Securing the Cloud with Fortinet

5 Key Areas Where Architects Must Augment Cloud-native Security Tools

Table of Contents

Executive Overview

Corporate DevOps teams are leading the way to the cloud, but many are overlooking the full security implications of the move. If they simply accept the security offerings of their cloud platform, they are likely to leave gaps that attackers can exploit to steal data or infiltrate other areas of the corporate network. There are at least five security areas that security architects need to ensure they have covered when building and managing security in the cloud.

Fortinet offers a critical layer of security that integrates with the broader security architecture. It includes solutions for cloud platform security management, native integration of purpose-built security into the cloud platform, as well as web application and application programming interface (API) protection. It also provides integrations that help DevOps teams to automate security tasks in their cloud environments. All these help organizations achieve a consistent security posture and an effective security life-cycle management operational model—and without recruiting dedicated security staff or investing development staff time in training on new tools.

Introduction: Security Tools Offered by Cloud Providers Are Insufficient

DevOps teams are at the forefront of cloud adoption; the cloud model is well-suited to their continuous integration and delivery (CI/CD) practices. In many organizations, development teams are power cloud users, with rights to deploy cloud infrastructure—compute, storage, networking, and other resources—as needed. As developers exercise those privileges, however, security teams assume the risks. Indeed, security architects list DevOps security as their foremost priority this year.[1]

Chief among these risks are misconfiguration-exploiting cyber threats. A successful attack on a cloud-based environment can possibly impact the entire company, damaging the organization's reputation, interrupting operations, and/or causing the loss of crucial business data.

Cyber criminals now use advanced technologies such as artificial intelligence (AI) and swarm technology—as well as DevOps itself[2]—to create single-use malware that targets a particular organization across several points of the attack surface.

