Unitrends Recovery
Success Story

Barracuda vs. Ransomware - Not so Good

Manufacturing Success Story | Beating Ransomware

Solution Highlights

Industry | Manufacturing

Protected Environment:

- VMware virtualized servers
- Physical servers
- Machine controllers

Solution

- Unitrends Recovery Series
- Spanning Backup for Office 365
- Unitrends Forever Cloud
- Unitrends DRaaS services

Benefits

- Automatic ransomware detection
- Rapid cloud data seeding
- 90 Day cloud data retention
- Full DRaaS services

> “If Unitrends had been their original backup solution our client would have recovered in a single day. Instead trying to recover with Barracuda meant they were down nine days.”

John Smith
CEO
Conversant Group

Are You Ready to Get Protected? Connect with us Today for a Customized Quote

The Challenge

In 2019 an employee of a mid-sized manufacturing company based in Tennessee opened a suspicious email and infected their computing infrastructure with ransomware. The ransomware brought business to almost a complete halt and demanded 2 bitcoin to unencrypt the data on each server, about $10,000 per machine. The CIO called in their new IT technology partner Conversant Group for help in determining how best to recover and ensure another infection can not happen again. The company was using a Barracuda appliance backing up to the Barracuda cloud so they thought they were safe. However when they tried to recover there were several nasty surprises. “Not every file was being backed up, files had changed locations so even backups that were being performed were not successful, and restoring from Barracuda’s cloud was horrendous at best.” reported Brandon Williams, Chief Operating Officer of Conversant Group.

The Solution

Conversant Group began the recovery by examining their alternatives. Due to the challenges with Barracuda they reached out to the ransomware criminals and were surprised to get almost an enterprise-level of communication. “They were using an internet language translation tool as the English was odd so we knew we were dealing with a foreign group.” said Williams. “They responded to our communications around the clock so it wasn’t just a guy in his basement. Because of the issues with Barracuda, we were forced to pay ransom on three critical servers and fortunately for the company the criminals kept their word and supplied files to decrypt the data.”

The company had purchased a Unitrends Recovery Assurance appliance just a week before, so it arrived just in time to be part of the recovery operations. As files were slowly recovered from Barracuda they were immediately backed up to the Unitrends appliance. “What was cool to see was that the automatic ransomware detection software in the Unitrends appliance was activated by the backups, so the company now knows they are protected by a superior solution and the chances of another infection is much, much lower.” said Williams. This is critical as ransomware criminals are known to reattack earlier victims that have shown they will pay for a recovery.

The Results

Shortly after the ransomware recovery the company lost a controller in a legacy storage array that had to be used for space during the ransomware recovery. Using their Unitrends Recovery Series appliance and the instant recovery feature, they were able to fully restore all their data in just a few hours. “If we were still using Barracuda it would have taken us days, not hours” said Williams. The company also purchased and have just begun to implement 8TB of Unitrends cloud storage and Unitrends Disaster Recovery-as-a-Service (DRaaS). This will ensure even faster recoveries in the future as their critical servers are now covered with a written guarantee of 1 hour recoveries.