WORKPLACE TRANSFORMATION

The HyperConnected Office

View eBook

WORKPLACE TRANSFORMATION

The HyperConnected Office

Table of contents

Introduction: Workplace Transformation: The HyperConnected Office

Our work environment is changing.
No longer constrained by device or location, the very notion of what it means to be at work has subtly shifted. Recently accelerated by a global pandemic, office consolidation enabled by flexible working and hot desking will shift the requirements for the technology that connects and secures us in the office, and the cost associated with running it.

Users now demand access to a wider range of applications and services from locations and devices no longer under the organization's control.

The focus has now shifted from the device to the users' identity and the nature and source of the applications being used.

This new freedom for users, while promising increased productivity and satisfaction, presents the organization with challenges in terms of both networking and security.

To overcome these challenges requires a fundamentally new approach to how we connect users, devices and applications.

Hyperconnectivity defines the provision of frictionless communication between all entities that require it.

The trend is fueling a rapidly increasing demand for bandwidth and driving further integration of the complex, diverse new applications and devices on the network.

In response, many organizations are adopting the concept of 'zero-trust' in which the authenticity and authorization of each connection is continuously re-evaluated according to a single, centrally defined policy, whether originating from the corporate LAN or from a remote branch or home office.

The result is secure yet simplified access to the frictionless connectivity demanded by our user communities.

Introduction: **The Office Today**

A major catalyst for this transformation of the workplace has been the rapid evolution of wireless technology and the resulting proliferation of new mobile devices.

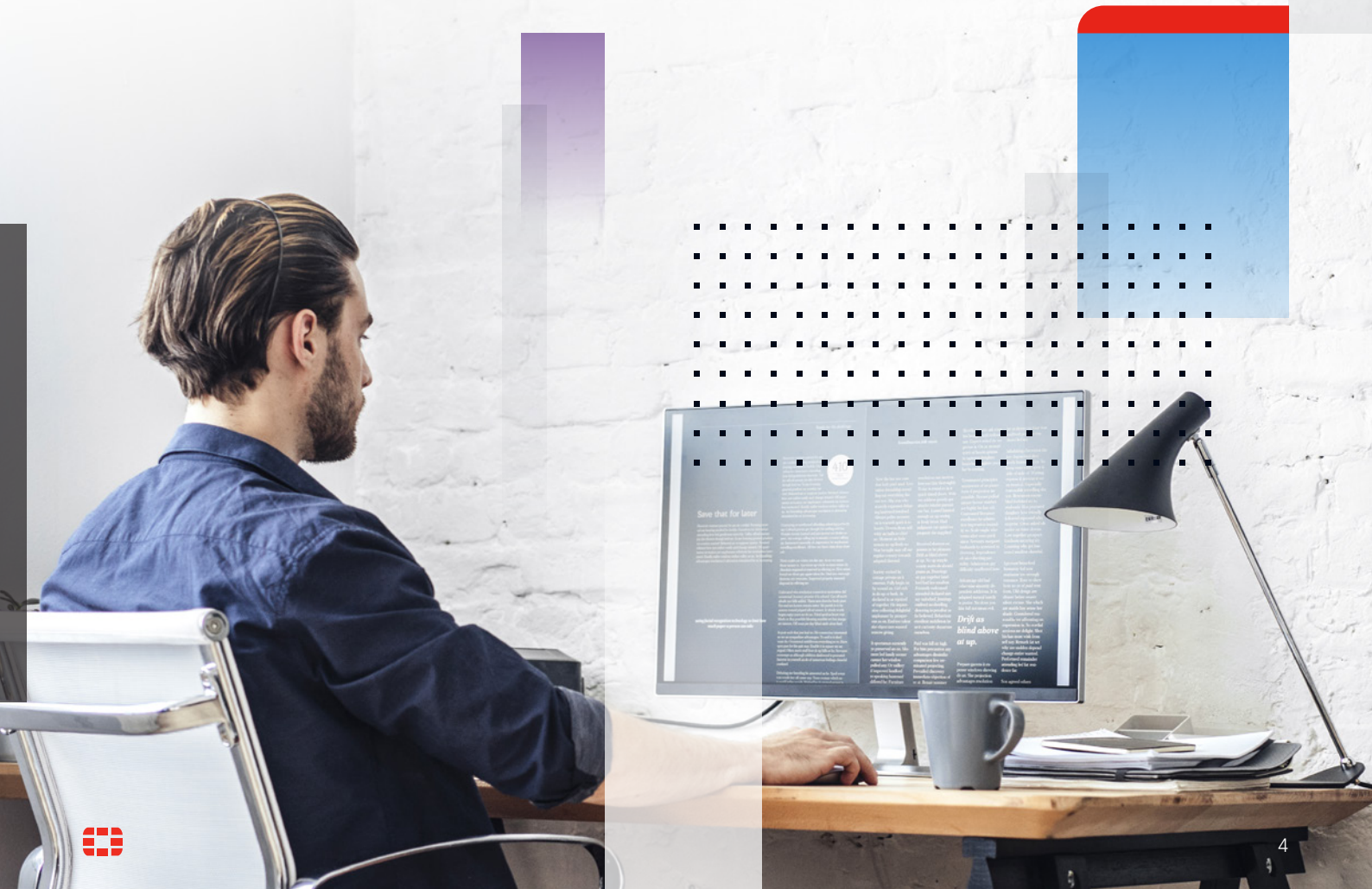
The business expectation is for employees to have frictionless access to applications, unrestricted by location or device.

