CASE STUDY

Chicago-based MSSP Powers Diverse Security Use Cases With the Fortinet Security Fabric

DefendEdge is a managed security services provider (MSSP) headquartered in Chicago, Illinois, and serving enterprises coast to coast, including those with global operations. The company works with businesses in highly regulated sectors, including financial services, healthcare, retail, energy, education, and government and aims to become a trusted advisor to its clients through its holistic, premium cybersecurity services.

DefendEdge's core portfolio comprises threat management platforms for external and employee-based threats, and managed detection and response capabilities that are enabled through a 24/7 security operations center (SOC). DefendEdge manages its customers' security infrastructures, augmenting, or in some cases managing, their entire networks, including incident response.

Taso Triantafillos, CEO at DefendEdge, explains: "Our clients come to us for trusted, unbiased expertise on the best way to protect their businesses. They understand that we only recommend and support products and services that we know will deliver on their specific security needs."

Protecting Highly Regulated Businesses

Operating in sensitive, highly regulated industries means that DefendEdge's clients have a unique array of security challenges. "These businesses are aware of the scale of the global cyber threat, and that they are regularly targeted by criminals and nation state actors alike," says Triantafillos. "As geopolitical instability increases, these organizations are much more focused on how they can prevent data breaches when, not if, they are targeted. The move to remote and hybrid working in the aftermath of the pandemic has exacerbated this challenge, as enterprises now must protect a more distributed threat surface."

DefendEdge mostly works with midsize and small businesses, and many of these organizations lack the resources needed for a robust security posture. As Triantafillos explains: "A lot of our clients simply do not have the budget to hire the requisite number of network security professionals to run a full-time SOC or threat management capability. That is why they come to us for help. We bring economies of scale that enable clients to have the capability they need at the right price point."

A Complete Fortinet Shop

Triantafillos had come across Fortinet prior to founding DefendEdge, and he had long intended to put Fortinet technologies at the heart of the company's service proposition. "I was extremely impressed with the integration provided by the Fortinet Security Fabric," says Triantafillos, "along with the ease of use, operational efficiency, and cost-effectiveness that comes with Fortinet products. As we evaluated security products for our practice, our conclusion was that Fortinet was at the top of best of breed, so it was clear from the outset that we would be a dedicated Fortinet shop."

DefendEdge

"I was extremely impressed with the integration provided by the Fortinet Security Fabric, along with the ease of use, operational efficiency, and cost-effectiveness that comes with Fortinet products. As we evaluated security products for our practice, our conclusion was that Fortinet was at the top of best of breed, so it was clear from the outset that we would be a dedicated Fortinet shop."

– Taso Triantafillos, CEO, DefendEdge

Details

Customer: DefendEdge

Industry: MSSP/Service Provider

Location: Chicago, Illinois

Business Impact

- Integrated solution to address industry-specific security needs of businesses in highly regulated industries
- 50% of DefendEdge clients leverage more than one Fortinet solution

DefendEdge employs the full range of Fortinet Security Fabric products both for its MSSP services and its own internal security needs. The solution set includes FortiGate Next-Generation Firewalls (NGFWs), Fortinet Secure SD-WAN (software-defined wide-area network), FortiAnalyzer, FortiDeceptor, FortiNAC (network access control), FortiMail, and much more. The company uses FortiConverter to migrate clients from legacy firewalls to FortiGate NGFWs, an approach that accelerates the process and reduces errors.

"Our aim is to be a holistic cybersecurity company," adds Triantafillos. "The scope of the Fortinet solution suite enables us to achieve this goal." As a complete Fortinet shop, DefendEdge is often among the first Fortinet partners to use new solutions. "FortiDeceptor is a case in point. We took up the solution as soon as it came out and had clients up and running in days," says Triantafillos. FortiDeceptor enables DefendEdge's clients to create an environment that simulates the real network and assets, enabling them to expose and eliminate external and internal threats early in the attack kill chain and before grave damage occurs. "Such innovations provide our company with a significant competitive edge," adds Triantafillos.

Clients of DefendEdge take advantage of the Fortinet Security Fabric. Roughly 50% of its clients leverage more than one Fortinet solution.

Enabling Secure Remote Working for Clients

Leveraging the Fortinet Security Fabric, DefendEdge is able to offer a broad range of services that meet the industry-specific needs of its customers.

In the financial services industry, one key use case is remote working, which has become increasingly common since the pandemic. Triantafillos comments: "Financial services companies are concerned about the implications of employees working outside the corporate perimeter, where they may be more exposed to malware and data exfiltration. Through the FortiGate NGFWs and the FortiClient EMS (endpoint management server) we can provide clients full visibility of user activity and empower them to block access to risky websites."

DefendEdge augments this capability with FortiMail, which provides advanced multi-layer protection against email-borne threats, and FortiSandbox, which allows clients to inspect and detonate malicious attachments and URLs in a secure environment.

