FORTINET®

Endpoint Solution Reference Architecture

Joe Martins, CISSP
Solutions Architect
Global Products & Solutions

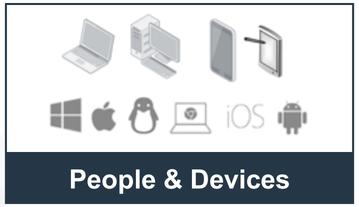
March 13, 2019

Endpoint Solutions Reference Architecture

Endpoint Solutions are a key part of Intent-Based Segmentation. (zero-trust is a subset)

People and connected devices are a key factor in protecting data not only on the endpoint but wherever the data resides in an ecosystem made up of endpoints, on premise data centers, cloud data centers and SaaS datastores.

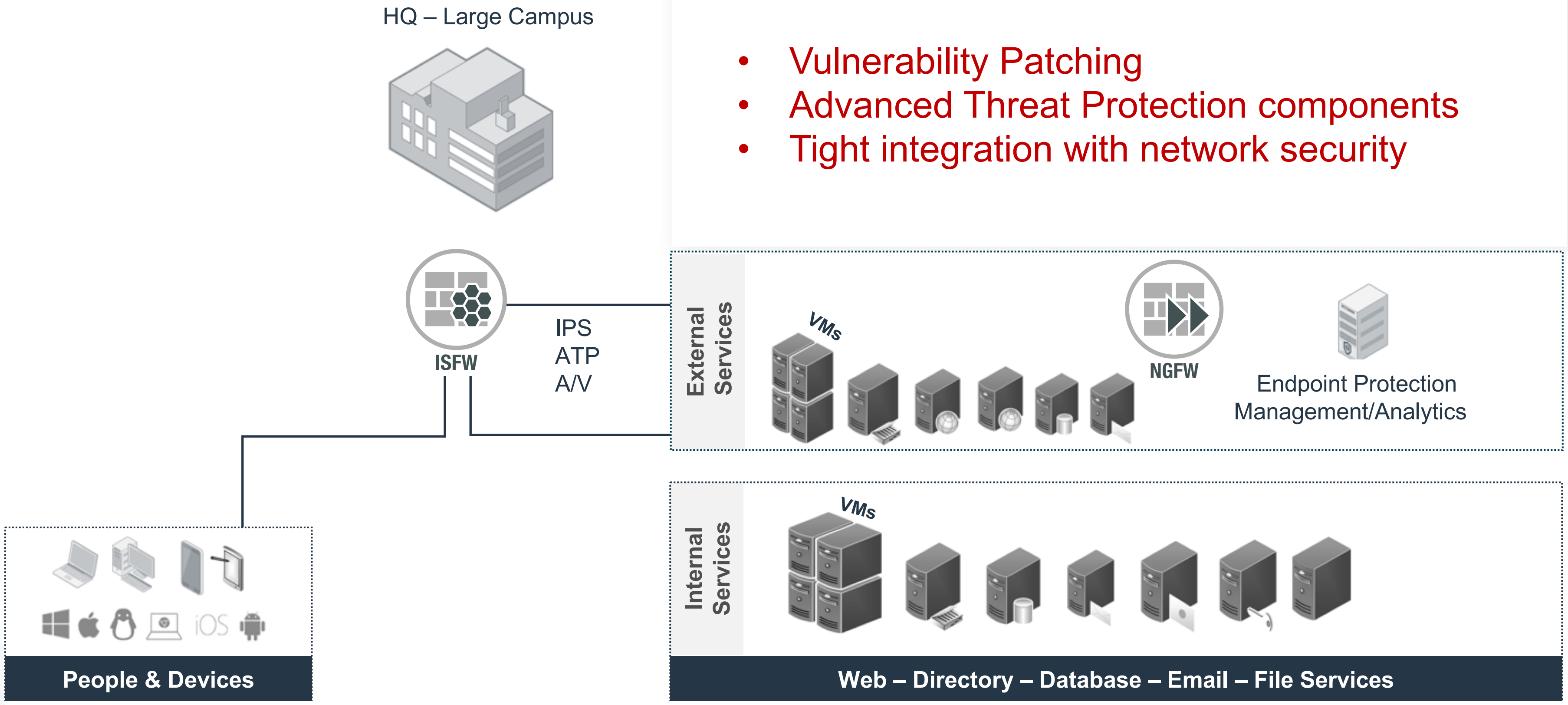
Endpoint Solutions encompass more than just antivirus and threat protection, and will include identity, network access control and other features.



Endpoint Solutions Reference Architecture

Depending on a company's infrastructure and requirements, a variety of endpoint security features may be necessary. Essential elements:

- Vulnerability Patching
- Advanced Threat Protection components
- Tight integration with network security

