SOLUTION BRIEF

Extending Enterprise Security Into Kubernetes Environments

Executive Summary

Container use continues to grow, and Kubernetes is the most widely adopted container orchestration system, managing nearly half of all container deployments.[1] For security architects looking to protect these deployments, Fortinet offers container-aware, container-integrated, container-enabled, and container-registry security solutions.

Fortinet and Tigera have partnered to deliver container-integrated solutions for the Calico network stack. To enable the successful transition of Calico-based Kubernetes pilot projects to enterprisewide application rollouts, companies must be able to extend their existing enterprise security architecture into the Kubernetes environment. In response, Fortinet and Tigera jointly developed a suite of Calico solutions for the Fortinet Security Fabric. These solutions deliver both north-south and east-west visibility and protection, as well as compliance enablement and advanced threat-intelligence capabilities for Kubernetes clusters.

Containers Proliferating, Yet Causing Concern[2]

- 47% of organizations have vulnerable containers in production; 46% are unsure if deployed containers had vulnerabilities.
- 60% of organizations experienced a container security incident, and 42% limited container adoption due to security concerns.

Security Challenges in Kubernetes

Because containerized services are highly purpose-specific, they depend heavily on access to external resources such as databases, cloud services, third-party application programming interfaces (APIs), and other applications. All this egress activity must be controlled for security reasons. However, traditional IP-based access control does not work in Kubernetes, where workloads are ephemeral (and typically stateless) and use short-term IP addresses. And while the Calico Enterprise security management interface provides customized control within the Kubernetes environment, using Calico Enterprise security in isolation from existing enterprise network security leaves organizations with disparate policy-enforcement regimes. Manual policy synchronization is inefficient and prone to errors, which are a major source of data breaches.

Maintaining two separate network security systems also hinders visibility into routing and connectivity within and between Kubernetes clusters. This complicates the process of troubleshooting issues that span Kubernetes and external environments. Moreover, because enterprise monitoring tools lack Kubernetes context, the impact of security policy changes are hard to predict, and the unintended consequences are difficult to diagnose.

Lack of visibility also has compliance implications. Like any on-premises or cloud-based networked services, Kubernetes production containers must fulfill both organizational and regulatory security requirements. If compliance teams cannot trace the history of incidents across the entire infrastructure, they cannot adequately satisfy audits into Kubernetes clusters.

Integrating Calico Enterprise and the Fortinet Security Fabric

Tigera is the inventor and maintainer of Project Calico, an open-source Kubernetes network security solution with more than 150,000 known clusters in over 160 countries. Developers spinning up Kubernetes-managed containerized environments on any major public cloud will likely find Calico security already in place on these platforms.

Meanwhile, other enterprise teams—such as infrastructure, security, networking, and compliance—will want to ensure that approved network security policies are faithfully reproduced in all the Kubernetes clusters that the developers launch.

Satisfying the needs of all these stakeholders is key to ensuring successful enterprisewide Kubernetes rollout and operations. To this end, Fortinet and Tigera have developed four key integrations that help ensure consistent and robust security, visibility, control, and compliance:

FortiManager Calico Kubernetes Controller enables Kubernetes cluster management from the FortiManager centralized management platform. This Fabric Connector translates FortiManager policies into granular Kubernetes network policies and pushes them out to the individual clusters in all Kubernetes environments. Thus, the Kubernetes environment becomes an integral part of the Fortinet Security Fabric, and can be seen and controlled from the FortiManager console.

FortiGate Calico Kubernetes Controller enables FortiGate next-generation firewalls (NGFWs) to control egress from Kubernetes pods to applications. It does this by automatically populating Kubernetes workload source IPs in FortiManager address group objects. FortiManager then deploys the updated object packages to FortiGate, so that FortiGate can enforce the access rules. This means that developers who add new containers to a Kubernetes pod can use business-level tags (such as department name or role) to identify them and rely on the controller to handle the underlying access rule configurations.

FortiGuard Threat Feed integration enriches the Calico threat database with global real-time threat intelligence from FortiGuard Labs. Calico Enterprise users gain broader protection from malicious traffic at the source in the Kubernetes cluster. For FortiGuard subscribers, this integration ensures that the most robust protection will cover their Kubernetes environment as well, at no additional cost.

The Calico FortiSIEM plug-in event correlation and risk management solution delivers the telemetry (metadata) that Calico creates—including DNS logs, flow logs, and audit logs—into the Fortinet security information and event management (SIEM) environment. This helps security operations (SecOps) teams leverage FortiSIEM to better design and automate their workflows for incident response.

