CASE STUDY

Major Hydraulics Company Selects Fortinet To Secure Its Endpoints and Provide Managed Detection and Response Services

Established in 1968, Hydradyne provides fluid power and motion control sales, service, and fabrication to over 8,000 original equipment manufacturers (OEMs) and maintenance, repair, and operations (MRO) businesses worldwide. Headquartered in Fort Worth, Texas, the company operates across more than 30 branches in the United States and is one of the largest motion control distribution companies in the country. From supporting oil fields and farmlands to automotive factories and manufacturing plants, its tagline is "we set IDEAS into MOTION."

Securing the Enterprise With Fortinet

When it comes to security, Hydradyne's priority is protecting its digital business systems. According to Paul Miller, IT manager at Hydradyne: "Our biggest attack vector is through the way we electronically conduct business. A big part of that is the human factor—with a company operating on the scale that we do, it is all too easy for someone to inadvertently open malware and expose our business to attack."

To secure its enterprise systems, Hydradyne has used FortiGate Next-Generation Firewalls (NGFWs) for the past six years. The NGFWs are deployed across 31 sites, and the company also uses a FortiGate Virtual Appliance to secure its public cloud environment. Hydradyne leverages FortiManager to centrally configure its FortiGate devices and FortiAnalyzer to troubleshoot system issues.

"The FortiGates have been excellent," says Miller. "Through them we have enabled strong web filtering policies, implemented robust intrusion prevention, certificate inspection, and application controls. The FortiGates are fully capable of preventing lateral movement through network-based segmentation to manage internal risks. With full web security capabilities, the team can be sure that external risks are managed as well. We also recently started using FortiMail for our secure email solution with Microsoft 365, which is important to us given the volume of phishing emails that come our way. The administration interface is incredible and far more intuitive than the system we had in place previously. It is simple for me to set up the controls we need, and when I have questions, the team at Fortinet has been highly responsive. With FortiMail, I do not have to worry about malicious email as an attack vector, and that is a significant benefit."

Enhancing Security Prevention

However, one area of Hydradyne's security infrastructure was presenting significant challenges: threat prevention. The company was using a mix of traditional and next-generation antivirus solutions, secure application protection capabilities, and endpoint threat protection services provided by many different vendors. The approach was falling far short of Hydradyne's expectations.

Hydradyne
We set IDEAS into MOTION

"The more we buy into Fortinet, the more I understand the value of the Security Fabric. I look at our infrastructure and add-on services and see it as a security ecosystem wrapped around our needs as a business."

– Paul Miller, IT Manager, Hydradyne

Details

Customer: Hydradyne

Industry: Distributor

Location: Fort Worth, TX

Business Impact

- Granular insights into endpoint devices
- Increased control over program installs by users
- Reduction of 15 hours per week managing endpoint security
- Enhanced ability to spot malicious activity on endpoints and combat lateral attacks

"With our previous antivirus and application protection vendors, we were given no insight into what was being blocked, so it was unclear if its systems were blocking a valid attack or infection. What is more, the systems did not allow for lateral movement detection, which is a significant capability gap.

"Meanwhile, our endpoint threat detection was expensive for the number of devices being covered, and there was a suspiciously low volume of activity picked up by the system—this was confirmed by the fact that activity was picked up on our antivirus that was completely missed by the threat detection system. This was happening in the opposite direction too, with the threat detection system picking up things that were being missed by the antivirus. It was clear we needed to move on."

Advanced Endpoint Detection and Response

Based on Hydradyne's solid experiences with other Fortinet solutions, and following a review of alternatives on the market, the company selected the FortiEDR solution for its endpoint detection and response (EDR) requirements. FortiEDR is a next-generation system that delivers real-time visibility, analysis, protection, and remediation for endpoints. Leveraging automation capabilities, FortiEDR reduces the attack surface for companies, preventing malware infection and detecting and defusing potential threats in real time. FortiEDR was deployed in conjunction with FortiClient, endpoint software that communicates with an organization's Fortinet systems to provide information, visibility, and control to that device. Hydradyne uses FortiClient to ensure patch management across the devices protected by its 500 FortiEDR licenses. An additional capability of FortiClient is that it includes a built-in client enabling secure remote access via virtual private network (VPN) or Zero Trust Network Access (ZTNA) for employees.

Solutions

- FortiMDR
- FortiClient
- FortiGate Next-Generation Firewall
- FortiManager
- FortiAnalyzer
- FortiMail

"The big win for me has been the additional information provided to us around what users are doing with our endpoints. Having this insight allows me to manage our IT resources and adjust policies as needed."

– Paul Miller, IT Manager, Hydradyne

As a second stage of the deployment, Hydradyne activated Fortinet's managed detection and response (MDR) service. Through the service, Hydradyne benefits from the expertise of Fortinet's team to help it analyze data from its systems to identify and shut down threats before they become a problem.

Greater Insight, More Control

With Fortinet's solutions in place, Hydradyne was immediately able to improve the performance of its enterprise security infrastructure. As Miller explains, "The big win for me has been the additional information provided to us around what users are doing with our endpoints. Having this insight allows me to manage our IT resources and adjust policies as needed. Users must now communicate with us before they install new programs, and that is not a trivial thing when it comes to securing the business."

Fortinet's MDR services have also quickly proven their value to the company. "We are happy to partner with Fortinet because their team has trained eyes. They know more about what the FortiEDR solution does and leverages their experiences from their customer base. That gives us a knowledgeable resource to stop threats and actively analyze our detection data. We experienced a network security event, and it was this experience that pushed us to take up the MDR services. We certainly feel much more secure having Fortinet's team on our side."

The solution also saves time and resources for the company. With its legacy systems, Miller and his team spent up to 25 hours per week managing the antivirus system, creating exceptions, and reviewing the configuration. Even now, with the Fortinet systems still in rollout phase, Miller's team only spends 10 hours per week at most managing FortiEDR. This includes reviewing the exceptions created by Fortinet's MDR team and optimizing the performance of the system.

The Fortinet Security Fabric

Looking ahead, Hydradyne is looking to exploit its Fortinet Security Fabric more fully. Miller concludes, "Next up, we are looking at how to make better use of the FortiManager and FortiAnalyzer tools to push out policy and configuration changes. We plan to use these tools to derive metrics on our Fortinet investment to demonstrate and prove the value of this system to our leadership.

"The more we buy into Fortinet the more I understand the value of the Security Fabric. I look at our infrastructure and add-on services and see it as a security ecosystem wrapped around our needs as a business. As a security team, we have long wanted to get things down to a single pane of glass to manage the infrastructure and other services. More recently, we have come to see the value of automated, connected security infrastructures where, for example, as soon as a rogue wireless device is identified it can be held captive and isolated from the rest of the network. With Fortinet, it feels like we are all but there, and I can think of no other vendor that comes close to matching them in that respect."

January 6, 2022 5:48 AM
1351578-0-0-EN