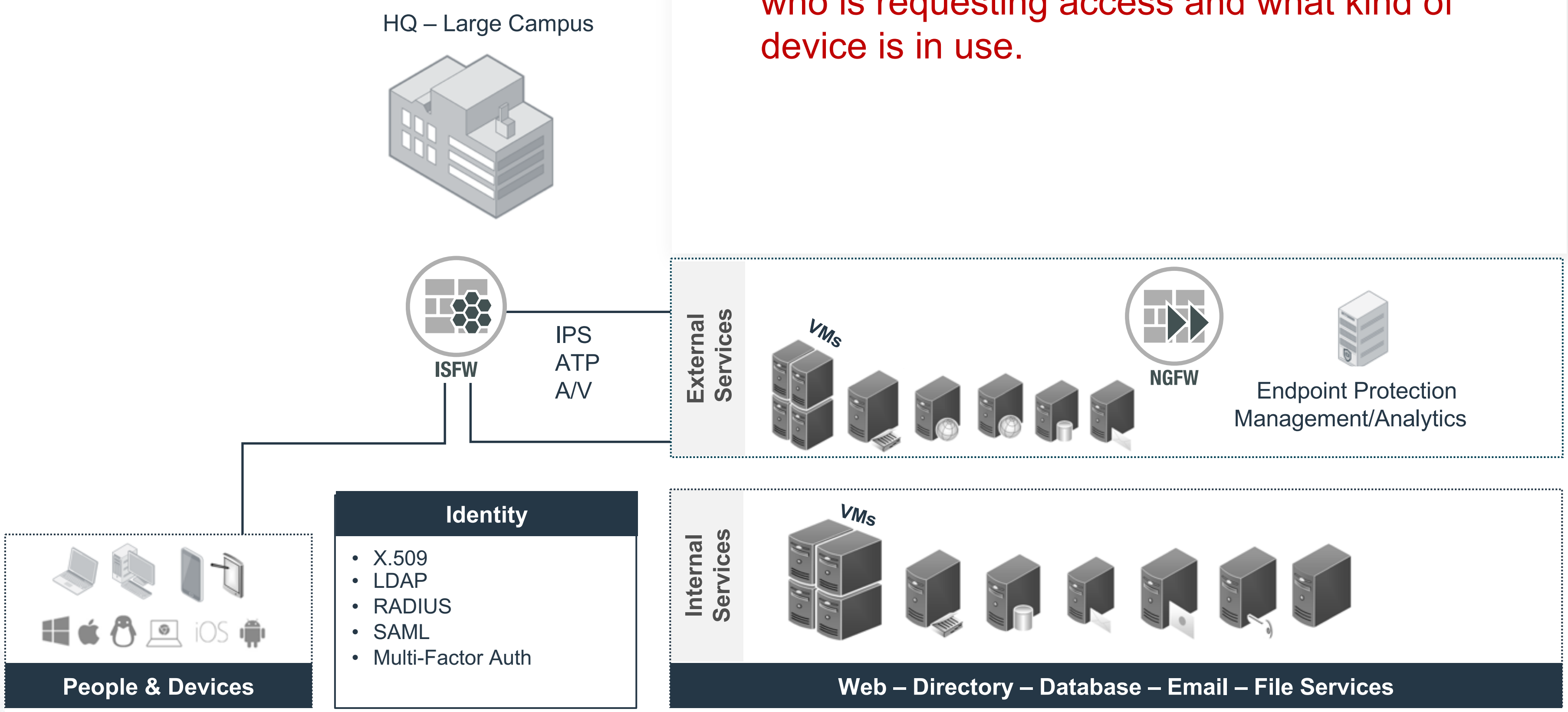


Endpoint Solutions – Features

- Fabric Connector
- Vulnerability Scanning
- Secure Access (VPN)
- Antimalware
- Web Filter
- Sandbox Connector
- Data Loss Prevention
- EDR / UEBA Components
- Identity Integration
- Host Firewall
- Application Firewall
- Host Intrusion Detection
- File Integrity Monitoring
- Network Access Control

Endpoint Solutions Reference Architecture

Identity and authorization features to detect who is requesting access and what kind of device is in use.



People & Devices

Identity

- X.509
- LDAP
- RADIUS
- SAML
- Multi-Factor Auth

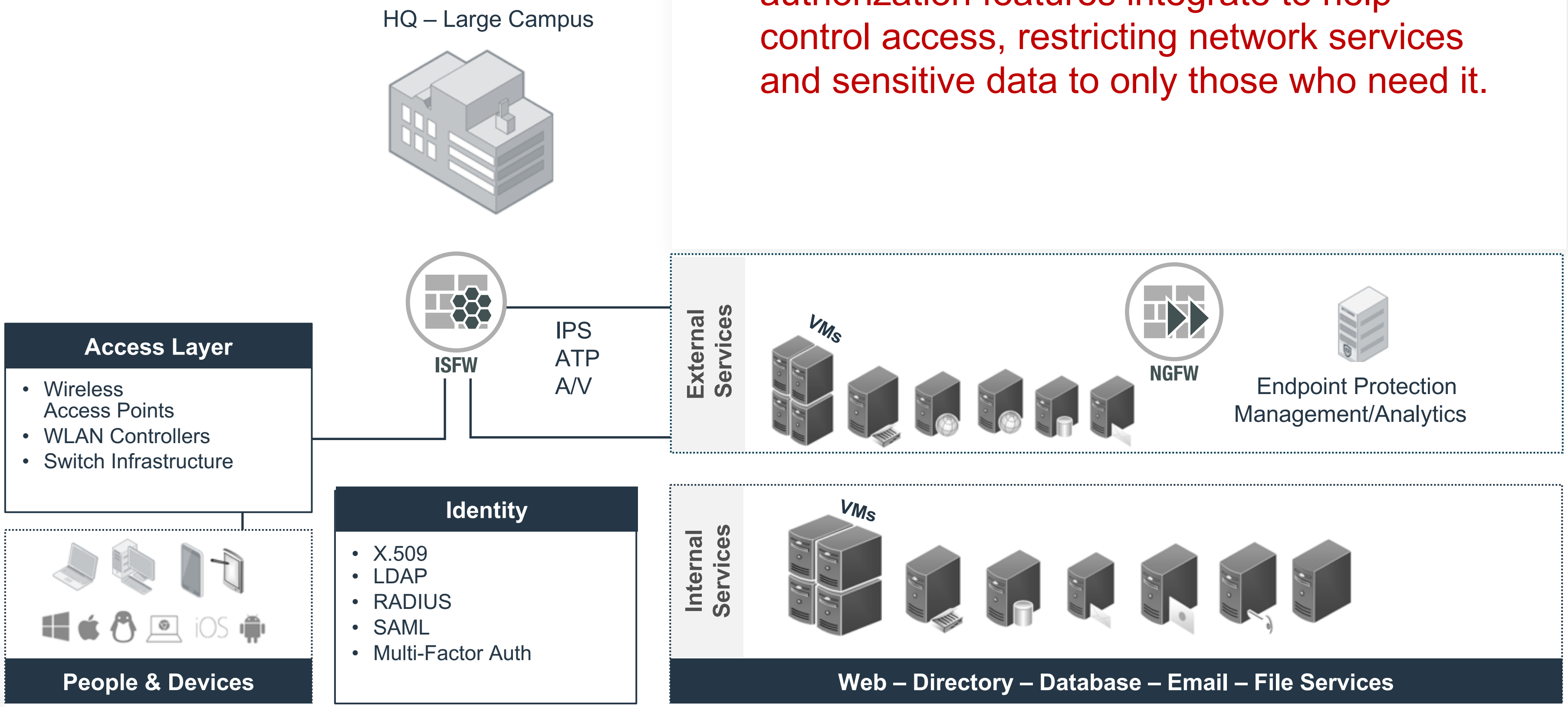
Web – Directory – Database – Email – File Services

