SOLUTION BRIEF

Reroute Threats Outside Your Network with FortiDeceptor-as-a-Service

Executive Summary

Attackers repeatedly prove that they can exploit security gaps to infiltrate your network and then move around undetected for extended periods. Most organizations cannot detect or respond to threats that have gained access to their network fast enough to prevent damage.

With FortiDeceptor-as-a-Service, you can leverage advanced deception technologies to deceive attackers into engaging with fake assets, data, and applications. This reveals the attack and enables your security team to stop it from progressing very early in the attack cycle. The service delivers high-fidelity zero false-positive alerts powered by rich threat intelligence and actionable insights. FortiDeceptor-as-a-Service is an agentless solution that does not impact network stability, performance, or business continuity.

Deception technology will become more pervasive in 2024 and become a security operations staple by the end of 2025.[1]

Today's Cybersecurity Challenges

Security teams face many issues, such as high false-positive rates, unknown risks evading detection, and sophisticated adversaries changing tactics. And, with networks continuing to become more complex and adding more attack surfaces, it's just a matter of time before a threat makes it into your network. The good news is that even when a threat has breached defenses, deception technology can detect it early and prevent it from causing damage.

FortiDeceptor-as-a-Service is a SaaS-based deception solution hosted in the Fortinet private cloud that detects and responds to in-network attacks, such as stolen credential usage, lateral movement, man in the middle (MITM), and ransomware. Deploying FortiDeceptor-as-a-Service transforms your entire network into a mirror maze with numerous authentic-seeming fake assets in minutes. When an attack is detected, high-fidelity zero-false-positive alerts are generated immediately. This enables your security team to detect human and automated attacks earlier in the kill chain and move them to the FortiDeceptor-as-a-Service cloud to avoid damage.

How FortiDeceptor-as-a-Service Works

Frictionless deployment of deception assets

Once deployed, FortiDeceptor-as-a-Service automatically performs asset discovery (active/passive), creates an asset inventory, generates decoys and deception tokens, and recommends their optimized deployment.

FortiDeceptor-as-a-Service provides many IT, OT, and IoT decoys. Decoys can also generate limited fake network traffic to ensure they appear in passive network scans the attacker runs. In addition, it generates deception tokens (fake cached credentials, data and configuration files, network share) placed on real assets. Deception tokens are agentless technology that serves as attractive targets for attackers, designed to deceive them to laterally move to the decoys. Any interaction with deception assets redirects attackers away from the network to the decoy hosted in the cloud.

Decoys run in the Fortinet private cloud, using your available, unused IP addresses. The IP addresses do not correspond to any real host or device on your network nor impact network availability. FortiDeceptor-as-a-Service also includes a local lightweight decoy connector, the FortiDeceptor 100G Edge, available as hardware or a virtual appliance. Deployed in your network, the FortiDeceptor 100G Edge uses a secure Layer 2 tunnel to connect the relevant decoys hosted in the Fortinet private cloud to the respective VLANs. The FortiDeceptor private Layer 2 tunnel is embedded with its own authentication and encryption methods and heartbeat checks on top of SSL and TLS encryption.

