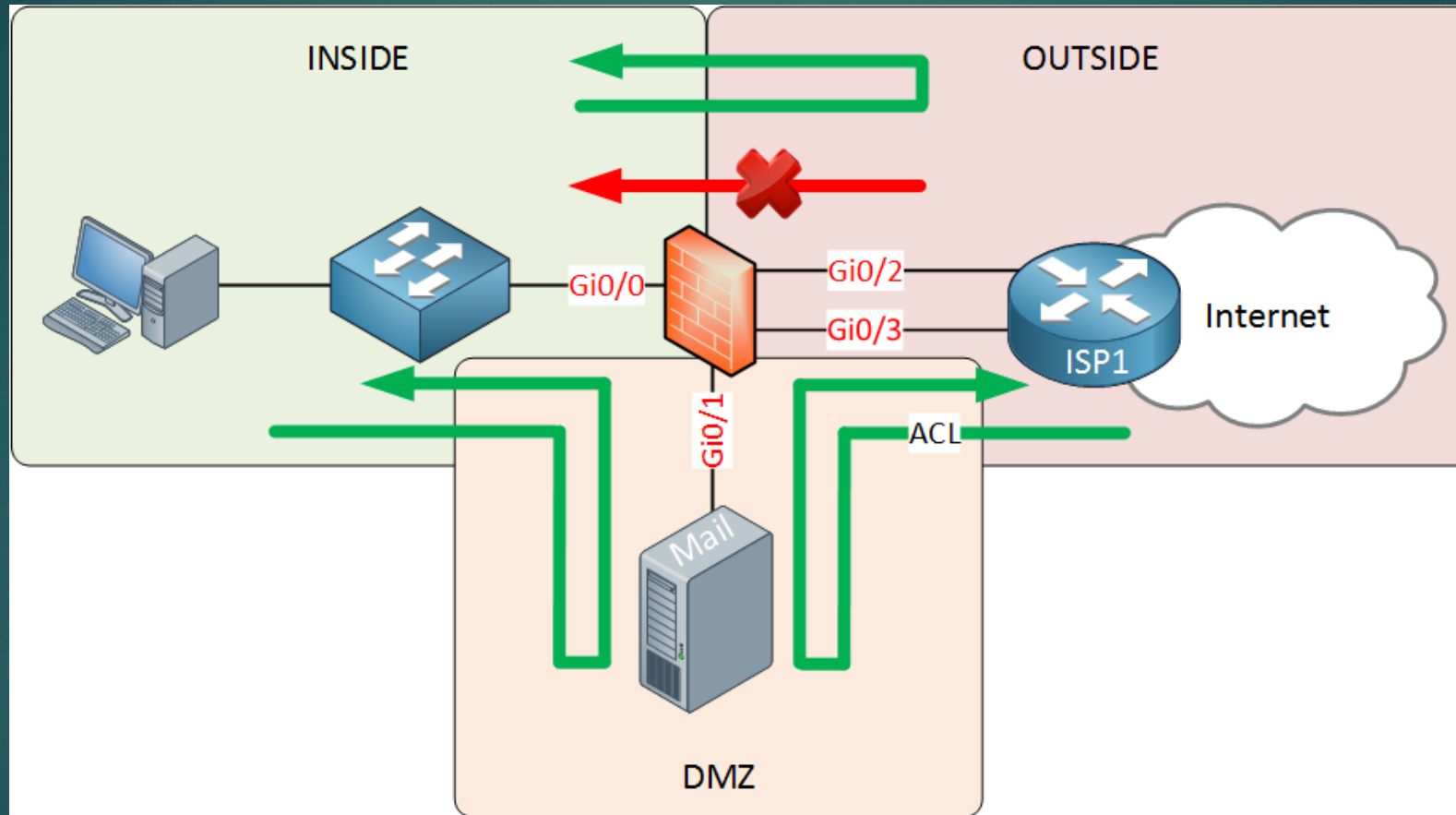




# NextGenerationSec

UNO SCORCIO AD UN FUTURO GIA' .....PASSATO

# Diciamo che partiamo almeno da qui





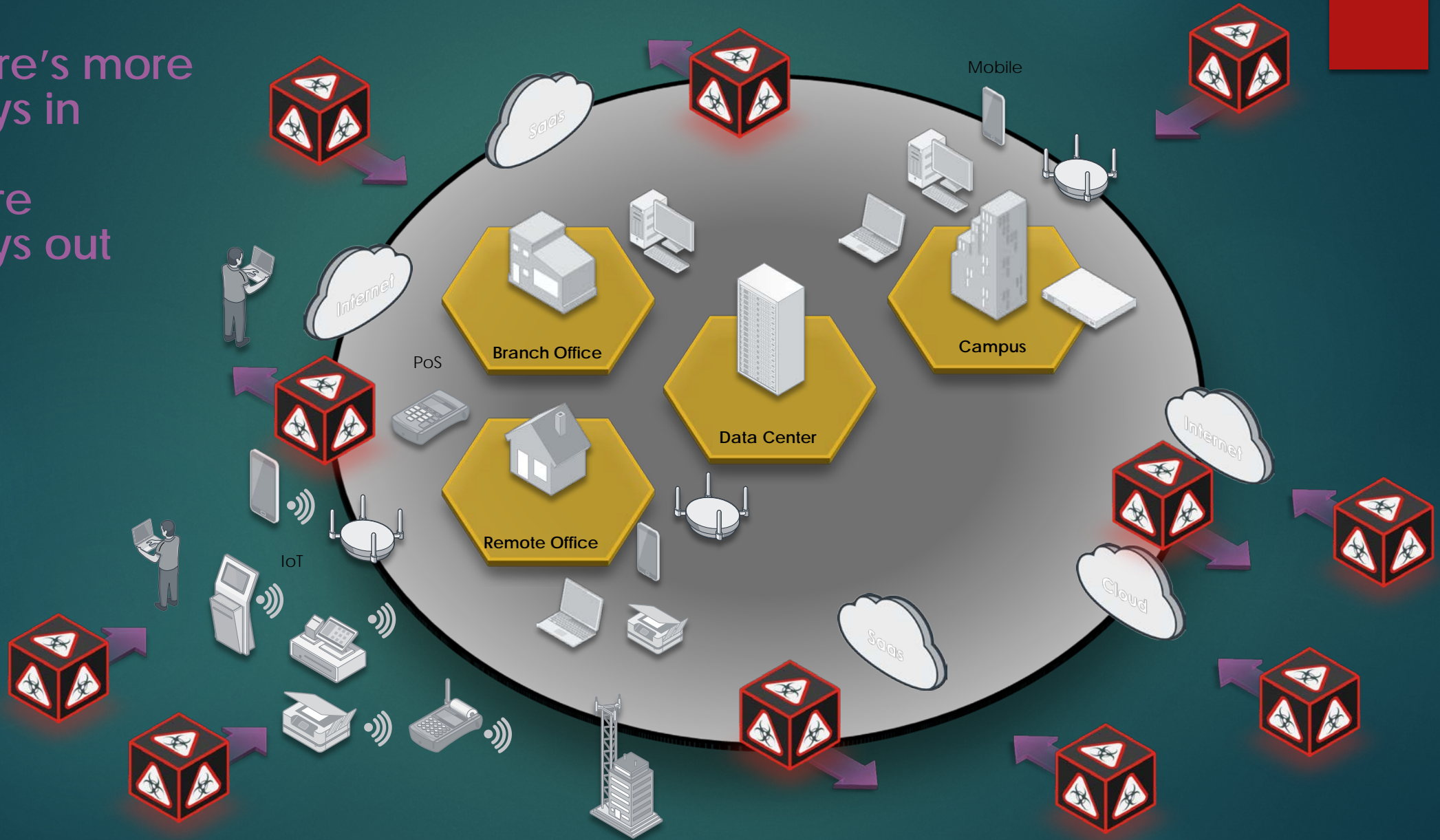




# Borderless Attack Surface










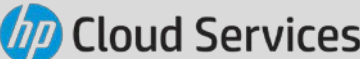















There's more  
ways in

More  
ways out



# Open – The Fabric allows integration of other security technologies



SDN/NFV	Cloud	Endpoint
    	    	 
