

FORTINET SMB SUMMIT

Expand with FortiSASE

Nov 28th 2024 | Nicosia, Cyprus

Konstantinos Diplas, IDEAL Technology Presales Security Engineer



Capitalize on your FortiGate investment to address new Security challenges

Solution for SMB



Agenda

1

Work from Anywhere:
How it is addressed today

2

FortiSASE:
Benefits for Customers



FORBES > INNOVATION > CONSUMER TECH

Work From Home Is The New Normal For Workers Around The World

Tim Bajarin Contributor @
I write about tech industry's impact on the PC and CE markets.

Apr 29, 2021, 02:37pm EDT



Work from home is here to stay GETTY

Source: Forbes |
Work From Home Is The New Normal For Workers
Around The World (forbes.com)

FOR SUBSCRIBERS
The Straits Times says
A new normal: Working from anywhere



PUBLISHED APR 30, 2022, 5:00 AM SGT

f w t ...

Source: The Straits Times | A new normal: Working from anywhere

Personal Banking > ... > Why Hybrid Working is Key in the New Normal?



STORIES & TIPS

Why Hybrid Working is Key in the New Normal?

Share

Why Hybrid Working is Key in the N Normal?

Source/ SCB
Why Hybrid Working is Key in the New Normal? (scb.co.th)

FORBES > LEADERSHIP > CAREERS

Remote Work Is Here To Stay And Will Increase Into 2023, Experts Say

Bryan Robinson, Ph.D. Contributor @

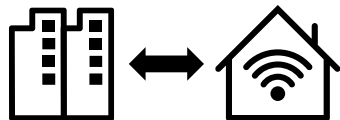
Feb 1, 2022, 06:24am EST



Experts predict a remote work force is a permanent fixture in the coming years. GETTY

Source: Forbes
Remote Work Is Here To Stay And Will Increase
Into 2023, Experts Say (forbes.com)

Accelerating Changes impact Security



Hybrid Workforce is the New Normal

“Remote/hybrid work is here to stay. Survey data shows that **80%** of workers continue to adopt hybrid workstyle

Gartner, Chaing IT practices for remote work-force , August 2022



Web is Top Attack Vector

“Web continues to be one of the top attack vector. 2022 Verizon Data Breach Report indicates **90%** of breaches use web applications.”

2022 Verizon Data Breach Report

TRENDS



Aging VPN Deployments

“VPN deployments must move away from implicit access to improve security posture.”

Gartner, Remote Access Options for Enterprise Endpoint – April 2022



Growing Shadow IT Presence

(use of web Apps unknown to IT)

“**91%** of organizations report that biggest surprises to cloud adoption are Lack of visibility and not enough having control .”

2022 Cloud Security Report; Cybersecurity Insiders

Work from Anywhere:

How is it addressed today?

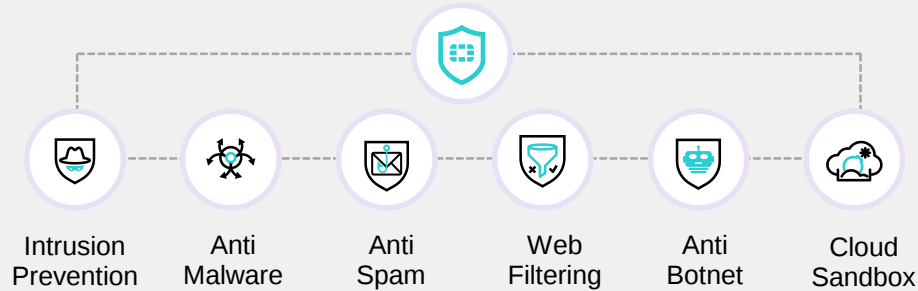


Work from Anywhere: Why is this no longer enough?

Most common Customer situation today

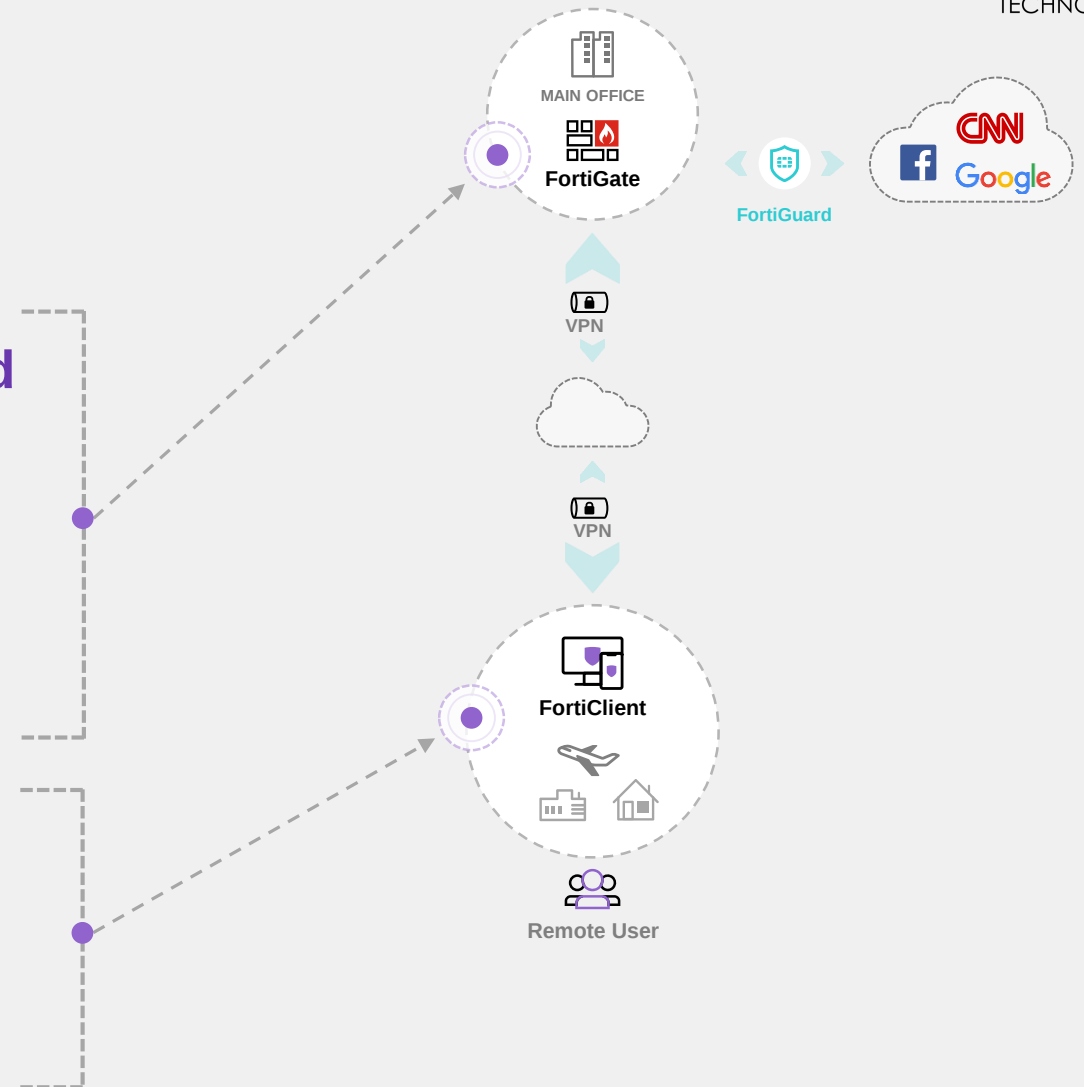


Office is protected with FortiGate + FortiGuard



Remote Users connect with FortiClient

- + Private **VPN** connection to the main Office
- + Secure **Internet Access** via **VPN** through main Office (protected by **FortiGate + FortiGuard**)



Work from Anywhere: Why is this no longer enough?

