FORTINET

IntegraONE

FortiSASE
Secure Access Everywhere

Evolving Trends Require Secure Access for Hybrid Workforce

Growing Cloud Adoption

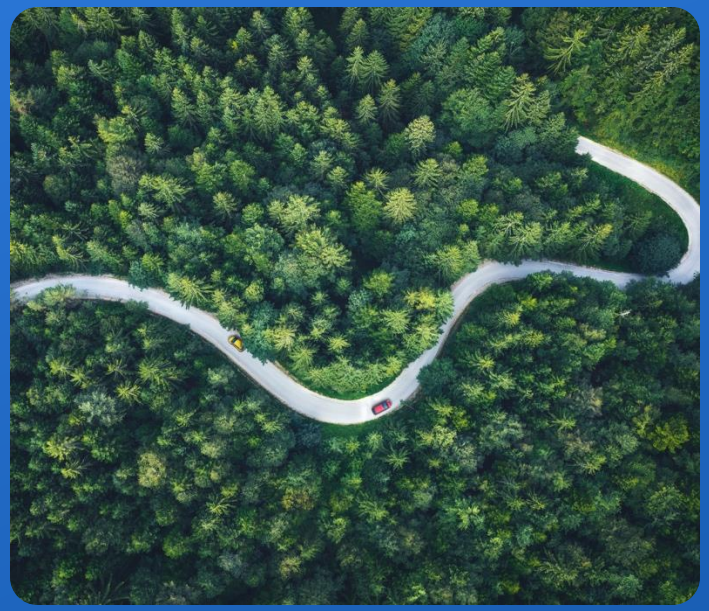
The rapid growth of Multi-Cloud and SaaS adoption requires visibility, control, and secure access to protect data. Up to **70%** of apps used within companies are SaaS based with companies that use them estimating that this will increase to 85% in 2025.

Managing Hybrid Workforce

A consistent security approach and user experience are essential for improving productivity in a Hybrid Workforce. According to Forbes, only 16% of companies are fully remote, meaning that **84%** are hybrid.

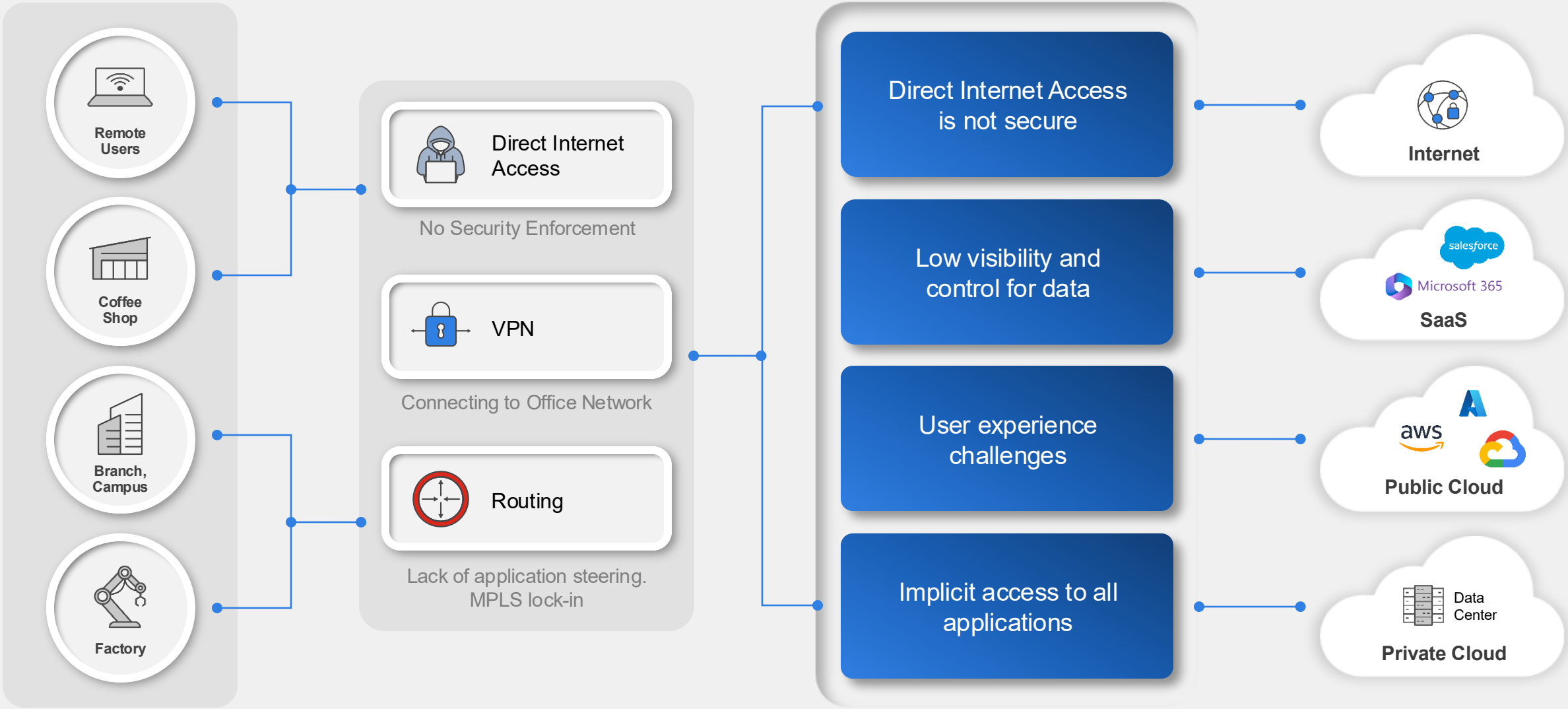
Journey to Zero Trust

Transitioning from implicit to explicit access for applications is essential for adopting a Zero Trust mindset. According to Gartner, **60%** of organizations will embrace Zero Trust as a starting point for security by 2025.



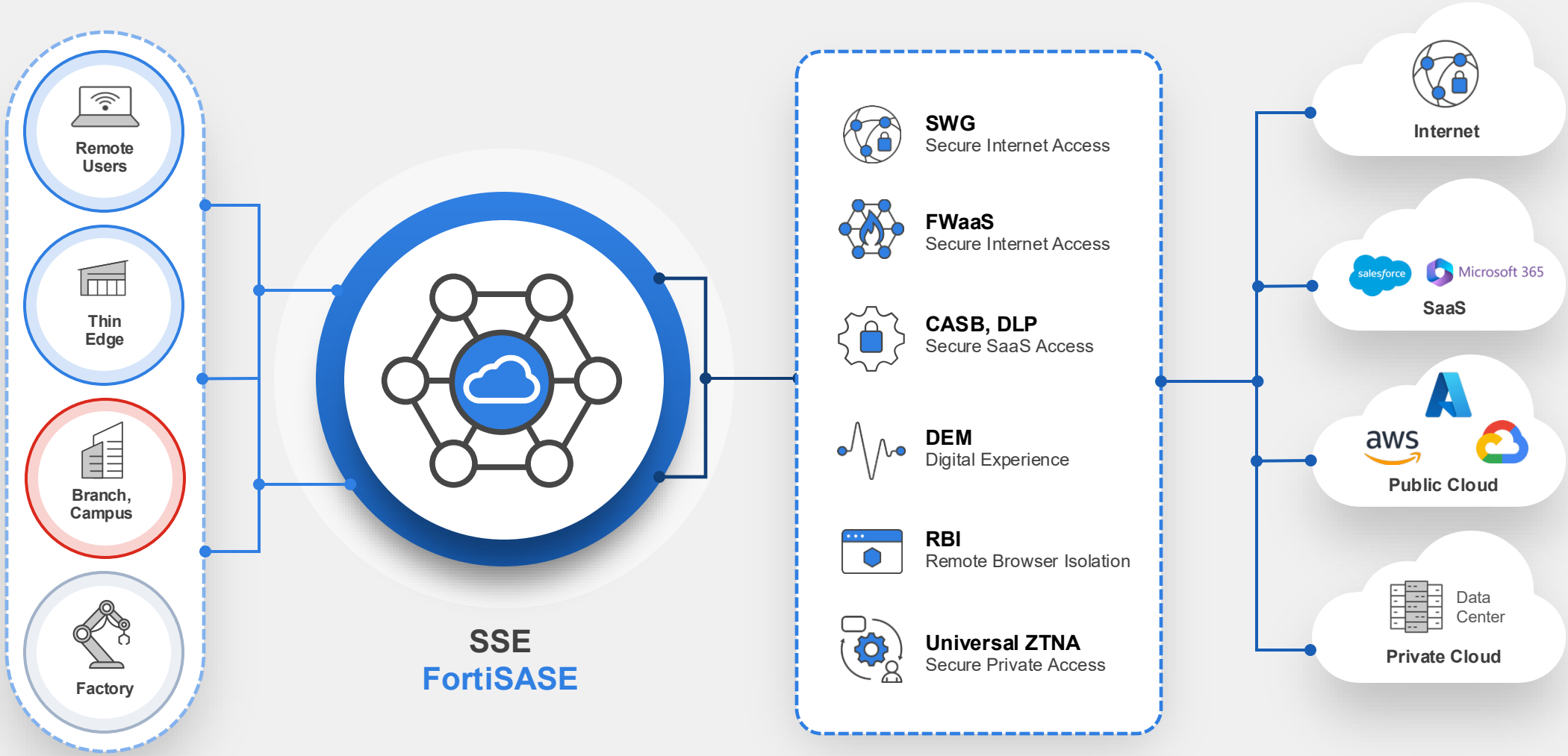
https://www.saasacademy.com/blog/saas-statistics
https://www.forbes.com/advisor/business/remote-work-statistics/?utm_source=chatgpt.com
https://virtualizationreview.com/articles/2022/06/23/gartner-predictions.aspx?utm_source=chatgpt.com

