WHITE PAPER

Extend Security Services Across Endpoints, Networks, and the Cloud

User-based Licensing Simplifies Security Implementation

Executive Summary

The move to remote work changed how companies do business almost overnight. And even as organizations bring employees back to the office, many plan to maintain a remote or hybrid work model. This accelerated adoption toward hybrid and remote workforces has resulted in a proliferation of devices and locations, further expanding the digital attack surface as more applications, devices, data, and users are exposed. Understanding and controlling data traffic across these divergent environments is a key to managing security.

Securing hybrid and multi-cloud environments requires strategies like establishing zero-trust access (ZTA), strictly enforcing identity and access management (IAM) policies, and protecting applications and platforms. But many organizations have struggled to manage a complex array of inflexible siloed offerings with different licensing models. FortiTrust offers a flexible set of security services that utilize cloud and network-based resources that are licensed per user, which helps simplify implementation and management and improve visibility.

Only 13% of organizations have strong adherence to zero-trust principles and 54% have been working on zero trust for less than two years. Although 74% are very familiar with the concepts, 76% expect zero trust to be complex to implement.[1]

The Driving Factors Influencing Security

In the last year, organizations have come to rely more on hybrid and multi-cloud environments to help support their evolving digital transformation requirements. According to a recent report from Fortinet, 76% of organizations surveyed reported using at least two cloud providers.[2] The result is that applications can reside anywhere—from on-campus to branch to data center to cloud. And now that the era of work from anywhere is upon us, organizations have had to rethink how they secure network edges both on-premises and in the cloud.

The shift almost overnight to remote work acted as a wake-up call that one single security policy had to be delivered everywhere. Regardless of the location, the device, and the network, users need to be granted access to their application environment. This access needs to be granted through a context-sensitive mechanism particularly to distributed architectures such as hybrid and multi-cloud. Multi-cloud architectures and ZTA strategies shouldn't be developed separately.

In today's networks, a user or an application could be anywhere, which changes the networking paradigm. The old paradigm focused on location. Where is the user connecting from? Where is the application located? In what server, in which data center?

Making Work From Anywhere a Reality

Work from anywhere requires connectivity plus security. Applications may be located in the data center, private clouds, or public clouds, so user identification, authentication, authorization, and access permissions have become critical.

To implement work from anywhere, more organizations are looking more closely at ZTA solutions. The basic premise of ZTA is that never assume anything can be trusted simply because it is "inside the network perimeter." ZTA limits user and device access to networks, which provides identity assurance. Zero-trust network access (ZTNA) builds on ZTA by limiting user and device access to the applications that users need to do their jobs. Combining these two approaches strengthens the company's security posture.

Looking at work from anywhere from an outbound perspective, secure access service edge (SASE) provides secure access for employees, customers, and partners across operating environments by securing any user, anywhere on the network. And then multi-factor authentication (MFA) provides the identity verification to control access. Additionally, a cloud access security broker (CASB) that sits between cloud service users (remote workers) and cloud applications can be used to monitor activity and enforce security policies.

Coping With Security Licensing Models

Implementing security in a complex, distributed hybrid environment that supports work from anywhere is a daunting task. It's complicated because it takes a multitude of solutions to prevent attacks. And then those myriad solutions often have different licensing models. For example, to protect endpoints, many endpoint detection and response (EDR) solutions require device-based licenses. And firewalls and other network solutions like software-defined wide-area networking (SD-WAN) require hardware-based licenses. And then to cover applications security, you may need to get user-based licenses for email security.

Pulling it all together holistically can be complicated and expensive. Many CISOs struggle to accurately understand and forecast their spending for an individual security use case like ZTNA because of this mixture of device-based, appliance-based, and cloud-based fees. Being able to price security capabilities easily is almost impossible because many current licensing models require custom quotes and challenging comparisons. Additionally, if it's necessary to add or reduce security capabilities as budget and needs change, it gets complicated because of the mixed structures and end dates.

CISOs need straightforward flexibility for their security capabilities with an easy path to upgrade or enhance their security services. To make adding security capabilities easier, Fortinet has added a new solution called FortiTrust to Fortinet's existing FortiCare and FortiGuard subscription services.

Add Security Capabilities With User-based Pricing

Because of the increase in cloud-based applications and services, there has been a move toward user-based licensing models. CISOs need straightforward flexibility for their security capabilities with an easy path to upgrade or enhance their security services. To make adding security capabilities easier, Fortinet has added a new solution called FortiTrust to Fortinet's existing FortiCare and FortiGuard subscription services.