Management	Systems Integrator	SIEM
    	  	    

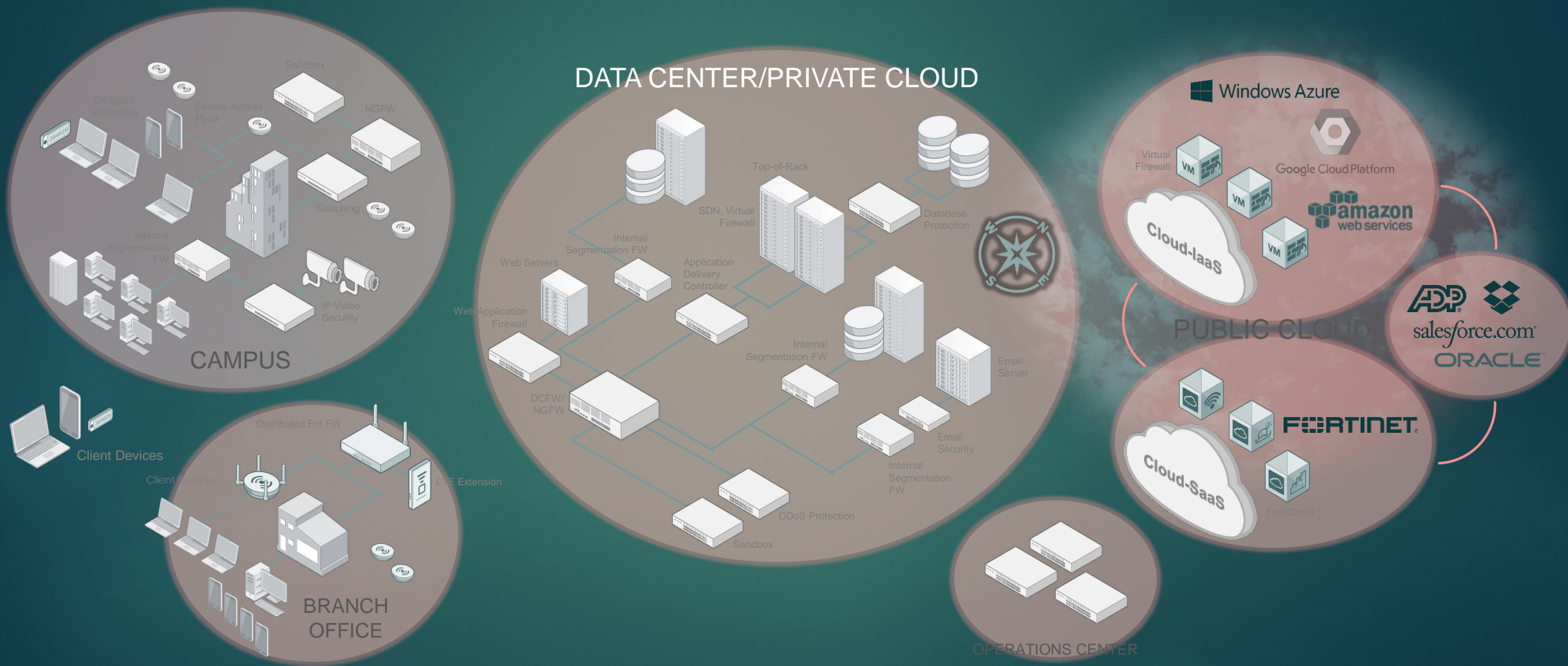
Alliances Partners





# THE FORTINET SECURITY FABRIC REALIZED

# FORTINET SECURITY FABRIC

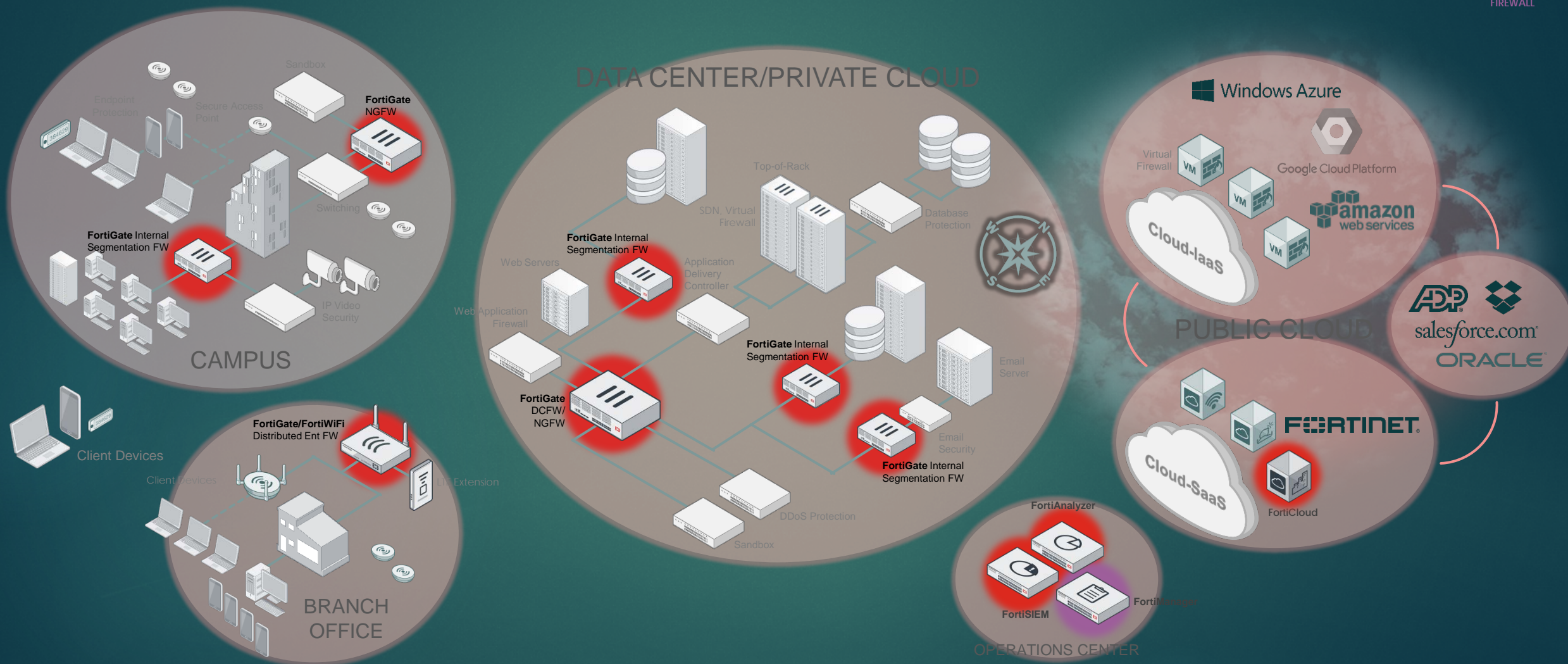




# FORTINET SECURITY FABRIC

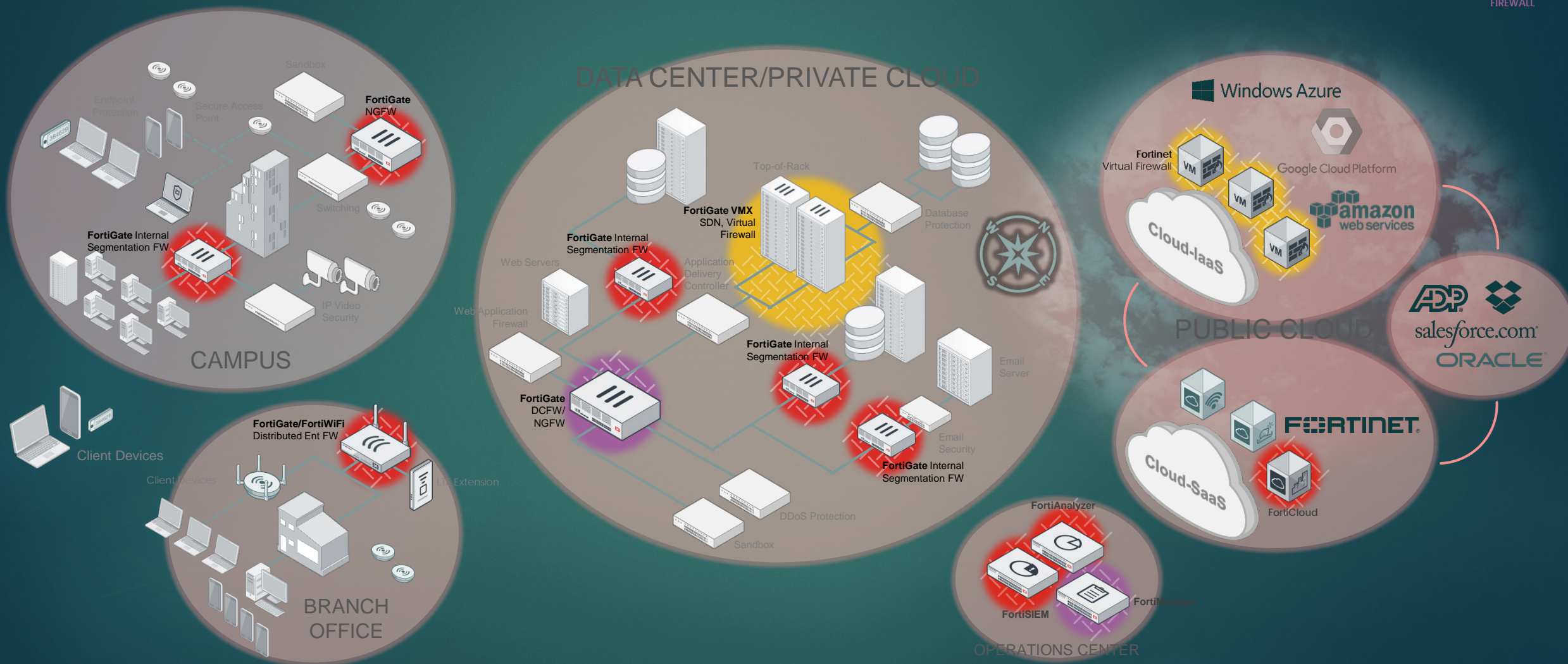


ENTERPRISE  
FIREWALL