Endpoint Solutions – Features

- Fabric Connector
- Vulnerability Scanning
- Secure Access (VPN)
- Antimalware
- Web Filter
- Sandbox Connector
- Data Loss Prevention
- EDR / UEBA Components
- Identity Integration
- Host Firewall
- Application Firewall
- Host Intrusion Detection
- File Integrity Monitoring
- Network Access Control

Endpoint Solutions Reference Architecture

In the Access Layer, identity and authorization features integrate to help control access, restricting network services and sensitive data to only those who need it.



Access Layer

- Wireless Access Points
- WLAN Controllers
- Switch Infrastructure

People & Devices

Identity

- X.509
- LDAP
- RADIUS
- SAML
- Multi-Factor Auth

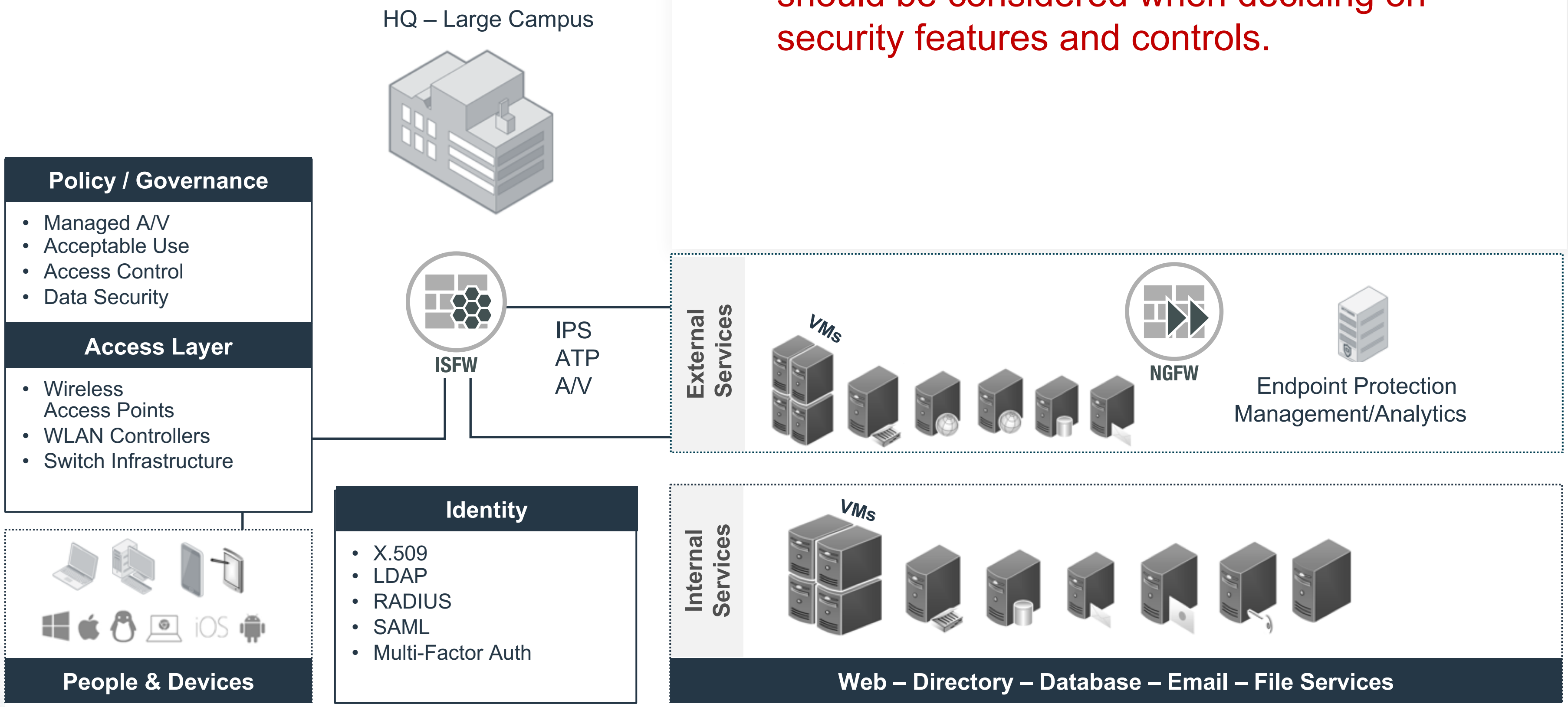
Web – Directory – Database – Email – File Services

Endpoint Solutions – Features

- Fabric Connector
- Vulnerability Scanning
- Secure Access (VPN)
- Antimalware
- Web Filter
- Sandbox Connector
- Data Loss Prevention
- EDR / UEBA Components
- Identity Integration
- Host Firewall
- Application Firewall
- Host Intrusion Detection
- File Integrity Monitoring
- Network Access Control

Endpoint Solutions Reference Architecture

Industry specific policies and governance should be considered when deciding on security features and controls.