Most common Customer situation today

Secure Remote Access - Issues

Employees connect directly to the Internet

- + **Not protected anymore** by FortiGuard security services
Exposure to intrusions, malware, spam, malicious URLs...



Network
Intrusions



Spam



Botnets



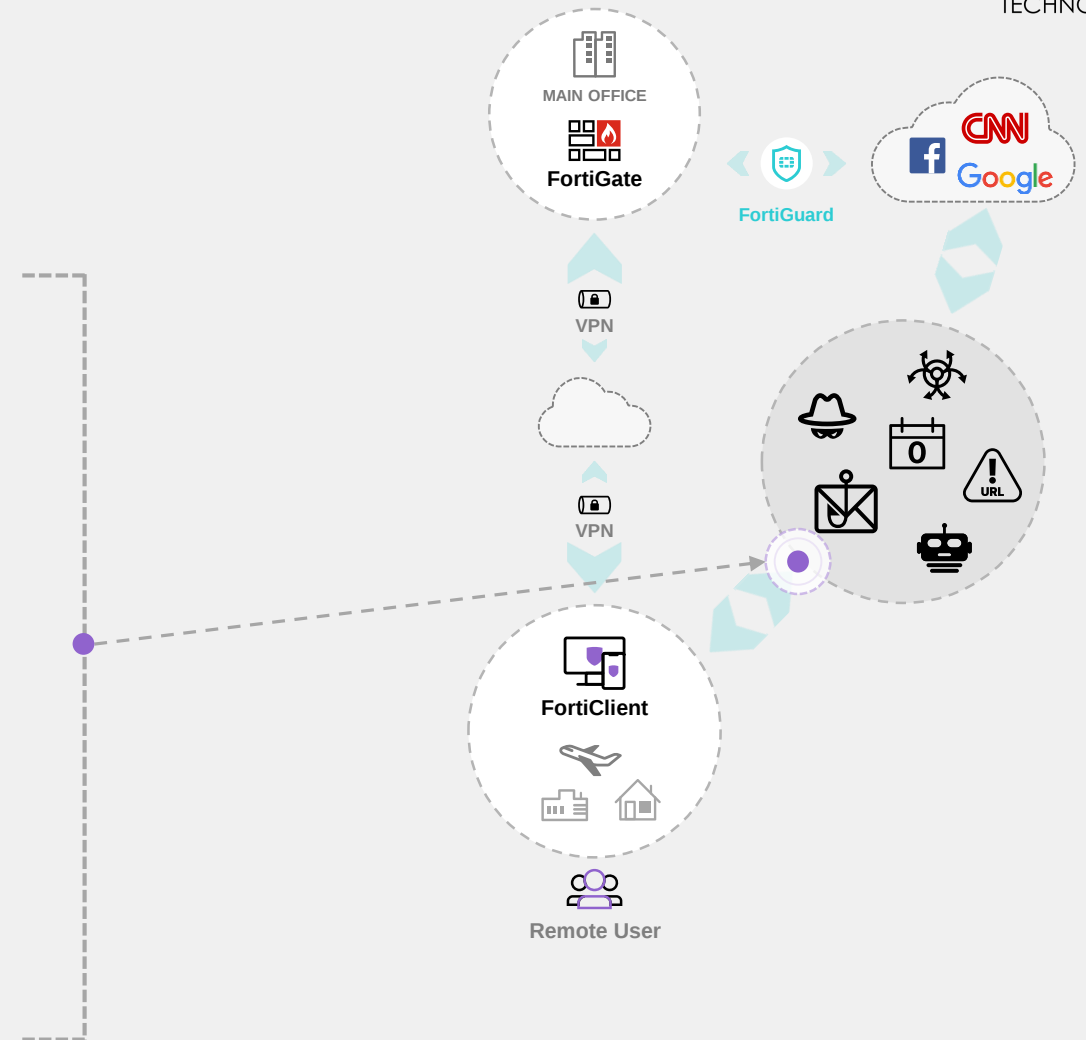
Malware



Malicious
Websites



Zero Day
Threats



Why is it Dangerous to connect Directly to the Internet?


Network
Intrusions



18.1 Million
NETWORK INTRUSION
ATTEMPTS
resisted per minute



22,876,649
MALWARE PROGRAMS
Neutralized Per Minute



Malware



Spam



36.4 Million
SPAM
Block Per Day

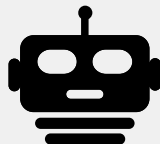
323,276
Malicious Website
ACCESSES



Blocked Per Minute



Malicious
Websites



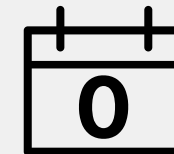
Botnets



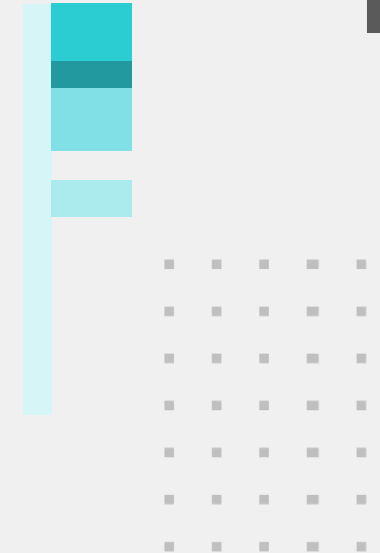
29.2 Million
Botnet C&C attempts
TWHARTED
PER MINUTE

1075 

ZERO DAY
THREATS DISCOVERED



Zero Day
Threats



Most common Customer situation today

Most common Customer situation today

- + **Unprotected connection to Corporate Apps** in the Cloud
- + Use of **Services unknown** to Corporate IT (**Shadow IT**), with risks of data leakage and security compliance issues

- + **Unprotected connection to Corporate Apps** in the Cloud
- + Use of **Services unknown** to Corporate IT (**Shadow IT**), with risks of data leakage and security compliance issues

- + Not possible to set special rules to access sensitive Corporate Apps

- + Not possible to set special rules to access sensitive Corporate Apps

- + **Direct access** to Internet is easier for End Users
- + **VPN might be slow** when connecting from very distant places
- + **No alternative solution** if VPN experiences availability issues

- + **Direct access** to Internet is easier for End Users
- + **VPN might be slow** when connecting from very distant places
- + **No alternative solution** if VPN experiences availability issues



How to capitalize on existing investments to solve these new issues?