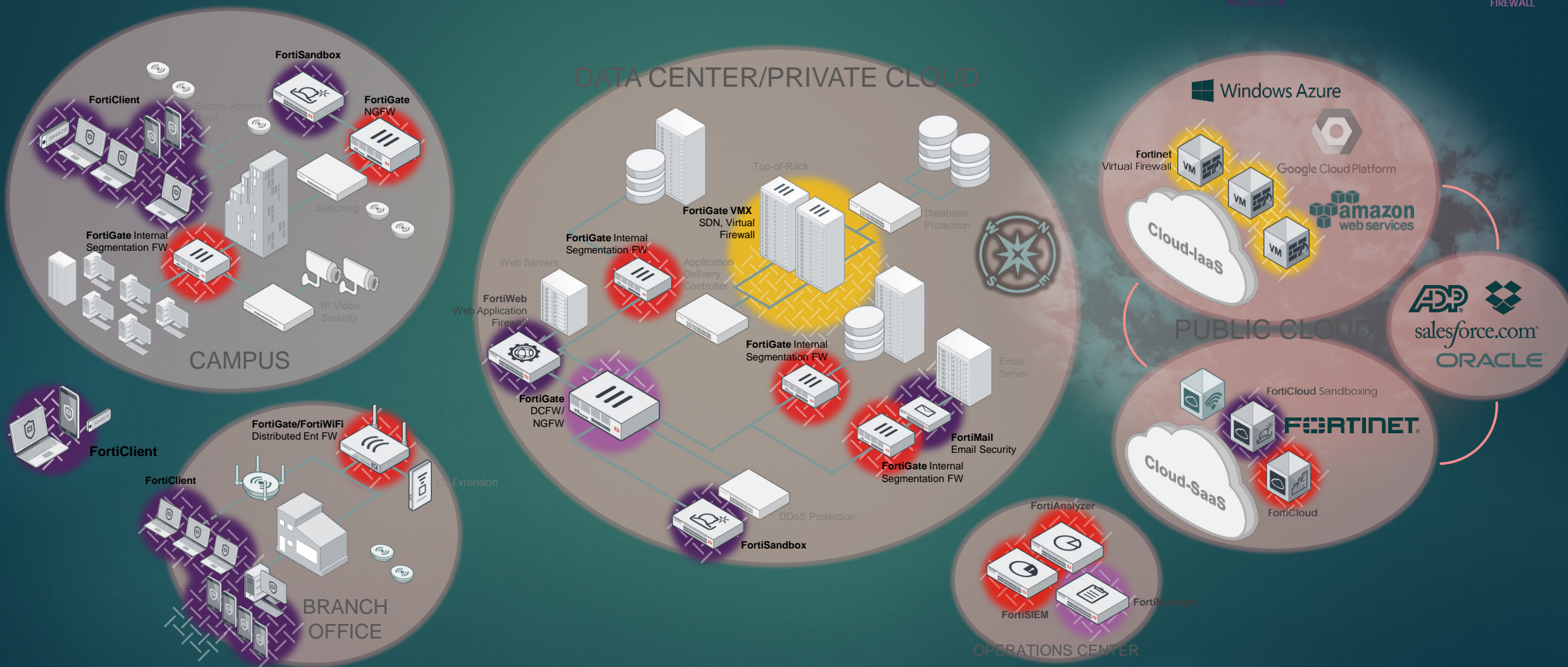


# FORTINET SECURITY FABRIC





# FORTINET SECURITY FABRIC





# FORTINET SECURITY FABRIC



APPLICATION  
SECURITY



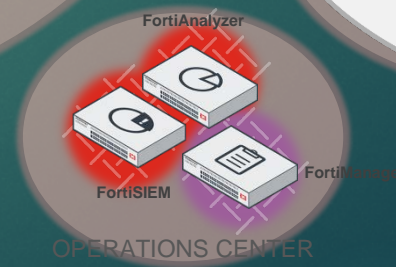
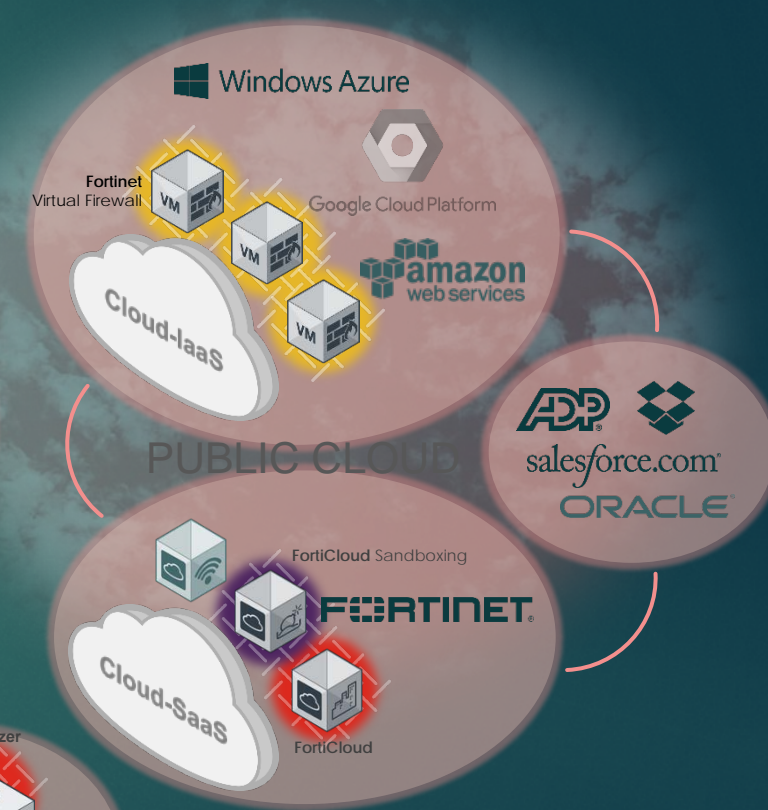
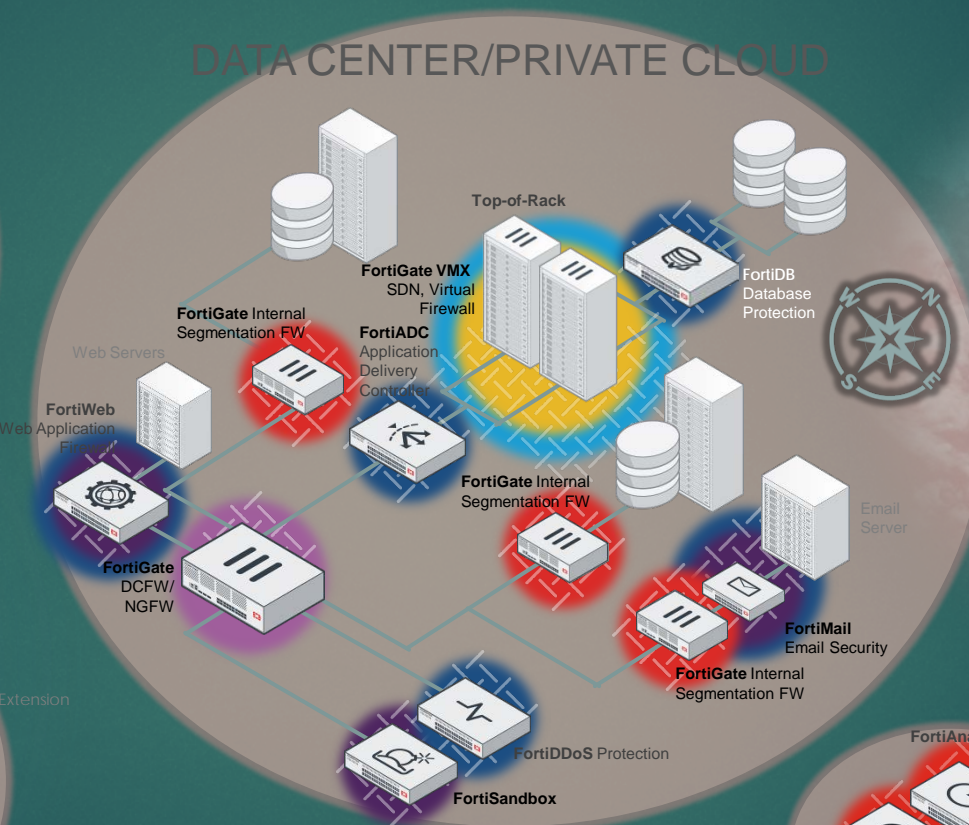
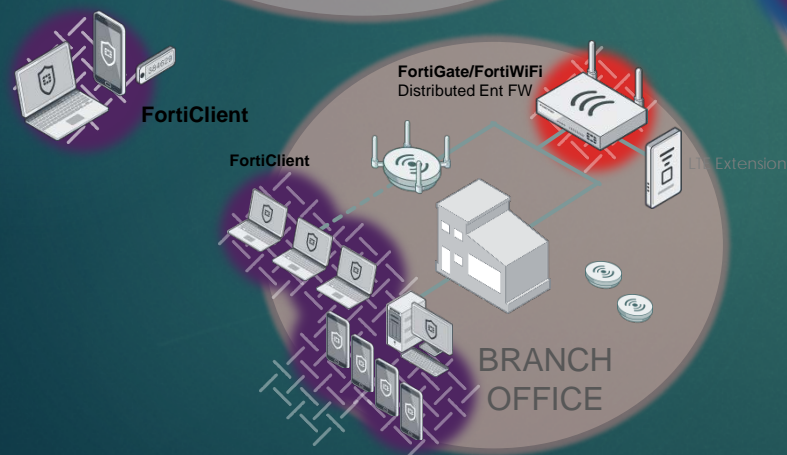
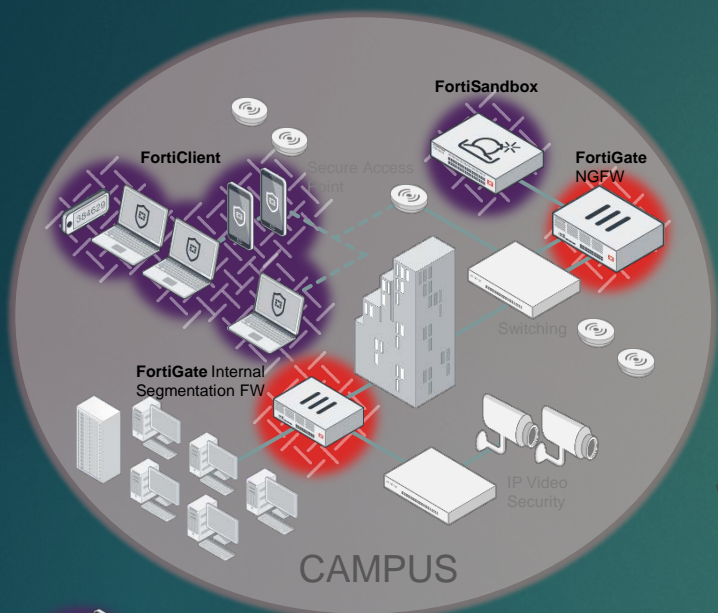
ADVANCED THREAT  
PROTECTION