Policy / Governance

- Managed A/V
- Acceptable Use
- Access Control
- Data Security

Access Layer

- Wireless Access Points
- WLAN Controllers
- Switch Infrastructure

People & Devices

Identity

- X.509
- LDAP
- RADIUS
- SAML
- Multi-Factor Auth

External Services

Endpoint Protection Management/Analytics

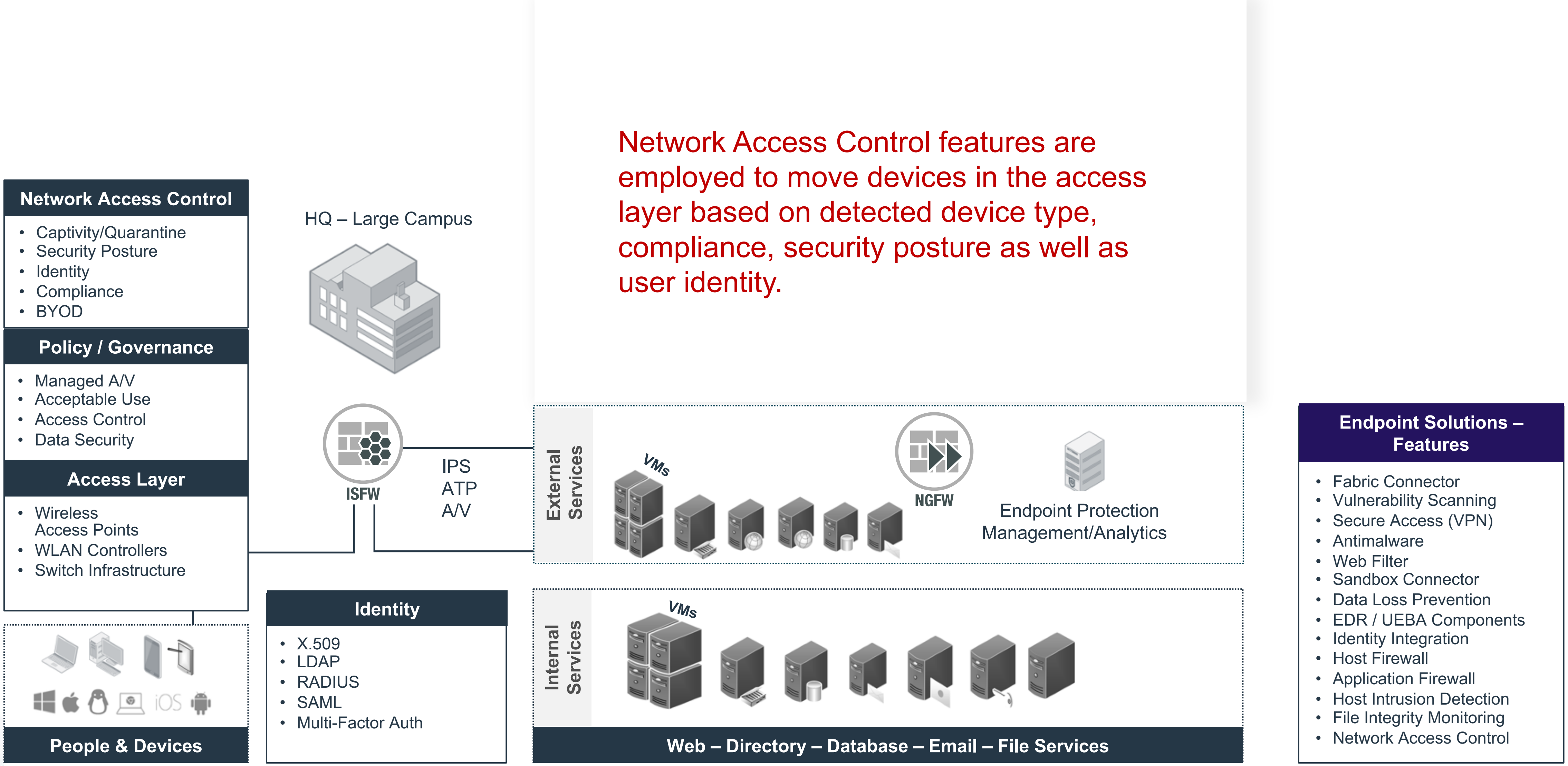
Internal Services

Web – Directory – Database – Email – File Services

Endpoint Solutions – Features

- Fabric Connector
- Vulnerability Scanning
- Secure Access (VPN)
- Antimalware
- Web Filter
- Sandbox Connector
- Data Loss Prevention
- EDR / UEBA Components
- Identity Integration
- Host Firewall
- Application Firewall
- Host Intrusion Detection
- File Integrity Monitoring
- Network Access Control

Endpoint Solutions Reference Architecture



Network Access Control features are employed to move devices in the access layer based on detected device type, compliance, security posture as well as user identity.