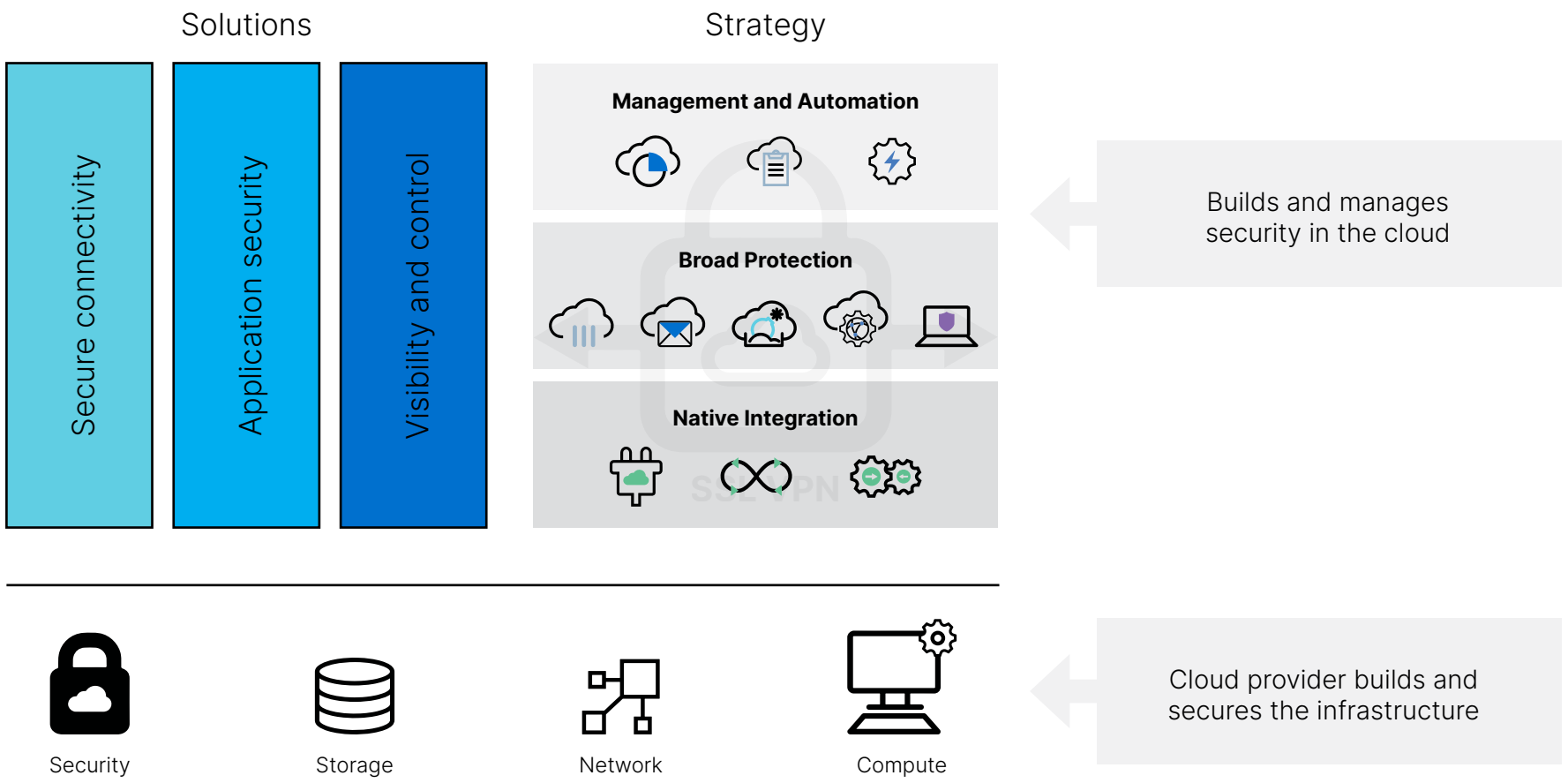


Figure 1: Cloud security solutions must provide secure connectivity, application security, and comprehensive visibility and control through management and automation, broad protection, and native integration capabilities.

Configuration complexity increases security risk

DevOps leaders may assume that they have cloud security covered. After all, public cloud services usually include security features such as security groups and access control lists (ACLs) that help cloud customers to control access privileges to these services. Customers can also take advantage of a variety of third-party cloud-based tools such as distributed next-generation firewalls (NGFWs), web application firewalls (WAFs), sandbox solutions, and cloud security posture management and workload protection solutions. The breadth of options and vendors can be overwhelming, and busy DevOps teams often fall back to basic security tools within the specific cloud environment. And, when necessary, they add point security tools to address identified gaps.

For security architects charged to mitigate DevOps security risks, this is problematic for several different reasons. First, even basic cloud tools contain extensive configuration options, and DevOps teams may not have the expertise to implement specific configurations for each and every available security service. In response, they often revert to the default configurations in the built-in security tool, which puts organizations at heightened risk.

To assist inexperienced cloud security users and ensure an effective security posture, DevOps teams often develop "golden" configuration templates that include preconfigured configuration services. Unfortunately, the configuration templates are prone to coding errors and may become obsolete, and the risk that any error introduces is amplified as the template is reused. Expectedly, data breaches caused by cloud misconfigurations have jumped 424% year over year, becoming 70% of all cloud data breaches.[3]

Data breaches caused by cloud misconfigurations jumped 424% year over year, comprising 70% of all cloud data breaches.[4]

The Solution: An Additional, Consistent Layer of Security

To minimize the risks of cloud security gaps without placing undue burdens on security teams, security architects can leverage the more robust protection of Fortinet cloud security solutions as an integrated part of the organization's broader, centrally managed security architecture. Specifically, Fortinet dynamic cloud security solutions cover four key areas of threat protection that are essential for organizations seeking the competitive advantages of DevOps agility and customer centricity without compromising corporate intellectual property or compliance.

1. **Cloud platform security**

   DevOps environments in the cloud change rapidly, and organizations are exposed to these changes from multiple cloud providers in an uncoordinated, siloed fashion. What security architects need to deliver to their DevOps counterparts, as well as the CISO, is centralized visibility and a control system that monitors the configuration state and posture of the entire cloud infrastructure.

   The **FortiCWP** cloud workload protection (CWP) enables security and DevOps teams to continuously monitor the security posture of their cloud environments. They can detect potential threats that result from misconfiguration of security settings, discover suspicious activity in their cloud infrastructure, analyze traffic moving in and out of cloud resources, and inspect data stored in the cloud for malicious or sensitive content.

What DevOps leaders need is centralized visibility and automated monitoring of the configuration state and posture of the cloud infrastructure.

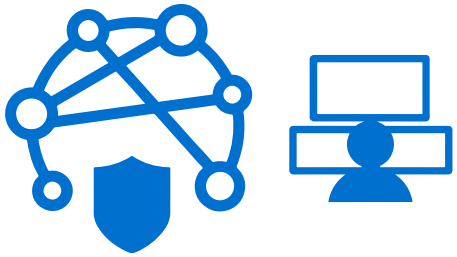
FortiCWP performs continuous configuration assessments, generating a risk score and offering best practice recommendations for improving it. Then, it continually monitors the configurations to ensure that issues are flagged and resolved in a timely manner. It also offers analysis tools that enable security architects to help DevOps leaders understand the life cycle of configuration changes across their multi-cloud environments.

2. **Native integration of FortiGate firewalls into the cloud platform**

   When considering how to secure their operations in the cloud, security architects need to design a security architecture that provides an enterprise-level view. They can achieve this by deploying FortiGate VM in virtualized (public and private cloud) environments and FortiGate appliances in physical domains.

