SOLUTION BRIEF

FortiGate and Darktrace Security Solution

Self-learning, AI-driven Response To Novel and Sophisticated Attacks

Executive Summary

Together, Darktrace and FortiGate provide artificial intelligence (AI)-driven detection and response across the enterprise, ensuring even the most novel and sophisticated threats are caught once inside. With the power of self-learning AI, Darktrace can detect and investigate even the most subtle signs of a threat, and Darktrace's Antigena Network can execute autonomous responses to neutralize attacks. Antigena Network can respond either via surgical self-directed actions or the FortiGate next-generation firewall (NGFW), updating its list of malicious IPs with bespoke, real-time input as attacks emerge. Meanwhile, the FortiGate NGFW shares insights with Darktrace's Cyber AI, enriching the system's visibility.

Defending the Evolving Enterprise and Dynamic Workforce

Enterprises are constantly expanding, supply chains and partner networks shift, business strategy changes, and working habits evolve. An increasingly dynamic workforce risks exposing data, creates new vulnerabilities, and is more susceptible to human error.

Static rules, threat signature lists, and playbooks have been unable to adapt fast enough to changing users and businesses, no matter how diligently and rapidly they are rewritten. Security solutions that rely on policies or retrospective data cannot keep up with the evolving workforce, nor can they manage the evolving threat landscape. Novel and sophisticated threats—from malicious insiders to zero-day ransomware—inevitably get in, and security teams urgently need solutions that can stop these attacks in real time.

Joint Solution

Darktrace and Fortinet have partnered to deliver an industry-leading security solution for real-time response to even the most subtle and novel cyber threats. The integration of the Darktrace Immune System and the Fortinet FortiGate, enabled through the Fabric-Ready Program in the Fortinet Open Fabric Ecosystem, delivers AI-driven Autonomous Response to your FortiGate NGFW, and ensures Darktrace's Cyber AI has all the context possible to extend the scope of its self-learning artificial intelligence.

Joint Solution Components

The Darktrace Immune System uses self-learning AI to identify and investigate otherwise unknowable threats as they emerge. The platform powers Antigena Network, the world's first Autonomous Response solution for the enterprise. The solution can interrupt attacks at machine speed and with surgical precision, even if the threat is targeted or entirely unknown. It can take action in various ways,

Joint Solution Components

- Darktrace Immune System
- Darktrace Antigena Network
- Fortinet Next-Generation Firewall (NGFW)

Joint Solution Fabric

- Detection of even the most unpredictable and novel attacks
- Real-time, autonomous response to emerging threats
- Adaptive defense that evolves with your business and the threat landscape
- Enriched visibility across the dynamic workforce
- Unparalleled network security protection provided by the industry-leading FortiGate Next-Generation Enterprise Firewall and Fortinet Security Fabric

whether through self-directed actions that enforce normal "patterns of life" and sustain normal operations by design, or via native integrations with firewalls and network devices, including the FortiGate NGFW.

Fortinet FortiGate NGFWs enable security-driven networking and consolidate industry-leading security capabilities such as intrusion prevention system (IPS), web filtering, secure sockets layer (SSL) inspection, and automated threat protection. Fortinet NGFWs meet the performance needs of highly scalable, hybrid IT architectures, enabling organizations to reduce complexity and manage security risks. As an integral part of the Fortinet Security Fabric, FortiGate NGFWs can communicate within the comprehensive Fortinet security portfolio as well as partner security solutions in a multivendor environment.

Joint Solution Integration

The Darktrace Immune System uses a unique approach grounded in unsupervised machine learning to learn what normal activity looks like for a business and to correlate all the weak deviations that may point to a threat—no matter how sophisticated or novel. The Cyber AI technology also powers Darktrace's Antigena Network, the industry's first and only Autonomous Response solution that can stop attacks in real time.

Antigena Network seamlessly plugs into and enhances your existing ecosystem, informing the FortiGate firewall about attacks that have gotten through your other defenses. Antigena executes intelligent, proportional actions to neutralize emerging attacks, and with the FortiGate integration can leverage the NGFW to autonomously respond to threats. This allows Darktrace's AI to take even more targeted action based on your firewall operators' specifications and ensures the FortiGate NGFW learns about advanced and zero-day attacks in real time.