Network Access Control

- Captivity/Quarantine
- Security Posture
- Identity
- Compliance
- BYOD

Policy / Governance

- Managed A/V
- Acceptable Use
- Access Control
- Data Security

Access Layer

- Wireless Access Points
- WLAN Controllers
- Switch Infrastructure

People & Devices

Identity

- X.509
- LDAP
- RADIUS
- SAML
- Multi-Factor Auth

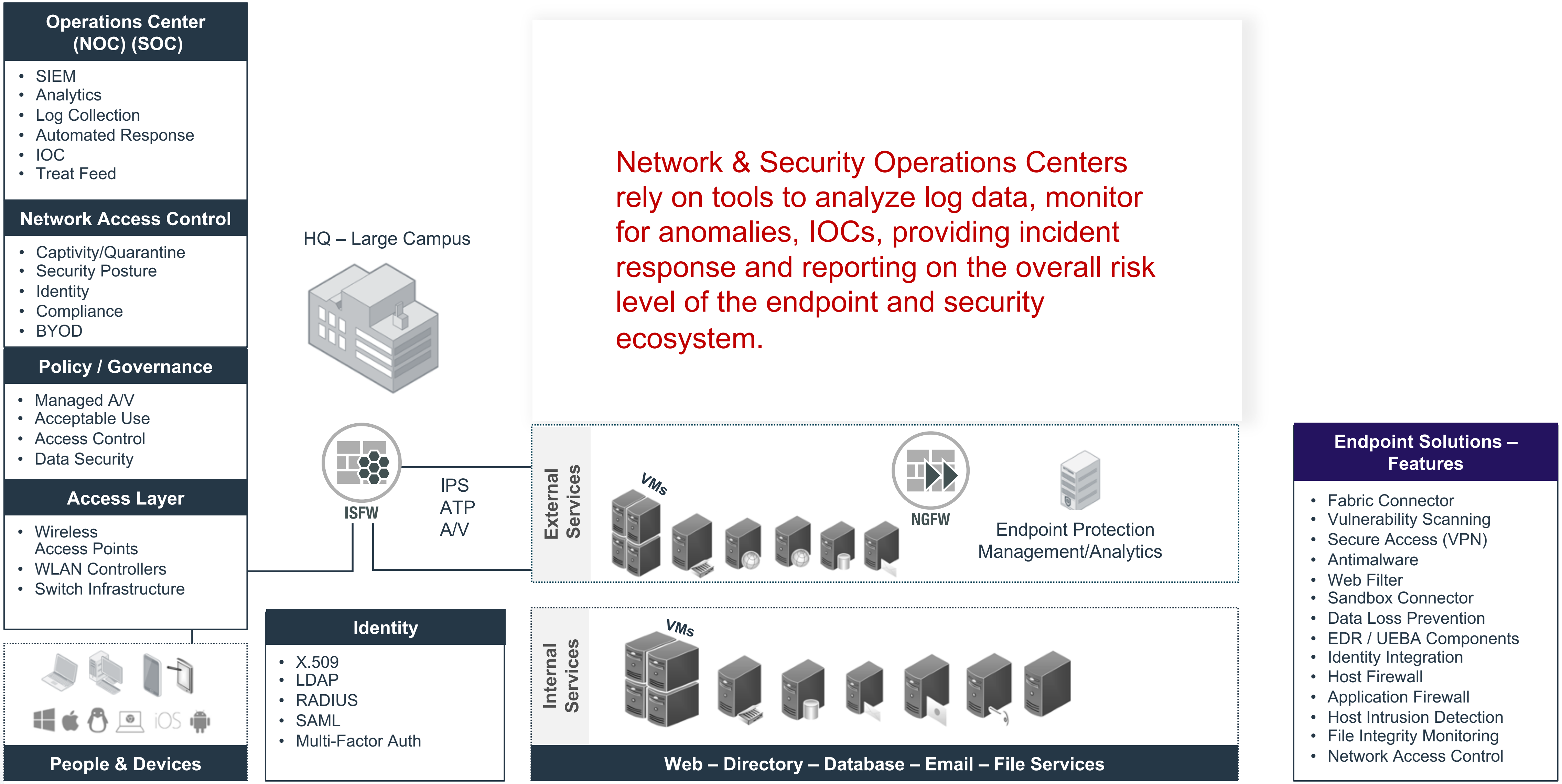
Web – Directory – Database – Email – File Services

Endpoint Protection Management/Analytics

Endpoint Solutions – Features

- Fabric Connector
- Vulnerability Scanning
- Secure Access (VPN)
- Antimalware
- Web Filter
- Sandbox Connector
- Data Loss Prevention
- EDR / UEBA Components
- Identity Integration
- Host Firewall
- Application Firewall
- Host Intrusion Detection
- File Integrity Monitoring
- Network Access Control

Endpoint Solutions Reference Architecture



Operations Center (NOC) (SOC)

- SIEM
- Analytics
- Log Collection
- Automated Response
- IOC
- Treat Feed

Network Access Control

- Captivity/Quarantine
- Security Posture
- Identity
- Compliance
- BYOD

Policy / Governance

- Managed A/V
- Acceptable Use
- Access Control
- Data Security

Access Layer

- Wireless Access Points
- WLAN Controllers
- Switch Infrastructure

People & Devices

HQ – Large Campus

ISFW

IPS
ATP
A/V

Identity

- X.509
- LDAP
- RADIUS
- SAML
- Multi-Factor Auth

Network & Security Operations Centers rely on tools to analyze log data, monitor for anomalies, IOCs, providing incident response and reporting on the overall risk level of the endpoint and security ecosystem.

External Services

VMs

NGFW

Endpoint Protection Management/Analytics

Internal Services

VMs

Web – Directory – Database – Email – File Services

Endpoint Solutions – Features

- Fabric Connector
- Vulnerability Scanning
- Secure Access (VPN)
- Antimalware
- Web Filter
- Sandbox Connector
- Data Loss Prevention
- EDR / UEBA Components
- Identity Integration
- Host Firewall
- Application Firewall
- Host Intrusion Detection
- File Integrity Monitoring
- Network Access Control

Endpoint Solutions Reference Architecture

Operations Center (NOC) (SOC)