Both virtual and physical FortiGate firewalls use logical information classification, based on tags and annotation metadata, as do all the other components of the Fortinet Security Fabric an organization uses. This enables security teams to maintain a consistent operational model and security posture across their dynamic multi-cloud infrastructure. Thus, threat response is rapid—and in many cases automatic—across the entire infrastructure, regardless of staff availability.

To keep pace with the aggressive timelines of competitive business application environments, Fortinet cloud security solutions feature native integration with a variety of cloud services, such as auto scaling, high-performance form factors with accelerated networking, cloud high-availability (HA) schemes, cloud configuration templates, and more. These integrations make cloud security more adaptable to the dynamic nature of the cloud infrastructure.



Security architects are challenged to maintain advanced threat protection with limited security skills on staff. Native integration between FortiGate and the cloud infrastructure eases this burden.

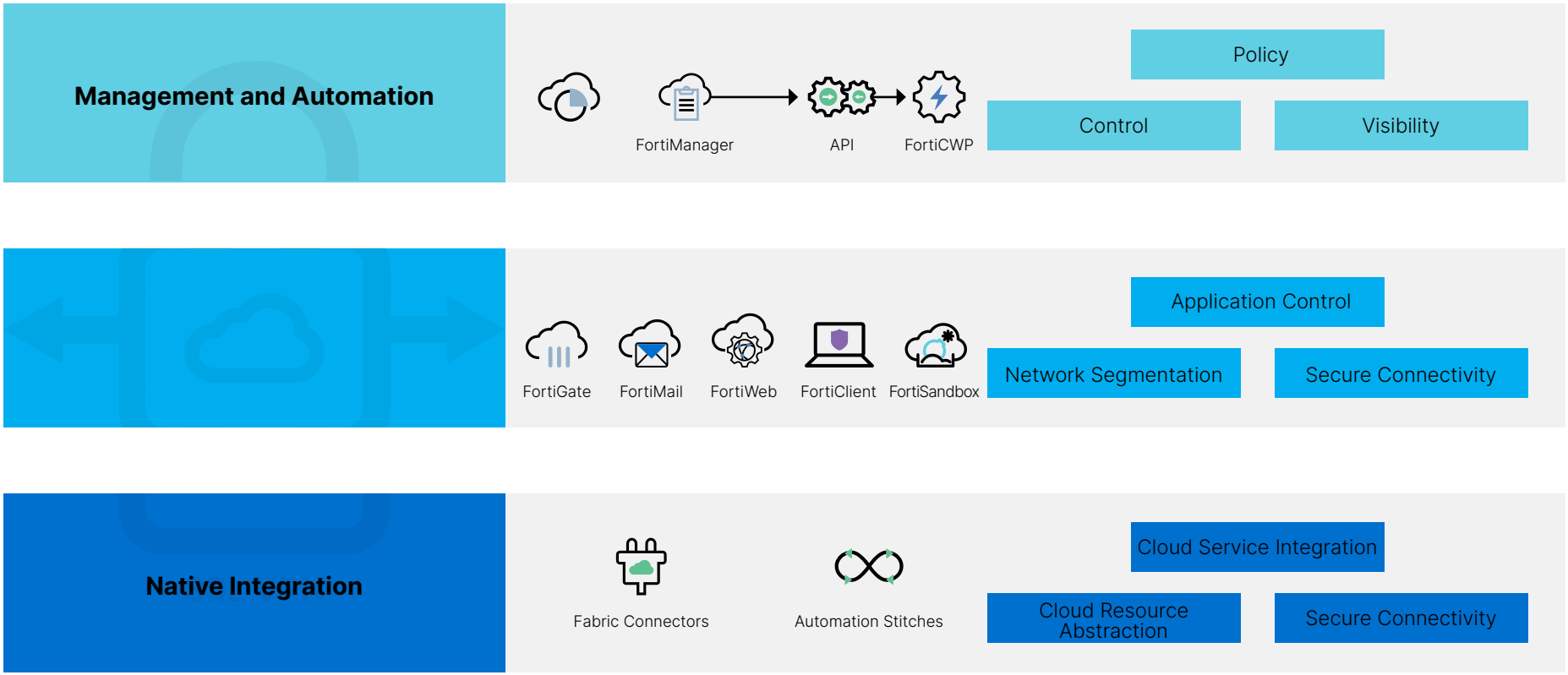


Figure 2: Fortinet offers a comprehensive cloud security strategy and targeted, integrated solutions that deliver management and automation, broad protection, and native integration.

3. Web application and API protection

Many companies fail to adequately secure their cloud environments because they do not understand the shared responsibility model. Cloud providers are responsible for protecting their infrastructure—including hardware and software components underlying their client services—and they generally do a good job of keeping these systems safe. However, cloud customers are fully responsible for protecting the applications they deploy and the data they store in the cloud. Indeed, the disconnect will grow in coming years: By 2023, 99% of cloud failures will result from customers failing to effectively uphold their end of the joint protection bargain.[5]

Unlike on-premises applications, which can be protected by controlling access to specific IP addresses, application traffic on the web (and all cloud-based traffic now is on the web) has no such security "choke points." In the cloud, threat detection needs to shift from the port through which the traffic flows to the application content and context of the traffic itself.

