Prelude to Ransomware:

How Clear Guidance Partners Stopped an Attack in Its Tracks

A surge of alerts one morning made it clear to CISO Anthony Cabral that this was no false alarm. A malicious hacker had breached his defenses and prepared to deploy ransomware. But they weren't the only ones watching. With Huntress Managed EDR and its industry-defining 24/7 SOC behind him, Cabral took the fight directly to the threat actor.

CLEAR GUIDANCE PARTNERS
STRATEGY + TECHNOLOGY

Company
Clear Guidance Partners

Location
Austin, Texas

Solutions Deployed
Managed EDR

About
Clear Guidance Partners was founded in 2019 and made security a cornerstone of the business. This resulted in the company 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, Texas, and has staff and clients across the state.

HUNTRESS

Background | A Rude Awakening

It started like any other morning for Anthony Cabral, CISO of Texas-based managed service provider (MSP) Clear Guidance Partners. The sun was rising. Coffee was brewing. Emails were being answered. It looked like another smooth day for the seasoned IT pro. That is until his phone lit up with an onslaught of alerts. Antivirus alarms were ringing off the hook, blaring of trojan installers on a client's devices.

Cabral knew the stakes: a small misstep could lead to a major disaster. He'd heard too many horror stories of companies falling to cyberattacks that crept in through the cracks.

But under his watch and with Huntress by his side, Cabral knew he wouldn't see anyone fall on this day.

A Perfect Match | Clear Guidance Finds a New Partner

Clear Guidance began its partnership with Huntress in 2019 to strengthen their cybersecurity beyond basic antivirus. But as endpoint threats escalated in the following years, it became clear they needed a more robust solution. Traditional endpoint detection and response (EDR) tools on the market fell short as they were often too complex, too expensive, and too noisy.

Then came Huntress' Managed EDR beta in February 2022. It was exactly what Cabral had been waiting for. What stood out to him wasn't just the leading-edge tech, but also the people behind it. Huntress' human-first, expert-driven approach made all the difference. Cabral felt confident he could finally bring powerful enterprise-grade cybersecurity to his clients who needed it most.

"Managed EDR was something to get excited about," Cabral admits. "It filled a big gap for us. It gave us increased visibility into endpoints and networks in a way that integrated seamlessly with our tech stack. Plus, it's automatically tuned for us and offered at a price that makes sense for our business. It was a no-brainer to try it out."

> The value Huntress provides, at the cost they charge, is unparalleled. I've never seen it anywhere in the industry, and it makes me proud to be a partner.
>
> Anthony Cabral
> CISO | Clear Guidance Partners

HUNTRESS

The Incident | A Swift Response to an Attack in Progress

The alerts that morning might've left Cabral feeling uneasy, but the Huntress Security Operations Center (SOC)—working alongside Managed EDR—immediately stepped in, digging deep to find malicious traffic that the antivirus had missed. By monitoring process executions and associated metadata on the endpoint, Managed EDR conducted near real-time forensics to detect and respond accurately to the attack. It didn't just flag suspicious activity. It pieced together a clear story of what was happening on the endpoint. The Huntress SOC promptly contacted Cabral and confirmed his worst fear—this wasn't a false alarm.

An attacker had already made their way into the client's network, moving around, running malicious scripts, and looking for weaknesses. But the Huntress SOC didn't just spot the suspicious activity—they tracked every malicious move the hacker made.

The SOC swiftly deployed the Host Isolation feature, severing the infected machines from the network and blocking the hacker's access. They also gave Cabral a personalized, easy-to-follow remediation plan. Working closely with the Huntress SOC, Cabral and his team successfully purged the hacker and patched all vulnerabilities.

In just 30 hours, the client's business was fully restored. All files were intact, and the crisis was contained.

.

> Huntress gave us a clear picture of what happened. We saw how the hacker breached the network and attempted 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's a huge win for us.

Anthony Cabral
CISO | Clear Guidance Partners

HUNTRESS

Post-Incident | Breaking Down the Attack and Learning From It

Following the incident, the SOC collaborated with Clear Guidance to reconstruct the attack chain. Their investigation traced the breach to using stolen credentials, which allowed the attacker to get in undetected. With ransomware deployment imminent, the attacker's plans were foiled just in time, preventing potential chaos.

"Huntress gave us a clear picture of what happened," says Cabral. "We saw how the hacker breached the network and attempted 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's a huge win for us."

Value of Managed EDR | Cabral Gets the Industry's Best Minds Behind Him

The attack exposed an unpleasant reality for Cabral and Clear Guidance: no business is immune to advanced cyberattacks. They all need layered security solutions to detect and respond to threats at every stage. For Cabral, that's exactly what Managed EDR delivered:

No more drowning in false positives

With a false positive rate of less than 1%, Managed EDR filters out the noise and flags only verified threats.

More visibility

...into endpoint activity without the complexity of traditional solutions.

24/7 monitoring

...and hands-on support from Huntress' SOC, which Cabral describes as a "force multiplier.

> Managed EDR was something to get excited about. It filled a big gap for us. It gave us increased visibility into endpoints and networks in a way that integrated seamlessly with our tech stack. Plus, it's automatically tuned for us and offered at a price that makes sense for our business. It was a no-brainer to try it out
>
> Anthony Cabral
> CISO | Clear Guidance Partners

HUNTRESS

"Minimizing false positives saves me hours every week," Cabral emphasizes. "And that's thousands of dollars in savings weekly!"

And it's not just about the tools. It's about the people behind them—and how they seamlessly work together. "We now have some of the best minds in cybersecurity at our disposal," he says. "They validate incidents, handle them, and level up our knowledge. Even a tier-one technician can undertake the next steps confidently with Huntress' reports."

The Huntress Advantage

As a long-time Huntress partner, Cabral appreciates how Managed EDR is evolving to meet emerging threats. "The value Huntress provides, at the cost they charge, is unparalleled. I've never seen it anywhere in the industry, and it makes me proud to be a partner."

With Huntress by their side, Clear Guidance didn't just survive the ransomware attack—they came out stronger than ever.

"This attack could've been a lot worse than it was," reflects Cabral. "A lot of companies can easily go out of business from an incident like this, but Huntress enabled us to prevent that from happening."

> "This attack could've been a lot worse than it was. A lot of companies can easily go out of business from an incident like this, but Huntress enabled us to prevent that from happening."
>
> Anthony Cabral
> CISO | Clear Guidance Partners

HUNTRESS