- SIEM
- Analytics
- Log Collection
- Automated Response
- IOC
- Treat Feed

Network Access Control

- Captivity/Quarantine
- Security Posture
- Identity
- Compliance
- BYOD

Policy / Governance

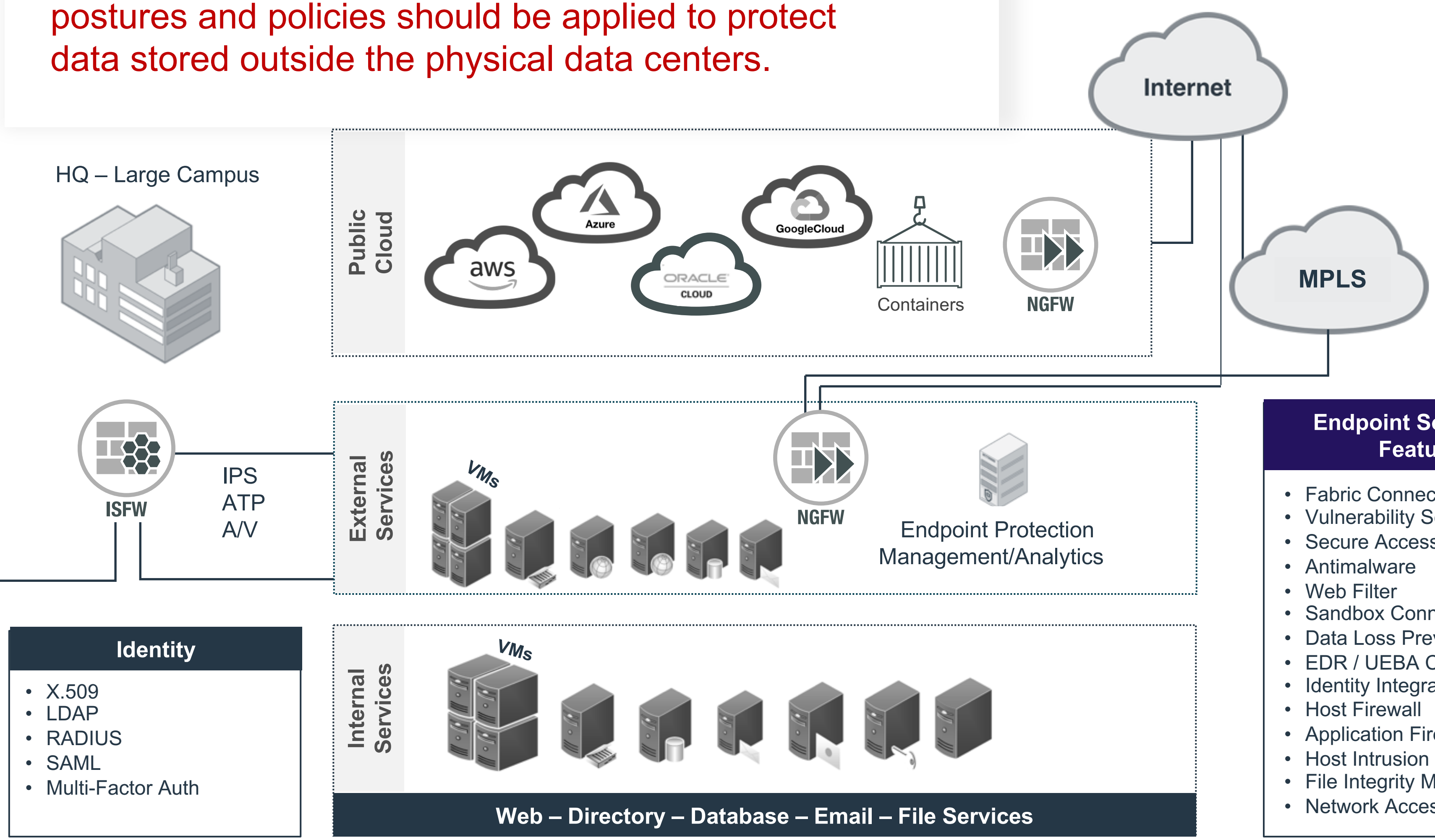
- Managed A/V
- Acceptable Use
- Access Control
- Data Security

Access Layer

- Wireless Access Points
- WLAN Controllers
- Switch Infrastructure

People & Devices

As a hybrid cloud data centers are adopted, security postures and policies should be applied to protect data stored outside the physical data centers.