Customer Challenges to Enable Secure Access



Meet FortiSASE, a key part of Fortinet Unified SASE solution

Security Service Edge



FortiSASE Global Infrastructure

Global Coverage
$1B+ Investment in Infrastructure

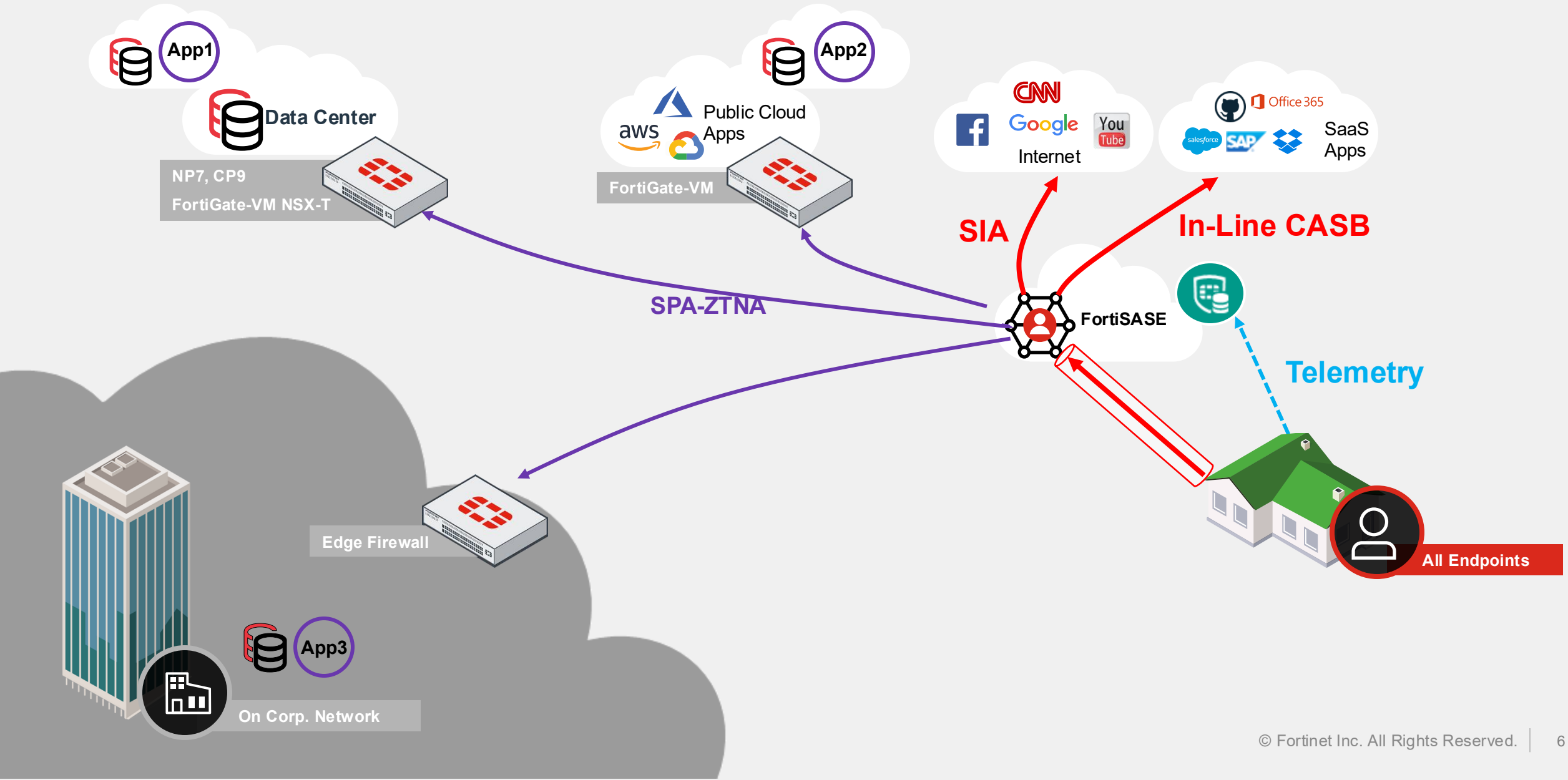
3.3M+ Owned
1.0M+ Leased
4.3M+ Total Sq Ft

160+ **Cloud Locations** superior user experience

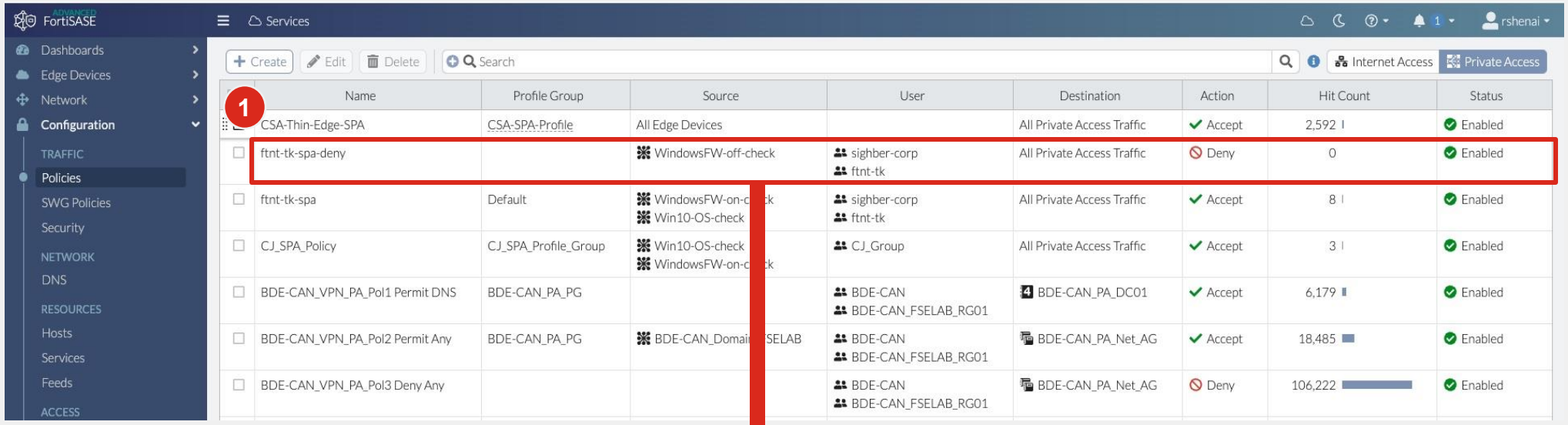
FortiStack
Organically built integrated solutions

