Fortinet and Alcide Security Solution

Broad, integrated and automated solution for continuous cloud security with enhanced threat detection and mitigation

Making the leap from hosting workloads in traditional on premise data centers to public or hybrid cloud environments requires a different way of thinking when it comes to securing those workloads. Existing tools, processes and practices don't readily translate to the on-demand, elastic nature of the cloud. Where once an organization's security team could define, enforce and monitor security policy for the entire stack, it now becomes a shared responsibility between the organization and the cloud provider.

Add to this, the increased complexity in the way that modern applications are deployed to cloud environments; it's easy to feel that control is slipping from our grasp. The workloads, delivered as a set of microservices running in containers, are distributed and transitory in nature. They may be hosted on and across multiple Kubernetes clusters, which in turn may be hosted across different cloud regions or even cloud providers. When workloads and infrastructure are distributed in this manner, the task of maintaining a robust security posture becomes an onerous one.

All of this necessitates a different approach to protecting the assets that organizations deploy to the cloud. It requires establishing policy for all of the disparate moving parts in the stack and across infrastructure boundaries, using an integrated and coherent approach. And, it requires the application of continuous threat intelligence in order to stay ahead of the ever evolving landscape of vulnerabilities and exploits.

Joint Solution Benefits

- Unified approach to threat management
- Combined analysis of north-south and east-west traffic
- Real-time, automated mitigation of suspicious workloads, through traffic restriction
- Continuous command and control
- Convergence on anomalous network activity
- Frictionless application delivery without compromising security

FORTINET Fabric-Ready

Joint Solution Description

Alcide's security platform, in conjunction with Fortinet's Security Fabric, provides an enhanced threat detection and mitigation capability that significantly reduces the risk for cloud native software applications.

North - South Traffic

Attacks normally originate outside the perimeter of the infrastructure that hosts application workloads. The ingress traffic that crosses the boundary into the infrastructure, and the egress traffic that flows in the opposite direction, is often referred to as north-south traffic. Detecting threats, and mitigating against potential threats, for north-south traffic is a problem that is well understood by Fortinet. FortiGate, its next-generation firewall technology is designed for the purpose of protecting the edge of the infrastructure from malware and other forms of unwarranted and unsolicited intrusion.

The industry-leading threat protection of FortiGate firewalls benefit from regular updates provided by the FortiGuard labs threat intelligence services, ensuring that organizations are protected against the very latest attack vectors.

East - West Traffic

When applications are architected as small, independent, loosely-coupled microservices, however, not only is traffic flowing in a north-south direction; it's also flowing in an east-west direction. Platforms like Kubernetes enable these services to be deployed and scaled across multiple nodes inside the boundary of the infrastructure, with the services inter-connected into a mesh of communication. It would be easy to assume that the perimeter of the infrastructure is the sole entry point for malware, but the truth is that malware can find its way onto internal networks in a variety of ways. This makes securing east-west traffic, equally as important as the north-south traffic at the boundary.

Courtesy of an agent that is run on each infrastructure component, Alcide's security platform analyzes east-west traffic and enforces security policy that has been defined in advance through its user interface. Alcide also comes equipped with a threat detection engine, and analyzes the data collected using machine learning algorithms which can detect behavior anomalies, and known security signatures. It can even use the FortiGuard threat intelligence feed to detect things like crypto mining and port scanning from within the internal network.

Multi-Cloud and Multi-Cluster Scenarios

Combining the capabilities of the Fortinet's FortiGate Firewall, and the Alcide platform's ability to consume and configure security policy at different layers of the stack, as well as detect anomalous behavior, presents a powerful solution to a very tricky problem. It's a solution that can be extended beyond a single cluster or virtual private cloud (VPC), and can be used to protect multiple clusters across multiple VPCs, regions or even providers.

Control and Visibility

Threat detection and automated mitigation is clearly an essential ingredient in maintaining a secure environment for cloud native applications. But, equally important is the ability to configure, visualize and monitor security policy across the whole stack, without having to use a profusion of native tools.

Alcide's security platform provides a central point of command and control for defining policy at different levels in the stack. Whether it's configuration of an AWS Security Group, or a Kubernetes Network Policy, the different components are abstracted away into a single interface for management and monitoring. It means that access policy can be configured to a granular level using a single user interface.

Fortinet Security Fabric

The Fortinet Security Fabric is an architectural approach that unifies the security technologies deployed across the digital network, including multi-cloud, endpoints, email and web applications, and network access points, into a single security system integrated through a combination of open standards and a common operating system. These solutions are then enhanced through the integration of advanced threat protection technologies and a unified correlation, management, orchestration, and analysis system.

About Alcide

Alcide provides a cloud-native security platform from code to production to continuously secure workloads running in Kubernetes. Companies use Alcide to discover, manage, and secure their cloud deployments, resulting in a frictionless experience to ensure the security of their mission-critical apps.

FORTINET®

www.fortnet.com

February 6, 2019 9:14 PM

123456-0-0-EN

Mac:Users:susiehwang:Desktop:Egnyte:Egnyte:Shared:Creative Services:Team:Susie-Hwang:Egnyte:Shared:CREATIVE SERVICES:Team:Susie-Hwang:2018:Collateral-Refresh-2018:Solution-Brief-Template:sb-template-gray Folder:sb-template-gray