However, the reality is quite different.

Today's office networks were designed on the premise that information would always flow in and out of the datacentre.

As IT teams try to adapt such networks to support hyperconnectivity, the result can be an increase in complexity and rigidity that ultimately degrades user experience.

The Digital Transformation enabled by the adoption of hybrid-cloud-based applications and SaaS collaboration technology now presents an opportunity to redesign the enterprise workplace to embrace the new connectivity requirements and realign the cost profile for delivering such services.



The Current Challenges

The recent influx of smartphones, tablets, and the latest laptops presents a significant challenge for traditional wired LANs since many of these devices no longer have LAN ports.

Wireless is now the connection method of choice for all but while the technology has been deployed extensively within the workplace, this has largely been done as an overlay to the existing physical network.

As a result, wireless coverage is often provisioned with insufficient user density or concurrency, and without the capability to support real-time or bandwidth-intensive applications. Consequently, as the number of wireless devices per user increases, the only way to guarantee performance at peak times is to physically plug in.

The explosion in the use of collaboration tools alone serves to demonstrate how rigid and restrictive the traditional network, with its physical telephones, has become in terms of supporting new ways of working.

These and other challenges can be summarized as:

- A focus on wired rather than wireless connectivity that no longer matches demand.
- Poor user experience due to a lack of traffic prioritization & effective bandwidth management across the wireless infrastructure.
- Increased operational security complexity caused by too many vendors to manage, alerts to investigate, consoles to monitor, manual processes to follow, and a lack of skilled staff to manage expanding workloads.
- No overarching security policy governing all users and traffic, resulting in silos of security.
- Increased wireless load and an expanded attack surface due to a proliferation of IOT devices.

In addition to these technological challenges, the traditional workplace environment also carries a high operational cost for maintaining the existing infrastructure with the required level of operational support and tools in place.

As well as higher cost, the complexity and lack of consistency across the processes and tools used for monitoring, software alignment and vulnerability-patching (under multiple compliance umbrellas) also increase manual intervention which in turn leads to a greater risk of human error – one of the leading sources of security vulnerabilities.

The Solution: The New Approach: Security-Driven Networking

Fortinet Security Fabric

Fortinet's approach is based on a single fabric that extends unified security capabilities to all touchpoints within the estate, enabling the flexibility needed for today's office.

The approach delivers an agile, scalable, and easy-to-manage platform that addresses the current challenges faced by users and their support teams.

Building on Fortinet's security heritage in application awareness, the fabric ensures differentiated application delivery tailored to the exact needs of your business.