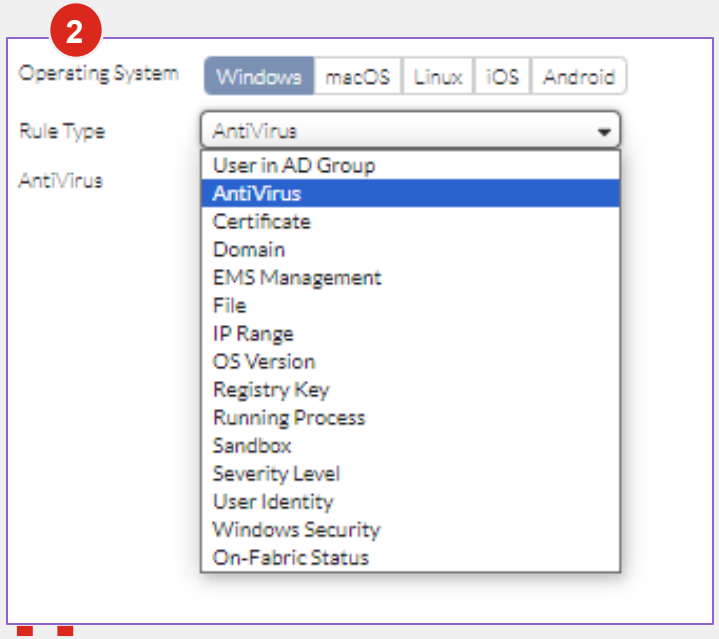
Cost Savings Drive Competitive Advantage

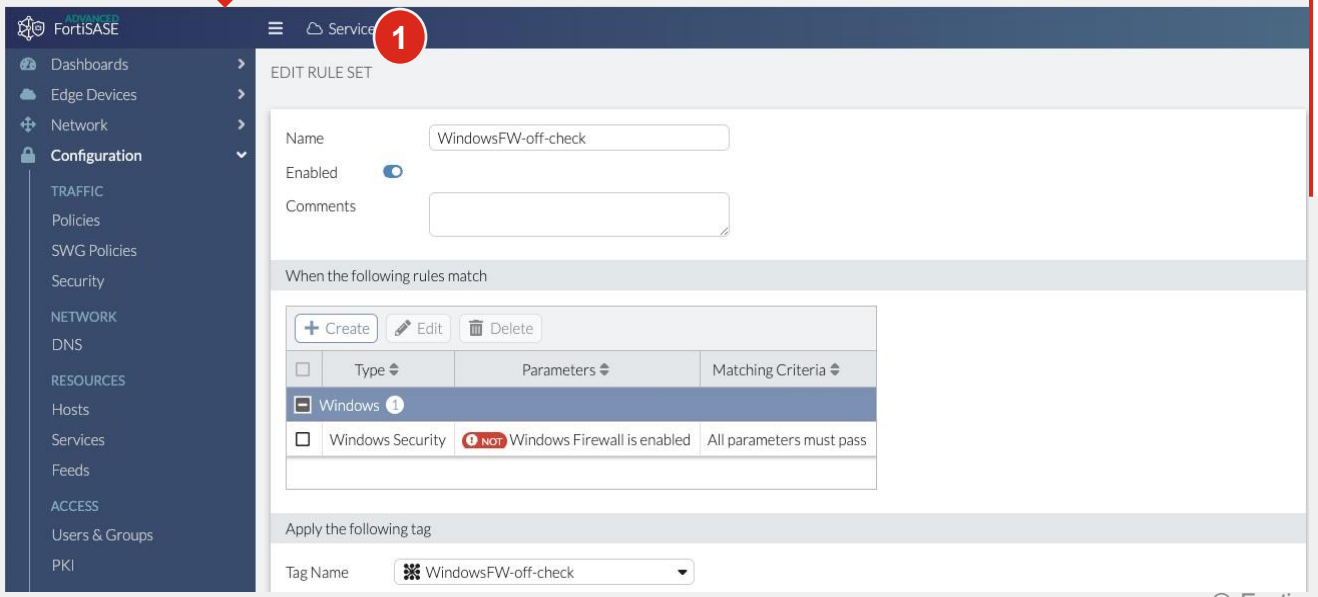
Private Access with FortiSASE



Zero Trust security for secure application access

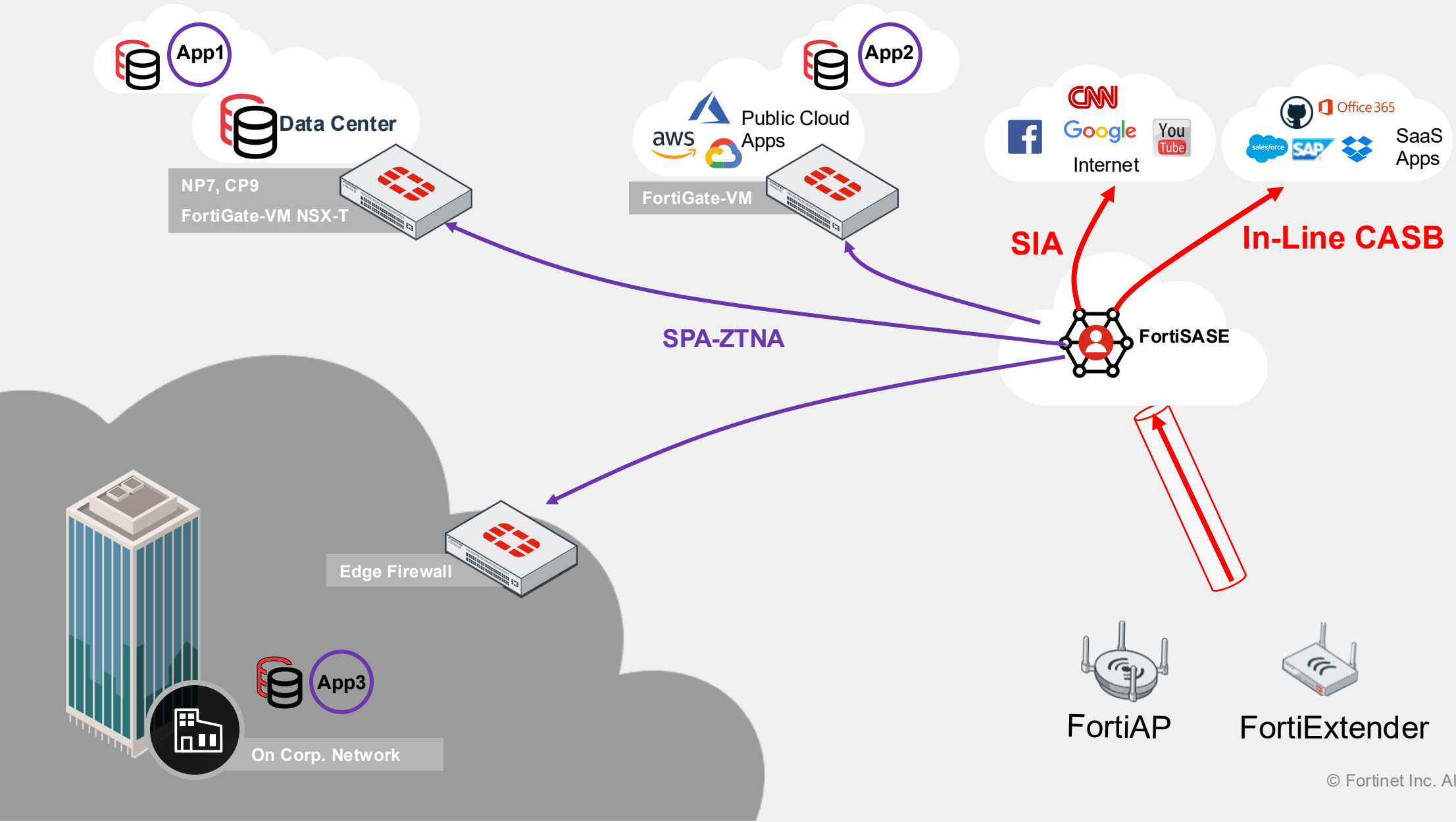






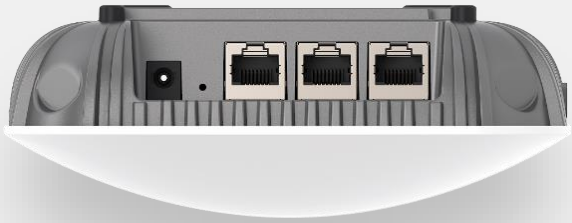
1. SPA policies defined with ZTNA tags
2. ZTNA tag rules supported for multiple OS's

