SOPHOS

PARTNER CASE STUDY

IronCloud Helps Small Businesses Stay Secure in the Cloud and On Premises with Sophos Synchronized Security

IRONCLOUD TECHNOLOGIES

Partner-at-a-Glance

IronCloud, a technology provider in the Midwest, focuses on transitioning small and mid-size businesses from onsite computing to cloud applications. The company has fully integrated the Sophos Synchronized Security approach into its business as a way of ensuring that their customers' data is secure both in the cloud and on premises.

IronCloud
IronCloud Technologies
100 Saw Mill Road, Suite 3000
Lafayette, IN 47905

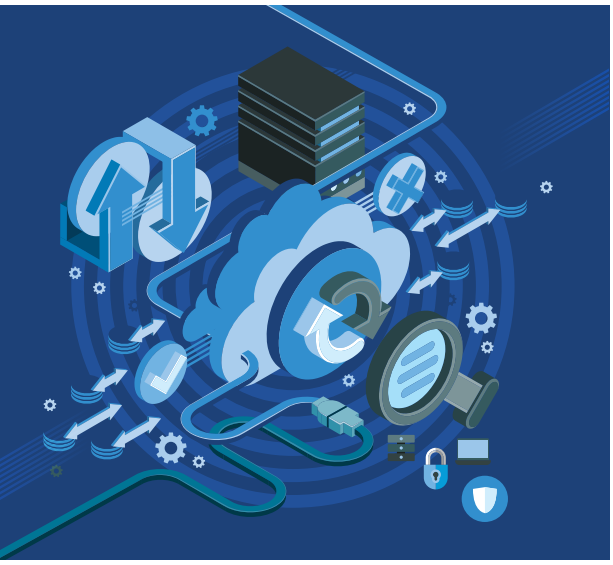
Industry
High Tech

Number of Users
50 clients

Website
www.ironcloudtech.com

Sophos Solutions
Sophos Security Heartbeat
Sophos Central
Sophos Endpoint Protection
Sophos XG Firewall

Sophos Partner
Since 2015



IronCloud, an information technology services provider headquartered in Lafayette, IN, has been in business for approximately one year and is a recent Sophos partner. Serving small to mid-size businesses across multiple vertical industries in the Midwest, IronCloud's primary area of focus is supporting its customers' computing needs, with an emphasis on assisting them with bridging the gap between onsite and cloud applications and securing both on-premises and cloud resources. IronCloud is collaborating closely with Sophos to help its customers fight threats like ransomware and to enable security that's transparent to the user.

'What I like about the Sophos XG Firewall is that it's incredibly effortless to configure. You can quickly install it and have the Firewall up and running in an hour.'

DJ Anderson
Chief Technology Officer
IronCloud

Business Challenge

As IronCloud educates its customers on the productivity and economic benefits of the cloud, the issue of security comes up in conversation as a key concern. "The number one question we get asked is how secure is the cloud? Our entire customer base is concerned about that crucial issue," Scott Brunton, IronCloud Chief Operating Officer, affirms. "Some customers are hesitant about moving to the cloud because of security concerns. At the same time, they often don't even realize that they are already using the cloud for backups, with their Office 365 hosted email, or via their Facebook accounts."

Brunton and his partner, DJ Anderson, IronCloud Chief Technology Officer are particular about their choice of vendors. "We always vet the companies that we want to work with and ensure they have solid security products firmly established. We normally recommend the same products that we use in-house every day," says Brunton. "Additionally, we read the publications like Gartner reports and white papers." Generally speaking, not all IronCloud customers have the time to become familiar with reports from industry analysts, so they trust Brunton, Anderson, and their team of experts to do the research and carefully scrutinize available security technologies. "Ultimately, our customers care more that we offer them a secure solution and that it's something that we rely on internally," remarks Brunton.

Sophos XG Firewall is a good example. In addition to using XG Firewall at the IronCloud office, Anderson also had a positive experience with Sophos network security solutions at a previous company. "I've seen Sophos perform better than various competing products I've encountered — like WatchGuard. In terms of usability and its spam filter, the Sophos Firewall is remarkable. Now with the latest version, I was impressed by how easy to manage XG Firewall is compared to other products I've experienced."

'We have no fear about what could be next on the security landscape because of Sophos' next-generation solutions. And, those solutions give us and our customers all the confidence we need.'

Scott Brunton
Chief Operating Officer
IronCloud

Good-Bye to Fire Drills

One of the key selling points for Sophos XG Firewall, according to Brunton, is that it simply works, without disrupting users.

Earlier in the year, one of IronCloud's bigger clients, a title insurance company, had an important requirement. This customer's concern was common, and similar for many industries: that all transmissions are encrypted or are on a secure channel in the cloud. Before working with IronCloud, this customer had WatchGuard, but none of the prevention, content filtering, or other advanced features were enabled because the previous vendor had failed to license the product properly. IronCloud found that Sophos XG Firewall was a solution customers could easily understand because the benefits correlated to the customer's needs, particularly the integration with endpoint antivirus capabilities.