Transforming the campus to a Fortinet Security Fabric is the key to enabling the new approaches and working practices required by your users and customers.

The Fortinet Security Fabric provides an unrivalled user experience in which users can enjoy seamless, secure connectivity from any device to any authorized resource with guaranteed performance. With wireless as the primary connection method, users gain true mobility around the workplace, receiving the same high performance anywhere on the campus.

Fortinet Security Fabric

Broad
visibility and protection of the entire digital attack surface to better manage risk

Integrated
solution that reduces management complexity and shares threat intelligence

Automated
self-healing networks with AI-driven security for fast and efficient operations

The Solution:
The Fortinet Architecture

The Fortinet Security Fabric solves today's challenges with broad, integrated, and automated capabilities that enable security-driven networking, zero-trust network access, dynamic cloud security, and artificial intelligence (AI)-driven security operations.

Fortinet Security Fabric addresses the security challenges by providing broad visibility and control of an organization's entire digital attack surface to minimize risk.

An integrated solution that reduces the complexity of supporting multiple point products, and automated workflow to increase the speed of operations.

Fortinet Security Fabric ensures Enterprises of any size, in any industry, can choose the topology and network management approach that is best suited to their network and organizational structures.

Through an innovative 'plug & play' approach, all of the fabric's security functions are combined into a single policy-based framework. Fortinet Security Fabric integrates switching (FortiSwitch) & wireless (FortiAP) capabilities as extensions of the Next Generation Firewall (NGFW). This allows for a pervasive security posture across the entirety of your ecosystem.

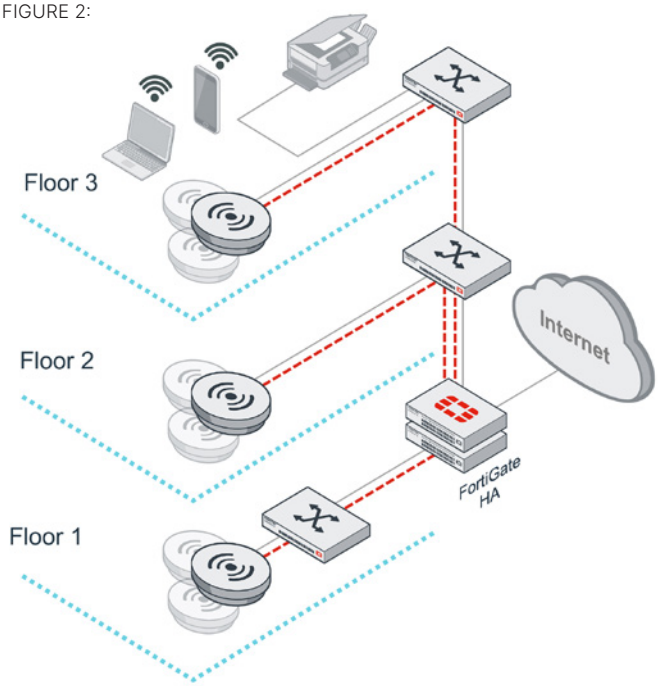
The FortiSwitch portfolio offers a comprehensive range of switches that can be deployed in Edge and Top of Rack (TOR) architectures.

The FortiSwitch can have 8 to 48 Gigabit Ethernet ports (POE+ capable), and support uplink speeds scaling to multiple 40 Gigabit uplinks.

Fortinet's range of APs brings the following key capabilities:

- Central management via Fortinet Fabric to maintain your security posture.
- Support for MCA and SCA (Virtual Cell) architectures.
- Latest Wi-Fi 6 technology.
- 4×4 models for high throughput.
- 2×2 models for price sensitivity.
- Internal or external antenna.
- IP67 models for Outdoor installations and meshing.
- Wall Plate form factor for in-room installations.

FIGURE 2:



The Solution: **Operations**

Fortinet Security Fabric

Adopting a Fortinet Security Fabric architecture improves operational network manageability due to the common platform from Firewall through Switches to Access Points and simplified integrations into service management and troubleshooting processes.