Edge Device with FortiSASE



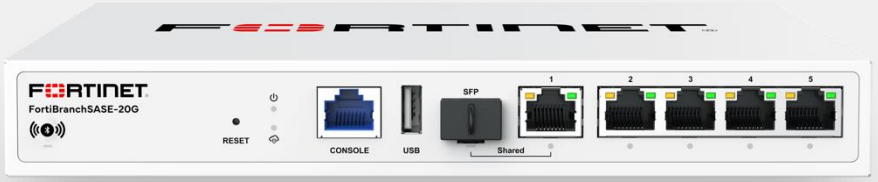
FortiBranch SASE - More Models and More Devices

Thin Edge Devices



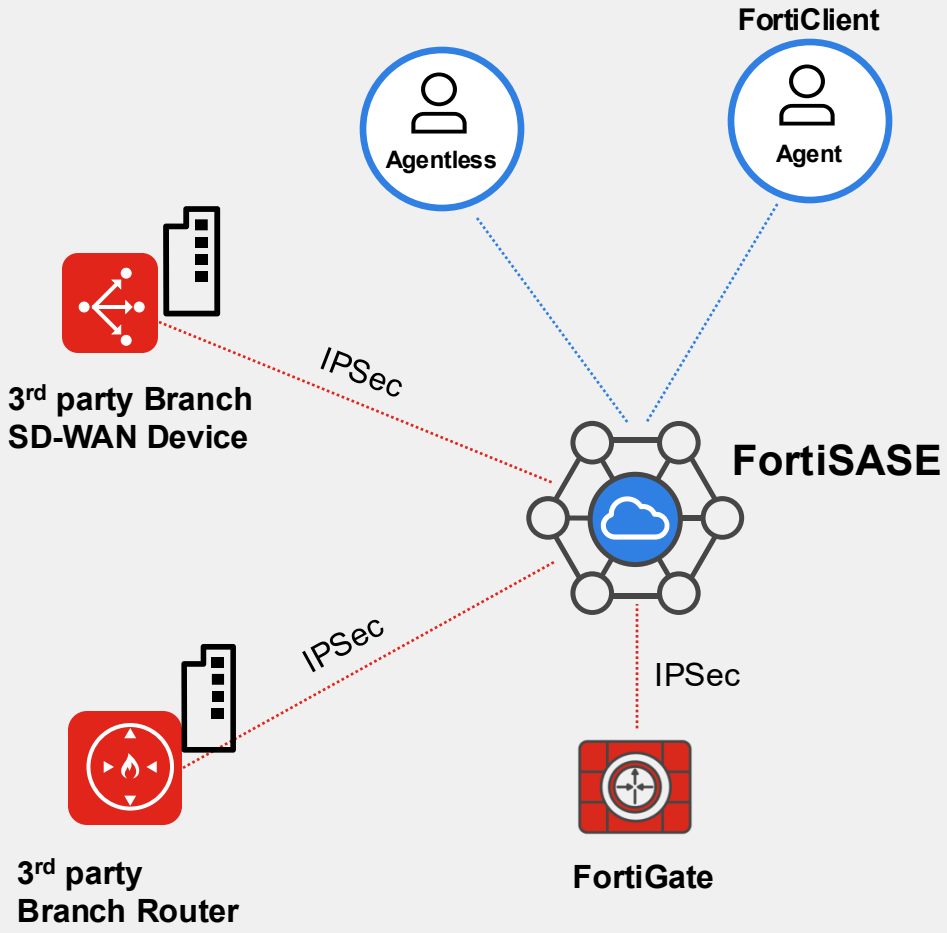
FortiBranchSASE 10F-WiFi

FortiBranchSASE 20G-WiFi



FortiBranchSASE 20G

Secure Connectivity from 3rd Party Branch Devices



FortiSASE 3rd Party Device IPSec Connectivity

Integrate with existing SD-WAN \ Router

Enables organizations to protect their current infra investments while strengthening their security posture

Architecture Support

IPsec

Supports IPsec from 3rd party vendor branches to 20 unique FortiSASE PoPs; each FortiSASE PoP supports 2000 maximum IPsec tunnels (total bandwidth of 1Gbps)

Licensing Requirement

Add-on SKU is required to enable this feature (allowed only with Advanced and higher tiers)

Key Differentiators of FortiSASE

ONE OPERATING SYSTEM

FortiOS

SD-WAN, SSE, NGFW, LAN

UNIFIED MANAGEMENT PLANE

SaaS Management

SSE, DEM, WLAN

ONE ANALYTICS ENGINE

Integration with SOC

Data lake for security operations

UNIFIED ENDPOINT AGENT

FortiClient

EPP, SASE, ZTNA, CASB

AI-Driven Security Services with Flexible Consumption with FortiPoints

FortiGuard Labs

FortiManager integration with FortiSASE

Opt-in Feature - Requires FortiManager 7.4.4

Objects

- Firewall Address
- Firewall Address Group
- Security Profile Group
- AV Profile
- WF Profile
- IPS Profile
- File Filter Profile
- DLP Sensor Profile
- DNS Filter Profile
- Application Control Profile
- SSL Inspection Profile
- Users / User Groups

SOC as a Service integration with FortiSASE

Seamless integration

Say No to False Positives!

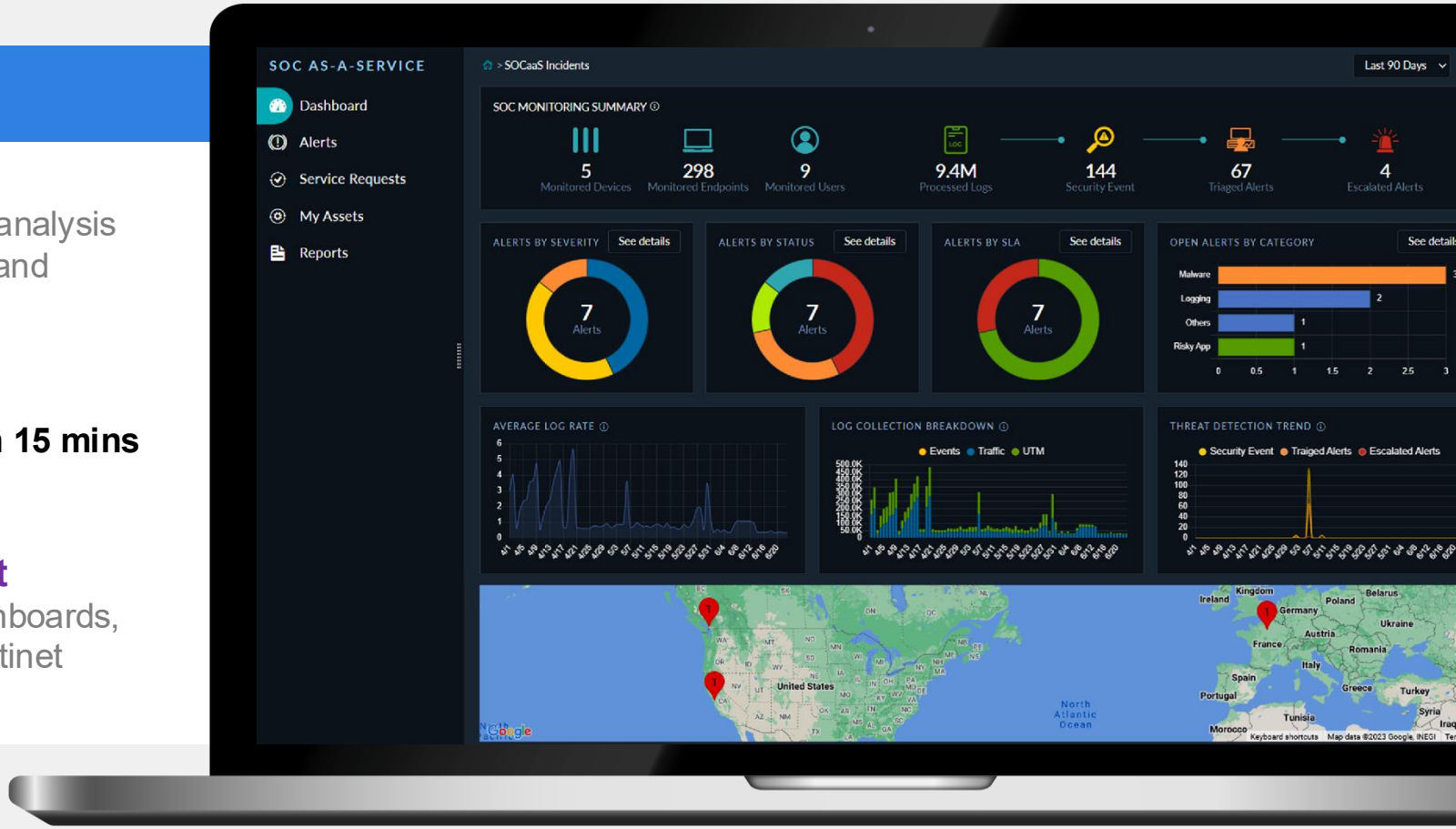
24x7 Human based Monitoring and analysis with weekly summary reports, alerts and notifications

