



Jennifer VanderWier
PRESIDENT
F1 SOLUTIONS

Jennifer VanderWier is President of F1 Solutions, a security-first managed service provider (MSP) based in Huntsville, Alabama. In light of the recent spike in cyberattacks—particularly those geared toward supply chains—Jennifer expanded her company's relationship with Huntress, growing from 500 endpoints to nearly 4,000.

F1 Solutions relies on Managed Antivirus—a new feature of The Huntress Security Platform—that allows users to reclaim existing investments in Windows Defender and centrally manage Defender right from the Huntress dashboard. In turn, her company has reallocated dollars invested in other antivirus solutions toward bolstering other parts of their security stack.



F1 Solutions

LOCATION

Huntsville, Alabama

THREAT ENCOUNTERED

Supply Chain Attack

In the Wake of Supply Chain Attacks Targeting SMBs, F1 Solutions Goes All In on Huntress to Secure Customers

Cybersecurity doesn't exactly sell itself—and sometimes, the best way for MSPs to demonstrate the need for a stronger cybersecurity stack is to face a crisis head-on as their clients watch from the sidelines.

That's exactly what happened to Jennifer VanderWier, President of F1 Solutions—a security-first MSP based in Huntsville, Alabama. She was overseas on vacation in July 2021 when a staff member called her, waking her up in the middle of the night.

"Huntress called to warn us that Kaseya's VSA has been the victim of a supply chain attack."

This phone call prompted Jennifer to do what many other leaders of MSPs were doing over the long Fourth of July weekend: research, investigate and communicate with customers.

This attack, which the ransomware group REvil executed, targeted Kaseya's remote monitoring and management platform (RMM). Attackers exploited the RMM to deploy ransomware to 1,500-2,000 SMBs through the nearly 60 MSPs that serve them.

Luckily, F1 Solutions' customers were ultimately unharmed in the supply chain attack—but this incident made Jennifer rethink the security offerings she wanted to present to her customers.

Rethinking the Security Stack

Even if their business comes out unscathed, major security events open the door for cybersecurity professionals to consider the what-ifs. "What if my customers had been victimized? How can I proactively work to make sure that doesn't happen?"

“

As cybersecurity practitioners, we have to let go of the old way of thinking that we've got to 'prevent' breaches—we have to assume breach. Bad actors can and will get in. The challenge is being alerted to a breach as soon as possible so you can react and minimize damage.

”

For Jennifer, that meant honing in on a message that she'd spread before in the past but really emphasized in light of recent events: prevention only goes so far. Arguably, what matters more is detection and response.

That focus is exactly why Jennifer chose to partner with Huntress two years ago. Huntress combines a powerful managed detection and response platform powered by a team of human threat hunters to help its partners protect their businesses and clients from savvy cybercriminals.

Jennifer wanted to make sure her customers were protected in ways that extend far beyond mere prevention of attacks. For her, this incident was the catalyst that made her next move easy: she chose to expand the number of endpoints Huntress covers from 500 to nearly 4,000. To her, Huntress marked a critical layer that was no longer optional. It was a priority.

Selling Cybersecurity

One of the major challenges of leading an MSP is striking the right balance between what customers actually need and what their budgets can support.

In Jennifer's case, she made the best out of what could have easily been a crisis situation for her and her customers. After ensuring that the breach didn't negatively impact her customers, she used this opportunity to follow up with her customers to send them a humbling reminder:

“This didn't impact us, but it serves as a wake-up call for those who work in cybersecurity. We're taking this incident as our sign to invest even further in your cyber safety. Stay tuned.”

That investment was Huntress—a revelation that customers warmly received and thanked Jennifer and F1 Solutions for making despite a slight increase in costs for some customers.



Cyber insurance is becoming increasingly critical to have, but checking all the boxes can be challenging for businesses. However, it's a worthwhile venture: businesses that can check all the boxes can save money.



Managed Antivirus

F1 Solution's move to Huntress for all customers aligned with Huntress' new Managed Antivirus feature, giving partners the ability to centrally manage Defender right from the Huntress dashboard. One of the most significant changes that Jennifer and her team had to explain to customers was switching antivirus products.

Jennifer explains that her customers are less hesitant during times of change when they get an explanation of why the changes are happening and what exactly is happening. Once Jennifer and her team explained the changes, she was pleasantly surprised by little to no pushback.

Ultimately, this switch took less than 30 total hours of work to complete. Even better, the F1 Solutions team was able to reallocate those dollars that were invested in other antivirus solutions toward other security measures to further boost their posture.

Admittedly, this transition was noisy at first. Jennifer comments that her team noticed a spike in alerts that turned out to be false alarms, so they worked with Huntress to deescalate some alerts—resulting in quieter workdays for the F1 Solutions team.

Mitigating Risk

Beyond compliance standards and regulations, Jennifer remarks on one of the biggest game-changers in terms of how an organization operates: insurance companies.

Cyber insurance is becoming increasingly critical to have, but checking all the boxes can be challenging for businesses. However, it's a worthwhile venture: businesses that can check all the boxes can save money.

Jennifer states that one of the most frequent questions her customers ask her is how to answer insurance questionnaires. Jennifer uses these instances as an opportunity to remind her customers of the measures that are necessary to take from a cyber insurance perspective.

“
It’s not just the threat hunters at Huntress; it’s the marketing team, the support team—holistically, the entire Huntress team is a partner to F1 Solutions. They’re just as excited about my business as I am.
”

Noting a best practice to customers only goes so far, but when money is on the line for a cyber insurance policy, decisions tend to be made faster.

Ultimately, Jennifer states that F1 Solutions’ partnership with Huntress enables more boxes to be checked when it’s time to fill out the forms for cyber insurance. In turn, this saves her and her customers money.

More Than Just Cybersecurity

Jennifer notes that F1 Solutions’ partnership with Huntress extends far beyond threat hunting and alerts.

She often takes advantage of the resources Huntress has on deck to help her market her security offerings to current and potential customers. She uses blog content, social media posts and even custom pieces of content to help her market her business to clients.

She also takes advantage of the custom-branded reports that she generates directly from The Huntress Security Platform to show each of her customers what goes on behind-the-scenes to keep them safe. She notes that this reflects her team’s proactive approach to cybersecurity, keeping attackers at bay without her customers’ needing to lift a finger.

About Huntress

Hackers are constantly evolving, exploiting new vulnerabilities and dwelling in SMB environments—until they meet Huntress.

Huntress enables our partners to find and stop hidden threats that sneak past preventive security tools. Founded by former NSA Cyber Operators—and backed by a team of ThreatOps researchers—we help our partners protect their customers from persistent footholds, ransomware and other attacks.

Ready to fight back against hackers? [Take The Huntress Security Platform for a test drive with a 21-day trial.](#)