Cloud Business Florida
Reduced Risk, Better Security

Cloud Business Florida is able to proactively manage the security of your IT and applications. With the comprehensive reporting capabilities of their remote monitoring and management software, we can effectively and securely manage your IT assets, contract entitlements, and support regulatory compliance.

Affordable Support for Regulatory Compliance

Small and midsized businesses 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.

Cloud Business Florida 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.

Cloud Business Florida 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 using Microsoft's Baseline Security Analyzer (MBSA), for example, Cloud Business Florida 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, Cloud Business Florida 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 site. Onsite Manager performs secure, comprehensive scans of your environment to gather the up-to-date information that Cloud Business Florida needs to manage your IT assets with unparalleled efficiency.

With Onsite Manager, we 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, environmental control devices and specialized equipment, internal and external websites, SaaS resources, virtual machines and much more.
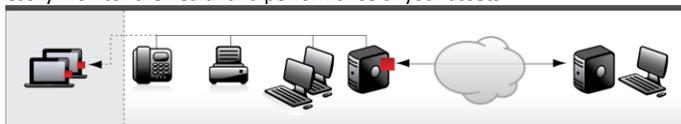
Device Manager
Installed on equipment that can't be directly monitored by Onsite Manager, such as roaming laptops, remote servers, home offices, or on an onsite Windows 7 PC if you don't have a server.

Service Center
A powerful, web-based, centralized dashboard that allows us 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.

With an Onsite Manager installed at your site, Cloud Business Florida can easily monitor the health and performance of your assets

Device Managers
@ Offsite Devices

Onsite Manager
@ Your Site

Service Center
Administered by
Cloud Business FL

Protecting Data and Assets

To protect your data and assets, Cloud Business Florida can monitor the status and operational efficiency of your firewalls, your backup tools and data storage assets 24 X 7. With immediate alerting, we 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), we can ensure customer assets and data are protected with immediate patching direct from Microsoft.

With all of these protective measures in place, we 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 accurate evidence of your compliance to security regulations as required and provide assurance to your customers.

"With this new monitoring I receive from Cloud Business Florida, I am confident my network and computers are running at peak efficiency."

- Ed Taylor, President, Second Chance Industries Plantation, FL

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-Billey (GLBA)
Financial Sector
Gramm-Leach-Billey (GLBA) was enacted in the US in 1999. It applies to any American financial institution, large and small, and its purpose is to ensure the integrity of financial and client data.

Health Information Portability and Accountability Act (HIPAA)
Health Care Sector
This 1996 act applies to all US-based health care providers. Its purpose is to ensure patient record privacy. The impact on IT is the mandate to improve security and interoperability of information systems as well as improve reporting systems.

Payment Card Industry Data Security Standard (PCI-DSS)
Global - Credit Card Processing Merchants
Created in 2004 by the major credit card companies to ensure that their merchants adhere to specific network standards 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.

Cloud Business Florida can offer you a comprehensive security package that includes the following:

- **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