Respond: Act Fast

Fortinet security experts notify **within 15 mins** – IOCs, remediation, why and what

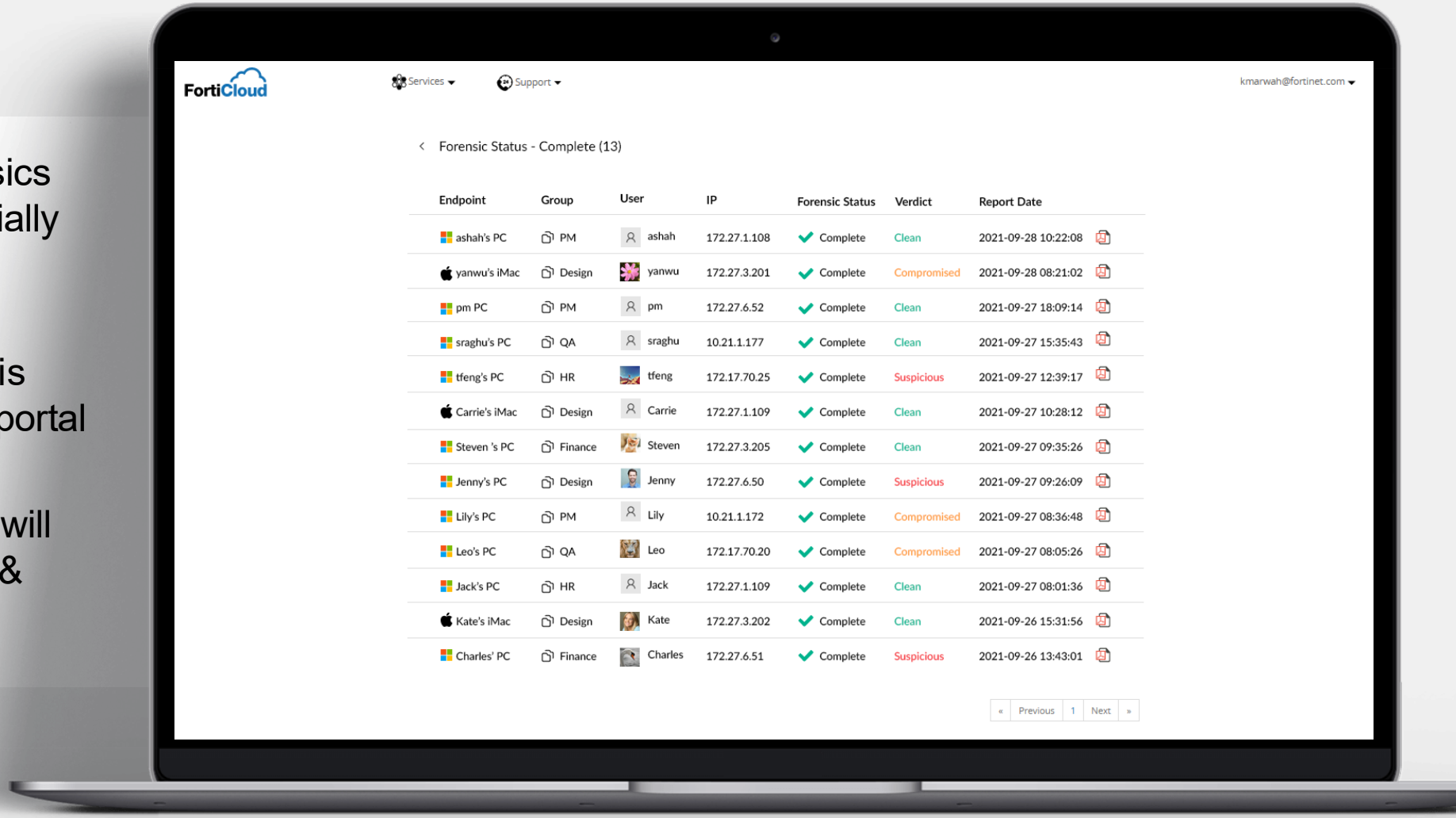
Improve: Maximize Investment

Cloud-based portal with intuitive dashboards, on-demand reports and quarterly Fortinet **expert meetings**



