"Return on Investment is a vital risk mitigator in the current government environment. How does your technology help agency IT leaders make their budget case?"

Patrick Hinojosa
Chief Technical Officer
Panda Software US

Virus protection software is supposed to stop infections in the systems in which it is installed. Yet, recent research has found that recovery costs incurred due to damage from virus infections have increased significantly over the past year.

The problem, of course, is that stopping infections requires that the software already know the exact threat. This data is provided to the software in the form of signature file updates. The average anti-virus industry response time to create and distribute updates is 6.76 hours. Infections can spread faster. What used to be measured in days is now being measured in hours.

Panda's average response time to major viruses is 2.2 hours. This cuts the risk of infection dramatically, greatly reducing the expense of responding to infection. However, infection is still possible. To handle recovery, SmartClean2, Panda's exclusive Technology, enables the software to automatically clean and repair system damage caused by infections without IT staff having to individually "touch" infected machines.

In addition, Panda now has proactive technologies - TruPrevent Technologies - to detect and eliminate new unknown threats, thus virtually slamming closed the window of vulnerability.

The savings of greatly-reduced time spent responding to and cleaning up after infections dramatically affects the ROI-based budget.

Paul Smith, Vice President,
Government Operations,
VERITAS Software

VERITAS technologies help agencies make a ROI-based budget case by creating operational efficiencies and enabling agencies to become more performance based. As a result, IT becomes a value center within the agency, and investments are aligned with the Federal Enterprise Architecture.

VERITAS storage, server and service-level management products automate tasks and provide insight into the environment through detailed reporting. By allowing administrators to set up policies for automated asset provisioning, use of existing hardware increases, and tasks require less manual intervention to improve administrator productivity. Automated reporting not only allows administrators to gain critical insight into the environment for better capacity planning but also tracks uptime and performance to ensure that service levels are met.

VERITAS CommandCentral™ and data protection products allow IT to centrally manage tasks and monitor heterogeneous assets through a single web-based console that is accessible from anywhere. This minimizes complexity to increase administrator productivity, increases availability by providing a centralized view of geographically dispersed assets, and creates standardization across functions or agencies.

Interoperability in heterogeneous environments is another key component of ROI. VERITAS products don't lock customers into a particular vendor solution, allowing agencies to leverage their existing technology investments and remain flexible when choosing new technology.

John Stringer
President and CEO
Wyse Technology Inc.

Thin-client solutions from Wyse Technology, the leader in server-centric computing, serve to dramatically improve return on investment and lower total cost of ownership in the form of reduced maintenance requirements, decreased downtime for staff, improved security, and lower hardware costs. Thin clients, defined as devices which access applications and data that are hosted centrally on a server, are more secure, manageable, affordable, and reliable than a client-server architecture, where data and applications reside on PCs spread throughout the organization.

One of the most important advantages in the agency environment lies in the security benefits of thin-client devices that do not house vulnerable applications at the desktop. Rather, thin clients remain in a "locked down" configuration, with no floppy drives, extraneous peripherals, or software downloads that can introduce additional security compromises. Thus, the threat and costs of deploying and redeploying technology typically associated with inherently insecure PCs, where hard drives can literally "walk off" the premises (as with the recent Los Alamos scandal) are eliminated. Management and reliability benefits also help reduce costs. One agency reports 50 percent fewer help desk calls, and calls that are half as long with thin clients than PCs.