

SOLUTION BRIEF

Making Cybersecurity Mesh Architectures a Reality With the Fortinet Security Fabric

Executive Summary

As networks become more complex and distributed, detecting and responding to threats has become increasingly difficult. It has also led to security sprawl that complicates management, fragments visibility, and limits the ability of organizations to respond effectively to threats. Case in point, today's enterprises have deployed an average of 45¹ security solutions across their network, most of which operate in a silo, making any sort of centralized management nearly impossible. Compounding this issue is that detecting and responding to a cyber incident requires coordination across many of these isolated tools, leading to complex workarounds that must be constantly managed and then reconfigured every time a device is upgraded. These and similar challenges of complexity and integration have made a cybersecurity mesh architecture essential for today's organizations.

The Fortinet Security Fabric delivers the broad, integrated, and automated capabilities needed to make a cybersecurity mesh architecture a reality. The industry's highest-performing cybersecurity mesh platform reduces complexity, streamlines operations, and increases threat detection and response capabilities to empower organizations to accelerate secured digital acceleration outcomes. And because more than 450 third-party technology partners support it, the Fortinet Security Fabric gives organizations the flexibility they need to implement a wide range of solutions that fit their individual needs now as well as in the future.

Complexity is a Bottleneck for Digital Acceleration

In today's world of digital acceleration, external forcing functions such as COVID-19 and an increasingly competitive digital marketplace are driving the rapid adoption of new technologies across networks, including migration to the cloud. But far too often, organizations move first and then ask themselves later how best to secure and manage these environments—with "accidental multi-clouds" being one all too frequent example.

Then there are those organizations whose internal processes, such as isolated lines of business, lead to silos of what solutions are chosen and how they are implemented—leaving security teams to deal with the mash-ups and complexities of the resulting patchwork deployments. This also creates a perfect storm for attackers and threats that exploit the resulting silos, complexities, and visibility gaps. And all of this is even further exacerbated by the resource and cybersecurity skills gaps that continue to plague many organizations.

To solve these challenges, organizations must move beyond their outdated "best-of-breed" approaches to cybersecurity that leave standalone solutions isolated across their network. Instead, they need to adopt a cybersecurity mesh architecture (CSMA) as the foundational building block to their digital acceleration initiatives. Doing so will help unify their fragmented infrastructure and deployments, creating cohesion and enabling collaboration and automation across the various products and solutions deployed across their environment.

Gartner® believes that "by 2024, organizations adopting a cybersecurity mesh architecture to integrate security tools to work as a collaborative ecosystem will reduce the financial impact of individual security incidents by an average of 90%."²

Keys to an Effective CSMA

An effective CSMA is built on the principle that organizations should adopt and deploy solutions that not only fit their needs but also work within and across an integrated ecosystem to share intelligence, automate and coordinate response, and simplify operations. Adopting a CSMA helps fundamentally shift an organization from its legacy “best-of-breed” approach built around isolated technologies to a new “best-of-breed AND integrated” cybersecurity strategy.

A broad, integrated, and automated platform, such as the Fortinet Security Fabric, is vital to seamlessly and successfully implement a CSMA. It provides centralized management and visibility, enables end-to-end automation, adapts to changing network environments, and supports and interoperates with a vast ecosystem of network environments and third-party solutions.

The Fortinet Security Fabric Delivers CSMA Strategy

For over a decade, Fortinet has spearheaded the doctrine that a broad, integrated, and automated security platform is essential for reducing complexity and increasing overall security effectiveness. To achieve this, Fortinet has integrated its CSMA strategy across its broad solutions portfolio, making the Fortinet Security Fabric the industry’s highest-performing cybersecurity mesh platform.

With the Fortinet Security Fabric in place, organizations can leverage a comprehensive portfolio of interconnected solutions to solve their cybersecurity challenges across four key solution pillars:

- Security-Driven Networking that offers the industry’s only converged networking and security solutions
- Adaptive Cloud Security to protect the entire application life cycle on any cloud
- Zero Trust Access to know and control all users and devices
- AI-driven Security Operations for the fastest security response