Defending Against the Insider Threat

One critical challenge faced by DefendEdge clients, particularly those in the legal and financial services sectors, involves highly privileged users accessing or downloading sensitive files to their workstations or uploading data to unapproved drives. Such activity can occur when employees leave an organization to work elsewhere and attempt to take sensitive files with them.

DefendEdge protects against such threats through its SiON Employee Threat Management Platform, which is built on the Fortinet Security Fabric. An application within the FortiGate NGFWs allows DefendEdge to help clients restrict inappropriate activity. Similarly, the FortiClient EMS enables the company to restrict the activities that can be carried out on clients' remote workstations.

Business Impact (cont.)

- Powerful capabilities for threat management and SOC use cases
- Ability to prove ROI to clients with clear analytics and reporting
- Enhanced internal security capabilities to protect company's own business
- Rich training resources and simple interfaces reduce training time for new engineers

Solutions

- FortiGate Next-Generation Firewall
- Fortinet Secure SD-WAN
- FortiAnalyzer
- FortiSwitch
- FortiAP
- FortiNAC
- FortiMail
- FortiDeceptor
- FortiAuthenticator
- FortiClient
- FortiConverter
- FortiExtender
- FortiManager
- FortiSandbox
- FortiToken
- FortiSIEM

"Fortinet's technology is highly effective," says Triantafillos. "Not only does it provide visibility into inappropriate user activity, but the detect and prevent capabilities means that the system can automatically stop users from downloading content inappropriately. That ability to take immediate, automated action is of huge value to our clients."

DefendEdge uses the Fortinet application programming interface (API) in its SiON platform to push actions out for clients based on internal policies. The policies are invoked primarily through the FortiGate NGFWs, the FortiClient EMS, and the FortiSandbox. "One implementation for this feature is geoblocking," says Triantafillos. "Clients can set SiON to trigger actions like blocking access to certain resources or knocking a workstation off the network it logs on from multiple locations at the same time —activity that is indicative of a compromise."

Delivering Benefits for DefendEdge

Whatever the client need, DefendEdge finds that Fortinet has a solution. From deploying FortiNAC to help oil companies protect access at wells, to leveraging Fortinet Secure SD-WAN to help banks connect branches cost effectively, the Fortinet Security Fabric is delivering for diverse user needs. Additionally, Fortinet is bringing an array of benefits to DefendEdge itself.

The first is through the usability of the Fortinet solutions. According to Triantafillos, most competing security systems are difficult to manage. "With other systems, you need to hire subject-matter experts with years' of experience using the technology. Fortinet's systems are highly intuitive, and it is much easier to train our people on their use. In addition, the Fortinet Training Institute provides us content and resources to help get our people up to speed."

> *"We view Fortinet as a strategic partner, and they will be with us every step of the way as we look to grow in the years ahead. We only work with Fortinet, so that means if we win a new client, it is because they have bought in to our Fortinet-centric proposition. We believe the Security Fabric offers the best solutions for a lot of the challenges that clients face, and we continue to see impressive innovations coming from the company. We look forward to a long partnership."*
>
> – Taso Triantafillos, CEO, DefendEdge

The second comes from using Fortinet products for its own security needs. "We need to be experts in the Security Fabric, so it makes sense for us to use the system in our own environment," says Triantafillos. "We also truly believe in Fortinet's products, or we would not offer them to clients."

In addition, during the current economic climate, clients' budgets are tighter than ever, and companies are taking a closer look at their costs to see if they can truly justify the outlay. "This is where Fortinet is providing significant value from a business perspective," comments Triantafillos. "FortiAnalyzer and FortiSIEM [security information and event management] allow us to track the number of tickets we are generating for clients and the hours we have spent servicing their needs. This transparency allows us to demonstrate the value they are receiving for our services and is easy to compare to the significantly higher sums that would come with hiring FTEs [full-time equivalents]."

Finally, Triantafillos shares that his clients find FortiAnalyzer dashboards and analytics reports—for example related to Fortinet Secure SD-WAN, network performance, and availability—extremely useful. "The metrics used help demonstrate the cybersecurity story through defendable data to our clients' executive leadership. Many of our clients use the reports and data points in their board briefing documents."

A Long-term Partnership

DefendEdge plans to continue operating as a dedicated Fortinet MSSP for the foreseeable future. “One of our plans is to extend into Zero Trust Network Access,” says Triantafillos. “Clients took a step back from considering ZTNA during the pandemic to focus on remote working, but it is now coming back on the radar. We also plan to extend our use of FortiDeceptor, given just how useful the tool is in limiting the impact of security breaches.”

Triantafillos concludes: “We view Fortinet as a strategic partner, and they will be with us every step of the way as we look to grow in the years ahead. We only work with Fortinet, so that means if we win a new client, it is because they have bought in to our Fortinet-centric proposition. We believe the Fortinet Security Fabric offers the best solutions for a lot of the challenges that clients face, and we continue to see impressive innovations coming from the company. We look forward to a long partnership.”

www.fortinet.com

October 14, 2022 7:29 AM
1753329-0-0-EN