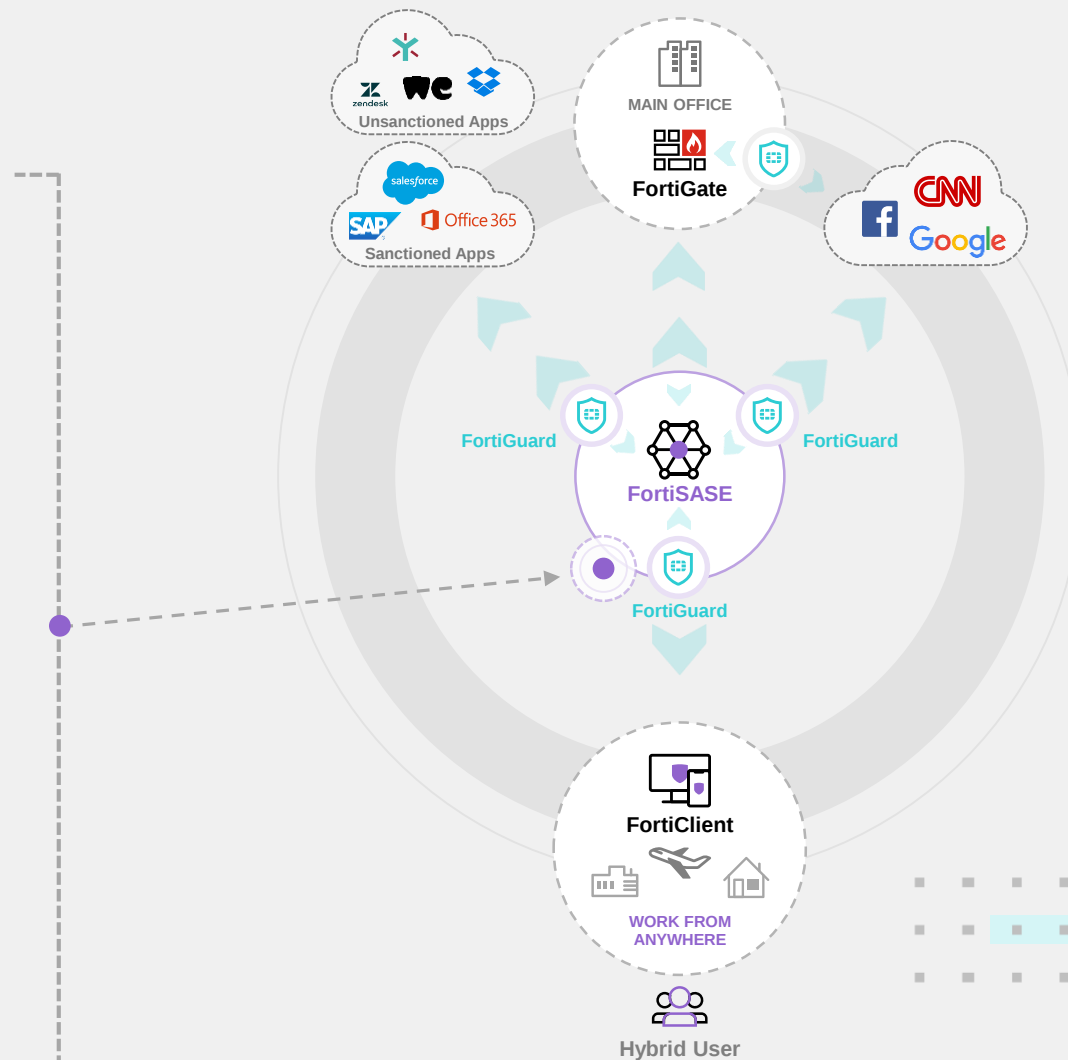
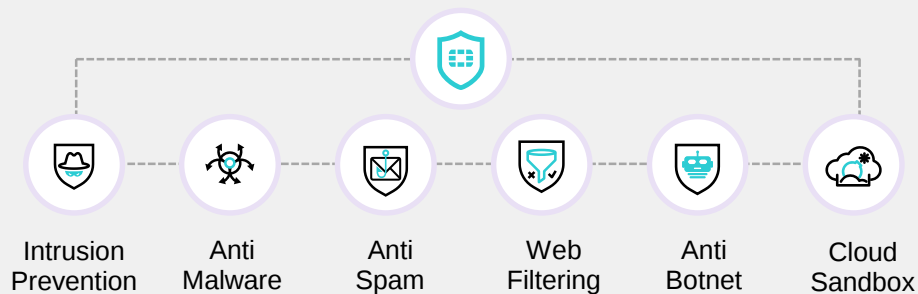


1 Full Protection... from Anywhere, All the Time

FortiGate + FortiGuard Protection even
when not connected to the VPN



FortiGuard Protection for ALL connections



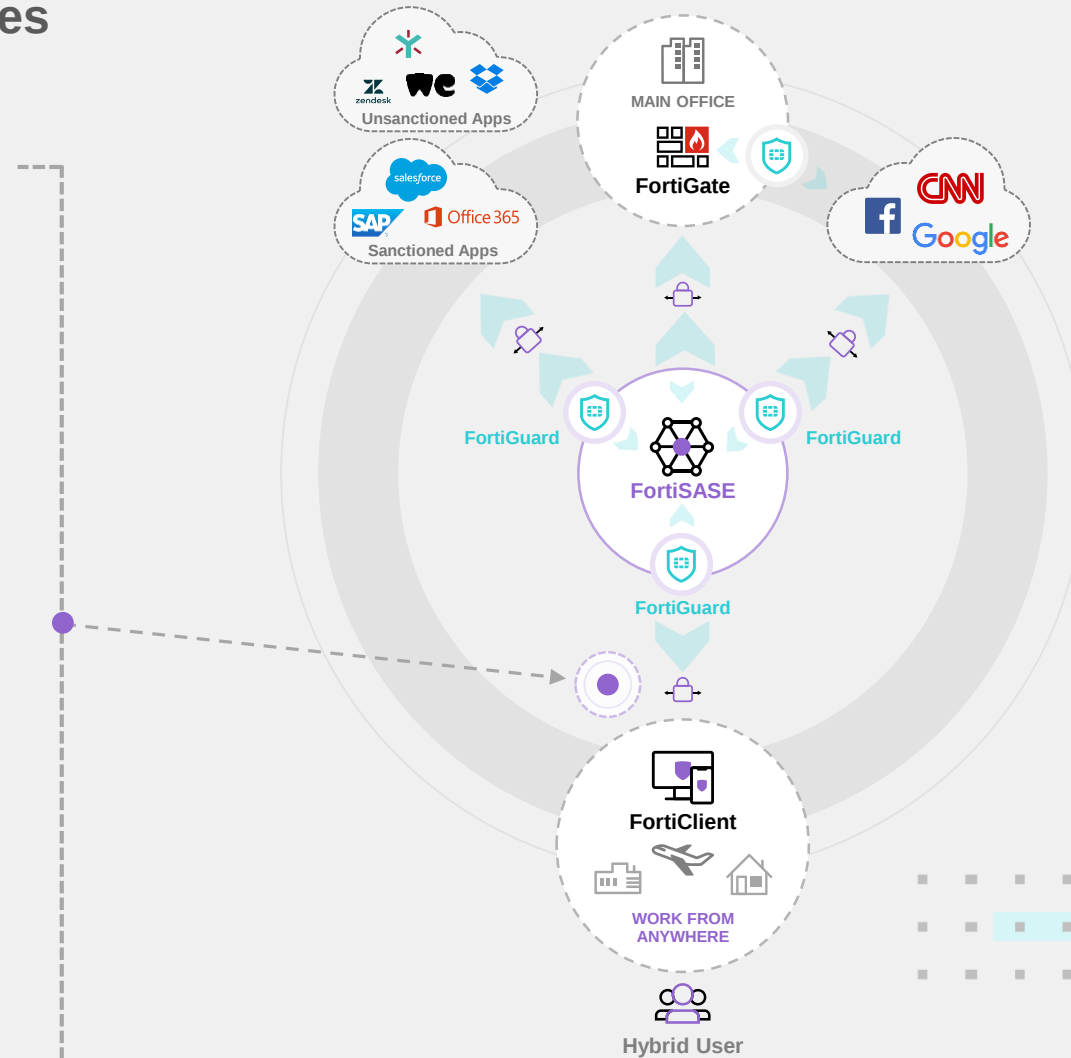
2 Secure Private Access... from Anywhere, All the Time

