Huntress' Process Insights with managed EDR capabilities provided an added layer of security to help catch an active ransomware incident in its tracks—and restore business operations within 30 hours of the attack.

CLEAR GUIDANCE PARTNERS
STRATEGY + TECHNOLOGY

Clear Guidance Partners

LOCATION

Offices in Austin, Dallas, Ft Worth and Houston TX

THREAT ENCOUNTERED

Ransomware

Clear Guidance Partners Leverages Huntress To Save a Client From a Dangerous Ransomware Attack

"This attack could have been a lot worse than it was," said Anthony Cabral, CISO at Clear Guidance Partners, a Texas-based managed service provider (MSP). "A lot of companies can easily go out of business from an incident like this, but Huntress enabled us to prevent that from happening."

Clear Guidance partnered with Huntress in 2019 to add another layer of cybersecurity for its clients on top of basic antivirus. As the landscape changed and threats evolved, Clear Guidance realized the need for advanced endpoint detection and response (EDR) capabilities but struggled to find a product that worked well for its business. "In today's threat landscape, EDR is a must-have for protecting our small and medium-sized businesses (SMBs). There are a ton of options out there, but none are truly built for service providers—they either don't play well with our existing tools, require extensive tuning or are just too expensive," said Anthony.

When Huntress announced the beta release of Process Insights, a new managed feature with EDR capabilities, Anthony was eager to join the public beta and roll it out to his client base.

"I don't get excited about too many product releases, but Process Insights was something to get excited about because it filled a big gap for us. Process Insights gives us increased visibility into our managed endpoints and networks in a way that easily integrated into our technology stack. Additionally, Process Insights automatically tunes itself and it's offered at a cost that makes sense for our business. It was a no-brainer to try it out."

Not only did Process Insights give us an early warning, it really gave us the affirmation we needed that what we were seeing was malicious—which helped us spring into action much faster.

Process Insights vs. An Active Ransomware Attack

It didn't take long for Anthony to see the value of Process Insights for himself. Early one morning, Anthony started getting alerts from his antivirus about attempted trojan installers on a few of his client's devices.

At the same time, Process Insights was picking up on some abnormal traffic and suspicious activity happening in the client's network. By monitoring process executions and associated metadata on the endpoint, Process Insights can conduct near real-time forensics to more accurately detect and respond to attacks as they happen.

In this case, Process Insights alerted the Huntress ThreatOps team, who were able to quickly confirm malicious activity on the client's network and discover additional east-west traffic that was missed by their existing antivirus, including network scans and malicious scripts being executed. ThreatOps then immediately contacted Clear Guidance to verify their suspicions of a cyberattack and provide personalized remediation steps, which included activating Huntress' Host Isolation feature to isolate the infected hosts and prevent further access for the bad actors.

"The pairing of Process Insights and Host Isolation changed what would have been a massive fire into a smaller, more manageable one," Anthony recalled. "Not only did Process Insights give us an early warning, it really gave us the affirmation we needed that what we were seeing was malicious—which helped us spring into action much faster."

Once the malicious activity was isolated, Clear Guidance was able to take the necessary steps to purge the bad actor from the network and get the client's business back up and running within 30 hours of the attack. And with the forensic data that Process Insights collected, Anthony was able to work with the Huntress ThreatOps team to retrace the attack chain and identify stolen credentials as the initial access point. "Post-incident, Huntress gave us a clear picture of what happened. We saw how the hacker breached the network and was attempting to encrypt files for ransom. The payloads were ready for detonation, but we successfully stopped them before they were activated. In the realm of security incidents, that is a huge win for us."

The value of the functionality Huntress provides, at the cost Huntress charges for it, is just unparalleled. I've never seen it anywhere in the industry and it makes me proud to be a Huntress partner.

The Value of Managed EDR for the Modern MSP

As the Clear Guidance team saw firsthand, SMBs are not exempt from today's advanced cyber threats—which proves the importance of layered security and the ability to see and respond to threats at every stage of the attack cycle. Process Insights is purpose-built to provide high-fidelity EDR capabilities to SMBs. And for people like Anthony, it's truly been agame changer.

Process Insights is purpose-built to provide high-fidelity EDR capabilities to SMBs. And for people like Anthony, it's truly been a game changer.

Unlike other EDR products, Process Insights filters out noise and only delivers alerts when a threat is verified or action is needed—saving partners the hassle of sifting through endless tickets. "Being able to minimize the number of false positives probably saves me hours each week, which is thousands of dollars a week," claims Anthony.

In addition to the time savings, Huntress also enables its partners with a secret weapon; ThreatOps, a team of security experts who provide 24/7 threat hunting to investigate and remediate cyberattacks.

"With Huntress ThreatOps, we have some of the best minds of cybersecurity at our disposal," said Anthony. "They help us validate incidents, handle them and also level up our own knowledge. With the context and information included in their personalized reports, any tier one technician can easily understand what threats have been detected and take the appropriate next steps—it's been a great force multiplier for us."

As a long-time Huntress partner, Clear Guidance appreciates how Huntress continues to add new functionality that helps them keep pace with both today's and tomorrow's threats. "The value of the functionality Huntress provides, at the cost Huntress charges for it, is just unparalleled. I've never seen it anywhere in the industry and it makes me proud to be a Huntress partner."

Learn more at huntress.com

Follow us on social @HuntressLabs

About Clear Guidance Partners

Clear Guidance Partners was founded in 2019 and made security a cornerstone of the business. This resulted in the business doubling in size in 2021 to 25 staff today. CGP focuses primarily on professional services (law firms, engineering, financial services) and manufacturing, and also has a back-office services team providing HR, billing, accounting and other operations for law firms. CGP is based in Austin TX, and has staff and clients across the state.

About Huntress

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

Huntress protects small and mid-market businesses from modern cyberattackers. Founded by former NSA Cyber Operators—and backed by a team of 24/7 threat hunters—our managed security platform defends businesses from persistent footholds, ransomware and other attacks.

We're on a mission to secure the 99%. Learn more at www.huntress.com and follow us on social @HuntressLabs.