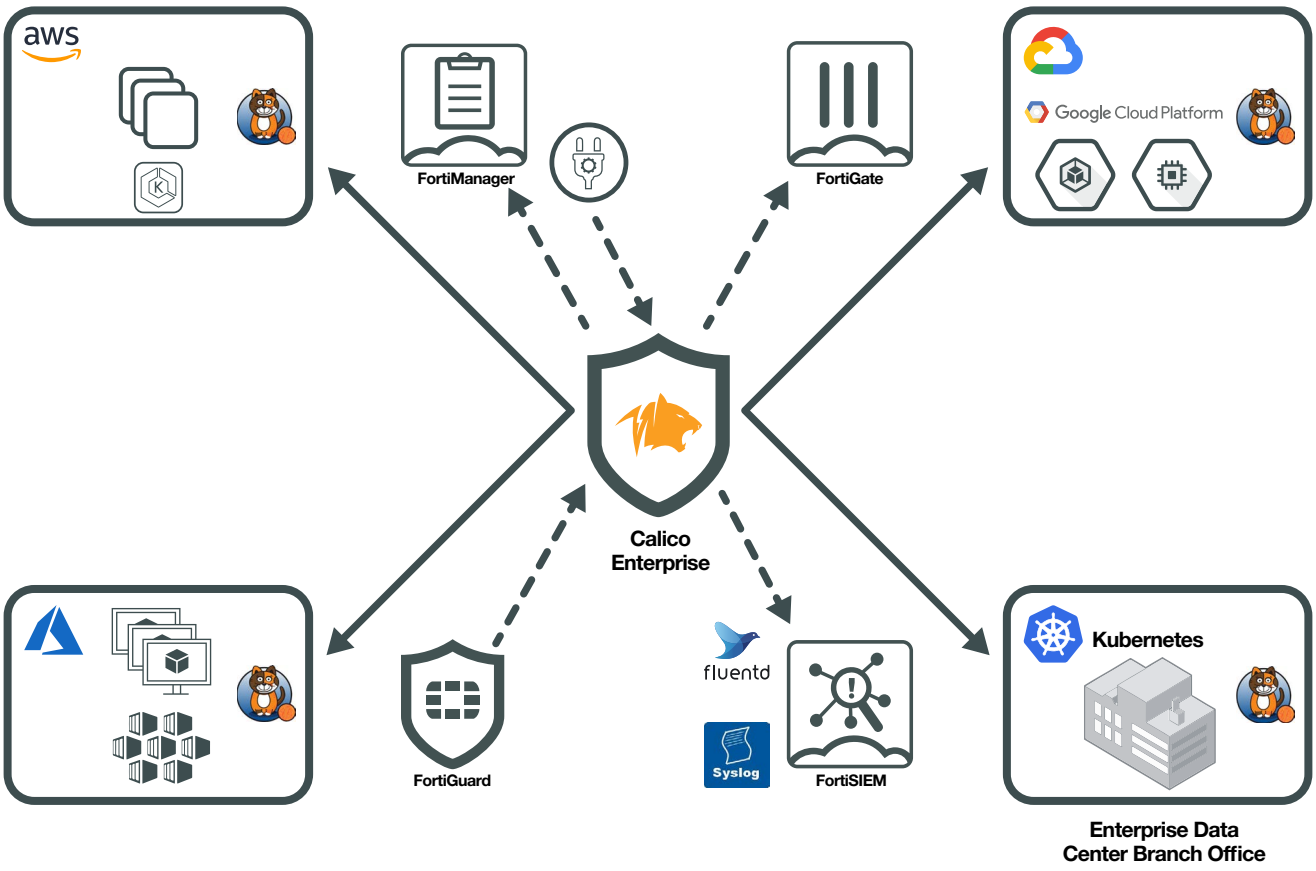

Figure 1: Calico for Fortinet solutions leverage Calico's Kubernetes expertise and broad installed base to benefit Fortinet Security Fabric customers.

Benefits for Fortinet Customers

Fortinet Dynamic Cloud Security solutions integrated with Tigera Calico Enterprise bring Kubernetes deployments into the fold of the Fortinet Security Fabric. As a result, organizations migrating to Kubernetes architectures maintain their security posture and ensure the successful adoption of the Kubernetes platform throughout the enterprise. On an operational level, integration between Fortinet and Tigera technologies provides the comprehensive insight needed to speed up troubleshooting, reducing mean time to resolution. These integrated technologies also reduce operational complexity, which reduces staff and training costs and minimizes configuration errors that can add significant attack risk to the organization. Security architects can also demonstrate the reduced risk in a timely fashion to comply with internal and external data-protection rules.

Enterprise-level Benefits of Calico/Fortinet Integrations

- **Security posture continuity.** Extend approved corporate network security policies to Kubernetes.
- **Full visibility into Kubernetes clusters.** Pinpoint specific sources of errors and risk.
- **Security-driven DevOps.** Shift Kubernetes security to an earlier stage in application development.
- **Collaborative security culture.** Ensure that security success is jointly owned by platform, security, compliance, networking, and DevOps teams.

[1] "RightScale 2019 State of the Cloud Report from Flexera," Flexera, 2019.

[2] "2019 Container Adoption Survey: Container Adoption Accelerates While Security and Data Management Concerns Remain Top of Mind," Portworx and Aqua Security, accessed January 31, 2020.

FORTINET®

www.fortinet.com

Copyright © 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

February 12, 2020 2:55 AM

588268-0-0-EN

D:\Fortinet\Solution Briefs\blue solution briefs\Calico\sb-FA-xtending-enterprise-security-into-kubernetes-environments