FORTIS By Sentinel

Advancing Your Protection

Quickly Establish Zero Trust Segmentation Across Your Clouds, Data Centers, and Endpoint Devices

Fortis by Sentinel is proud to partner with Illumio, an innovative provider of Zero Trust segmentation solutions. Illumio Core utilizes proven segmentation technology to protect your organization's critical applications and valuable digital assets. It can be deployed either on-premises or through the cloud.

Fortis and Illumio: Better Together

While Illumio Core is available as a standalone solution, it also seamlessly integrates into the Fortis by Sentinel security portfolio. It can be monitored through the Fortis Security Operations Center (SOC) as well as our SIEM, which is powered by Splunk. Illumio's innovative features and analytics give our experts a more complete picture of your environment, which makes it easier to detect anomalies, issue alerts, and set stronger security policies.

Architecture

Policy Compute Engine (PCE) - Manage and control your segmentation using Illumio's PCE. It collects telemetry information to deliver real-time mapping of traffic patterns and recommendations for optimal allow-list rules based on your environment, workloads, and processes.

Virtual Enforcement Node (VEN) - A lightweight agent installed on the guest OS of a host or endpoint, the VEN collects flow and metadata information then transmits them to the PCE. It receives firewall rules from the PCE in order to program the managed host's L3 & L4 firewalls. The VEN does not enforce firewall rules or route traffic.

Agent-Less Visibility and Segmentation Enforcement - In environments with no agents, Illumio Core ingests flow data from networking equipment, cloud metadata, cloud-native security information, and flow logs. This creates a unified map of communication flows across your digital infrastructure. Illumio uses Access Control Lists (ACLs) to segment your routers, switches, and load balancers. It also recommends and programs policies to optimize cloud-native security groups.

Features

Illumination - Gain real-time visual insights into your application communication flows so you can better understand critical pathways, detect anomalous behavior, build segmentation policies, and test new segmentation rules.

Core Services Detector - Machine learning helps quickly identify critical infrastructure services, then recommends labels and Zero Trust segmentation policies to secure legitimate traffic.

Enforcement Boundaries - Guided workflows, visualization, and reporting to assist with the safe transition from an allow/deny-list firewall rules approach to a true allow-list model. This avoids the complexity of fully managing a priority order of firewall rules.

Policy Generator - Policy Generator uses flow history to recommend optimal segmentation policies for your application workloads, no matter their type or location. Policies can be created without in-depth knowledge of networking details.

Explorer - Search the historical traffic database in the PCE, analyze traffic patterns, and generate reports to assist with audits, threat hunting, troubleshooting, and creating allow-list rules.

Vulnerability Maps - A combination of application dependency maps and vulnerability data from scanning tools, vulnerability maps enable a more detailed understanding of potential pathways taken by malware and hackers so you can apply segmentation to limit their movement.

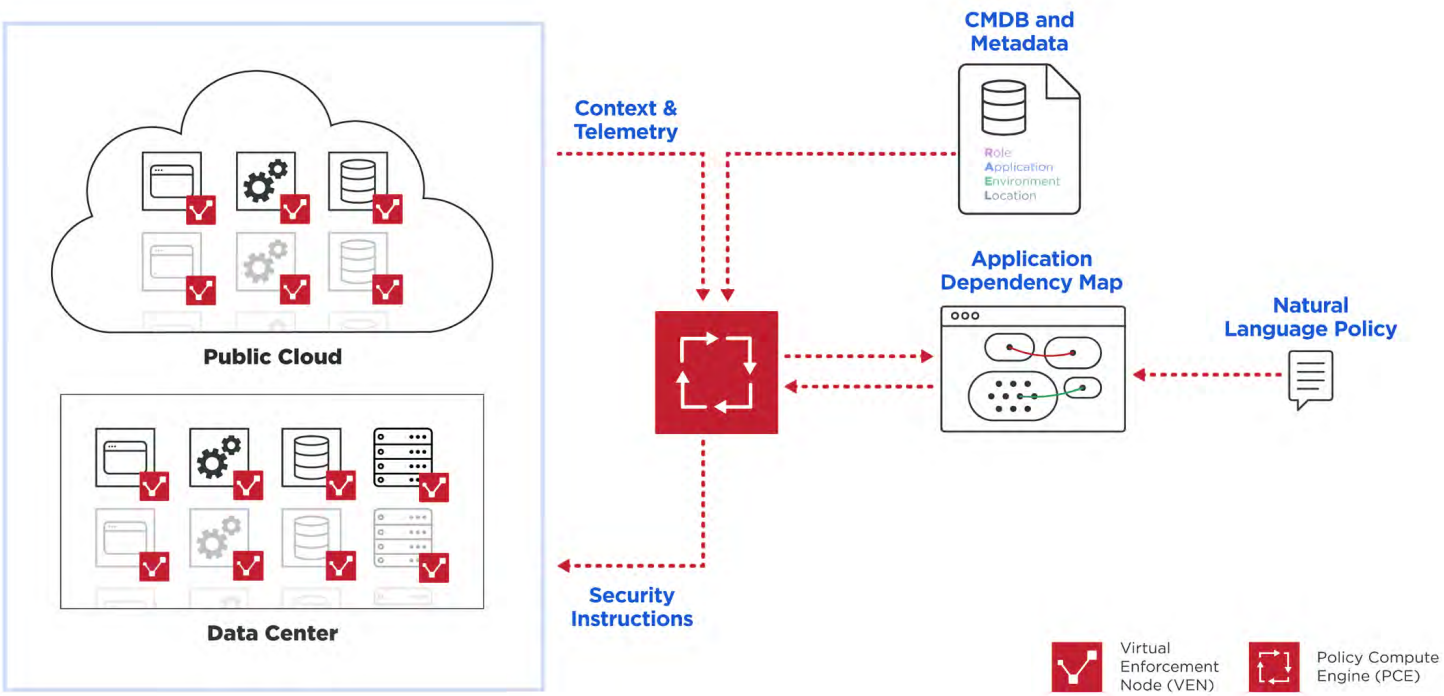
SecureConnect - SecureConnect supports on-demand, host-to-host traffic encryption between paired workloads by using the built-in encryption libraries of host operating systems. SecureConnect is policy-driven and managed by the PCE.

FORTIS By Sentinel
Advancing Your Protection

Benefits

- Automated security that immediately enforces allow/deny-list rules
- Obtain real-time views of your traffic flows and application communications to help strengthen security
- Lower your overall risk profile and optimize segmentation policies
- Operates entirely on a Zero Trust framework
- Easily integrates into any type of IT environment
- Enhanced capabilities when paired with Fortis by Sentinel's SIEM and SOC monitoring

Illumio Core Architecture



Source: Illumio Core Technical Brief

If you would like to learn more about Illumio Core, contact Sentinel today!

www.fortisbysentinel.com
1.800.769.4343 (main)
1.844.297.4853 (Incident Response Hotline)
infoSENter@sentinel.com