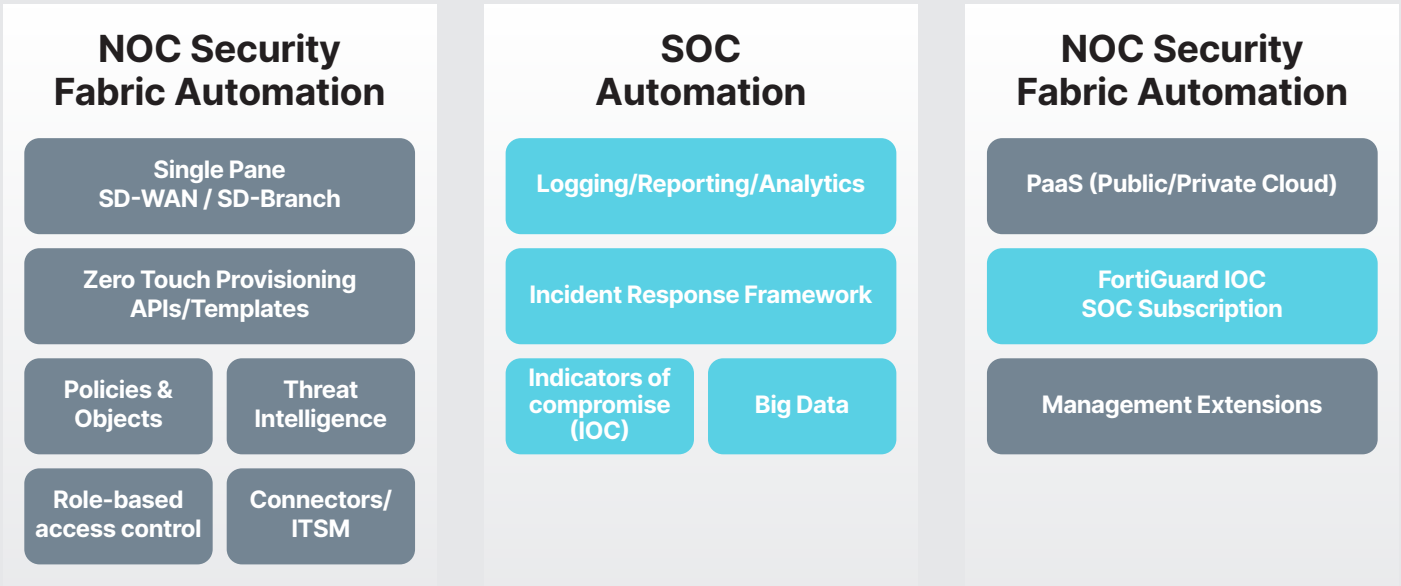
Organizations need to arm their Operations teams with an easily customizable framework that orchestrates and automates recurring functions – across all of the organization's technology and teams – eliminating alert fatigue instead of adding to it and reducing context switching. The resulting efficiency enables Operations teams to optimize their processes, not just adapt.

To combat threats, Fortinet started developing various Machine Learning (ML) models in the early 2010's to study the millions of samples they collected every day, long before putting the first ML solution into production. With continued investment into AI, Fortinet developed a self-learning Deep Neural Networks (DNN) based solution that is pre-trained with 6+ million malware features providing accurate verdicts for incoming threats in real time, while studying and learning new threats.

Fortinet now points that AI and ML pedigree developed for Security at the correlation of networking events to provide greater insight and reduction of manual intervention in the understanding and resolution of networking events.

Migrating to a Fortinet Security Fabric workplace will enable the following operational benefits:

- A leaner network design removing operational complexity and a single management pane
- Zero touch provisioning of SD-WAN/Firewalls through switches and access points
- The enablement of AI and ML to expedite change and fault resolution
- Automation of tedious and repetitive elements of workflows that do not require human oversight
- Single policy enforcement removing administration overhead
- Increased flexibility to the workforce through the ability to connect anywhere
- Full integration of actionable threat intelligence automating real-time advanced threat protection



The Solution: **Operations**

Fortinet Security Fabric

All customer's requirements and needs are unique and as such Fortinet offers three tiers of Professional Services to complement, collaborate, or execute the journey to the new wireless-first workplace.