Four or five months into the initial deployment, IronCloud discovered that the title insurance company was battling ransomware, which blocks access to computer files, often via encryption, until a sum of money is paid to the perpetrator. While enjoying lunch at a local restaurant one afternoon, Brunton and Anderson were alerted by the Sophos antivirus feature that there was a ransomware-related infection on a PC at the customer site.

Anderson put down the menu, immediately tapped into the Sophos console, and saw that malicious traffic was detected. "It only took approximately two minutes to find out that everything was under control. Sophos XG Firewall detected the threat and Security Heartbeat allowed the infected host to be immediately identified, isolated and cleaned up in short order," relates Anderson. "Best of all, the user wasn't inconvenienced by any disruption. We discussed the situation with her afterwards to let her know what happened and did an antivirus scan just to ensure everything was perfectly clean, which it was. The Sophos Security Heartbeat technology worked.

Instead of going into fire drill mode, we were able relax and finish our lunch, knowing our customer was able to do her job and carry on with her day, as planned."

Revolutionary Sophos Synchronized Security, which enables networks and endpoints to communicate through the advanced Security Heartbeat connection, helped coordinate and engage the title insurance company's defenses in this ransomware scenario. Threat information about overall security status and the health of each endpoint is automatically shared. The firewall detects threats and initiates actions that help remediate such issues. In the case of ransomware like CryptoLocker, an endpoint infected with malware dropped in from a malicious link in a phishing email will try to connect to the hacker's command-and-control center, which sends an encryption key that locks down the computer's files and documents. With the intervention of Sophos Sychronized Security, if the endpoint tries to engage with the command-and-control center, Sophos XG Firewall can block that traffic and prevent the ransomware threat from fully realizing.

Responsiveness Contributes to Quicker Issue Resolution

Both Brunton and Anderson agree that IronCloud's relationship with Sophos has been nothing but positive. They appreciate the responsiveness of both the Sophos Support team and their local sales representative. "We really appreciate the way the Sophos Support model works. If an issue arises, we are immediately transferred to a tier-two technical support team member. The last several cases were resolved quite quickly," states Anderson. "As for our dedicated account team, they are great about responding to our emails and our rep is a real asset. He's always proactive about getting answers to our questions or providing us with direction."

Simple to Use with a Wealth of Easy-to-Access Data

One of the biggest appeals of Sophos XG Firewall for IronCloud and IronCloud customers is its simplicity. "What I like about the Sophos XG Firewall is that it's incredibly effortless to configure," asserts Anderson. "You can quickly install it and have the Firewall up and running in an hour. It's far easier to configure than any other firewall that I've worked with before. Sophos XG Firewall has rules and a layout which are straightforward to follow. You can simply determine how everything works at a glance, and, if you do need to dig deeper, it's quite easy to find information."

Brunton agrees, saying that, after working with the product for a short while, he now "navigates through the console like a well-seasoned pro."

The IronCloud team also values the fact that all the information they need is instantly accessible and readily available in an easy-to-digest format. For instance, Anderson mentions that the current log system in Sophos XG Firewall made it painless to locate an iOS smartphone that was trying to access a client's server during a major patch. With the help of Sophos XG Firewall, the IronCloud team found the culprit and shut the device down by examining the network logs. "We've had phenomenal success with the Sophos XG Firewall solution," reveals Brunton. "Our customers are particularly pleased about the VPN functionality, which enables their employees to connect from any location securely."

Future Sophos Additions to IronCloud's Portfolio

As a new business on a growth path, IronCloud is looking to expand its product offerings in the near future. Brunton and Anderson are especially interested in the Sophos UTM, an all-in-one, next-generation network security appliance that includes firewall, VPN, advanced threat protection, intrusion prevention, email, web filtering, and application control.

The IronCloud team also feels that their target customer base would find Sophos Sandstorm a valuable enhancement to their existing Sophos security. Sophos Sandstorm is a cloud-based sandboxing and file-filtering system that examines attachments to determine whether they are malicious. If the malicious software is a known threat, it's immediately eradicated. If it's an unknown, or zero-day threat, Sophos Sandstorm isolates it and runs the code in the sandbox to see if it's doing something wrong. The user receives notification that the file is being checked. If the file comes back clean, it's released. If it's not, it's wiped out.

Another new next- generation technology that has captured IronCloud's attention is Sophos Intercept X, a particularly effective defense against ransomware, a growing problem for businesses of all sizes and types. Sophos Intercept X detects unauthorized encryption processes. If it detects spontaneous encryption by hackers, the process is killed and computer files are rolled back to their previous state. It also provides intelligence about the attack: what, where, when, and how it happened and what needs to be done next.

As IronCloud helps their customers move into the future, there is no question that with the help of Sophos, they will be ready for anything that comes next. "We have no fear about what could be next on the security landscape because of Sophos' next-generation solutions. And, those solutions give us and our customers all the confidence we need," concludes Brunton.

Start your free trial of Sophos XG Firewall today.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North America Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

SOPHOS

2016-10-20 CS-NA (RP)