CLOUD SECURITY



ENTERPRISE  
FIREWALL





# FORTINET SECURITY FABRIC



SECURE ACCESS



APPLICATION  
SECURITY



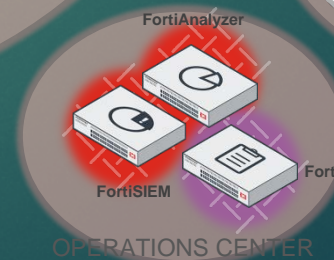
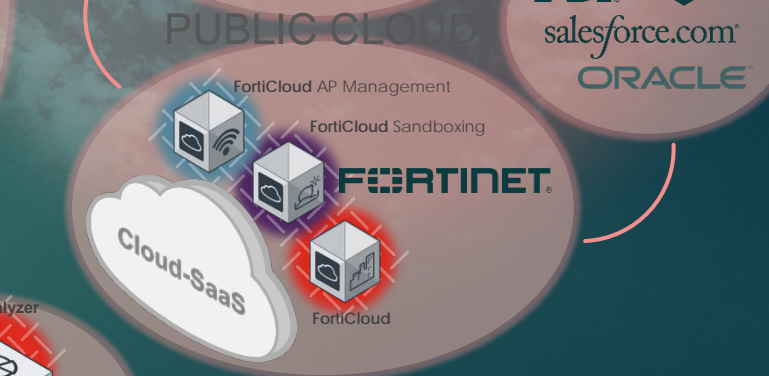
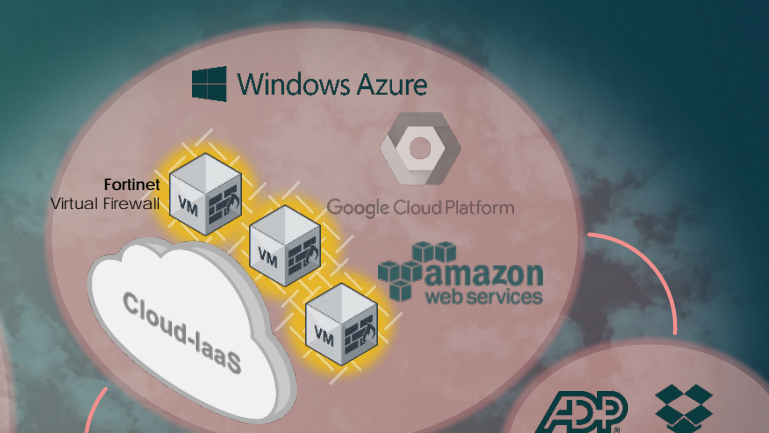
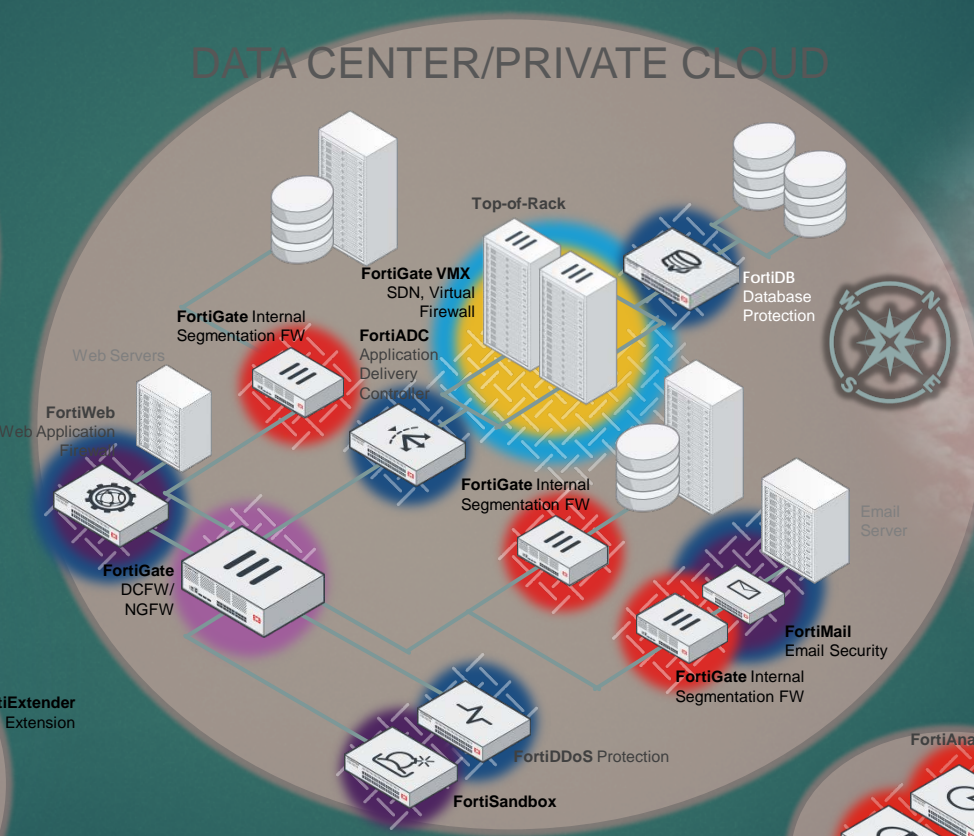
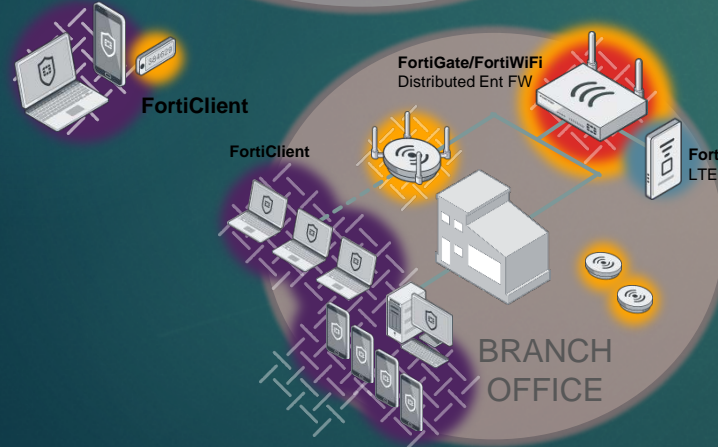
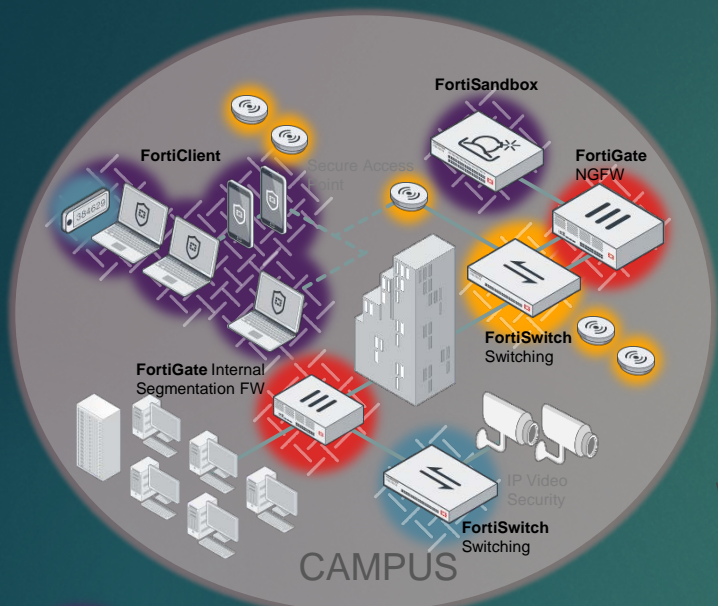
ADVANCED THREAT  
PROTECTION



