



PCS Managed Services

Reduced Risk, Better Security

PCS is able to proactively manage the security of their customers' IT and applications.

With the comprehensive reporting capabilities of their remote monitoring and management software, PCS can effectively manage your IT assets, contract entitlements, and support regulatory compliance.

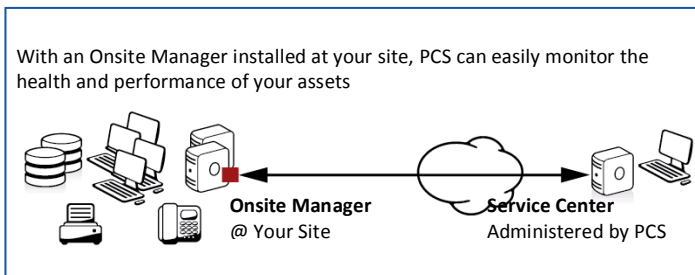
Affordable Support for Regulatory Compliance

Small and midsized business are increasing their reliance on IT and adopting more complex systems, many of them operating in regulated industries such as law, accounting, or health care. Over the last few years, governments worldwide have been enforcing new regulations to protect the privacy of customer data and the integrity of business reporting. All of this exposes small and midsized business owners—across industries—to increased fiduciary and legal risk associated with complex contract management, regulatory reporting, and compliance to security and data protection standards.

PCS can support your legislative compliance efforts in many ways, starting with regular reports that show the status of the security measures you have in place.

PCS can also enable continuous monitoring for virus, worms, spam, malware and other security threats to help assure the security of your assets and data. By leveraging Microsoft's Baseline Security Analyzer (MBSA), for example, PCS can also ensure that maximum security and data protection is achieved and documented on an on-going basis.

With automatic asset discovery and network scanning capabilities, PCS can monitor software deployments and detect illegal or unauthorized installations that may represent security vulnerabilities, such as bandwidth-heavy peer-to-peer software.



Solution Overview

Managed Workplace consists of:

Onsite Manager

A single, lightweight piece of software, installed once at each customer site. The Onsite Manager automatically performs secure, comprehensive scans of customer environments to gather the up-to-date information that solution providers need to manage their customers' IT assets with unparalleled efficiency.

With an Onsite Manager, PCS can monitor and manage anything with an IP address, including: desktops, laptops, servers, managed switches, routers, firewalls, gateways, VoIP switches and phones, printers, faxes or scanners, off-the-shelf and custom applications, specialized equipment and environmental control devices, internal and external websites, SaaS resources, virtual machines and much more.

Service Center

A powerful, web-based, centralized dashboard that allows PCS to:

- view the asset health and performance data sent by the Onsite Manager;
- “drill down” to details as required;
- perform rapid remote remediation;
- configure advanced services;
- produce a range of useful reports so you'll know exactly what's going on in your environment; and much more.



PCS Managed Services

Reduced Risk, Better Security

Protecting Data and Assets

To protect your data and assets, PCS can monitor the status and operational efficiency of your firewalls, your backup tools and data storage assets 24 X 7. With immediate alerting, they are equipped to respond rapidly to eliminate or mitigate the impact of security threats and malicious attacks.

Using extensive automated patching capabilities for Microsoft systems and software based on Windows Software Update Services (WSUS), PCS can ensure customer assets and data are protected with immediate patching direct from Microsoft.

With all of these protective measures in place, PCS can produce a range of relevant reports and detailed documentation about your hardware and software inventories and the security processes that you have implemented, so that you can supply abundant, accurate evidence of your compliance to security regulations as required and provide assurance to your customers.

Overview of Key Regulations

Sarbanes-Oxley (Sarbox)

Companies Publicly Traded on an American Stock Exchange

Sarbanes-Oxley (Sarbox) was enacted in the US in 2002. Its purpose is to ensure the accuracy of a company's financial information and the reliability of the systems that generate it.

Gramm-Leach-Bliley (GLBA)

Financial Sector

Gramm-Leach-Bliley (GLBA) is another US act from 1999. It applies to any American financial institution, large and small, and its purpose is to ensure the integrity of financial and client data.

Payment Card Industry Data Security Standard (PCI-DSS)

Global - Credit Card Processing Merchants

The standard was created in 2004 by the major credit card companies, to ensure that their merchants adhere to specific network standards in order to protect credit card systems against any security vulnerabilities, and to protect cardholders from fraud. The standard applies to any credit card processing merchant, and has five key goals: build and maintain a secure network; protect transaction data; guard against vulnerabilities; implement strong access control measures; and regularly monitor and test networks.

PCS can offer you a comprehensive security package that includes:

Firewall Monitoring – monitor status and operational efficiency of your firewalls on a 24 X 7 basis.

Patch Management – ensure your network are protected with immediate patching direct from Microsoft

Antivirus and Anti-Spyware Update Management – monitor your antivirus and anti-spyware software to ensure it's always up-to-date

Data Backup Reliability – protect your customer data by monitoring the progress and status of your backup solutions

For more information on this and other IT services, contact Joe Popham at joep@pcsc.com or the IT department at PCS at 712-263-3106.