.

The Vanguard Enforcer 4.2 is one of several surveillance technologies that make up the Vanguard Security Solutions™ line of products. Using a mainframe environment, Enforcer 4.2 achieves previously unattainable levels of automated security management. It offers protection 24 hours a day, 7 days a week, while maintaining standards, policies, and operating system settings (such settings are continuously benchmarked against policy baselines and best practice security standards).

Enforcer 4.2 automatically sends notification of discrepancies or violations to individuals responsible for system oversight. Enforcer supports all Simple Mail Transfer Protocol-compatible e-mail systems, and will permit multiple recipients per notice. Once a discrepancy or violation is detected, the system will provide the option to automatically generate and execute the necessary commands to return the system security to the level defined in the baselines generated by the user.

According to Ronn Bailey, studies over the past 20 years have demonstrated that as much as 70 percent of actual information system losses have been the result of authorized users, the majority of which caused by human error, and some by malicious intent.

Moving forward, Bailey notes that there is a major commercial focus on protecting the Internet and networks with layers of firewalls (systems that enforce access control between two networks) and network intrusion detection. However, he adds that since the bulk of intrusions are tied to authorized, inside users accessing the computers that host critical information and transactions, the erroneous or malicious acts of these individuals fall out of the reach of firewalls and network intrusion detection. This theory applies to vital corporate, state, national, government, and military information that is stored and maintained on

mainframes behind the Internet, networks, and firewalls.

With this in mind, Vanguard is committed to expand upon its success with NASA to deliver superior security technology to corporations and other various entities all across the Nation. According to Bailey, “Enforcer is the first security software developed to defend a system against its own authorized users.” “We take great pride in knowing that this technology is protecting all manned space program missions. Vanguard is honored to bring this advanced security technology to all businesses.”

One customer that has benefited from the Vanguard Enforcer is The Depository Trust & Clearing Corporation (DTCC), the largest



financial services post-trade infrastructure organization in the world. Headquartered in New York, New York, with operating facilities throughout the United States and overseas, DTCC has become “far more proactive” in security measures with the use of the Vanguard Enforcer, according Paul de Graaff, the company’s corporate information security officer and vice president. de Graaff also notes that the Vanguard technology transcends paper-based reporting methods, is easy to maintain and track, and helps keep overall surveillance “clean.” ❖

Ronn Bailey, Vanguard Integrity Professionals’ chief executive officer and chief technology officer (left foreground), confers with a client during an attempted security breach. The Vanguard Enforcer™ software intercepts the attempted hack on the system, which is displayed on the monitors in the control room of the server farm.

Vanguard Enforcer™ and Vanguard Security Solutions™ are trademarks of Vanguard Integrity Professionals.