CLOUD SECURITY

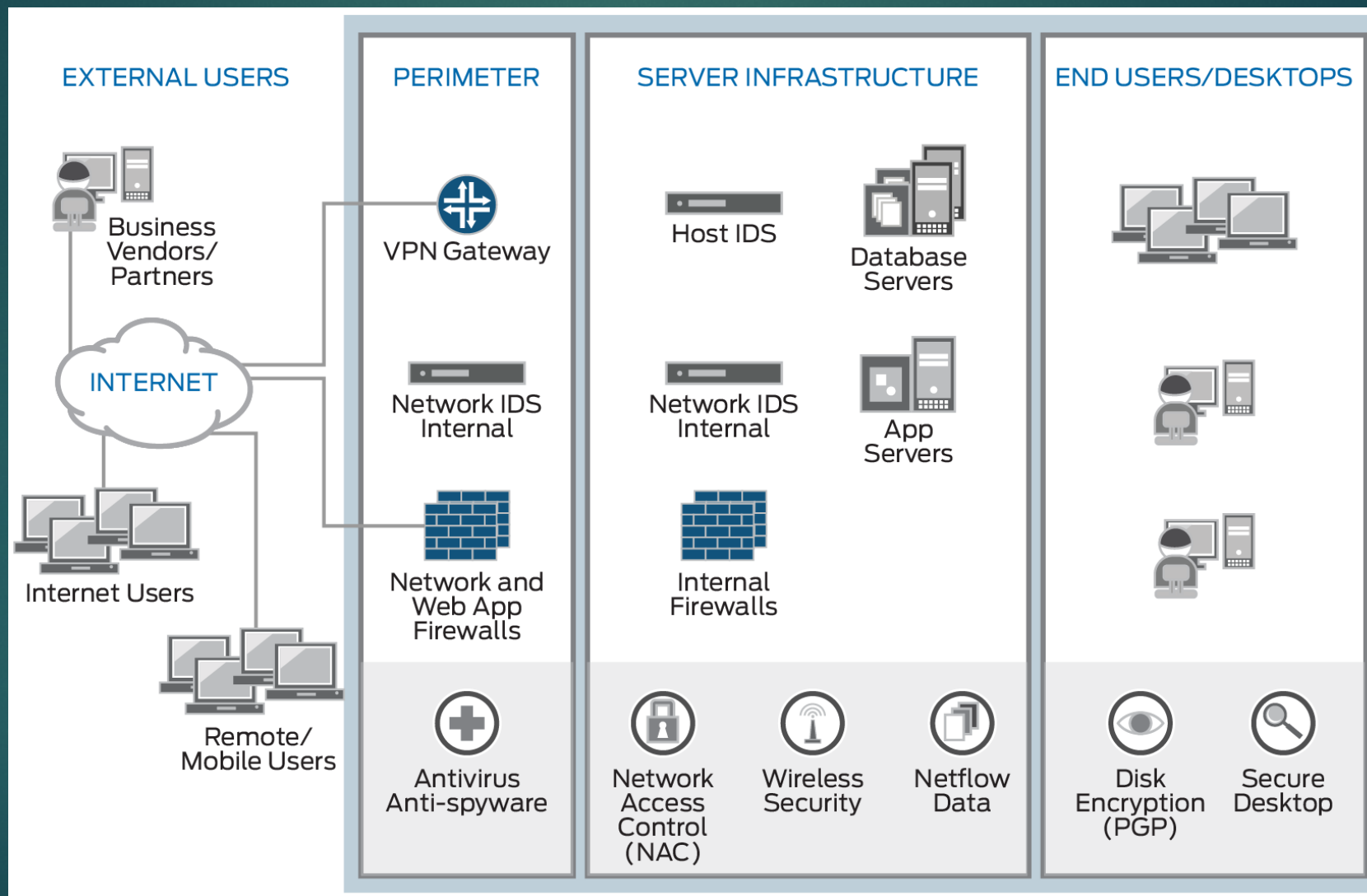


ENTERPRISE  
FIREWALL

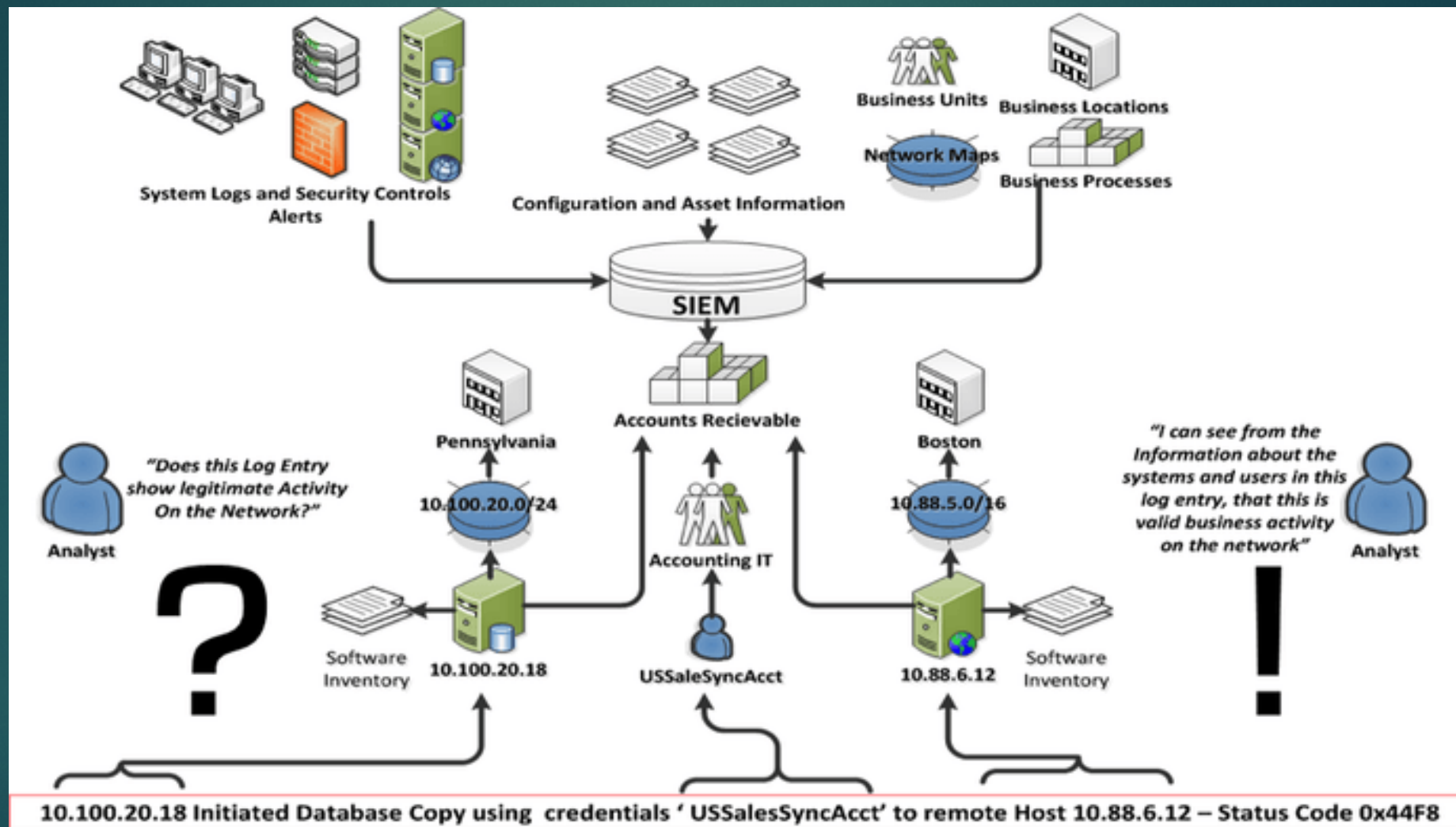




# SIEM



# SIEM





# CRITICAL CONTROL

## Solution Provider Poster Sponsors

Through their sponsorship, the technology providers below helped bring this poster to the SANS community. Sponsorship had no connection with the rankings of product measurement capabilities.

 <b>accelops</b>	<b>Going Beyond SIEM</b>
 ALLEN WEST	<b>CIS Critical Security Controls – Accelerated &amp; Simplified</b>
	<b>Securing the Enterprise – Enterprise-wide, Standards-based Continuous Monitoring of Automated Security Controls</b>
	<b>Maintaining Continuous Compliance – A New Best-Practice Approach</b>
 <b>LogRhythm</b> The security operations company	<b>The Ransomware Threat: A How-To Guide on Preparing for and Detecting an Attack Before It's Too Late</b>
	<b>Top 7 Security Controls to Prioritize</b>
	<b>Attack Your Attack Surface – How to Reduce Your Exposure to Cyber Attacks with an Attack Surface Visualization Solution</b>
 <b>Symantec</b>	<b>2016 Internet Security Threat Report</b>
 <b>tenable</b> network security	<b>CIS Critical Security Controls: Technical Control Automation</b>

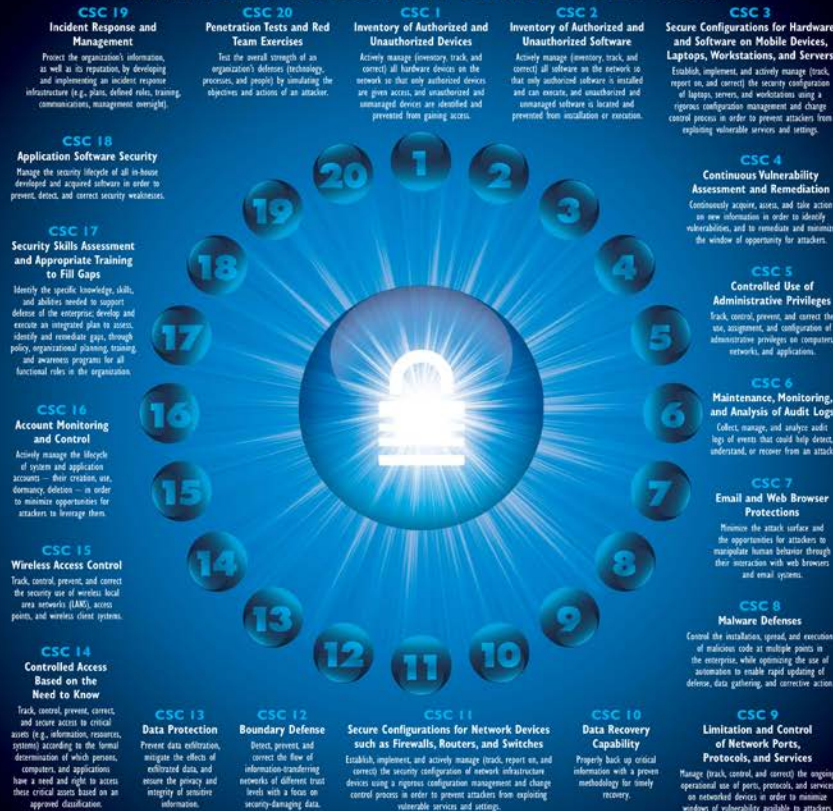
# SANS

# Monitoring and Measuring the CIS Critical Security Controls

## POSTER

*Products and Strategies for  
Continuously Monitoring and  
Improving Your Implementation of the  
CIS Critical Security Controls*

THE CENTER FOR INTERNET SECURITY (CIS)  
**CRITICAL SECURITY CONTROLS V6.0**



## The CIS Critical Security Controls Are the Core of the NIST Cybersecurity Framework

In February 2011, the President issued Executive Order (EO) 13526, Improving Critical Infrastructure Cybersecurity, directing National Institute of Standards and Technology (NIST) to develop a voluntary framework based on existing standards. This has become known as the NIST Cybersecurity Framework or CSF. At the time this poster was produced (Summer 2014) Version 1.0 was the latest version, but NIST has announced that revisions based on community comments would be released in 2017.

Like all frameworks, the NIST CSF does not specify any priority of security controls or recommend sequences of actions. That is where the Critical Security Controls shine – they map directly to the CSF core requirements and provide a realistic and community-driven risk management approach for making sure your security program will be both effective and efficient against real-world threats.

The chart below maps the Center for Internet Security (CIS) Critical Security Controls (Version 3.0) into the most relevant NIST CSF (Version 1.0) Core Functions and Categories. If you are using the NIST CSF, the mapping (thanks to James Tarala) lets you use the Critical Security Controls to prioritize measuring and monitoring the most important core NIST Framework elements.

