Weigel's Farm Stores

Executive Overview

HQ:	Powell, TN, Since 1931
Industry:	Convenience and Fuel Retail
Size:	68 Locations
Solution:	Extended Detection and Response

Business Challenges

- Keeping up with network and endpoint security
- Ill-prepared to prevent sophisticated cyber criminals
- Too much time spent updating legacy antivirus products leading to poor time management

"PDI doesn't operate like a 'vendor,' and they don't treat us like a 'customer'; it's a true partnership."

– Greg White, IT Director, Weigel's

pditechnologies.com

A 2019 survey found that 58% of SMBs consider a shortage of in-house cybersecurity skills to be their biggest security operations challenge.

Overview

Weigel's Farm Stores (Weigel's) operates a chain of convenience stores in East Tennessee. From its humble beginnings in 1931 when it began selling raw milk produced from its "herd" of four cows, the fifth-generation, family-owned business has grown steadily to 68 stores with over 3,000 team members.

With their polished store aesthetics and high-quality products, Weigel's continually advances the convenience store model, establishing industry best practices that transcend far beyond the southeastern United States.

While expanding both its physical and digital footprint over the past several years, Weigel's realized its cybersecurity vulnerabilities had become more prominent, involving a complex network that includes critical operating systems as well as sensitive customer data. Protecting those assets is paramount to preserving its reputation as an industry-best retailer with fiercely loyal customers.

The Challenge

The convenience store industry has come under siege by data attacks, with cyber criminals targeting critical operating systems as well as customer card information. The attacks have yielded significant returns—little surprise, as most retailers are ill-prepared to prevent these sophisticated attacks from compromising their endpoints.

"The convenience store industry operates on razor-thin margins, and unfortunately IT is usually the last thing considered," says Greg White, IT director of Weigel's. "Malicious groups understand that, and they are focusing their attention on us. They recognize the vulnerabilities and opportunities."

With limited IT resources and a staff that was already strained, managing security threat detection and response internally became impractical for Weigel's. Much of White's team spent a disproportionate amount of time updating legacy antivirus products, leaving them little time to attend to proactive threat management. "None of us were getting any sleep at night," White says. "Our staff is so small, we were responding to calls and looking at logs at two o'clock in the morning. It was impossible for us to keep up."

PDI TECHNOLOGIES

"Maintaining security for our resources and the financial data of hundreds of thousands of customers, that's a very heavy weight to bear. It's simply not possible in this age to do it effectively on your own. You have to have a partner."

– Greg White, IT Director, Weigel's

Choosing a solution was fraught with challenges. Weigel's needed advanced protection that didn't compromise performance and that was compatible with its existing hardware infrastructure. No easy task. It also had to be easy to deploy, maintain, and update, thereby freeing its IT staff to attend to other corporate security concerns. And most importantly, it needed to deliver results, not promises.

The PDI Solution

After assessing Weigel's risks and internal IT capabilities, PDI recommended its Extended Detection and Response (XDR) service to effectively manage the company's network and endpoint security.

The PDI XDR service includes a rich mix of crucial threat detection and prevention activities, powered by SIEM and AI-driven endpoint security. But while these components automate critical tasks (at impossibly fast speeds), it is XDR's human monitoring that ensures everything runs smoothly.

XDR taps the abundant resources of the PDI Security Operations Center (SOC), a 24/7/365 operation that provides comprehensive threat monitoring, detection and targeted response services. That's dedicated, high-level expertise that maintains watch over the security of a network, no matter its complexity.

XDR relieves the strain placed on internal IT departments, identifying intrusions in real time and preventing them from executing on system endpoints.

Capabilities include:

- Running targeted threat hunting sequences to trace anomalies
- Examining alerts to separate true concerns from false positives
- Addressing and mitigating threats in real time

Additionally, the PDI XDR service alleviates the time-intensive chore of maintaining logs, as it collects, aggregates, and normalizes an organization's log data from servers, endpoints, applications, and security devices. This delivers a critical time and resource savings, freeing up IT resources to focus on growing their company's business.