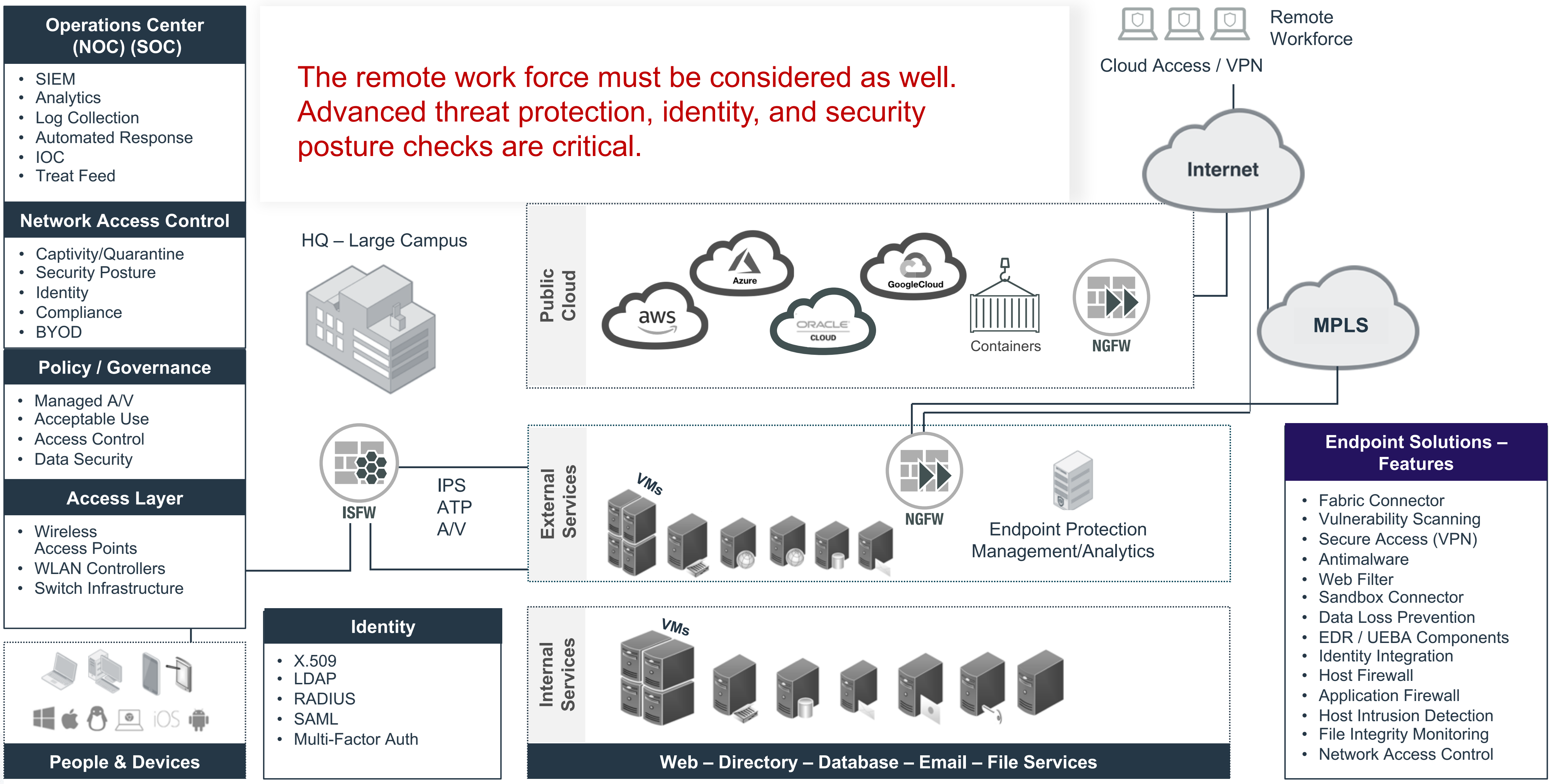
Identity

- X.509
- LDAP
- RADIUS
- SAML
- Multi-Factor Auth

Endpoint Solutions – Features

- Fabric Connector
- Vulnerability Scanning
- Secure Access (VPN)
- Antimalware
- Web Filter
- Sandbox Connector
- Data Loss Prevention
- EDR / UEBA Components
- Identity Integration
- Host Firewall
- Application Firewall
- Host Intrusion Detection
- File Integrity Monitoring
- Network Access Control

Endpoint Solutions Reference Architecture



The remote work force must be considered as well. Advanced threat protection, identity, and security posture checks are critical.

Operations Center (NOC) (SOC)

- SIEM
- Analytics
- Log Collection
- Automated Response
- IOC
- Treat Feed

Network Access Control

- Captivity/Quarantine
- Security Posture
- Identity
- Compliance
- BYOD

Policy / Governance

- Managed A/V
- Acceptable Use
- Access Control
- Data Security

Access Layer

- Wireless Access Points
- WLAN Controllers
- Switch Infrastructure

People & Devices

Identity

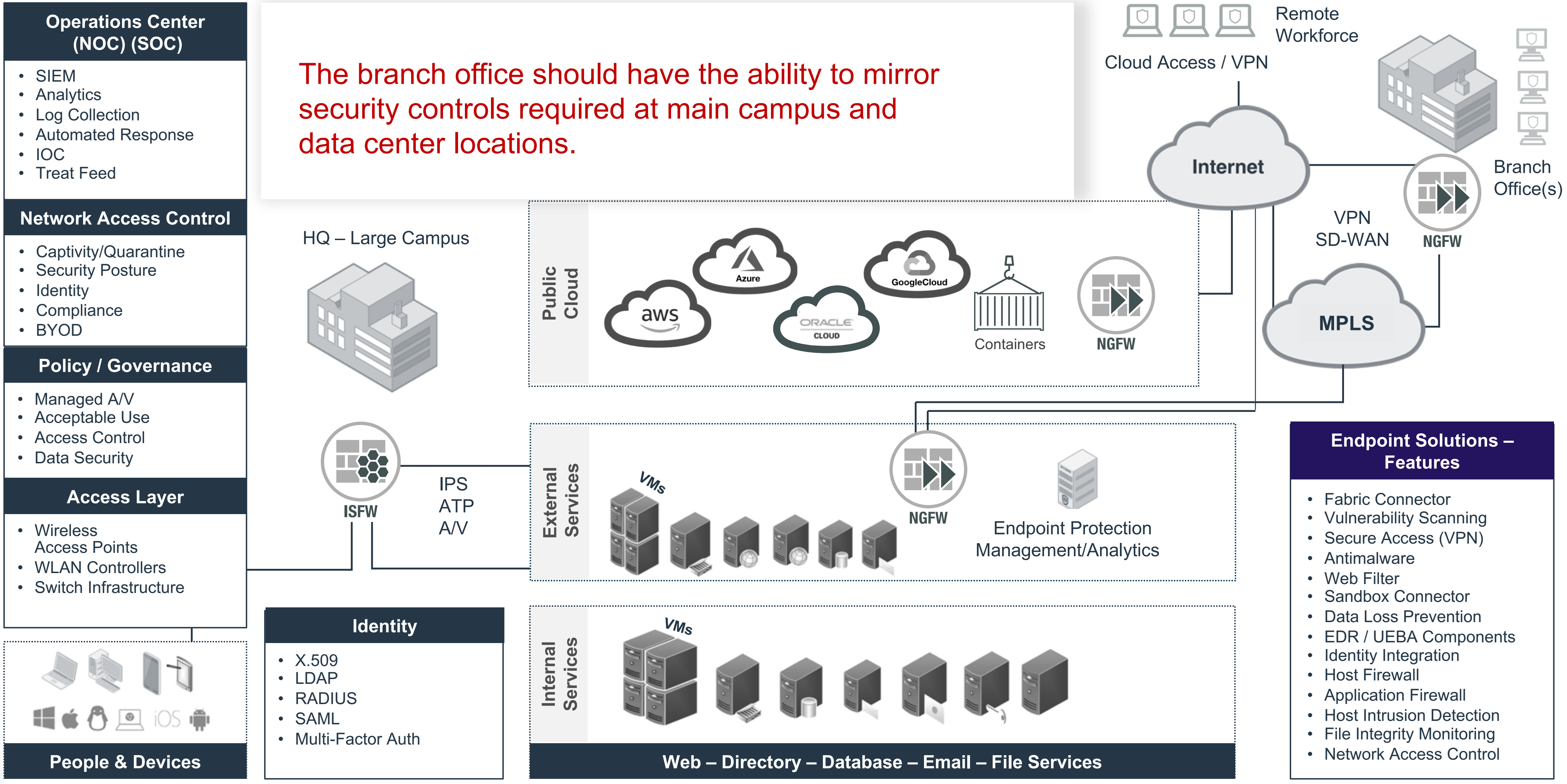
- X.509
- LDAP
- RADIUS
- SAML
- Multi-Factor Auth

Web – Directory – Database – Email – File Services

Endpoint Solutions – Features

- Fabric Connector
- Vulnerability Scanning
- Secure Access (VPN)
- Antimalware
- Web Filter
- Sandbox Connector
- Data Loss Prevention
- EDR / UEBA Components
- Identity Integration
- Host Firewall
- Application Firewall
- Host Intrusion Detection
- File Integrity Monitoring
- Network Access Control

Endpoint Solutions Reference Architecture



Operations Center (NOC) (SOC)

- SIEM
- Analytics
- Log Collection
- Automated Response
- IOC
- Treat Feed

Network Access Control

- Captivity/Quarantine
- Security Posture
- Identity
- Compliance
- BYOD

Policy / Governance

- Managed A/V
- Acceptable Use
- Access Control
- Data Security

Access Layer

- Wireless Access Points
- WLAN Controllers
- Switch Infrastructure

People & Devices

The branch office should have the ability to mirror security controls required at main campus and data center locations.