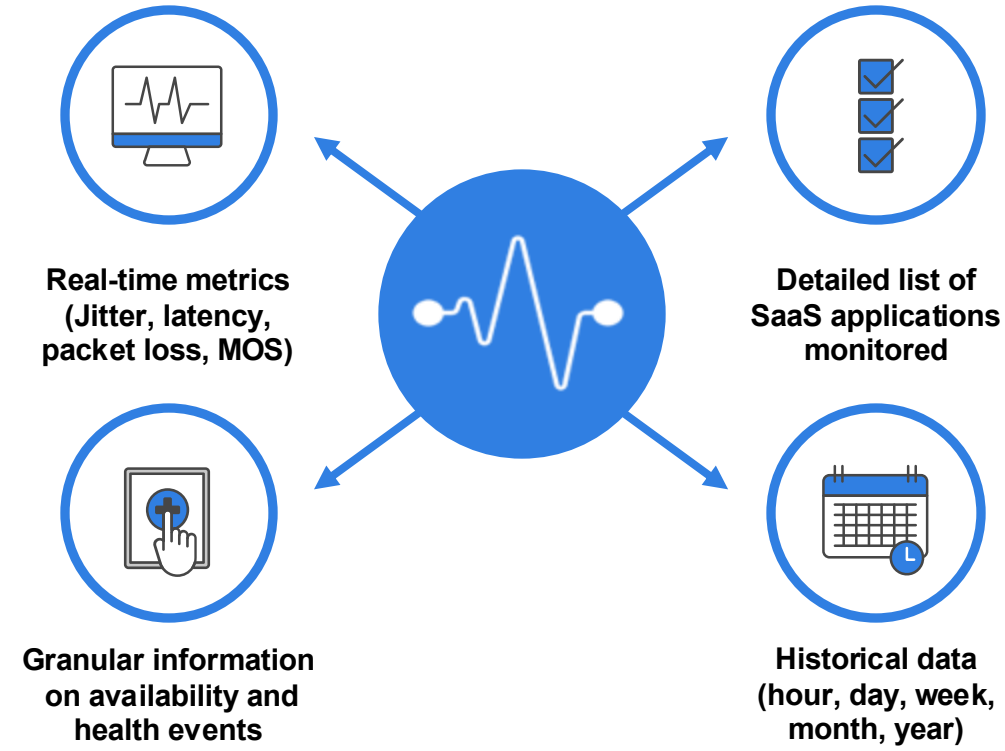
Security – FortiGuard Forensics

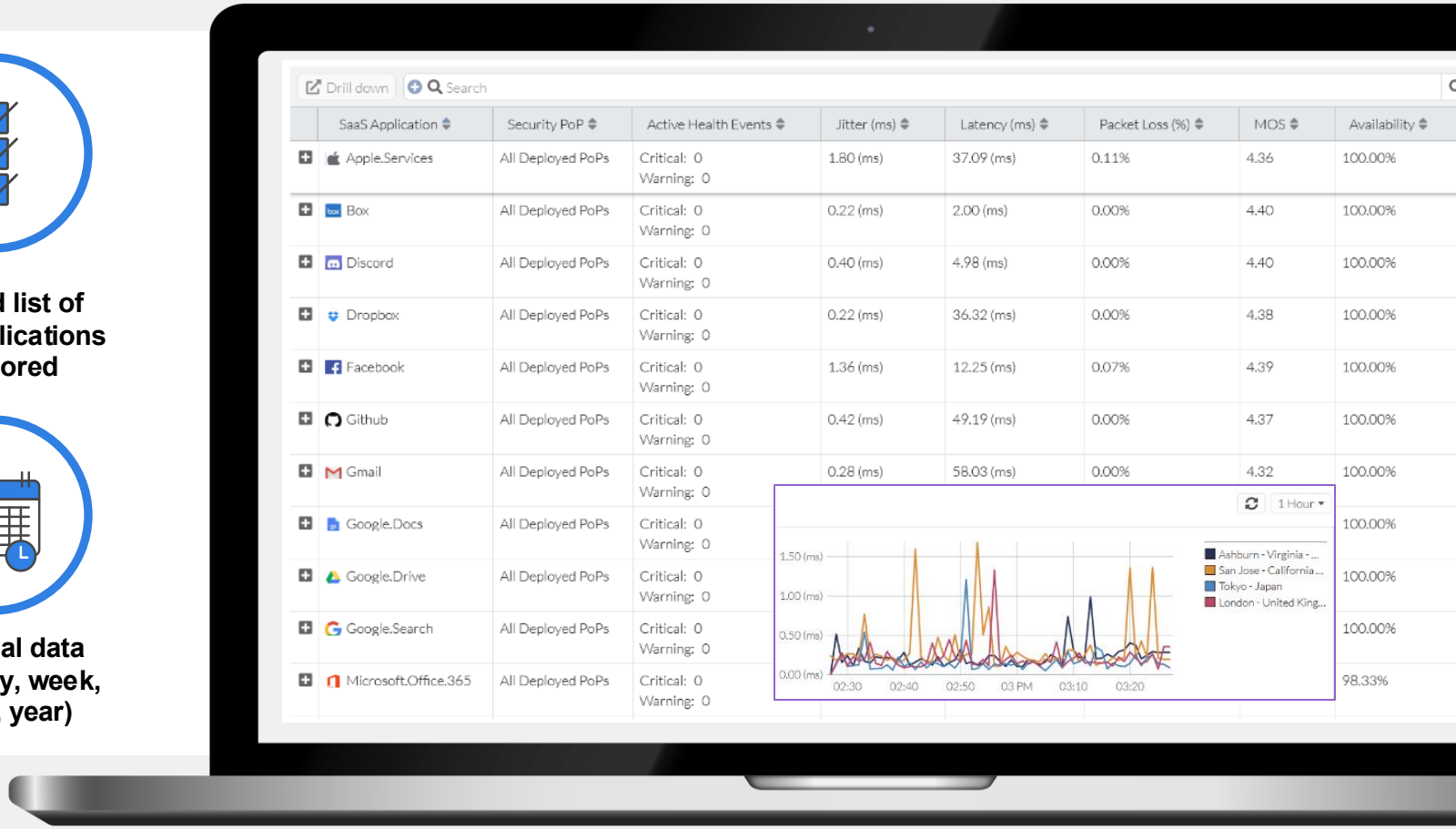
- Leverage FortiGuard Forensics service to investigate potentially compromised endpoints
- Submit Endpoints for analysis directly from the FortiSASE portal
- FortiGuard Forensics Team will analyze and provide verdict & details report on findings



Digital Experience Monitoring

Comprehensive visibility | Metrics and alerts correlation | Proactive response





Agentless ZTNA Use Cases & Benefits

Remote Access for Employees

Allows secure access to corporate applications and data from personal devices

Simplify Experience

https://fortinet.sharepoint.com/sites/[illegible]/Fortinet-SASE.aspx

Third-Party Vendor Access

Allows secure access to vendors or contractors for specific applications

Data Loss Prevention

Consistent Policies for all users

FortiSASE allows agent and agentless config from same console

Scalable with instant deployment

Allow BYOD users seamless access to Private Applications

Portal for Unmanaged Devices

IdP

Fortinet or 3rd party

2. FortiSASE verifies user's identity and role (IAM + MFA)

3. FortiSASE checks policies / profile groups

- **Inline Malware Protection**
- **IPS with TLS decryption**
- **Remote Browser Isolation**
- **Data Leak Prevention**

1. User connects to FortiSASE portal to access corporate private applications

FortiSASE

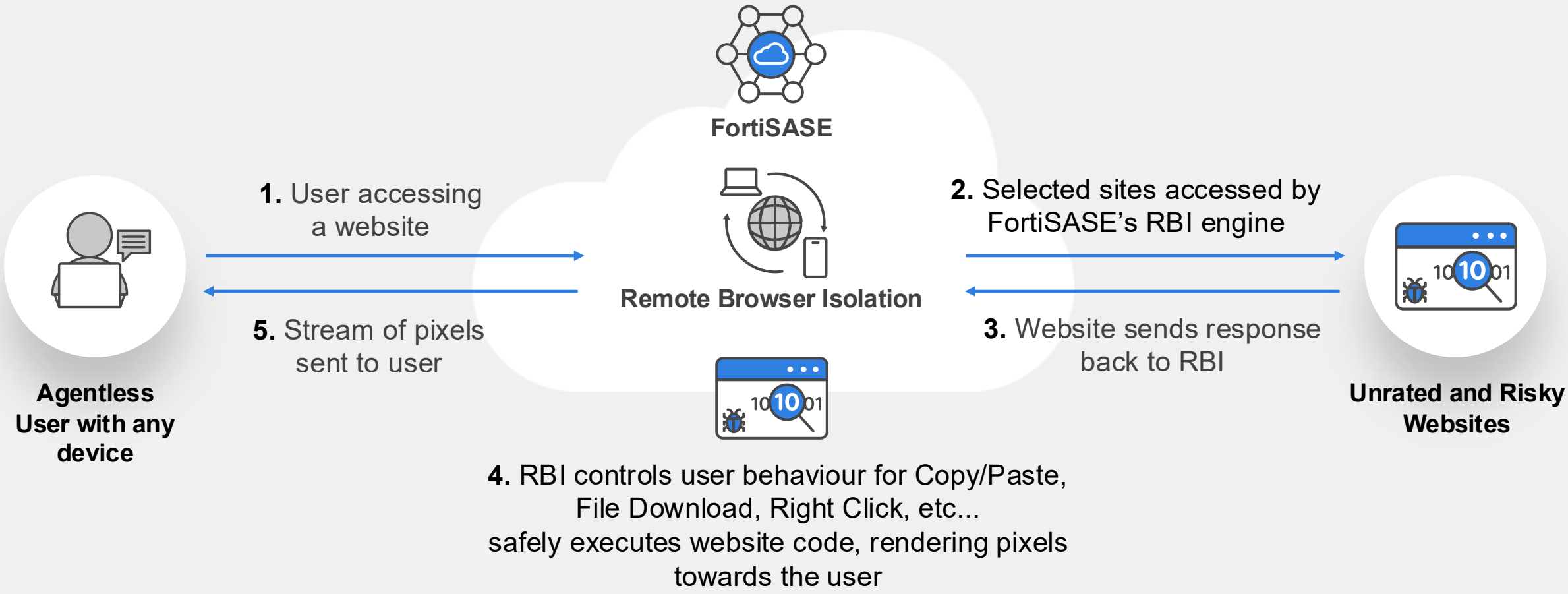
4. FortiSASE connects user to the private application

