DisrupTech

DisrupTech Adds NeuShield Into its Security Stack to Give MSPs a Competitive Edge

DisrupTech is a leading value-added distributor of layered cybersecurity technology to managed service providers (MSPs). With headquarters in Sydney, the company brings together unique and best-in-class security solutions that address multiple areas, from endpoint security and instant data recovery to security awareness training, risk-based vulnerability management, data exfiltration protection, and more. With over 250 MSPs, DisrupTech offers solutions that meet the needs of hundreds of end customers across Australia, New Zealand, and Asia.

DisrupTech is unique from other technology distributors, building a value-added bridge between technology vendors and MSPs. Typically, technology distributors vet a wide range of solutions that can include many hundreds of products. They usually offer multiple products within a category, such as endpoint security, from different vendors.

DisrupTech has a more focused approach, offering distinctive cybersecurity products sold individually or collectively as part of its security stack. Each solution is in its own category, often with a first-mover technology advantage protected by patents. They also bundle products with complementary technologies, providing MSPs and their customers a robust and targeted security package. One such bundle has essential cybersecurity technologies, including endpoint security with a deep learning cybersecurity framework, instant one-button data and OS recovery, zero trust login and authentication, and individualized cybersecurity awareness training.

DisrupTech Resolves Common Challenges

The following case points highlight some of DisrupTech's solution offerings:

Case Point #1 – DisrupTech's addition of NeuShield to its security stack proved to be a lifesaver for one of its MSP partners. The MSP deployed NeuShield for a customer seeking advanced protection against the escalating incidence of ransomware. Shortly after rolling out

NeuShield, the customer was indeed hit with a ransomware attack.

While planning the policy settings of their new endpoint security deployment, the customer, unfortunately, put the endpoint security in detect mode only, not prevent mode, leaving the company vulnerable. Fortunately, NeuShield quickly restored the data on all the infected user computers and the system and data on an infected server. The entire process only took a few hours. Without NeuShield, the MSP would have taken at least three days to rebuild and restore all the systems.

“NeuShield uniquely protects our MSP partner’s customer data and endpoints from malware and ransomware breaches,” states Angus Button, Co-Founder and Director at DisrupTech. “The streamlined support process of instantly remotely rolling back customer data and computer OS’s saves the MSP significant tech support hours, enabling them to be more profitable and cost-competitive.”

Case Point #2 - Many technology distributors face challenges when different security products are brought into an IT environment, creating technology conflict. DisrupTech eliminates these issues by thoroughly vetting and testing each product to work together seamlessly.

Additionally, DisrupTech ensures that clients receive the convenience, affordability, training, education, and product support they need to succeed. Because DisrupTech sells to MSPs, their solutions must be cost-effective, reliably address security risks, be easy to deploy and configure, and lower maintenance and support costs.

Case Point #3 - DisrupTech has an MSP partner in New Zealand with a large customer in the legal industry with over 50 users running computers with highly complex software. When a user’s system has a problem, it can take the MSP many hours to rebuild and restore a single computer. The company experiences these tech support issues almost weekly. To mitigate these ongoing issues, DisrupTech worked with the MSP to roll out NeuShield to the customer.

When the customer contacts the MSP, the support tech goes into the NeuShield portal, pushes the customer’s recovery button for that device, and a message box automatically appears for the MSP to notify the user that their machine will begin rebooting. The reboot takes approximately 15 minutes to return the computer’s system and/or data to pre-event status. Once the recovery is completed, the customer is automatically notified to log back into Windows, and the issue is resolved.

“NeuShield not only protects MSPs and their customers from cyber breaches like malware and ransomware, but it also saves them many tech support hours that they can now spend on more productive projects while providing better customer service,” states Button.

NeuShield Data Sentinel's unique approach mitigates recovery challenges

NeuShield's unique recovery technology uses a deletion process rather than restoring an entire image. It can retrieve a previous version of a file prior to an event from historical files. NeuShield supports revision history on file types and revision history on any data folder.

NeuShield protects data files and Windows operating systems with its patented mirror shielding approach. It does the same for preventing cyber breaches by making attackers believe they have access to a computer's original data files and OS when they are only accessing a mirror image. Fully undetectable (FUD) and Zero-Day threats are quickly and easily recovered in minutes, preventing significant downtime and conserving valuable tech support time. Issues related to ransomware and other cyber threats, failed Windows and driver updates, software changes, and accidental file deletion can be handled quickly and without major business disruption.

Companies have backup systems, but those solutions are complex, and the restoration process can take a long time. To restore one computer hit with ransomware, MSP tech support must go to the customer's location, boot up the device from a USB drive, rebuild the machine, and possibly reload Windows. Then, they must bring a backup image of the device down from the cloud that could include many gigabytes of data. If multiple, or worse yet, all of the computers on the customer's network are breached, all the image data for every device will simultaneously download over the Internet, slowing the company's network to a crawl. The entire process could take days and even weeks.

DisrupTech views NeuShield Data Sentinel as an essential solution in instantly restoring systems impacted by user actions and as a vital protection against cyber threats. NeuShield's one-click restore makes it easy for MSPs to remotely undo changes to their customer's systems to regain access to computers, applications, and data quickly. This saves them many hours of tech support time and resources for each customer.

NeuShield keeps files and operating systems protected from the latest known and unknown malware threats without managing continuous updating or relying on backup systems. NeuShield restores systems to their known good state, protects against encrypted and corrupted operating system files, and removes known and unknown malware threats.

It's easy for MSPs to integrate NeuShield into their systems through an executable with multi-tenancy that enables them to manage each customer's covered devices efficiently. NeuShield is also very light on memory and CPU utilization. "A product or solution is only as good as the service and support behind it," said Button. "It's all about three things: service, service, and service. NeuShield support has been highly valuable and excels at meeting the needs of DisrupTech and our MSP partners."

About DisrupTech

DisrupTech provides innovative multi-layered cybersecurity solutions to Australia, New Zealand, and Asia as the leading software distributor in the region. DisrupTech empowers MSPs with exclusive access to state-of-the-art solutions that give them a distinct advantage in today's competitive market.

About NeuShield

NeuShield delivers a revolutionary approach to data protection. Rather than trying to detect and block threats one-by-one, the company's patented NeuShield Data Sentinel product shields important data to prevent threats from modifying it. Businesses and consumers use NeuShield Data Sentinel as a simple, reliable and budget-friendly way to revert digital files and devices back to their pre-attack state when other malware defenses, like antivirus and anti-ransomware, fail.

200 Brown Road, Suite 306, Fremont, CA 94539 | (510) 239-7962 | www.neushield.com