Secure Private Access in all circumstances



Secure Private Access for ALL connections

- + **Better User Experience**
 - Same feel as direct connection to Internet
- + **Always ON**
- + **VPN still available**, whenever required



3 Consistent Security Posture for better Security and Compliance

Consistency + Cloud-based Management & Reporting Capabilities



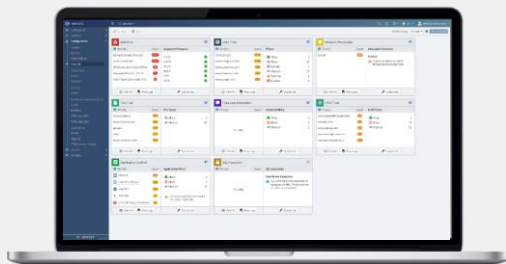
Consistent Security Posture

- + Increased **security**
- + Better capability to satisfy **compliance** requirements

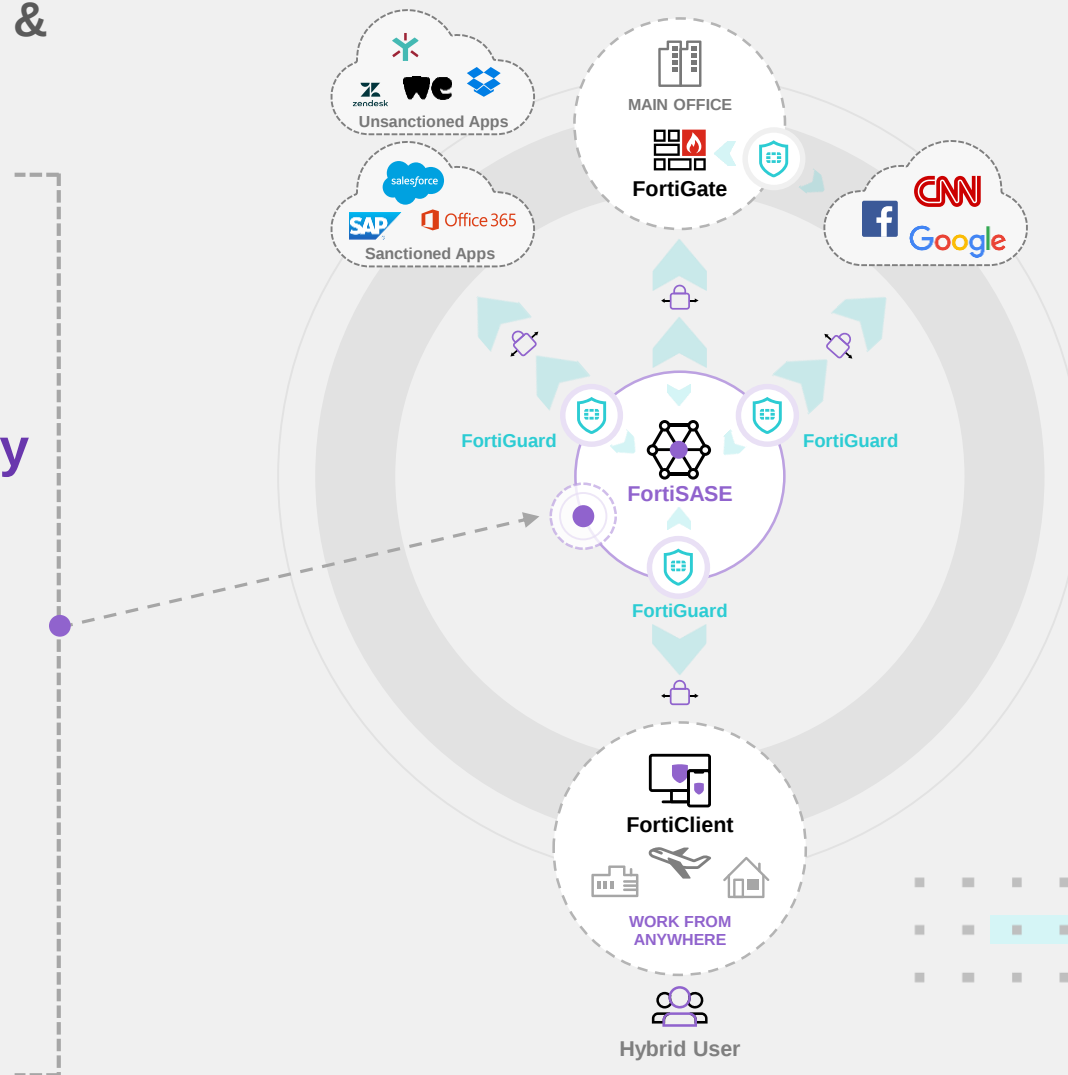


Fully Managed Remote Connectivity

- + Cloud-based **management** and **reporting** capabilities



CUSTOMIZABLE DASHBOARD



4 Visibility and Control on Shadow IT

Capability to see public web Apps used unbeknown to IT, and set access controls on them