Agentless User with any device / BYOD

Public or Private Data center with private applications

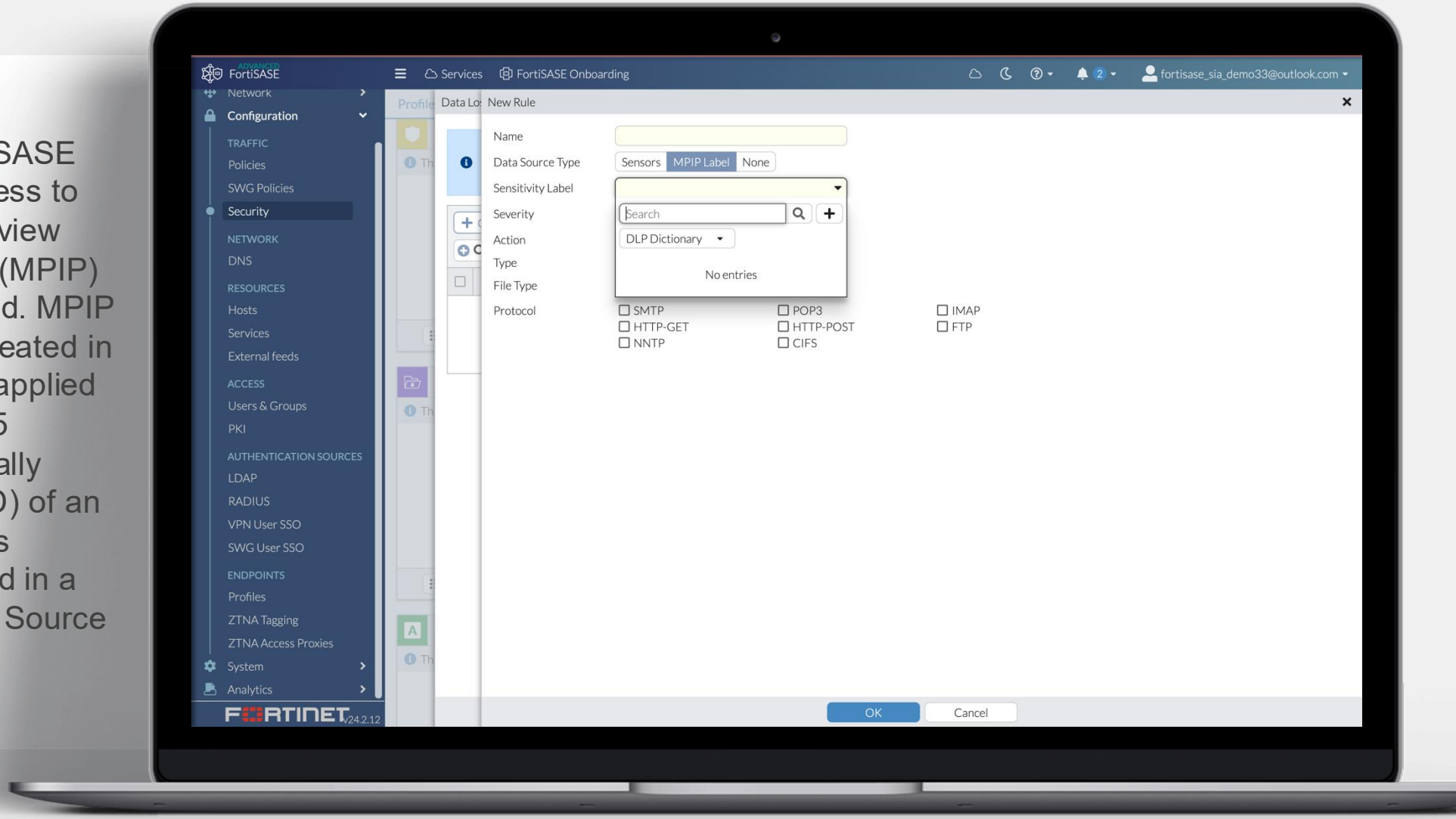
Safeguard your Users from Browser Threats

Optimum performance and enhanced security with native RBI



DLP Support for Microsoft MPIP labels

- Added support in FortiSASE DLP for managing access to files with Microsoft Purview Information Protection (MPIP) sensitivity labels applied. MPIP sensitivity labels are created in a Microsoft portal and applied to files using Office 365 applications. The Globally Unique Identifier (GUID) of an MPIP sensitivity label is configured and selected in a DLP rule with the Data Source Type of MPIP Label.



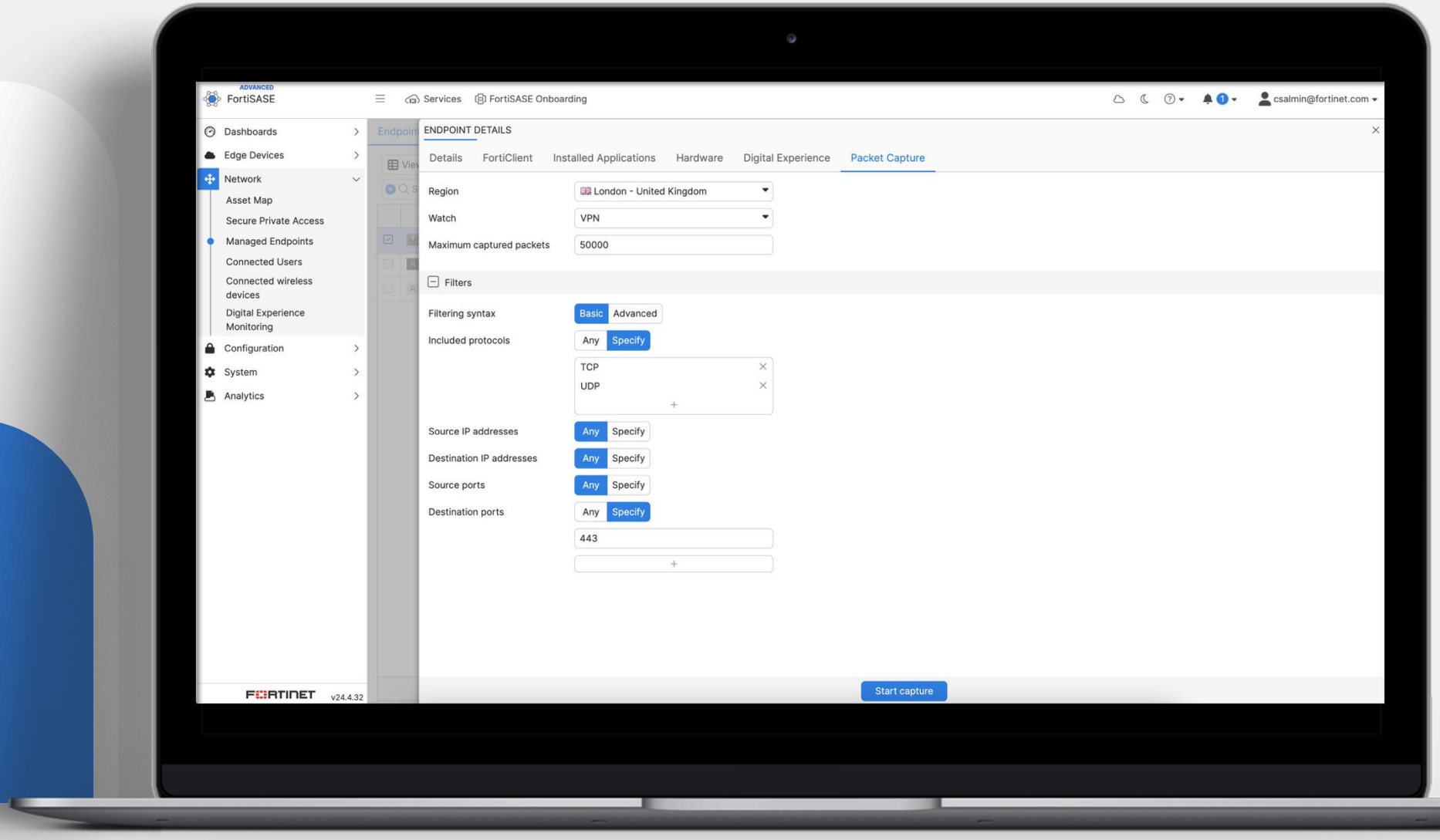
Packet Capture on FortiSASE Security PoP