Antigena Network integrates with Fortinet FortiGate firewall devices via Hypertext Transfer Protocol Secure (HTTPS) using the FortiOS representational state transfer application programming interface (REST API). To implement actions, Antigena Network creates Address Objects within the firewall to intelligently flag IP addresses that are related to detected threats, and assigns them to Address Groups associated with blocking policies.

This integration method allows for precise separate service control if desired by your firewall operators. Blocking policies are defined in the firewall, allowing security teams to decide the best course of action for Antigena intelligence. The FortiGate NGFW also provides extended visibility to the Darktrace Immune System, enriching the system's bespoke understanding of your organization's context and its high-fidelity decision-making power around detection, investigation, and response.

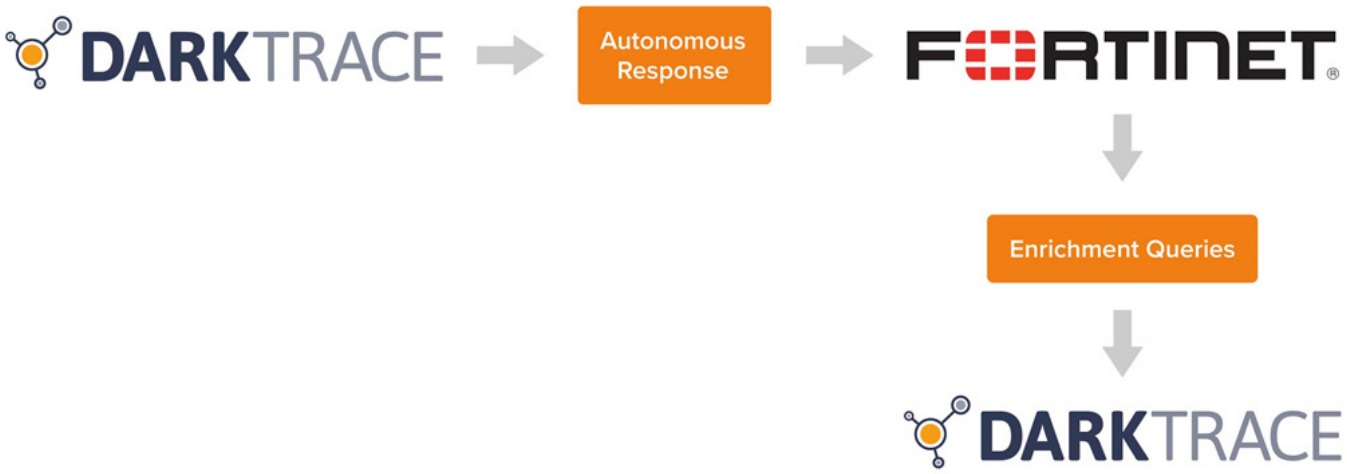
Joint Use Cases

Use Case 1: Block IPs Related to Novel and Unpredictable Attacks

With Darktrace's unique self-learning approach, Antigena Network can neutralize insider threats and zero-day attacks—even before attribution of zero-day attacks or updated tactics, techniques, and procedures (TTPs) are publicly available. This partner solution allows Antigena Network to autonomously action your FortiGate NGFW to respond to emerging attacks and block previously undetected malicious behavior.

Use Case 2: Enrich Self-learning Analysis With FortiGate Logs

This partner solution allows the Darktrace Immune System to ingest logs from the FortiGate NGFW, extending the platform's visibility and ensuring Cyber AI has as much contextual information as possible. This enriches the system's understanding of "self" for the unique business, augmenting Darktrace's autonomous decision-making.



About Darktrace

Darktrace is the world's leading cyber AI company and the creator of Autonomous Response technology. Its self-learning AI is modeled on the human immune system and used by over 4,500 organizations to protect against threats to the cloud, email, IoT, networks, and industrial systems.

The company has over 1,500 employees and headquarters in Cambridge, UK. Every 3 seconds, Darktrace AI fights back against a cyber-threat, preventing it from causing damage.

March 24, 2021 10:38 PM

D:\Fortinet\2021 Rebranded templates\Solution Briefs\March\Dark Trace\sb-FA-fortigate-and-darktrace-security-solution-362021\sb-FA-fortigate-and-darktrace-security-solution-362021

920912-0-0-EN