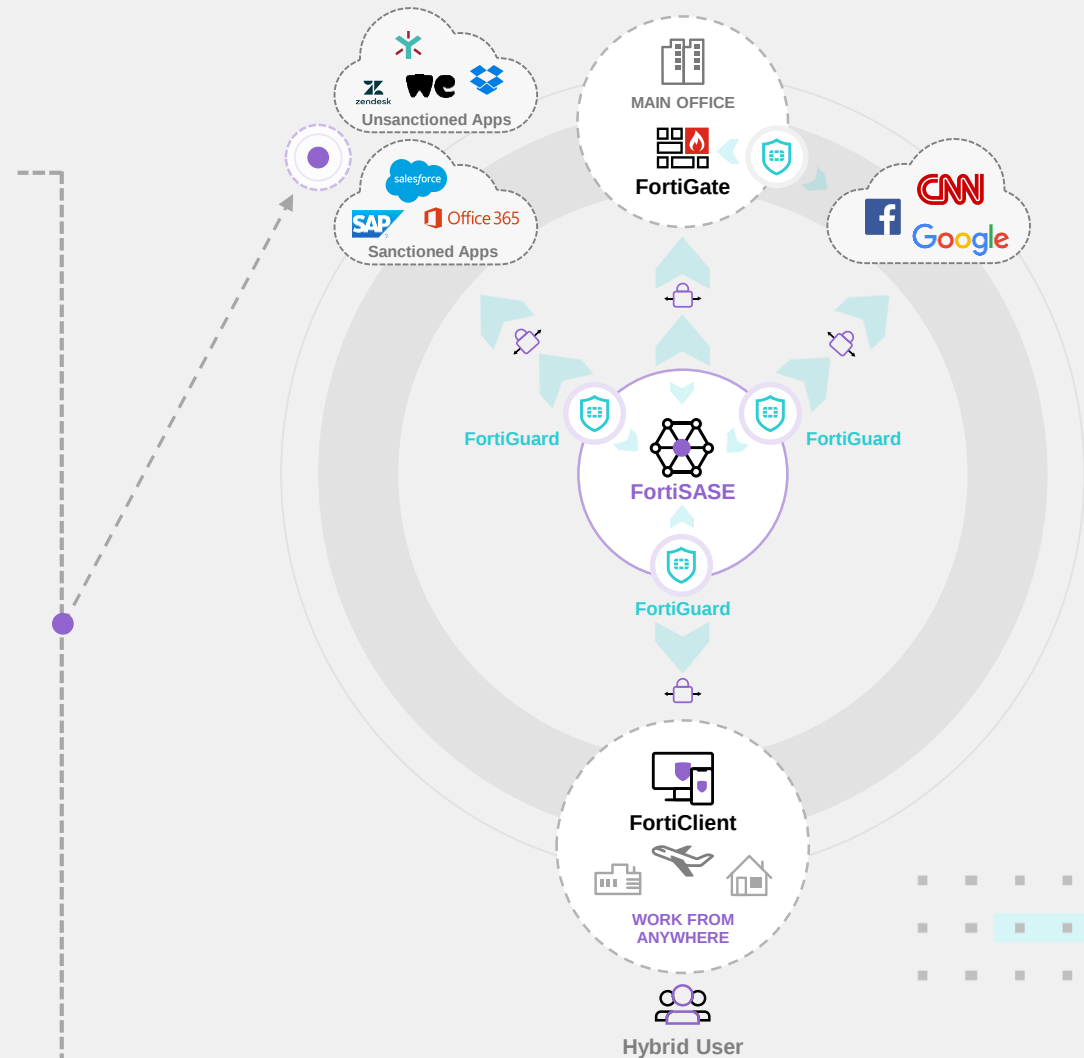


Visibility & Control on Shadow IT

+ **CASB**: see + decide which web Apps can be accessed

IT Department becomes able to:

- + **Identify** key public web apps used by employees
- + **Report** on their usage
- + **Lock down** access to undesirable apps
- + Ensure **secure access** to desirable apps



5 Context-based Access Control to sensitive Apps & Data

Capability to define context-based conditions to access sensitive Applications and Data

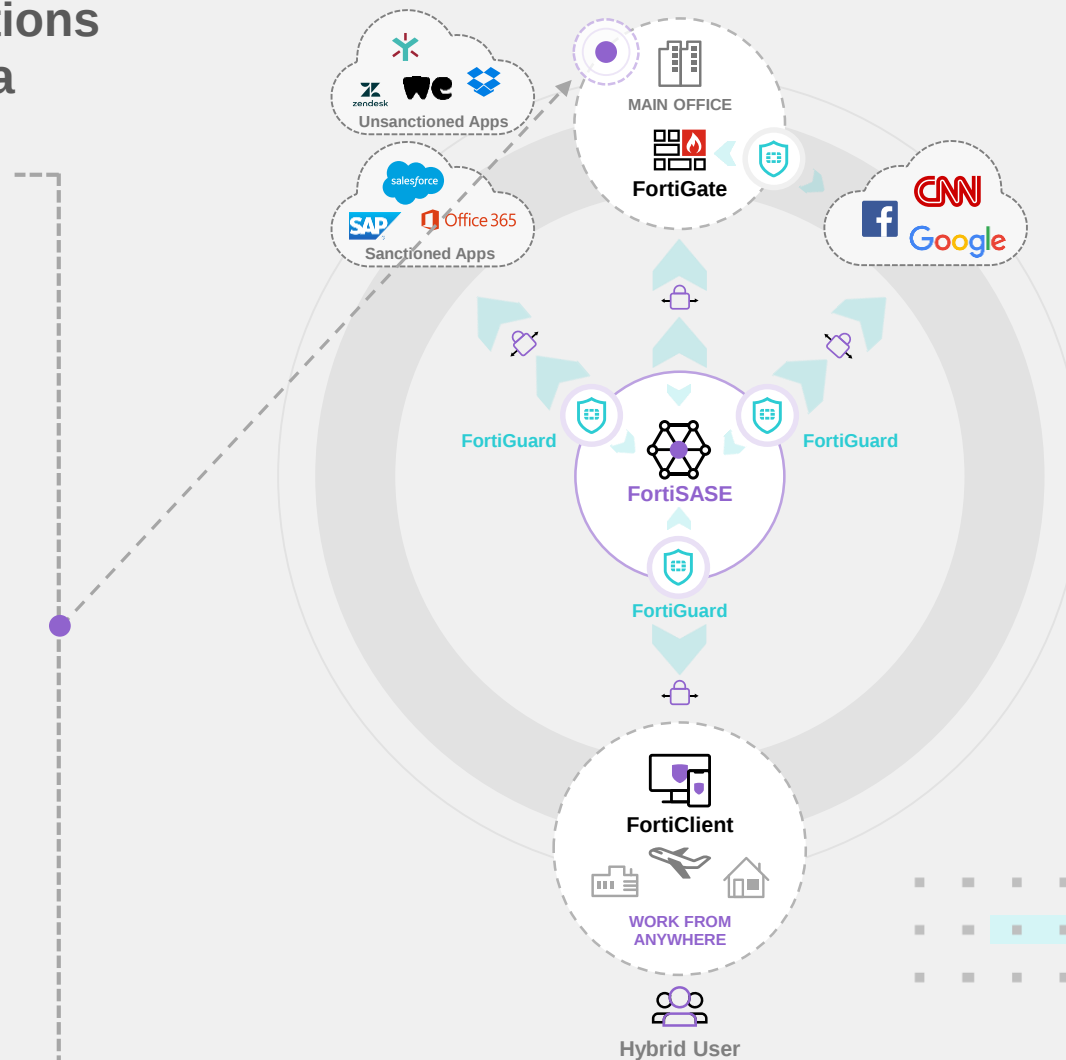


Context-based Access to sensitive Applications / Data

+ **ZTNA**: access control to sensitive Apps or Data

IT Department becomes able to:

- + Set **Context-based Access** to sensitive Apps
e.g. Ensure that sensitive App is not accessible to employees using their home computer (BYOD)
- + Check **Security Posture** continuously
e.g. Block access as long as a critical vulnerability remains unpatched



IDEAL
TECHNOLOGY

- + Best User Experience

A diagram of a node, represented by a light purple circle. Inside the circle, a black dot (the node) has four black arrows pointing outwards to four red dots, representing outgoing edges.