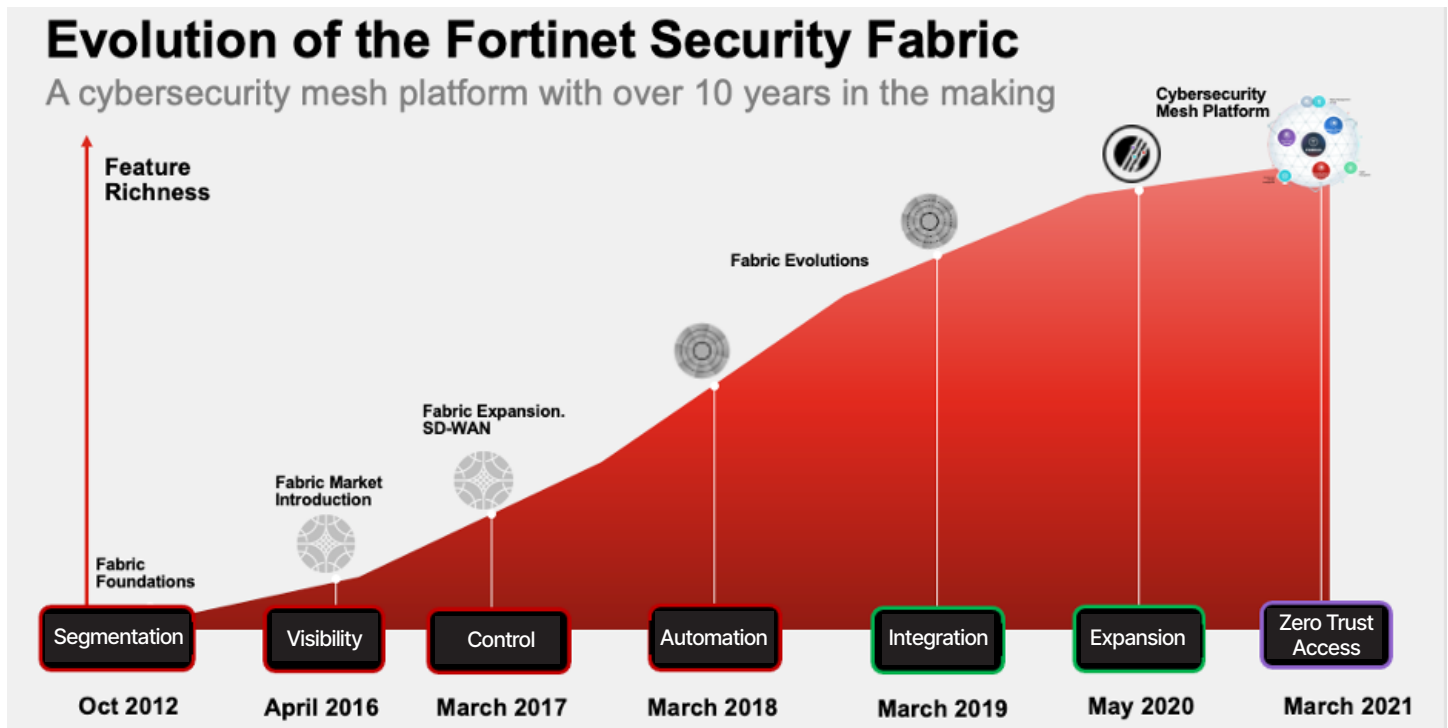
Fortinet also believes that a true cybersecurity mesh platform should break down technology and vendor silos by enabling and supporting a broad open ecosystem of technology partners. And to deliver on this vision, Fortinet currently integrates and interoperates with over 450 third-party Fabric-Ready technology partners as part of the Fortinet Security Fabric.

An open ecosystem empowers organizations with deployment flexibility while consolidating and converging their operations, visibility, and security across their distributed hybrid networks. It also preserves its existing technology and solutions investments while implementing a fully integrated and automated Security Fabric experience.

Organizations looking to immediately reap the benefits of leveraging a CSMA today can do so through the Fortinet Security Fabric. Such benefits include the ability to:

- Gain deep visibility across all their network edges
- Centrally manage and deploy solutions with consistent policies and configurations
- Leverage intelligence collected from their own security fabric, as well as anonymized threat data from global Fortinet Security Fabric customers and third-party integrations to get the best real-time protection for known and never-seen-before attacks
- Automate actionable responses across their hybrid deployment





Count on a Proven and Reliable Architecture

William Shakespeare once wrote, “A rose by any other name would smell as sweet.” So too is a broad, integrated, and automated cybersecurity platform. Whether one wants to call it a “cybersecurity mesh architecture,” a “cybersecurity platform,” or “Fortinet Security Fabric,” the important thing is that organizations embrace and adopt it as part of their digital acceleration initiatives. Its broad, integrated, and automated capabilities reduce complexity, simplify operations, and improve security effectiveness regardless of where their digital journey takes them. With a Fortinet Security Fabric architecture in place, organizations gain the confidence and benefits of implementing a broad mesh platform with a proven track record of over 10 years of worldwide deployments.

¹ [“Cost of a Data Breach Report 2021,” IBM, 2021.](#)

² [“Top Strategic Technology Trends for 2022: Cybersecurity Mesh,” Felix Gaehtgens, James Hoover, Henrique Teixeira, Claudio Neiva, Michael Kelley, Mary Ruddy, Patrick Hevesi, 18 October 2021”](#)

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.



www.fortinet.com

Copyright © 2021 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.