CS Critical Security Controls (CIS)	NIST Core Framework	Cybersecurity Framework (CSF) Core				
		Identify	Protect	Detect	Respond	Recover
1 Inventory of Authorized and Unauthorized Devices	CM.1.1 CM.1.2 CM.1.3 CM.1.4	AM				
2 Inventory of Authorized and Unauthorized Software	CM.1.2 CM.1.4	AM				
3 Secure Configuration of End-User Devices	PR.1.1	IP				
4 Continuous Vulnerability Assessment & Remediation	DM.1.1 PR.1.2 DE.1.1 DE.1.2 DE.1.3	RA		CM	MI	
5 Controlled Use of Administrative Privileges	PR.4.1 PR.4.2 PR.4.3 PR.4.4	AC				
6 Patch Management, Monitoring, and Analysis of Audit Logs	PR.1.1 DE.1.1 DE.1.2 DE.1.3 DE.1.4 DE.1.5		AE	AN		
7 Email and Web Browser Protection	PR.1.1	PT				
8 Firewall Defense	PR.1.2 DE.1.4 DE.1.5	PT	CM			
9 Limitation & Control of Network Ports, Protocols, and Services	PR.4.5 DE.4.1	IP				
10 Data Recovery Capability	PR.4.1					RP
11 Secure Configuration of Network Devices	PR.1.1 PR.1.3 PR.1.4	IP				
12 Boundary Defense	PR.1.2 PR.1.5 PR.1.6 DE.1.1		DF			
13 Data Protection	PR.1.1 PR.1.2 PR.1.3 PR.1.4	DS				
14 Controlled Access Based on Need to Know	PR.1.4 PR.1.5 PR.1.6	AC				
15 Wireless Access Control		AC				
16 Account Monitoring and Control	PR.4.1	AC	CM			
17 Security Skills Assessment and Appropriate Training	PR.1.1 PR.1.3 PR.1.4 PR.1.5 PR.1.6	AT				
18 Application Software Security	PR.1.1 PR.1.4 PR.1.5	IP				
19 Incident Response and Management	PR.1.1 DE.1.1 DE.1.2 DE.1.3 DE.1.4 DE.1.5 DE.1.6 DE.1.7 DE.1.8 DE.1.9		AE	RP		
20 Penetration Tests and Red Team Exercises				RM	RM	

## Defining Continuous Monitoring

National Institute of Standards and Technology (NIST) 800-137 is the U.S. government's guide to "Information Security Continuous Monitoring for Federal Information Systems and Organizations." It defines continuous monitoring as:	Frequency (FedRAMP) 800-53 Control	CS Critical Security Control
Continuous and Ongoing Auditable Events	(U) Maintenance, Monitoring, Analysis of Logs	
Continuous Assessment	(U) Assessment of Process	

	“... ongoing measures of information security, vulnerability, and threat” to support organizational risk management decisions. The terms “threats” and “ongoing” in this context mean that security controls and organizational risks are assumed and analyzed as a frequency response to support risk-based security decisions to adequately protect performance information. Data collection, to make low frequency, is performed at discrete intervals.”	
		<p>Component Inventory (1) Inventory of Devices</p> <p>Incident Response (17) Incident Response and Management</p> <p>Vulnerability Scanning (4) Continuous Vulnerability Assessment &amp; Remediation</p> <p>Audit Review Report (8) Performance, Monitoring, Analysis of Logs</p> <p>Vulnerability Scanning (4) Continuous Vulnerability Assessment &amp; Remediation</p>
		<p>Security Policy Management (6) Continuous Monitoring, Analysis of Logs</p>

<p>The SIMS simplified version of this is as:</p> <ul style="list-style-type: none"> <li>Establish and measure <b>meaningful security metrics</b></li> <li>Monitor those metrics <b>frequently enough to minimize incident impact</b></li> <li>Take <b>action rapidly, efficiently and effectively</b> to improve overall security</li> </ul>	<p>Security Issue Monitoring (1) Maintenance, Monitoring, Response or Logs</p> <p>File Remediation (2) Secure Configurations</p> <p>Schedule/Role Integrity (3) Software Inventory</p> <p>Asset Functionality (4) Location &amp; Control of Network Ports, Services</p>
---	---

The CFI Critical Security Groups have proven to be an effective starting point for selecting your security metrics. It frequent question "Is this frequency a continuous?" NST 100-131 points to get another security document, SP 800-17 "Guide to Applying the Risk Management Framework to Federal Information Systems," for a risk-based methodology for making this decision. But there is an easier way.

## Collecting Meaningful Security Data – Monitoring the Right Stuff

Security monitoring has no value on its own unless it leads to meaningful action to prevent or reduce damage from cyber attacks. More prevention, faster detection, and more accurate response require measuring different CS Critical Security Controls to reduce vulnerabilities, detect and mitigate attacks, and optimize incident response and restoration. SANS has mapped the Critical Controls across the CyberDefense lifecycle.



### PREVENTION METRICS

should include both quantity and time – how quickly you detect new misconfigurations, vulnerabilities, attacks.



**REACTION/RESOLUTION METRICS**  
How long is direct vs. indirect?  
How long is to investigate/resolve?

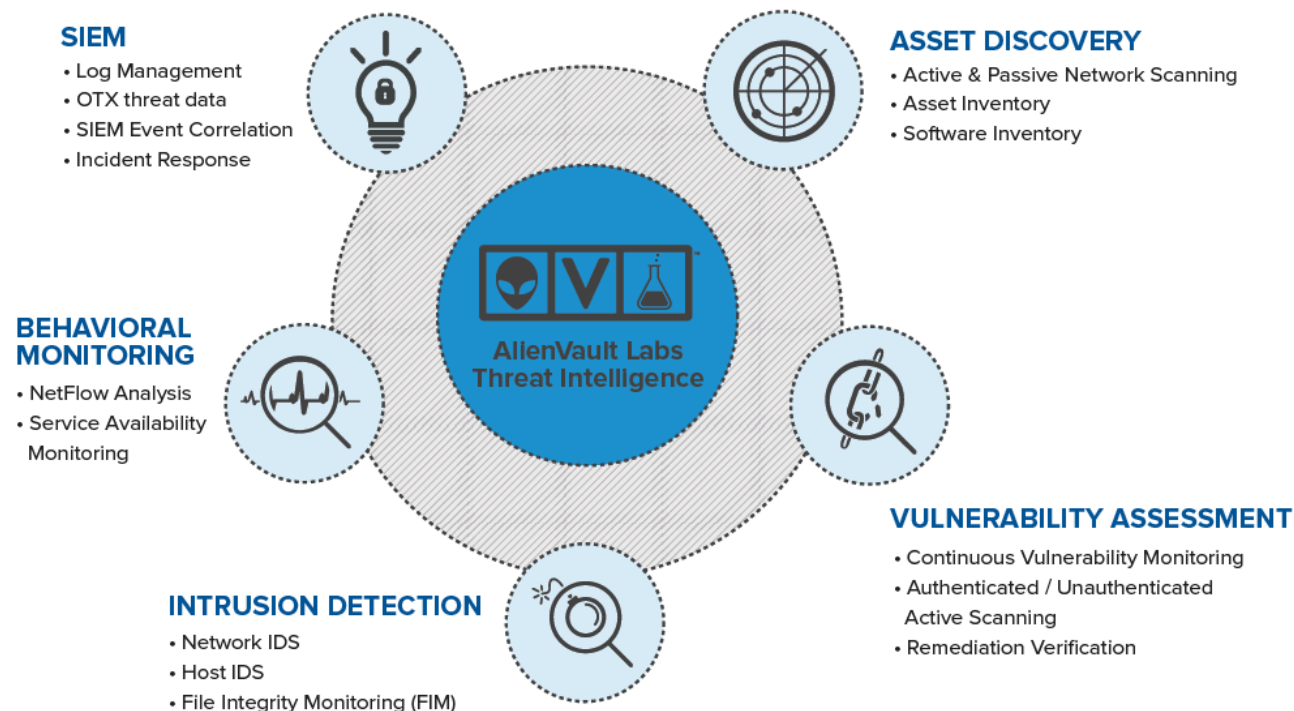


# SANS White paper OSSIM



Interested in learning  
more about security?

## AlienVault USM™



## SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

### OSSIM: CIS Critical Security Controls Assessment in a Windows Environment.

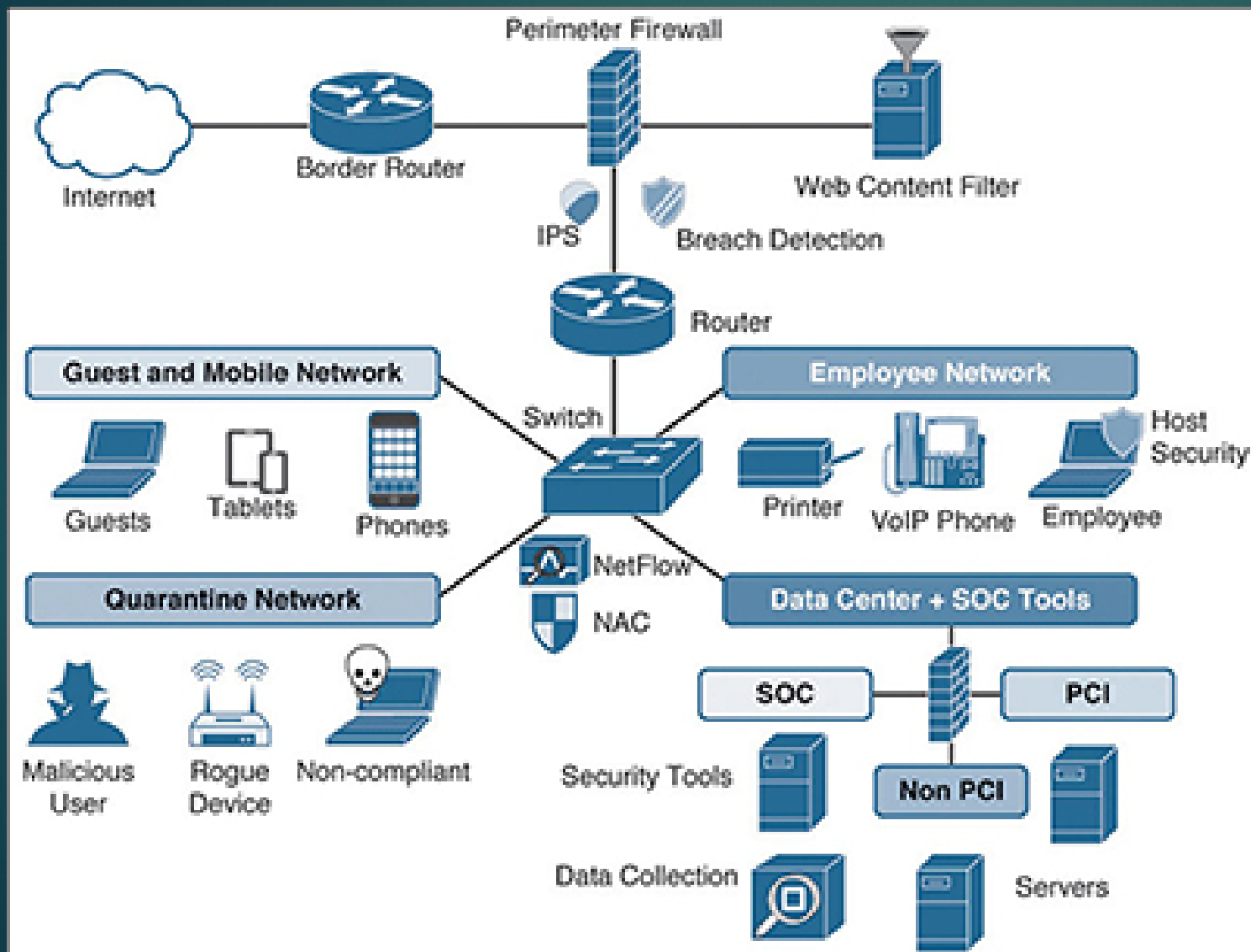
Use of a Security Information and Event Management (SIEM) or log management platform is a recommendation common to several of the CIS Critical Security Controls For Effective Cyber Defense (2016). Because the CIS Critical Security Controls (CSC) focus on automation, measurement and continuous improvement of control application, a SIEM is a valuable tool. AlienVault's Open Source SIEM (OSSIM) is free and capable, making it a popular choice for administrators seeking experience with SIEM. While there is a great de...