7 Agentless connectivity for users without FortiClient



Agentless connectivity for Users without FortiClient

+ Enable Guests & Subcontractors to get same security



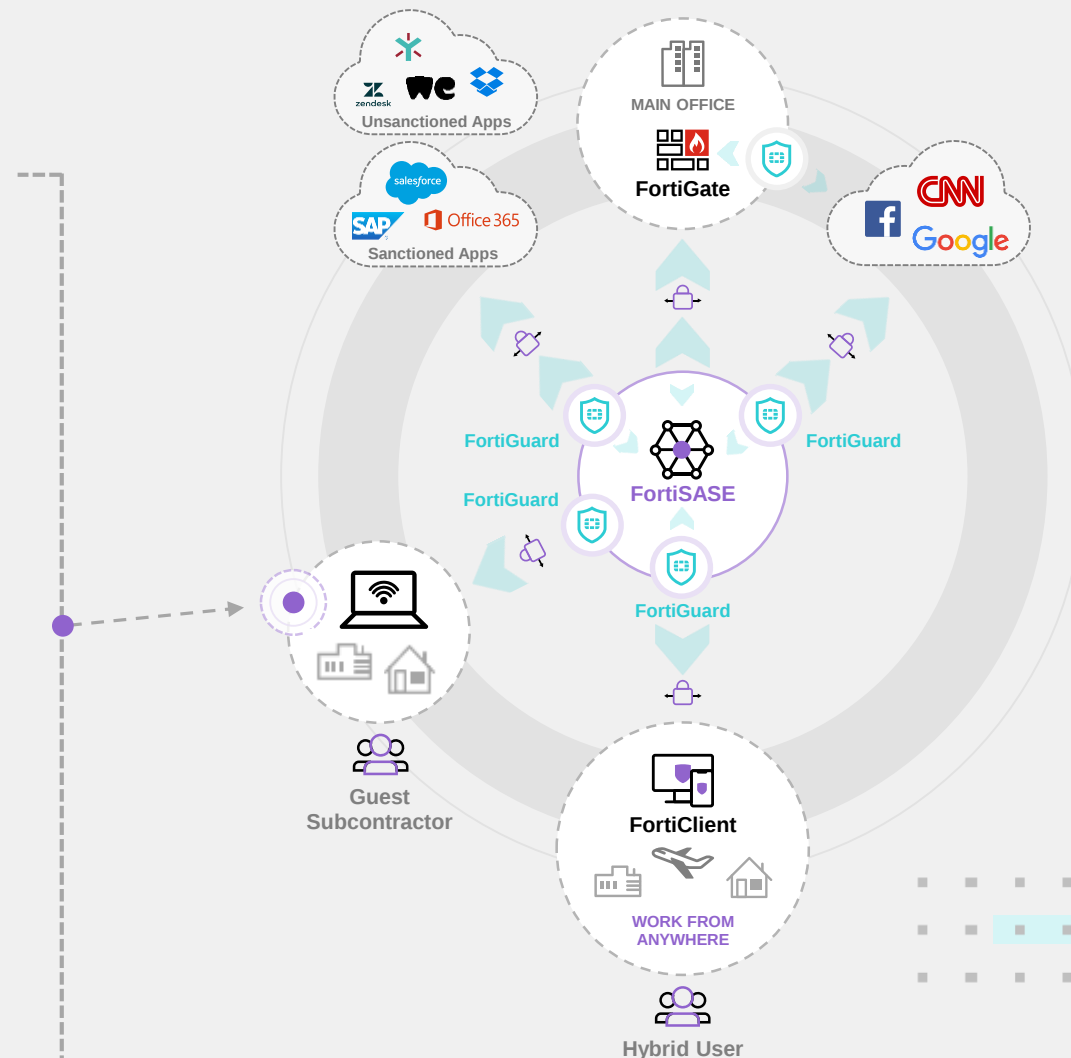
FortiGuard Protection for ALL connections



Secure Private Access for ALL connections

Useful for temporary Guests or Subcontractors who don't have FortiClient installed

More advanced security benefits require FortiClient



8

Endpoint Protection

(Free Option)



Endpoint Protection from Fortinet is included with FortiSASE

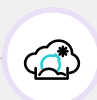
- + **Free option:** May potentially replace 3rd Party Endpoint Protection = better ROI + simpler Endpoint Security Management
- + **Flexibility:** FortiSASE works along with 3rd Party Endpoint Protection