The Challenge

- Currently customers admin don't have visibility of what's happening at PoP level
- Require Fortinet TAC to troubleshoot

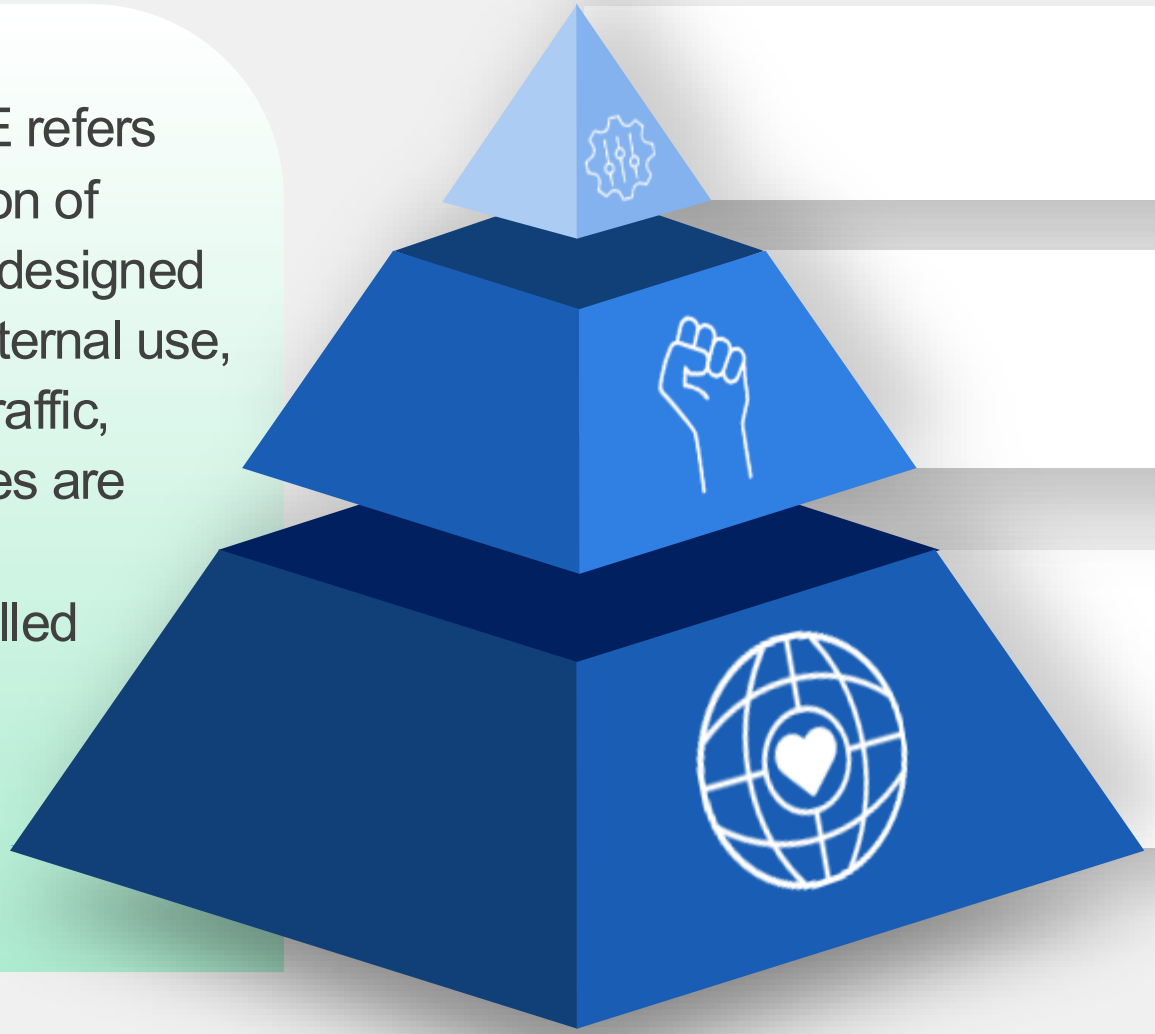
The Solution

- Run packet capture at Security PoP level
- IT admin can do initial troubleshooting before contacting Fortinet



What is Sovereign SASE

Sovereign SASE refers to the privatization of SASE services, designed for internal or external use, where all data, traffic, logs, and services are managed within customer-controlled infrastructure



Customizable Services

- Autonomy over architecture
- Customized to customer requirements

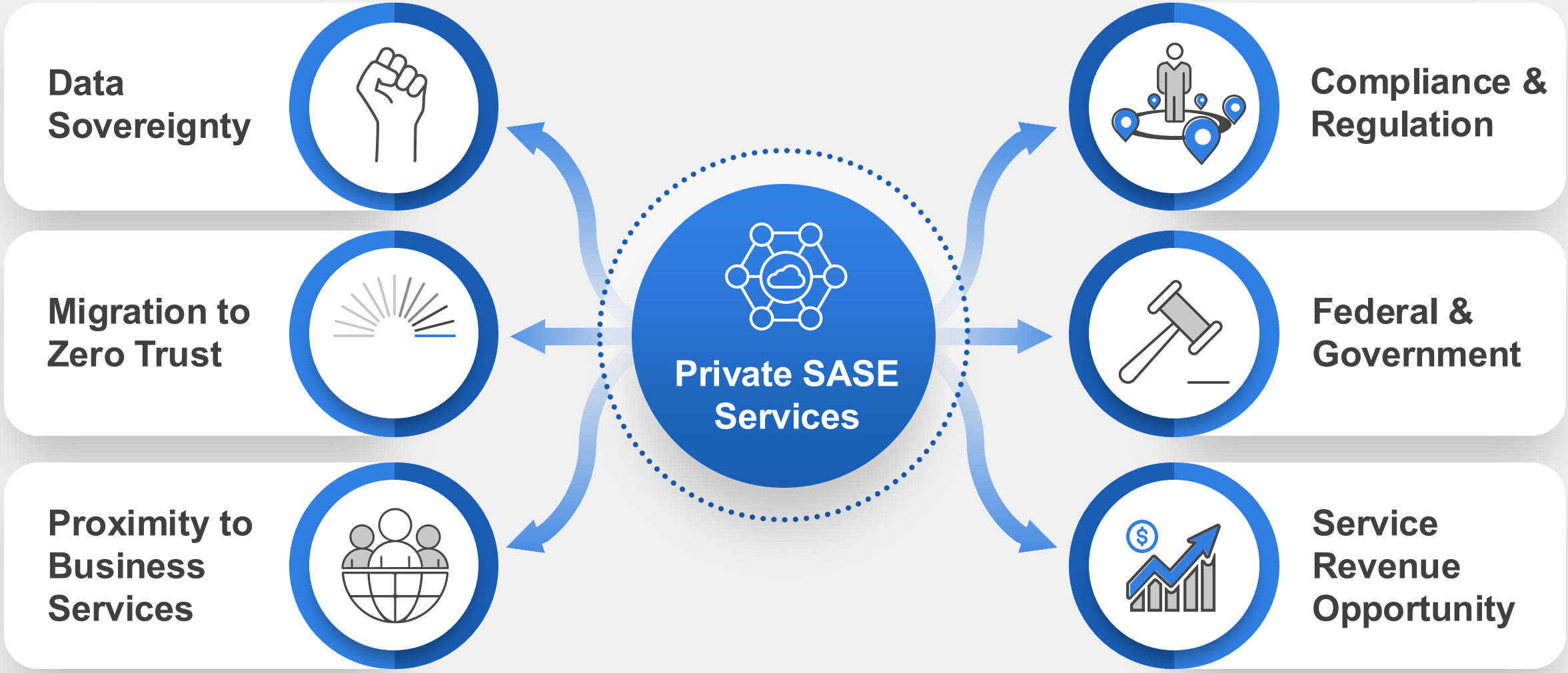
Controlled Infrastructure

- Data plane and security inspection
- Proximity to business services

Data Sovereignty

- Ownership and control over data and logs
- Data and logs stay private, within customer environment

Sovereign SASE Use Cases




FORTINET