PDI TECHNOLOGIES

"Most people forget about the little guys. Not PDI. Not only do they look out for the smaller operations, their solution is scalable and grows with you as your footprint expands. We kept throwing new things at the PDI team and they continued to integrate them into a solution."

– Greg White, IT Director, Weigel's

Why They Prefer PDI

- **Exceptional Service.** Weigel's has worked with PDI and its predecessor companies since 2009, relying on them for a myriad of IT security and networking tasks. "There are a lot of companies to choose from today, but I have not experienced the caliber of service that PDI provides," White says. "To have people writing all new parsing rules within two days so that I can move forward on a major project, that's unheard of. But PDI gets it done."

- **A True Partnership.** "PDI doesn't operate like a 'vendor,' and they don't treat us like a 'customer'; it's a true partnership," White says.

- **C-Store Specialization.** PDI understands the challenges that are unique to the convenience store industry. "Other companies try to lump us with big-box dynamics, but not PDI," says White. "They specialize in the c-store space and that experience shows in everything they do. Their entire approach is strategic and deliberate, and tailored for us."

- **Up and Running.** The PDI XDR deployment replaced numerous piecemeal security solutions Weigel's had been managing. "We kept throwing new things at the PDI team and they continued to integrate them into a comprehensive solution," says White. "We had everything up and running quickly and seamlessly."

- **A Committed Relationship.** Since 2009, Weigel's has looked to PDI to protect its most valuable assets, a deliberate choice that reflects years of demonstrated success. "There are hundreds of vendors in the cybersecurity space." notes White. "But we've known PDI's top executives from the very beginning, and they have a deep-rooted interest in our growth and success." That commitment is rare in an industry that continues to evolve. "The security threat landscape has changed immensely in the 11 years of our PDI partnership," White adds. "But through it all, PDI has demonstrated consistency in its high level of expertise and the unwavering integrity of its team members."

PDI TECHNOLOGIES

> "Unless you have a partner with cybersecurity and round-the-clock operations like PDI, you're doing it yourself. Or worse, not doing it at all. And if you're doing it yourself, you're not sleeping."
>
> – Greg White, IT Director, Weigel's

The Result

Since deploying PDI XDR across its network and endpoints, Weigel's has achieved continuous, real-time insights into the security of its entire enterprise, all while under the watch of experts at the PDI SOC.

The numbers tell a compelling story:

- 68 stores
- 69 POS systems
- 145 endpoints
- 68 wireless devices

With XDR, Weigel's can access automated reports from any digital device, neatly organized in a customized, online dashboard. "At a glance, I can quickly find any security event or incident; who's logged into our system, PCI logs, authentication reports," White says. "If I see something unfamiliar, I can investigate it."

Weigel's retains control over filtering, adding customized rules to comply with corporate guidelines. "We don't want our people on social media during work, for example," says White. "So if they do access these types of sites, we get an immediate alert. These alerts help us maintain a secure environment."

PDI notifies Weigel's of all questionable threats, allowing it to act against real ones while dismissing those that are inconsequential. Either way, everything is addressed immediately, and real intrusions are appropriately elevated and addressed.

Asked to summarize the PDI relationship, White says, "Unless you have a partner with cybersecurity specialization and round-the-clock operations like PDI, you're doing it yourself. Or worse, not doing it at all. And if you're doing it yourself, you're not sleeping."

PDI TECHNOLOGIES

"At a glance, I can quickly find any security event or incident; who's logged into our system, PCI logs, authentication reports. If I see something unfamiliar, I can investigate it."

– Greg White, IT Director, Weigel's

Customer Results

- Continuous, real-time insights into security
- Access to automated reports from any digital device
- Control over filtering, and customized rules to comply with corporate guidelines
- Immediate notification of all questionable threats

> With PDI, I know that I'm secure. I've got a partner that is monitoring my system 24 hours a day. And that takes a lot of pressure off me and my team.
>
> – Greg White,
> IT Director, Weigel's

PDI TECHNOLOGIES