



Eliminating ATM Infrastructure from Government Networks: Keep the Benefits, Lose the Hardware

Live Webcast: April 20, 2011 @ 12:00pm ET



WHEN

April 20, 2011
12:00pm ET

[Register Now >](#)

Want to win an iPad?

Just register and attend this webcast and you will be entered to win. All attendees will be eligible to win an Apple iPad™.



The Office of the Secretary of Defense has released a memorandum mandating the removal of unsupportable ATM equipment from the Global Information Grid. Agencies outside of the Department of Defense, while not affected by the mandate, will face similar challenges as legacy ATM equipment becomes more difficult and more expensive to sustain.

Fortunately, alternative technologies exist that enable the benefits of ATM and many organizations have already begun investing in them. But in a time of dwindling IT budgets, one thing is almost certain: you won't be able to transition everything overnight. The main challenge then lies in the transition effort and in the continued support of applications requiring legacy interfaces.

So how do you gracefully migrate while minimizing impact to customers? How do you minimize expense on legacy support, while maximizing support and bandwidth by leveraging network security?

If you are facing the challenge of transitioning from ATM technology, please participate in this webcast to explore:

- Alternative technologies that can provide many of the benefits of ATM
- Interworking strategies to simplify transition from legacy applications and interfaces
- Network architectures that can support both legacy and modern IP-based applications
- Network encryption technologies that keep your data's integrity without effecting your network

[Register Now >](#)

About SNR Systems: SNR Systems enables secure convergence for the Department of Defense. SNR identifies best of breed products that provide the necessary building blocks for secure, converged networks by thoroughly testing and validating those products in one of our two technology evaluation labs. With these facilities, SNR provides low-risk innovation by ensuring new technologies and products perform as expected and meet stringent DoD security and availability requirements before being introduced into the networks we design. Our personnel are trained on these products and are prepared to provide engineering, installation or support services. SNR technical personnel are likewise proficient in legacy technologies. This understanding of past, present and future technologies makes SNR uniquely qualified to support technology refresh initiatives. SNR customers include the Defense Information Systems Agency, the US Army, Air Force, and Navy and the DoD intelligence community. Additional information can be found at www.snr-systems.com.

SNR Systems, LLC, 1890 Preston White Drive, Suite 260, Reston, VA 20191 USA
SNR Systems protects your personal data in accordance with our [privacy policy](#).

Copyright © 2011 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. Junos® is a trademark of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks, 1194 North Mathilda Avenue, Sunnyvale, CA 94089-1206 USA
Juniper Networks protects your personal data in accordance with our [privacy policy](#).

KASNR Technologies Inc., 11608 Tall Pines Drive, Suite 101, Germantown, MD 20876
KASNR Technologies Inc. protects your personal data in accordance with our [privacy policy](#).

SafeNet, Inc., 4690 Millennium Drive, Belcamp, MD 21017
SafeNet, Inc. protects your personal data in accordance with our [privacy policy](#).