Anti
Malware



Anti
Ransomware



Cloud
Sandbox



Anti
Exploit



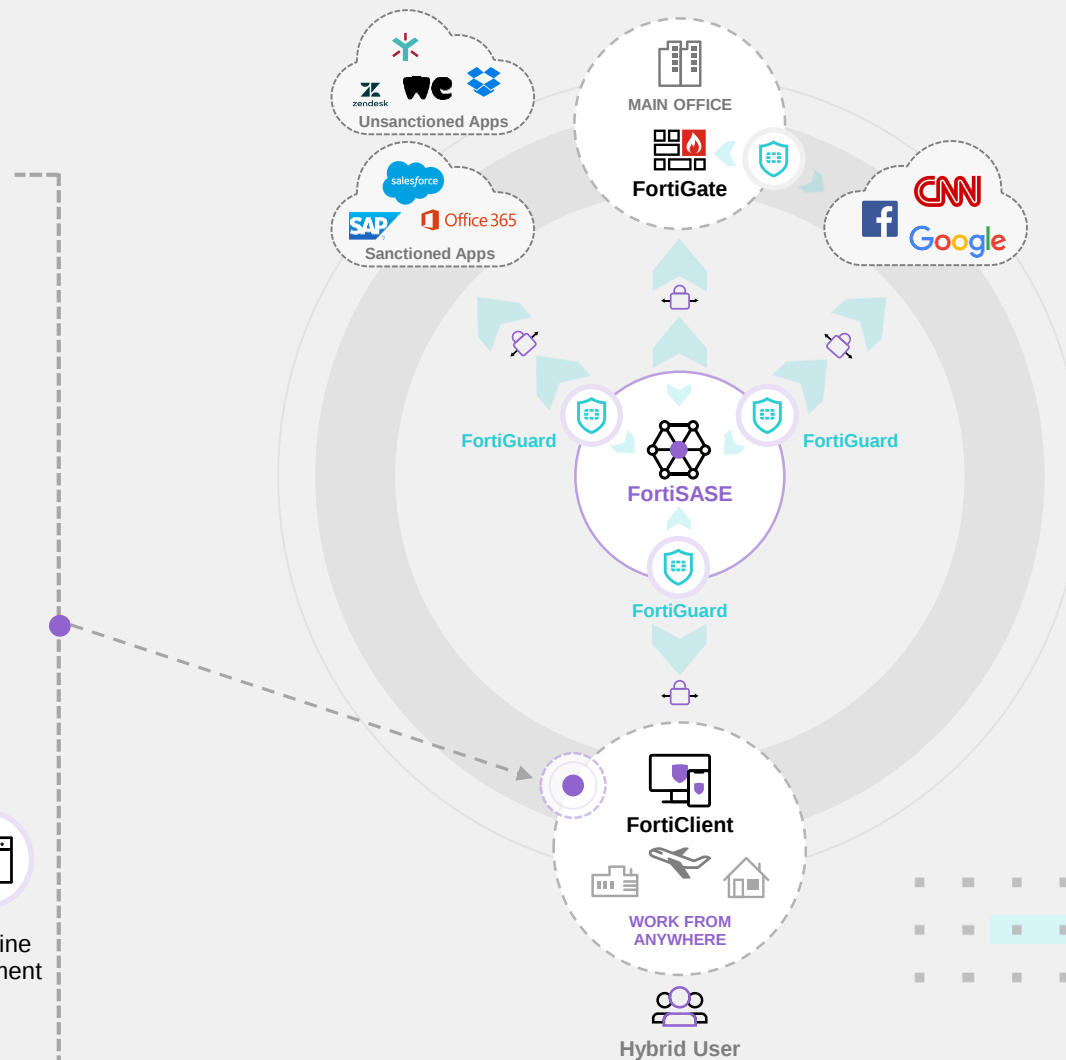
Vulnerability
& Remediation



USB Device
Control

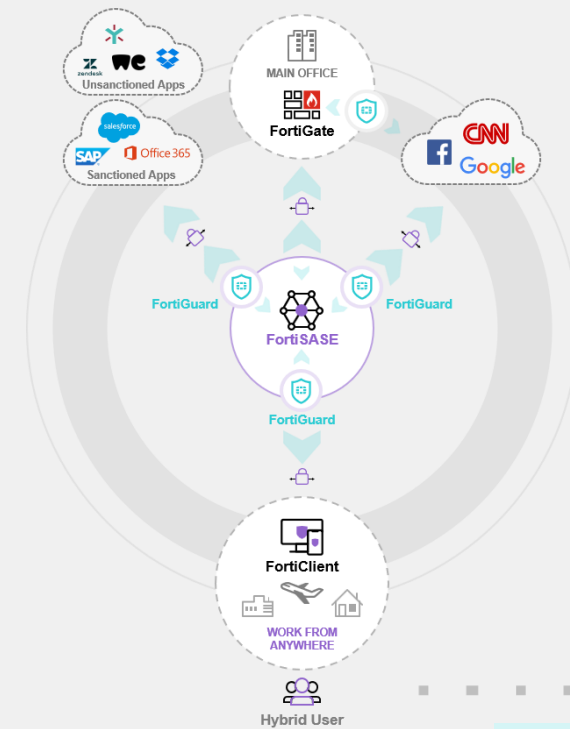
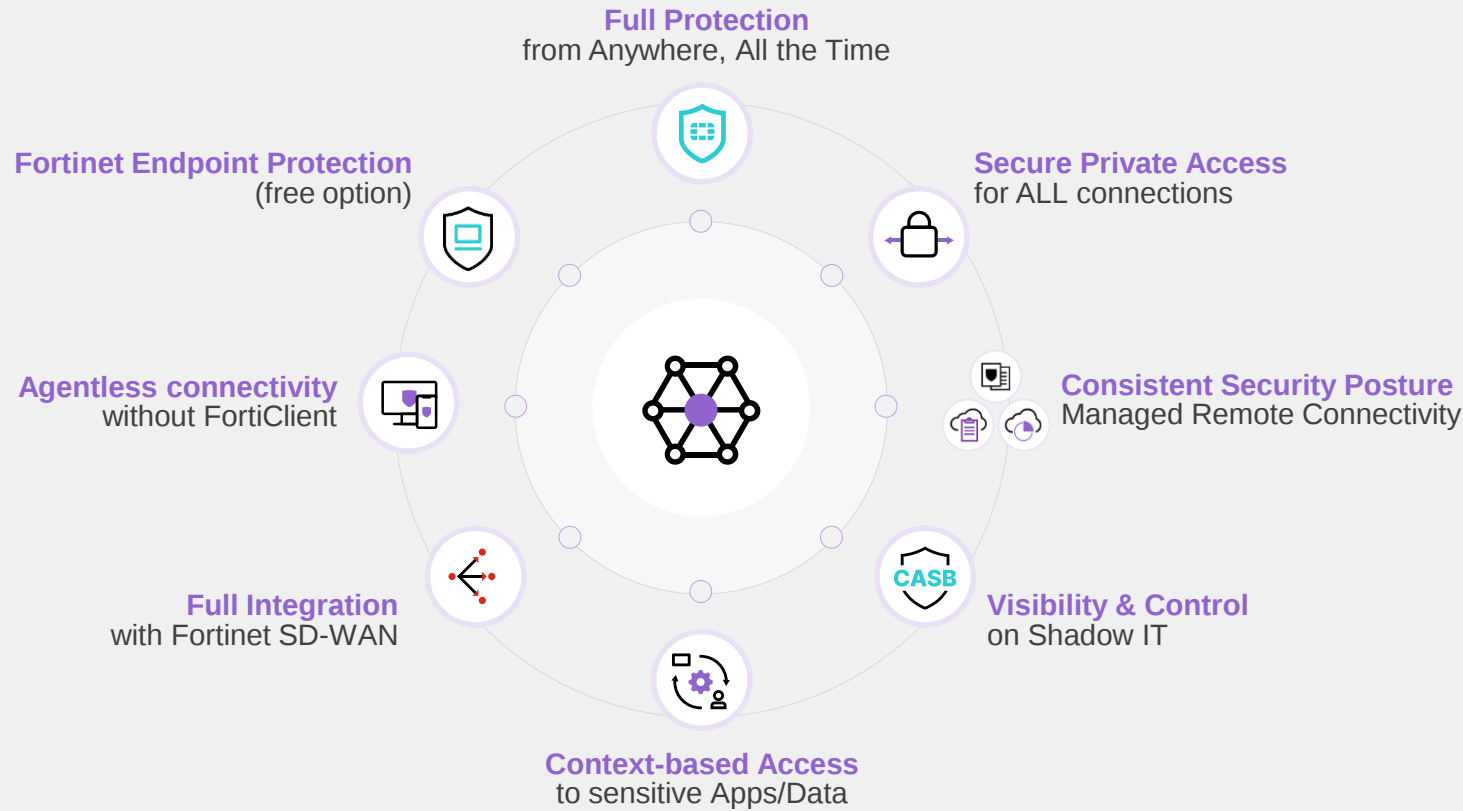