Copyright SANS Institute  
Author Retains Full Rights

DEEPAARMOR®



# SOC



ciscopress.com

## 5 Steps to Building and Operating an Effective Security Operations Center (SOC)

Date: Dec 21, 2015 By [Joseph Muniz](#)

Joseph Muniz, co-author of [Security Operations Center: Building, Operating, and Maintaining Your SOC](#), provides a high-level overview of the steps involved in creating a security operations center to protect your organization's valuable data assets.

As security threats in the wild continue to advance in capabilities, demand increases for organizations to develop a Security Operations Center (SOC, pronounced sock). Relying on basic security solutions such as firewalls and anti-virus software is not good enough; this minimal approach is equivalent to protecting a bank merely by locking the front door. Cyber security requires layers of defenses, similar to how a bank protects valuables with a security strategy that includes cameras, guards, safes, and other measures beyond locking the front door. Layering cyber security solutions requires somebody to be responsible for enabling and maintaining security, which leads to the demand for a SOC.

### NOTE

For detailed discussion of all the topics reviewed in this article, see my book [Security Operations Center: Building, Operating, and Maintaining Your SOC](#).

### Starting the SOC Conversation

The biggest challenge in starting the conversation about the need for a SOC is justifying the cost to people who don't understand the threat landscape or the value of being proactive rather than reactive about security. According to the [2015 Verizon Data Breach Investigation Report](#), "In 60% of cases, attackers are able to compromise an organization within minutes," and "75% of attacks spread from Victim 0 to Victim 1 within one day (24 hours)." Waiting to react to a breach until after damage has been done will most likely lead to an extremely costly recovery. We have all seen in the news the amount of money lost from data breaches. Showcasing a few data breach examples from a source such as [DataLossDB](#) will surely make your point.

One way to help justify the SOC budget is by posing the following questions to the organization's leadership:

- How can you detect a compromise?
- How do you judge the severity of the compromise?
- What is the impact of the compromise to your organization?
- Who is responsible for detecting and reacting to a compromise?
- Who should be informed or involved, and when do you deal with a compromise once it is detected?
- How and when should you communicate a compromise internally or externally? (Note that sometimes engaging the authorities is required by law.)

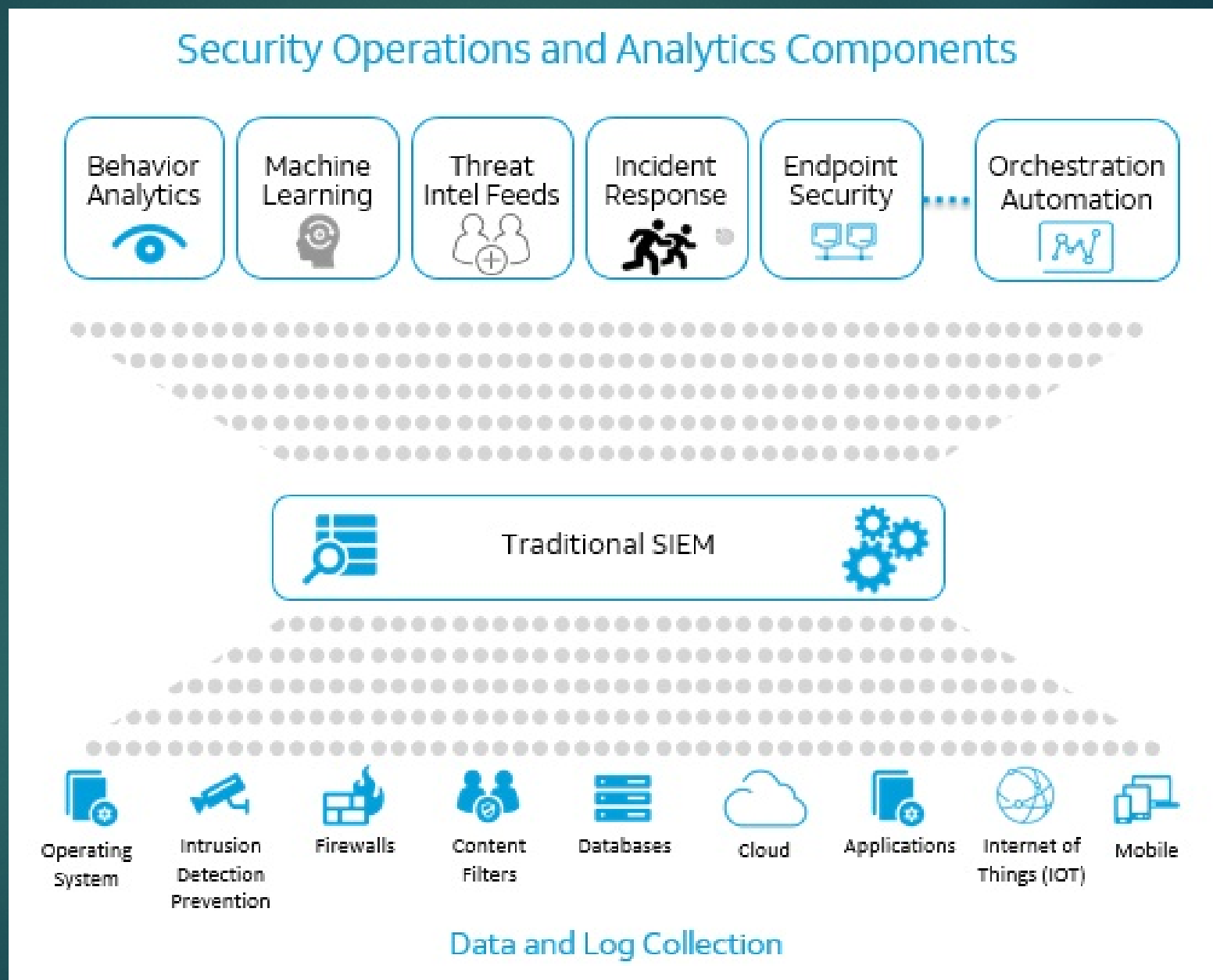
These questions are designed to make the organization's leadership think about the impact of an incident and judge their existing cyber security capabilities. Many organizations find that they need to develop a better incident-response plan—one that requires a group within the organization to be responsible for it. That group should be the SOC.

Five major steps are involved in developing a SOC:

1. Planning the SOC.
2. Designing the SOC.
3. Building the SOC.
4. Operating the SOC.
5. Reviewing the SOC.

The following sections review the actions required in each step of SOC development.