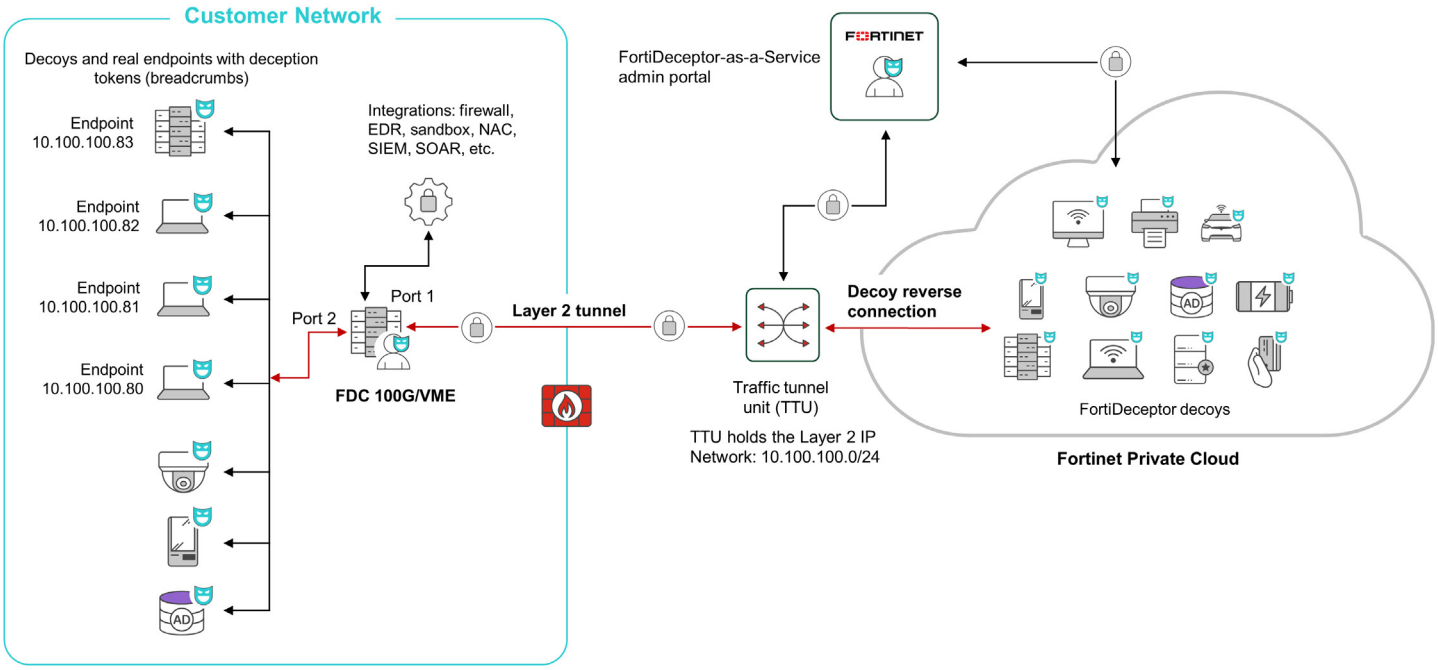

Figure 1: FortiDeceptor lightweight 100G Edge appliance connects via Layer 2 to Fortinet TTU, linking an organization's available IP addresses to the relevant decoys. The service provides decoys in the cloud and tokens on real endpoints and servers.

Enhanced threat intelligence and accelerated response

Any engagement with deception assets triggers an alert in the FortiDeceptor-as-a-Service user interface and can be shared with SIEM, SOAR, or any other threat-hunting solution. In parallel, it immediately starts capturing and analyzing indicators of compromise and tactics, techniques, and procedures in real time. It uses eight built-in engines: IPS, web filter, AI/ML, VirusTotal, sandbox, malware AV, packet capture analysis, and anti-reconnaissance and anti-exploit services to provide detailed forensics. This intelligence can also mitigate threats by enabling automatic response. For example, FortiDeceptor can quarantine infected endpoints using built-in isolation capabilities or out-of-the-box integration connectors with third-party tools, including firewall, endpoint detection and response, and network access control products.

Credible deception layer

FortiDeceptor Manager is automatically updated with the latest threat intelligence from FortiGuard Labs and enriches the decoys with the most up-to-date exploitable vulnerabilities to ensure early detection.

Multitenant capabilities

Ideal for MSSPs and MSPs, the service includes an intuitive, multitenant management portal, enabling security teams to oversee tenants' activities and streamline operations.

Key Benefits

FortiDeceptor-as-a-Service is a key layer of defense that:

- **Detects and stops ransomware attacks:** Once malware encrypts a fake file (FortiDeceptor token), FortiDeceptor-as-a-Service identifies it as a ransomware attack, generates an alert, and quarantines the infected endpoint to limit the attack from spreading.
- **Detects zero-day threats:** High-interaction decoys with real operating systems can detect zero-day exploits and techniques.
- **Delivers pre-breach warnings:** By deploying decoys in the DMZ or perimeter, SOC analysts receive alerts on adversary activities early in the attack cycle and can adjust the security posture accordingly to stop attacks at the perimeter.
- **Protects unpatched legacy OT and IoT systems:** Decoys (fake PLC, HMI, SCADA, IoT sensors) are deployed in every zone of the Purdue model, providing a layer of defense without impacting uptime or halting processes. FortiDeceptor-as-a-Service supports the MITRE ATT&CK for ICS framework and provides extensive IT, OT, and IoT decoys and protocol support. It also provides non-intrusive asset discovery for decoy creation and placement recommendations.
- **Uncovers security gaps and prevents future attacks:** Enhances pen testing by simulating real IT, OT, and IoT environments, so that red teams and pen testers can easily create a lab environment, for example, to detonate and simulate attacks and evaluate the efficacy of security defenses.
- **Detects stolen credential usage:** Detects compromised credential usage if used to access web applications or VPN decoys deployed in the DMZ. This is enabled by FortiDeceptor-as-a-Service integration with Active Directory (AD) or an authentication list file that will trigger alerts once an adversary uses legitimate credentials against a fake DMZ asset. In addition, to detect compromised user attempts early, FortiDeceptor spreads fake user credentials (tokens) on real endpoints. Any use of these fake credentials will be discovered automatically.
- **Provides AD deception:** Provides AD decoys (real AD decoy server and decoy as part of the domain) and AD deception tokens that detect threats targeting AD.
- **Enhances ZTNA policy:** A ZTNA policy can redirect attacks to decoys (apps, databases) for further analysis and isolation. ZTNA-enabled deception also eliminates lateral movement by updating compromised users' ZTNA policies and endpoint protection agents, such as FortiClient, once FortiDeceptor-as-a-Service detects a compromised identity to enforce, for example, user quarantining.
- **Detects Layer 2 attacks:** Detects MITM attacks, NBNSSpoofSpotter, NBT-NS, mDNS, LLMNR spoofing, using both active and passive methods.

Summary

FortiDeceptor deceives, exposes, and eliminates internal threats early in the attack kill chain, proactively blocking them before any significant damage occurs. In addition to FortiDeceptor-as-a-Service, FortiDeceptor is available as a hardware and virtual appliance and in a ruggedized version ideal for harsh environments.

FortiDeceptor-as-a-Service is part of the Fortinet Security Fabric, our unified platform of Secure Networking, Unified SASE, and AI-Driven Security Operations, which redefines cybersecurity, helping you respond faster to an ever-evolving cyberthreat landscape.

Learn more about FortiDeceptor.

[1] Jon Oltsik, "Active Defense and Deception Technology: The Time is Now!" Enterprise Strategy Group, June 2023.

FORTINET

www.fortinet.com

March 12, 2024 10:47 PM
2574781-0-0-EN