FortiCare offers advanced support and proactive care for Fortinet products, and FortiGuard offers artificial intelligence (AI)-enabled security capabilities that assess risks and adjust protection across the Fortinet Security Fabric. And now the new FortiTrust service makes it easier to add security services with user-based licensing for specific use cases, such as ZTNA or MFA.

In much the same way that the Fortinet Security Fabric covers the products into a single, integrated blanket, FortiTrust does the same thing for services. It weaves the security products you need for a particular use case such as ZTNA into a single license.

FortiTrust offers a comprehensive, flexible set of security services that use cloud and network-based resources. Although delivering the use case may involve device agents, hardware appliances, and cloud services, the use case is implemented through the single license.

FortiTrust simplifies the purchase and ongoing management of end-user security. Getting started is simple. You pick the service:

- **FortiTrust Access for ZTNA** to extend secure access controls to applications for any user, whether they are on or off the network
- **FortiTrust Identity for cloud-based MFA,** which provides the identify verification required to control application access

The licensing costs are then based on the number of users you want to protect. The FortiTrust subscription service also includes FortiCare support. FortiTrust's initial services portfolio includes FortiTrust Access and FortiTrust Identity. Additional service options for SASE, CASB, and endpoint protection (EPP) are planned to be released later.

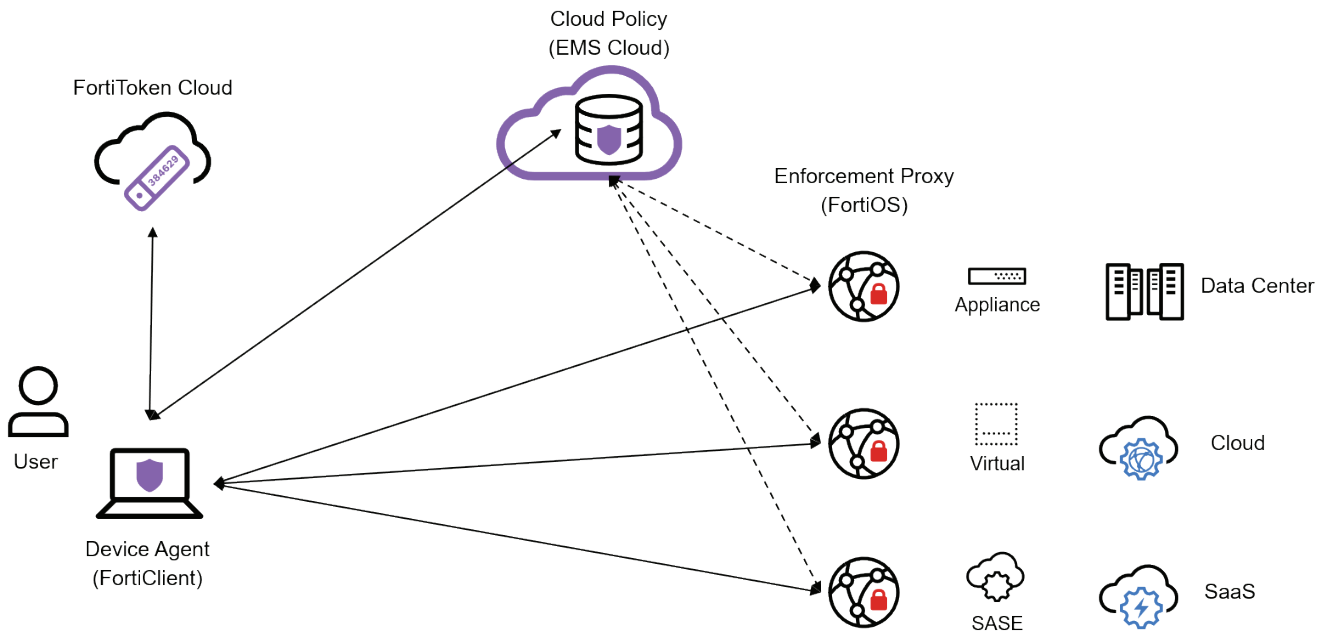

Figure 1: FortiTrust Access Service.

Providing Security Everywhere

FortiTrust expands on the Fortinet Security Fabric's ability to protect people, devices, applications, and data everywhere. It offers a unified service to secure the organization across any network, endpoint, or cloud with simplified consumption and one licensing model for all form factors. The expansion of subscription services to include FortiTrust along with FortiCare and FortiGuard gives organizations the comprehensive and flexible protection they need to secure today's hybrid and highly distributed networks.

[1] John Grady, "ESG Master Survey Results: The State of Zero Trust Security Strategies," ESG, May 12, 2021.

[2] "2021 Cloud Security Report," Fortinet, 2021.

August 13, 2021 8:08 PM

1175664-0-0-EN