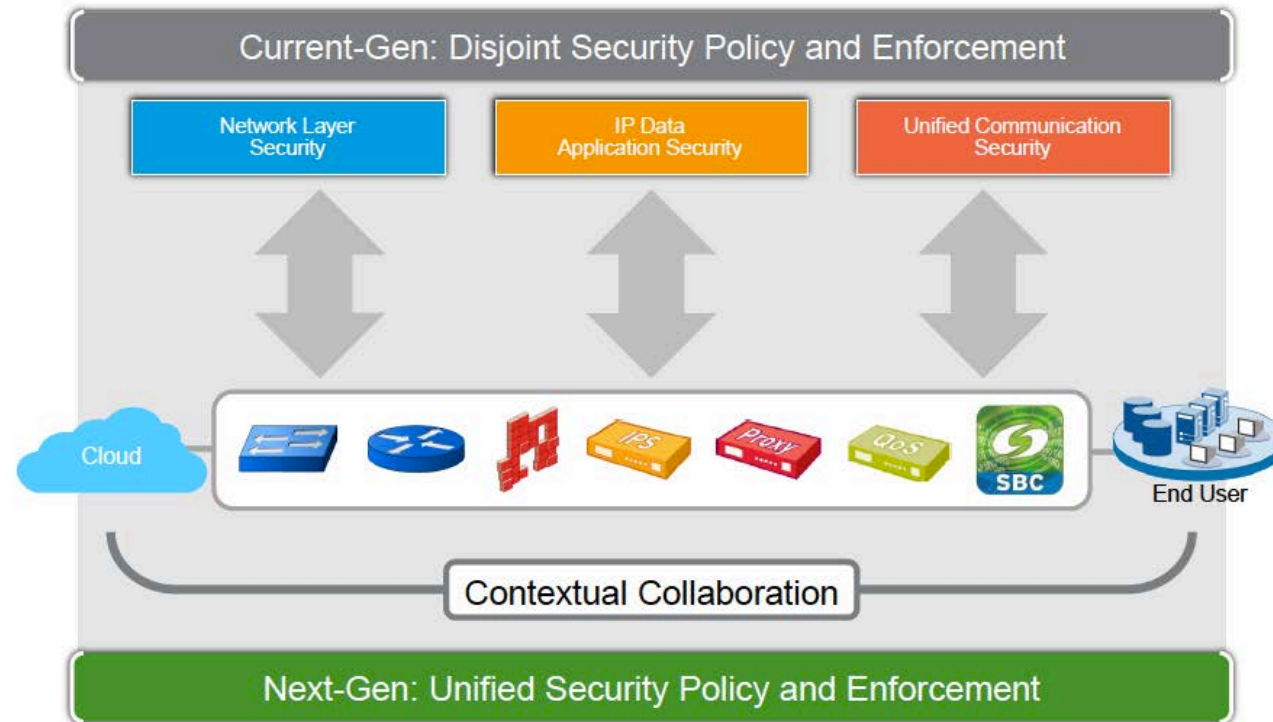
# SOAPA





# Firewall distribuiti

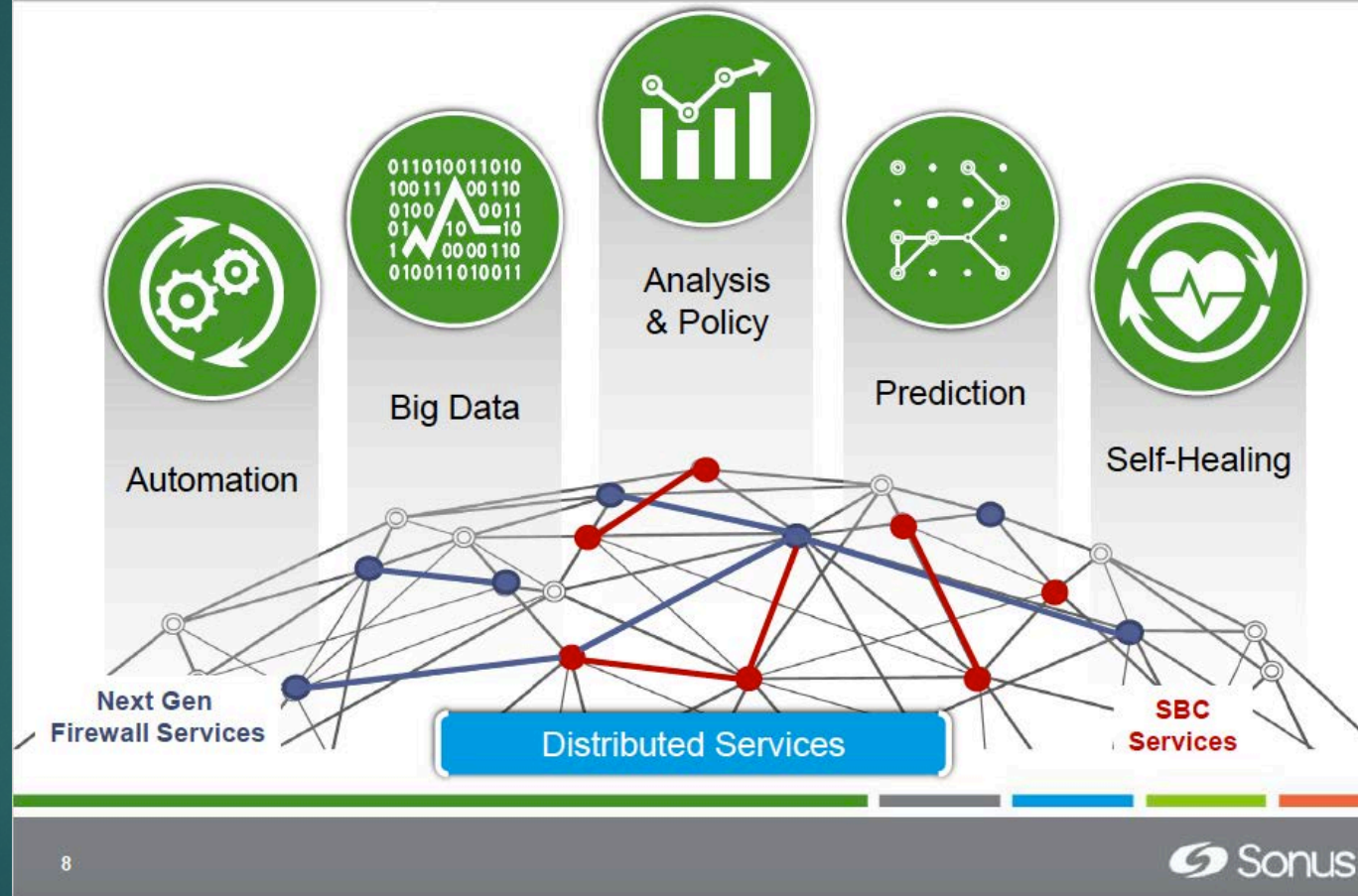
## Unifying the Security Stack





# Firewall distribuiti

## The DNA of the Re-Architected Security Stack

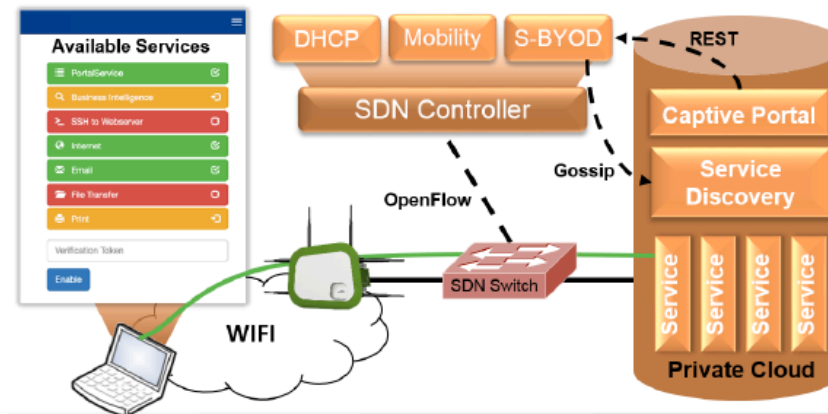




# Firewall distribuiti

## Fine-granular Access Control

- ▶ On-demand personalized virtual network
  - BYOD scenario
  - Strict flow isolation
  - Minimized attack surface
- ▶ Technical implementation
  - 2FA Authentication
  - No MDM required

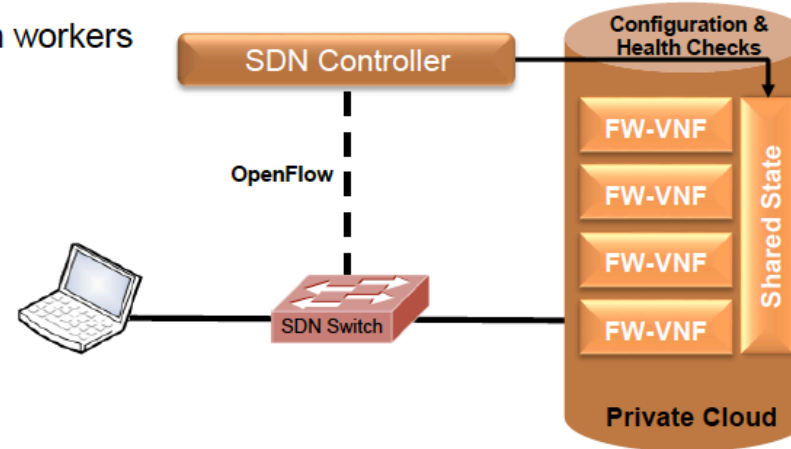




# Firewall distribuiti

## Scalable & Resilient Stateful Firewalling

- ▶ NFV-based stateful firewall
  - Run as software in the cloud
  - Dynamic n+1 protection
- ▶ Technical implementation
  - SDN switch as load balancer
  - State decoupled from workers



# Firewall distribuiti

## Demo Setup



[https://www.youtube.com/watch?v=e\\_CmcGPXJGY](https://www.youtube.com/watch?v=e_CmcGPXJGY)



# Firewall distribuiti

## Sources

- ▶ Michael Jarschel, Thomas Zinner, Tobias Hoßfeld, Phuoc Tran-Gia, Wolfgang Kellerer, **Interfaces, Attributes, and Use Cases: A Compass for SDN**, *IEEE Communications Magazine*, 52, 2014
- ▶ Gebert, S., Zinner, T., Gray, N., Durner, R., Lorenz, C., Lange, S., **Demonstrating a Personalized Secure-By-Default Bring Your Own Device Solution Based on Software Defined Networking**, *International Teletraffic Congress (ITC 28)*, 2016
- ▶ Lorenz, C., Hock, D., Scherer, J., Durner, R., Kellerer, W., Gebert, S., Gray, N., Zinner, T., Tran-Gia, P., **An SDN/NFV-enabled Enterprise Network Architecture Offering Fine-Grained Security Policy Enforcement**, *IEEE Communications Magazine*. 55, 217 - 223 (2017)
- ▶ Gray, N., Lorenz, C., Müssig, A., Gebert, S., Zinner, T., Tran-Gia, P., **A Priori State Synchronization for Fast Failover of Stateful Firewall VNFs**, *Workshop on Software-Defined Networking and Network Function Virtualization for Flexible Network Management, SDNFlex 2017*
- ▶ Pfaff B., Scherer J., Hock D., Gray N., Zinner T., Tran-Gia P., Durner R., Kellerer R., Lorenz C., **SDN/NFV-enabled Security Architecture for Fine-grained Policy Enforcement and Threat Mitigation for Enterprise**, *ACM SIGCOMM Computer Communication Review*, 2017

# From BlackHat

- ▶ Battlefield network link
- ▶ Pay no attention to the hacker behind....
- ▶ My bro the elk



# Battlefield Network

# PAY NO ATTENTION TO THAT HACKER BEHIND THE CURTAIN: *A LOOK INSIDE THE BLACK HAT NETWORK*

Neil R. Wyler

Bart Stump

@grifter801  
@theStump3r



# My Bro The ELK

Obtaining Security Context from Security Events



**Travis Smith**  
tsmith@tripwire.com