CASE STUDY

IronOrbit
Cloud Computing Solutions

C.O.D. Capitol

Finance & Retail

ABOUT C.O.D. CAPITOL

C.O.D. Capital is a collect on delivery (COD) solutions provider. A COD is a type of transaction where customers pay for an item when it's delivered to them instead of when they order it. C.O.D. Capital's solution enables the buyer in a COD transaction to delay the payment of the COD for 30 to 60 days for a nominal fee (only 1.5 percent of the transaction). The 30 to 60 day window gives the buyer an opportunity to sell the item and raise the money to cover the cost of the COD purchase before the check is cashed. The COD's sellers, meanwhile, are paid the full amount of the COD purchase by C.O.D. Capital at the time of delivery, so the sellers are off the hook if the check bounces and don't have to wait any extra time to receive their payment.

THE CHALLENGE

For financial services companies like C.O.D. Capital, the security of their IT solutions is of the utmost importance. Their customers need to be able to trust them with their financial information. Oftentimes, a single security breach (which businesses are required by law to notify their customers about) or a single failed IT security audit are enough for a financial services company to lose many of its customers. Therefore, the IT solutions of financial services companies should be protected from hackers and malware, as well as from physical theft and inappropriate access by users and IT personnel.

It's also important for the IT solutions of financial services companies to be reliable and to have a disaster recovery system. Businesses need to be able to depend on financial services companies like C.O.D. Capital to be available as much as possible. Transactions delayed because of the unavailability of C.O.D. Capital's email, CRM, or payment processing systems, for example, might result in unhappy customers, lost sales, and the disruption of a vendor's supply chain or cash flow. Not only do the IT solutions of financial services companies have to be persistently maintained, however, but the IT solution should also be supported with a disaster recovery system in order to limit or prevent downtime and data loss in the event of an unexpected shutdown.

THE SOLUTION

C.O.D. Capital ended up selecting IronOrbit hosted desktops, which had the advanced security, reliability, and disaster recovery features the company wanted in an IT solution.

All IronOrbit hosted desktops are protected from IT security threats with features that include:

- **Cisco firewalls, to block unauthorized users from accessing the desktops**

- **Intrusion detection and prevention systems (IDS/IPS), which detect and thwart attempts by unauthorized users to access the desktops**

- **Gateway antivirus, which identifies and removes malware at the network level**

IronOrbit
5101 E. La Palma Ave. Suite 200
Anaheim Hills, CA 92807

☎ 888-753-5060
✉ sales@ironorbit.com
🌐 www.ironorbit.com

• Content filter, which prevents users from accessing websites that are the most common sources of malware, such as adult websites, gambling websites, social media networks, and Yahoo, Hotmail, and Gmail accounts

• Operational security, which prevents IronOrbit personnel from accessing the hosted desktops except when absolutely necessary, and encompasses ISO 17799-compliant access logs and change management procedures

• Physical security, in which we protect all of our data centers from unauthorized access with 24/7/365 onsite security personnel, closed-circuit video monitoring, and alarm monitoring

• Dedicated hosting, in which all hosted desktops have their own dedicated operating system (OS), so that users are prevented from accessing each other's data, and hosted desktops that have been infected by malware or infiltrated by hackers can be isolated and secured

> *I would **highly** recommend IronOrbit to any business owner that asked me if I was happy with my cloud solution.*

Darren Fishman, President of C.O.D. Capital

In addition, when users access their IronOrbit desktops, the only data actually transferred to the users' devices are the visual and audio streams of the hosted desktops—i.e., what appears on the users' screen and comes out of their speakers as they use the desktops. Everything else, including all of the desktops' files and applications, always remains on the servers in IronOrbit's datacenters, ensuring that the data is always protected by the Cisco firewalls, IDS/IPS, gateway antivirus, etc., of the IronOrbit security system.

Businesses that sign up for IronOrbit hosted desktops therefore don't have to worry about their users relocating important or sensitive files from a secure device to a less secure device (a common occurrence with onsite IT infrastructures and decentralized hosted IT infrastructures), or even be very concerned with the security of users' devices, since none of the company's data is contained on them.

Because of all of these advanced security measures, IronOrbit hosted desktops comply with most data security regulations, including the Payment Card Industry Data Security Standard (PCI DSS), Sarbanes-Oxley (SOX), and the Gramm-Leach-Bliley Act (GLBA). In addition, IronOrbit's datacenters are SSAE 16 compliant, meaning that an independent auditor has evaluated and verified the security controls at our hosting facilities.

In addition to being secure, IronOrbit hosted desktops are also reliable, since they're monitored and maintained around-the-clock by IronOrbit's personnel and are built with technologies from trusted, industry-leading software developers like Microsoft, VMware, and Citrix; furthermore, IronOrbit hosted desktops are backed by a 100 percent uptime guarantee. Finally, IronOrbit hosted desktops are also supported by a disaster recovery system that includes onsite data backups, network-stabilizing load-balanced switching, and fault-tolerant redundant SAN storage arrays, with an industry-leading recovery point objective (RPO) of four hours and a recovery time objective (RTO) of 12 hours—so that even if a downtime incident does occur, it won't last more than a few hours at most and won't result in any significant data loss.

THE RESULT

After signing up for IronOrbit hosted desktops, C.O.D. Capital is now thoroughly protected from security breaches, downtime, and data loss. C.O.D. Capital no longer has to worry about losing any customers because of the insecurity or unreliability of its IT infrastructure. "I would highly recommend IronOrbit to any business owner that asked me if I was happy with my cloud solution," said Darren Fishman, President of C.O.D. Capital. "Please consider me a happy, loyal customer who is proud to be on your client."

> “*Please consider me a happy, loyal customer who is proud to be on your client.*”

ABOUT IRONORBIT

IronOrbit, a division of SACA Technologies, is a privately owned and fully integrated Information and Communications Technology (ICT) powerhouse. With more than 300 years of combined industry expertise, IronOrbit innovates, develops, and produces comprehensive ICT solutions, specializing in GPU-accelerated cloud workspaces.

IronOrbit operates their own global footprint of private data centers across more than twenty regions worldwide, utilizing SOC 2 Certified, Tier 4 facilities to provide cloud services and their flagship hosted desktop solution, INFINITY Workspaces, to thousands of customers, including the US government.

IronOrbit
5101 E. La Palma Ave. Suite 200
Anaheim Hills, CA 92807

☎ 888-753-5060
✉ sales@ironorbit.com
www.ironorbit.com