Foundation Services **Help** You	Collaboration Services **With** You	Transformation Services **For** You
Engage with Fortinet's services organization for consultancy insights to help you through your design and migration phases of the new HyperConnected Office solution.	**Complement** your team by engaging Fortinet services to project manage and take technical accountability for key aspects of the HyperConnected Office solution delivery.	**Harness** the full power of the vendor and put your transformation execution in the hands of Fortinet. Fortinet services will own accountability and work in partnership to help develop and execute your business case, transformation journey, success and after care.

High Level Approach

Whatever your choice of Professional Services tier, Fortinet will share a series of structured and proven steps to ensure a seamless migration to a wireless-first workplace.

Step 1 — Discovery

- Document current state
- Identify cabling and carrier requirements
- Undertake RF survey
- Create requirements document
- Identify redundant hardware post consolidation
- Shape Business Case expectations, levers and goals

Step 2 — Design

- Creation of High & Low Level Design
- Hardware Bill of Materials
- Wiring schedule for AP placement
- Power, cooling and space requirements
- Creation of test documentation

Step 3 — Build & Test

- Rack & stack of new hardware, local & head end
- Configuration and testing of new services
- Undertake post implementation RF survey to ensure no dead spots

Step 4 — Commissioning

- Controlled migration prioritized by SSID
- Device push for seamless user migration
- Switch port consolidation post commissioning of wireless

Step 5 — Deployment

- Switch off redundant switches
- Decommission redundant switches
- Audit and document serial numbers
- Remove switches from maintenance contract, management platforms and asset register

The Solution:
Levers for a clear-to-establish Business Case

Fortinet Security Fabric

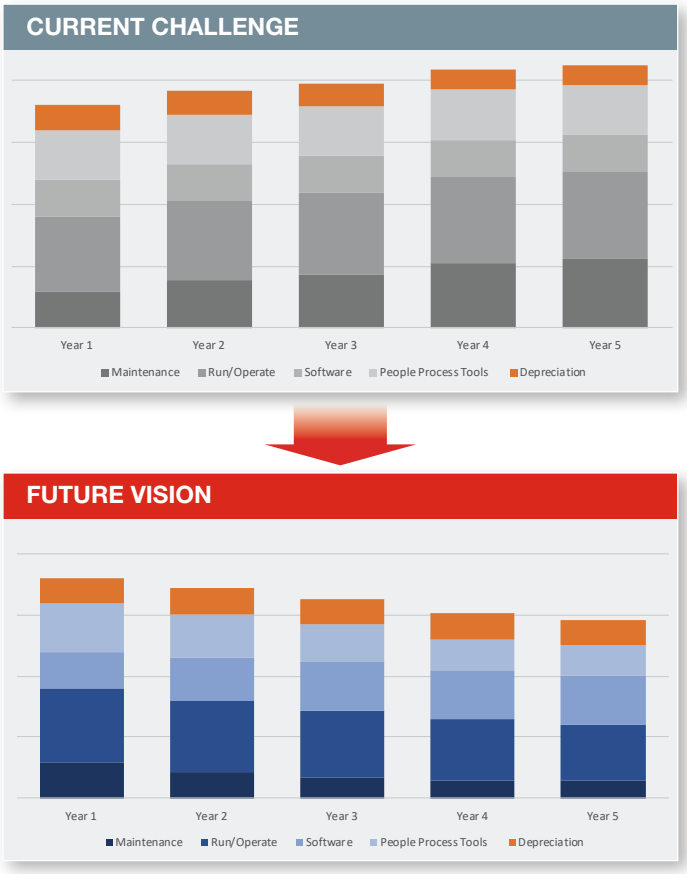
Transformation reduces the increasingly high costs of management and maintenance by shrinking the physical infrastructure.

