FORTINET

CASE STUDY

IT Solutions Provider Chooses FortiDeceptor to Detect and Block In-Network Attacks

Headquartered in the northeastern region of the United States, is one systems integrator and technology reseller that optimizes its customers' IT environments. This IT solutions provider has delivered custom-designed projects based on cutting-edge technologies for over three decades, serving organizations across a wide range of sectors.

"We are committed to consistently delivering innovation to both our customers and partners," says the company's network security tech lead. "This is why we are always on the lookout for the best available solutions to implement in-house and to recommend to our customers, so that they can build a resilient security program that can effectively deal with unexpected changes in the attack surface. We have access to a wealth of security tools, but we carefully select and implement only the best solutions for both our customers' environments and for our own internal operations. This is what sets us apart from the competition, and it is why we are consistently choosing to work with Fortinet solutions. And this is also the reason we decided on FortiDeceptor as a strong and viable solution to protect our network."

A Network Under Fire

As part of its broad services offering, the company hosts many of its customers' websites at its data center, which results in a significant amount of inbound traffic that is known to peak during large global events, such as the World Cup soccer games. Adds the network security tech, "A portion of the traffic is malicious, stemming from scanning tools and other attack methods that send requests to our firewalls. We had days when we detected tens of thousands of security incidents per day. It was clear that we needed a way to stop these attacks without impacting our business."

To ensure that the company's firewalls were only processing genuine requests, the network security tech and his team decided to deploy decoys in the network's "demilitarized zone" (DMZ). One of the key benefits of deception deployment is that the decoys catch and block malicious activities early. Any engagement with the DMZ decoys is attack-related, and therefore immediately detected and blocked. "Once a malicious IP address is detected by the decoys, the data is sent to our firewall management platforms, and is added to our IP blocked list," says the network security tech. "This allows us to stop attacks early at the network perimeter, independent of the underlying network infrastructure."

Unlike attackers or attack tools, legitimate users always use legitimate, known IPs, as they are not aware of any other IPs. However, attack tools that scanned the technology company's DMZ environment to find a way in purposely discover other IPs that are used by the decoys. The decoys are very attractive targets for the attacker, essentially deceiving and trapping them very early in the attack cycle.

"Given our extensive deployment of the Fortinet Security Fabric, FortiDeceptor was the obvious choice for this project. In our experience, the further you extend on the Security Fabric, the greater the overall benefit. So, when we decided to go down the deception route, no other company was in the running."

Network Security Tech Lead
IT Solutions Provider

Details

Customer: IT Solutions Provider

Industry: Technology

Headquarters: United States

Business Impact

- Reduce daily inbound threats by proactively stopping attacks at the perimeter
- Protect undersecured non-production environments

By continuously detecting and blocking traffic from malicious IP addresses, the company managed to significantly decrease unwanted activity affecting its firewalls within weeks. According to the network security tech, "FortiDeceptor provides us with a nonintrusive way to detect and block malicious activity with zero false positives, which tremendously helps us to stop malicious activity very early and at the perimeter. When we turned on FortiDeceptor, we were alerted to tens of thousands of incidents every day. These numbers fell dramatically, as FortiDeceptor continuously identified malicious activities originating from certain IP addresses. Now, we see only a few alerts per day. Our senior executives are extremely impressed."

The network security tech adds, "We have shared this approach with some of our customers, who were impressed with the results and decided to implement FortiDeceptor in their own environments."

External threats, however, were not the only challenge keeping the network security team awake at night. There were other critical network segments, such as test labs that were underprotected, where security measures were not as strict as those in the company's production environments. Therefore, the company decided to deploy deception assets in these segments to detect any malicious activity during the test phases.

Dynamic Deception Helps with Zero-Day Threats and Unpatched Vulnerabilities

In most attack scenarios, when newly discovered vulnerabilities present themselves, attackers are quick to exploit them. To protect its network, the company uses FortiDeceptor to deploy decoys with recently disclosed vulnerabilities. This allows the team to lure attackers into engaging with these decoys first and detect them early.

An example of this was during the discovery of the Apache Log4j2 vulnerability. The company deployed vulnerability outbreak decoys for this threat throughout its environment, which increased detection probability.

"Using FortiDeceptor vulnerability outbreak decoys provides us with an up-to-date and reliable layer of defense against new and emerging threats," says the network security tech. FortiDeceptor automatically and continuously updates the decoys, without any manual work or release upgrades required on our end."

Ease of Deployment and Maintenance

For close to 18 months, the company has used FortiDeceptor to deceive, expose, and eliminate internal threats, drawing on the FortiDeceptor solution's extensive decoy library to generate an authentic decoy layer across its network. The network security tech adds, "Although we mainly use decoys from the library, there is also the option to build your own. This allows us to add real value by ensuring that our decoys accurately resemble the types of assets one would expect to find on our network."

The network security team was also impressed by the usability of the system, as FortiDeceptor is packaged with playbooks and optional configurations that enable users to create new decoys automatically. "Basic deployment is so simple," says the network security tech, "we got it up and running in an hour. Plus, with FortiDeceptor solution's passive asset discovery, we ensure decoys are generated and placed in strategic locations across our network, saving us valuable time and resources."

Business Impact (cont.)

- Gain full visibility into network assets using FortiDeceptor passive and active discovery capabilities
- Effectively handle emerging threats and vulnerabilities with a continuously updated decoy library
- Rapidly isolate human or automated attacks

Products and Solutions

- FortiDeceptor
- FortiGate Next-Generation Firewall
- Fortinet Secure SD-WAN
- FortiSwitch
- FortiAP
- FortiClient
- FortiManager
- FortiAnalyzer
- Fortinet Security Fabric

"FortiDeceptor provides us with a nonintrusive way to detect and block malicious activity with zero false positives, which tremendously helps us to stop malicious activity very early and at the perimeter."

Network Security Tech Lead
IT Solutions Provider

For the company, the passive asset discovery feature also proved useful in other ways. As the organization has a large facility, passive asset discovery helps the team not only in scanning and mapping the environment for decoy creation and placement, but to discover devices added to the network or orphaned devices that would be more vulnerable to attack.

Usability and the Power of the Fortinet Security Fabric

The company has also deployed the Fortinet Security Fabric in its own organization, protecting its network edge using FortiGate Next-Generation Firewalls (NGFWs). Some of these are deployed in branch facilities as Fortinet Secure SD-WAN solutions alongside FortiSwitch secure Ethernet switches and FortiAP access points. The company also uses FortiClient endpoint protection to provide secure remote access, FortiManager centralized network management for single-pane-of-glass management, and FortiAnalyzer network analytics and automation to improve its detection and response capabilities.

www.fortinet.com

April 28, 2023 12:17 AM

2078458-0-0-EN