Quarantine
Management



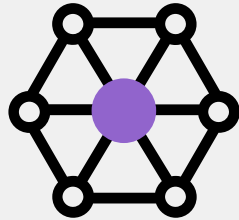
Summary of FortiSASE Benefits

Enabling secure Work from Anywhere



Summary of FortiSASE Benefits

Enabling secure Work from Anywhere



Capitalize on your Existing Investments



FortiGate



FortiGuard



Fortinet SD-WAN



FortiClient

Extend Protection Anywhere, All the Time

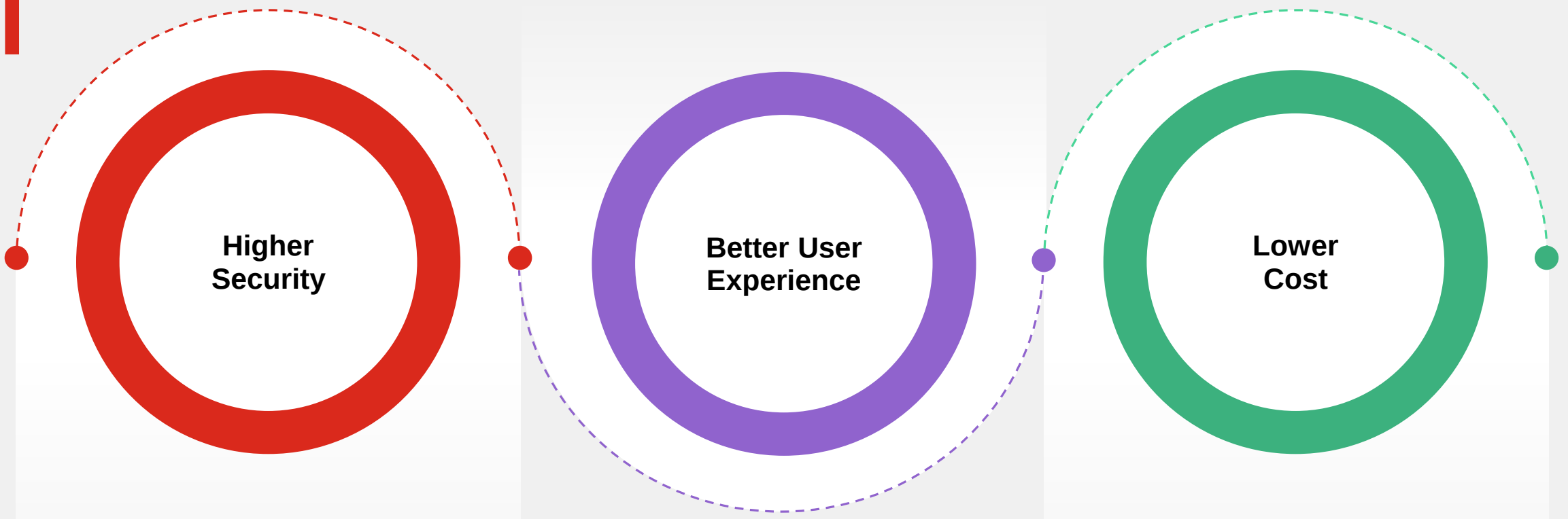
Increase Security

Increase Visibility and Control

Improve Compliance & Management

Key Business Outcome with FortiSASE

Enabling secure Work from Anywhere



Higher
Security

Overcome **Security Gaps**
Consolidated & converged

Better User
Experience

Same user experience everywhere
with the same level of security

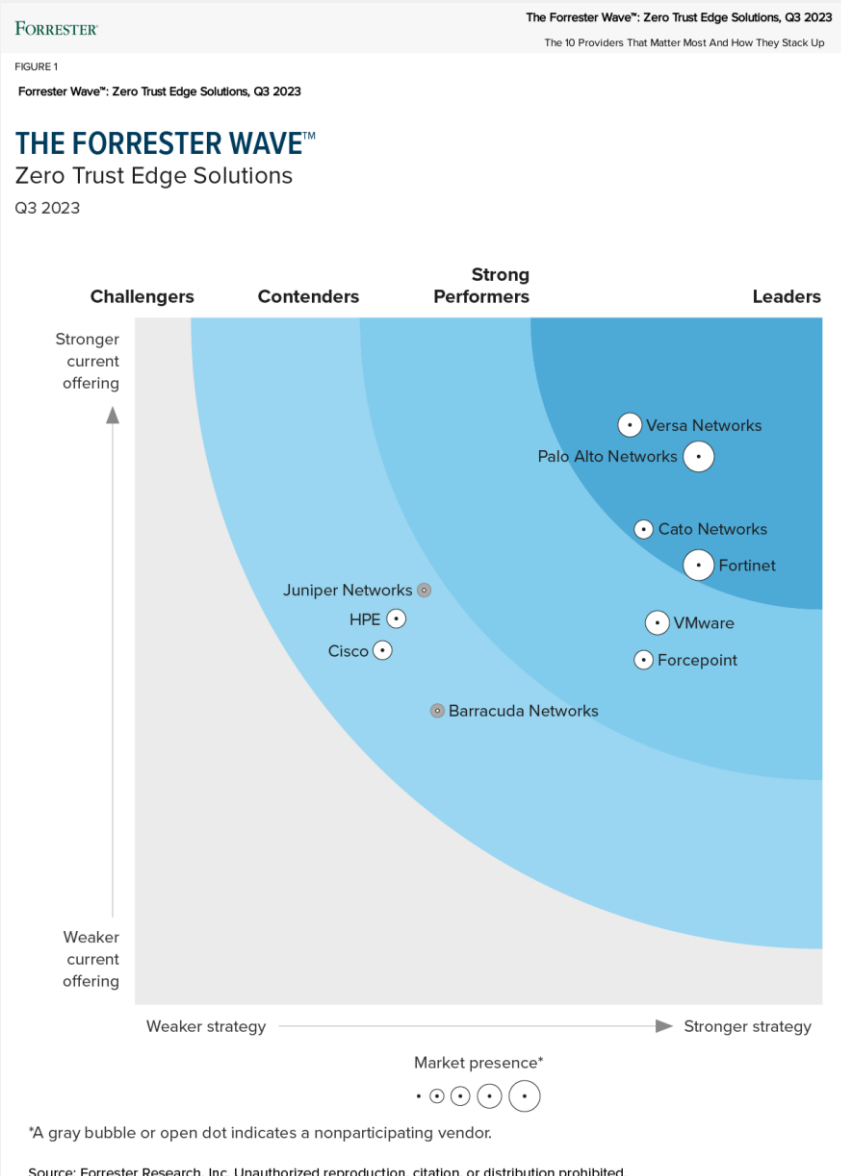
Lower
Cost

Consolidate point products
with **integrated approach**

Solution Validation



Fortinet Named a Leader in the Forrester Wave™: Zero Trust Edge (ZTE) Solutions, Q3, 2023



Fortinet Received the Top Score in the Strategy Category (Tied) and the Second Highest Score in the Market Presence Category

"Fortinet balances security and networking with eye-popping value"



The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester Wave™ is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave™. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change..

Fortinet Recognized as a Challenger in the Inaugural 2023 Gartner® Magic Quadrant™ for Single-Vendor SASE

Figure 1: Magic Quadrant for Single-Vendor SASE



Fortinet named a Challenger in this report, 1st ever Magic Quadrant™ for Single-Vendor SASE

Gartner, Magic Quadrant for Single-Vendor SASE, Andrew Lerner, Jonathan Forest, Neil MacDonald, Nat Smith, Charlie Winckless, 16 August 2023

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

Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's Research & Advisory organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from [insert client name or reprint URL].



FORTINET®

Contact us
security@ideal.gr