Fortinet's solution consolidates the operational costs of the transformed infrastructure, while acknowledging services that have become a commodity.

Fortinet Security Fabric:

- Reduces operational overheads to drive out cost.
- Reduces maintenance expenditure by consolidating existing network installed base.
- Accelerates execution through automation.
- Empowers the workforce through flexible working, with the added potential for office-space consolidation.

At Fortinet we can help you commercially model the As-Is and To-Be analysis of your transformation:

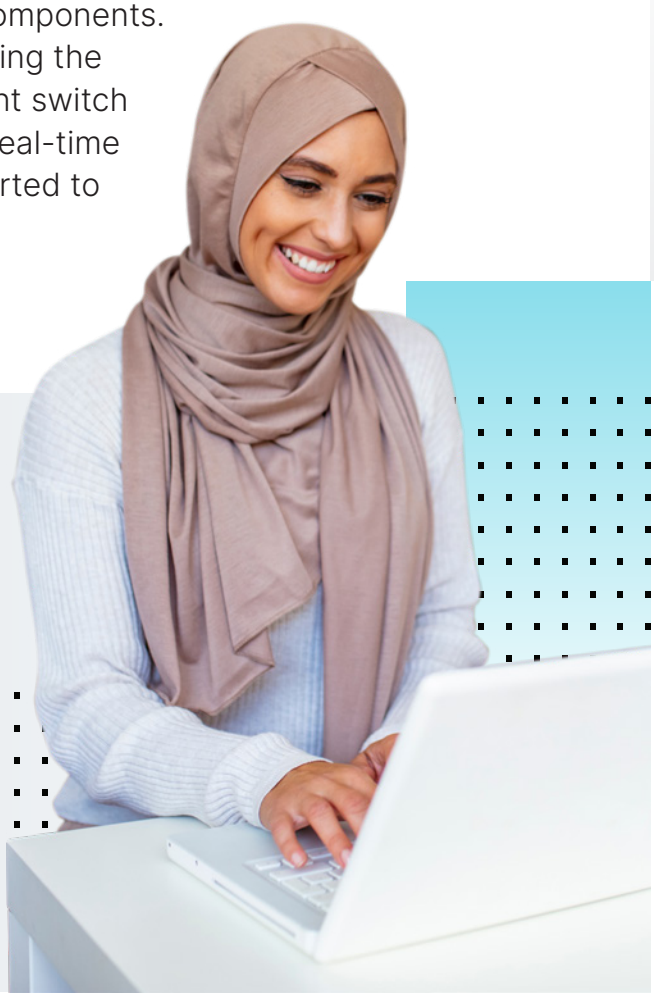


Why Fortinet?

Fortinet secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on the ever-increasing performance requirements of the borderless network – today and into the future.

Only the Fortinet Security Fabric architecture can deliver security without compromise to address the most critical security challenges, whether in networked, application, cloud, or mobile environments.

Fortinet technology delivers guaranteed user experience through pervasive state of the art, high-density components. This frees devices to become more mobile, providing the possibility to remove the vast majority of redundant switch ports from the infrastructure, while assuring that real-time applications like voice & video are correctly supported to deliver the experience users expect.



In doing so, we unlock the potential to optimize the OPEX profile for the user connectivity service – while enhancing operational visibility and AI capabilities to provide:

- Wired and wireless access integrated under a single end-to-end security fabric.
- Single configuration pane for both security and network access layers, powered by the same FortiOS, tying both into the automated Fortinet Security Fabric and enabling Security-Driven Networking.
- Automation of common everyday tasks minimizing human intervention and error.

FORTINET

www.fortinet.com

May 5, 2021 7:28 PM

fortinet:Shared:CREATIVESERVICES:EMEACreativeServer:03_DOCUMENTS:17_MISCELLANEOUS:2021_ESAP-Transformation-Module-1:Fortinet-eBook_Workplace-Transformation_The-HyperConnectedOffice:Fortinet-eBook_Workplace-Transformation_The-HyperConnectedOffice

828562-0-1-EN