

Keeping Data and Applications Secure

When a company has millions of dollars tied up in projects, any breach of security, whether purposeful or accidental, could have a lasting impact on that company's bottom line.

Petris' application service provider uses the Citrix secure gateway (CSG) technology to protect access to data and applications. With this technology, Petris can safely deploy business-critical applications to employees, business partners, and customers via the Internet – all while maintaining manageability, scalability, reliability, and control. This secure gateway provides an encrypted tunnel for data traveling across the Internet between MetaFrame XP

presentation servers and client devices. A company can access PetrisWINDS NOW! through ports 80 and 443, which are the standard ports most companies use to permit access to the Internet. Overall, Petris' security is the same type as that used by commercial banks and credit card companies to protect financial transactions.

The standards-based encryption passes the presentation server connection through secure socket layer (SSL) or transport layer security (TLS) protocol, using encryption modules certified with U.S. Federal Information Processing Standard 140 requirements. This security allows Petris to deploy application simply and easily across the Internet using standards-based (SSL/TLS) encryption.

It also gives Petris the ability to security pass the user's desktop to the server, eliminating the need for multiple system and application authentication and minimizing authentication tasks required of users.



Houston, TX
+1 713-956-2165
+1 877-9PETRIS

Toulouse, France
+33 581 330 020

London, UK
+44 20 8202 2433

www.petris.com



Physical Security

Petris maintains physical security of the Citrix servers by utilizing the resources of VeriCenter, a Class A-managed hosting facility in Houston, to warehouse all its hardware. The VeriCenter maintains redundant HVAC climate control, UPS, fire suppression system, and diesel generator power backup as well as monitoring 24 hours a day, 365 days a year. Physical security for hardware and software is achieved via limited physical access to authorized personnel with multiple levels of access control.

Petris also engages multiple Internet providers to ensure 99.9% uptime. VeriCenter itself deploys firewalls intrusion detection probes, software, and other security devices.

Security Highlights

- ▶ Double Internet firewall
- ▶ Secure buildings
- ▶ Hourly virus monitoring
- ▶ Automatic failover system
- ▶ Secure Socket Layer (SSL)
- ▶ Daily backup

Continuous Monitoring

Data backup is performed daily with tapes archived at an off-site data protection vault. All systems are continuously monitored by patrol software, which provides usage reports, network traffic, and predictive error alerts. Petris also monitors performance data on all systems with respect to central processing unit usage, disk usage, and memory utilization.

www.petris.com

© Copyright 2006 Petris Technology, Inc. All rights reserved.

PetrisWINDS is a registered trademark of Petris Technology, Inc. in the United States and other countries. Other parties' trademarks and service marks are the property of their respective owners, and should be treated as such. Information in this document is subject to change without notice, and does not represent a commitment on the part of Petris Technology, Inc.

Ver.061506