SOLUTION BRIEF

FortiDeceptor Enables a New Breach Protection Approach

Executive Summary

Whether a security breach happens due to an external or internal attack, it can take months for an organization to discover the breach and begin remediation. During this timeframe, extensive and irreparable financial and reputation damage can occur. To avoid this situation, forward-thinking cybersecurity architects can use Fortinet FortiDeceptor to deploy a network of lures to redirect attackers away from an organization's valuable assets. This greatly reduces the risk of breaches resulting from unknown threats.

FortiDeceptor is a deception-based technology intended to deceive, expose, and eliminate both external and internal threats before any significant damage is done. Creating a network of deception VMs that appear ripe for attack, FortiDeceptor then analyzes any threat activity and shares information via the Fortinet Security Fabric across all security components to protect the network. Unlike other threat-deception solutions, FortiDeceptor is easy to manage, integrates with an organization's existing security architecture, and automates threat response.

FortiDeceptor Helps Avoid Security Breaches By:

- Complementing an organization's breach protection strategy
- Redirecting attacks to deception hosts
- Acting as an early-warning system for threats
- Automatically responding to external and internal threats
- Enabling rapid deployment and use of deception technology on day one

Challenges in Timely, Effective Breach Response

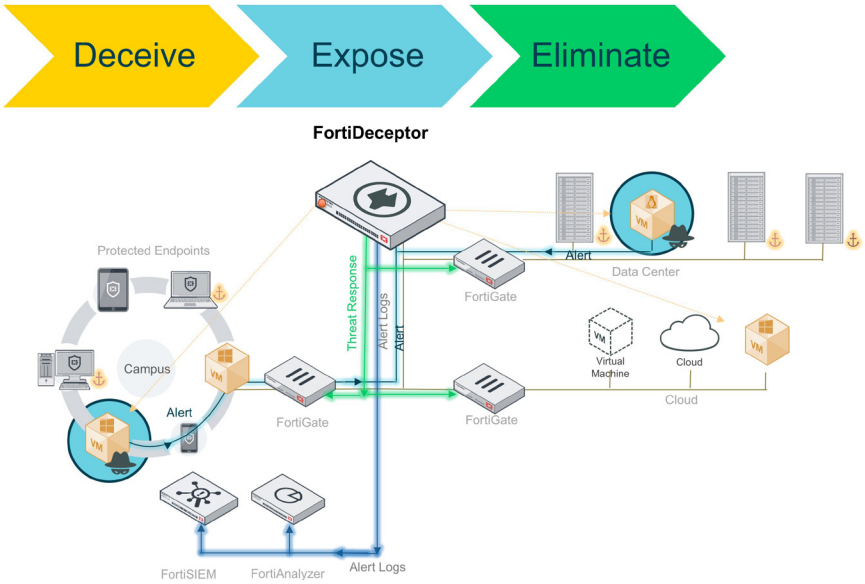
Breaches can originate from external and/or internal attacks; however, most security solutions focus on only one of the vectors, not both. The Verizon 2018 Data Breach Investigations Report found that two-thirds of breaches stem from external attacks, with the remaining one-third originating from internal actors. Even when a breach is discovered, 68% of breaches took months before being discovered.[1] But when breaches go undetected for this amount of time, the eventual repercussions can grow exponentially.

While cyber-threat defenses are evolving in step with attackers and malware, new advanced threat-protection technology often requires significant resources to deploy, provision, and maintain. In addition, these new technologies are usually offered as a stand-alone security solution, creating a disjointed security architecture.

Deceiving, Exposing, and Eliminating Threats

Fortinet FortiDeceptor leverages deception technology to detect and respond to both external and internal threats. It creates a network of honeypot VMs and integrates threat analytics and real-time protection via the Fortinet Security Fabric. FortiDeceptor follows the deception life-cycle paradigm shown in Figure 1.

In the initial Deceive phase, the cybersecurity team deploys deception VMs and decoys across the organization's campus, data center, or cloud that simulate real assets. Deception VMs simulate endpoints such as user and IoT devices and data-center servers. Decoys are lures installed on a deception VM or actual endpoint. In this case, authentic-looking data, applications, and services act as lures for both external and internal threat actors.



Next, in the Expose phase, an attacker's activity and lateral movement throughout the network are captured and correlated to form a timeline with details presented in the context of a broader threat campaign. In parallel, security administrators are alerted, and the threat is rapidly validated via a GUI-driven workflow. Logs can also be shared with security information and event management (SIEM) solutions for single-pane security event management.

Finally, in the Eliminate phase, intelligence gathered allows the security team to investigate and either take manual remediation steps or allow FortiDeceptor to automate mitigation for proactive damage control.

Actionable, Automated, and Easy Threat Deception

FortiDeceptor offers several advantages over competing threat-deception solutions. By integrating with the Fortinet Security Fabric to automatically synchronize with other security components such as FortiGate next-generation firewalls, it can automate protection and block attacks in real time before damage occurs.

It also provides actionable visibility, with a GUI-driven threat map that enables cybersecurity architects to quickly uncover threat campaigns targeting an organization, monitor attacks, and facilitate forensic investigations with correlated timelines and activity.

FortiDeceptor is also easy to deploy and manage. It can be deployed as a VM or as an on-premises appliance, or in the cloud. Administrators can centrally manage and automate the deployment of deception VMs, decoys, and services. The upside with FortiDeceptor for administrators is that they can set it up and it runs without ongoing management, something that is important for security teams that are often overburdened.

A Deceptively Simple Innovation

With the introduction of user-friendly threat-deception technology, Fortinet continues to be a security innovator. FortiDeceptor is effective against both external and internal threats and can prevent these threats from doing significant and lasting damage. By integrating with the Fortinet Security Fabric, which shares actionable intelligence to automatically respond to threats, FortiDeceptor is designed with busy cybersecurity architects in mind.

[1] "2018 Data Breach Investigations Report," Verizon, March 2018.

FORTINET

www.fortinet.com

March 21, 2019 10:52 AM

375208-0-0-EN

Macintosh HD:Users:bhoulihan:Documents:_Projects:Solution Brief:sb-FortiDecptor:sb-fortideceptor-032119-1100am