To provide this deeper level of insight requires ongoing granular adjustments to web application security policies. Because this is not a sustainable manual task—certainly not at scale—security architects need to use an artificial intelligence (AI)-driven approach with **FortiWeb**. In addition to the signature-pattern matching techniques that are typical of many WAFs,FortiWeb uses dual-layer machine-learning (ML) engines to protect web applications against zero-day threats. The ML enabled capabilities enable the solution to detect anomalies in user or application behavior and to protect against evolving botnets in a much more scalable and accurate manner.

In addition to the above, FortiWeb effectively protects web applications from the Open Web Application Security Project (OWASP) Top-10 threats, as well as from known and unknown attacks originating from vulnerability exploits, bots, and malware.

As everything becomes web-connected—from applications to middleware to mobile app back ends—organizations are placing increasing importance on threat protection at the web layer. Yet, their approaches vary in the way they choose to implement protection. Some organizations need a VM to perform security for multiple applications, while others opt for a container approach—attaching a web AppSec (application security) container to each application as a microservice. Still, others prefer a Software-as-a-Service (SaaS) solution to address their entire set of web application security needs without needing to manage the underlying infrastructure. In this case, security architects have deployment flexibility, as FortiWeb is available in a variety of form factors to accommodate all of these operational requirements.

4. Automation of security information

Although DevOps is an IT function, studies show there are significant skill-development gaps when it comes to security. For example, only 42% of developers have been taught to code securely, and 57% of operations staff do not follow security best practices.[6] To compensate for the lack of security skills on DevOps teams and to avoid the need to recruit DevOps-specific security administrators, security architects should seek ways to help DevOps automate its security functions as much as possible.

In the cloud, the focus of threat detection needs to shift from the network context to the application context.

The Fortinet Security Fabric helps facilitate this automation through plugins (called Fabric Connectors) that provide visibility of objects from cloud platforms. This makes it easier for DevOps and security teams to keep pace with application changes without necessitating updates to the security policies every time application attributes change.

In addition to Fabric Connectors, security teams can leverage APIs to the FortiOS operating system that allow for the automation of security operations. They can also download FortiOS configuration scripts through automation frameworks such as Terraform and Ansible.

Terraform is one of the most popular platforms for IT life-cycle automation, and with new Terraform FortiOS Provider Modules, Terraform automation now includes any FortiOS-related operations on both physical and virtual FortiGate devices. As a result, developers can integrate FortiGate Terraform configurations alongside other application elements to quickly spin up portable secure application stacks.

Red Hat Ansible automates the configuration of FortiGate VM. As Ansible modules for FortiOS are available on GitHub, developers can leverage existing skills to complete their FortiGate configuration tasks entirely within the Ansible Tower environment. This can deliver significant savings in developer training.

Another automation resource for developers is the Fortinet Developer Network (FNDN). It offers documentation and tutorials that explain and demonstrate how to leverage FortiOS RESTful APIs to directly automate Fortinet functionality.

70%

Security architects are challenged to maintain advanced threat protection with limited security skills on staff.[7] Native integration between FortiGate and the cloud infrastructure eases this burden.

Conclusion: Adding Fortinet Security to Cloud-native Tools Is Essential and Attainable

The security tools that come standard on public cloud services are inadequate when it comes to protecting a dynamic, multi-cloud environment. Misconfigurations are inevitable, and the resulting security gaps can inflict damage on an entire organization. While these risks may not be fully visible and felt in the early stages of software development, security architects should not wait until they are.

By augmenting cloud-native security with Fortinet solutions, security architects can close cloud security gaps while alleviating security management burdens. The broad range of advanced security technologies, seamlessly integrated functionality, and AI-driven capabilities of the Fortinet Security Fabric complement and strengthen enterprise security strategies.

[1] "The Security Architect and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, June 29, 2019.

[2] "2019 State of DevOps Security Report," Fortinet, May 10, 2019.

[3] Phil Muncaster, "Breached Records Fall 25% as Cloud Misconfigurations Soar," Infosecurity, April 6, 2018.

[4] Ibid.

[5] "Key Principles and Strategies for Securing the Enterprise Cloud," Fortinet, December 3, 2018.

[6] Daniel Newman, "5 Reasons DevOps And Security Need To Work Together," Forbes, September 30, 2018.

[7] Ian Barker, "Most organizations are not fully embracing DevOps," BetaNews, June 14, 2018.

FORTINET

www.fortinet.com

May 2, 2021 8:28 AM

eb-securing-the-cloud-with-fortinet-522021

430753-A-0-EN