Identity

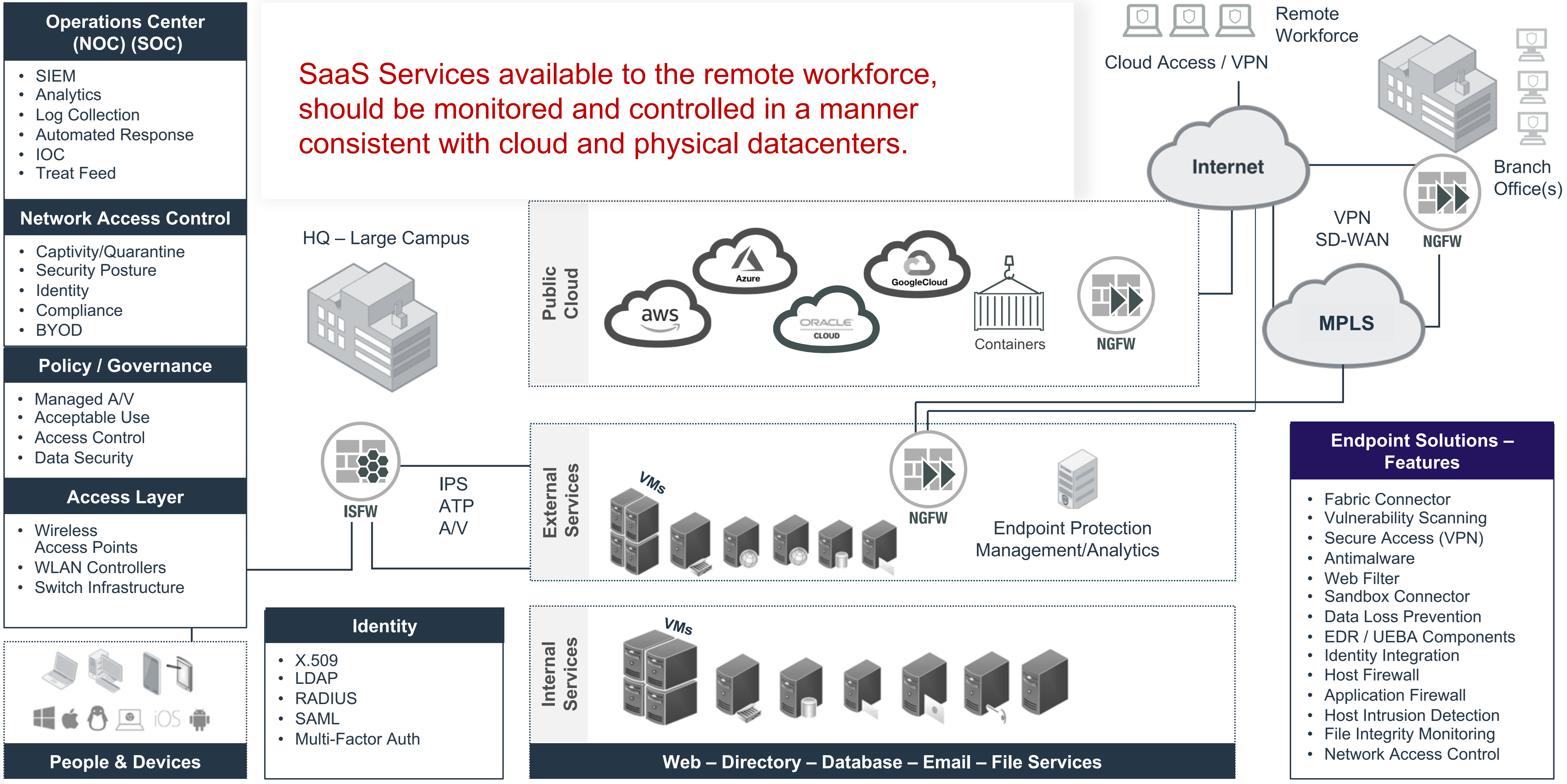
- X.509
- LDAP
- RADIUS
- SAML
- Multi-Factor Auth

Web – Directory – Database – Email – File Services

Endpoint Solutions – Features

- Fabric Connector
- Vulnerability Scanning
- Secure Access (VPN)
- Antimalware
- Web Filter
- Sandbox Connector
- Data Loss Prevention
- EDR / UEBA Components
- Identity Integration
- Host Firewall
- Application Firewall
- Host Intrusion Detection
- File Integrity Monitoring
- Network Access Control

Endpoint Solutions Reference Architecture



SaaS Services available to the remote workforce, should be monitored and controlled in a manner consistent with cloud and physical datacenters.

Operations Center (NOC) (SOC)

- SIEM
- Analytics
- Log Collection
- Automated Response
- IOC
- Treat Feed

Network Access Control

- Captivity/Quarantine
- Security Posture
- Identity
- Compliance
- BYOD

Policy / Governance

- Managed A/V
- Acceptable Use
- Access Control
- Data Security

Access Layer

- Wireless Access Points
- WLAN Controllers
- Switch Infrastructure

People & Devices

Identity

- X.509
- LDAP
- RADIUS
- SAML
- Multi-Factor Auth

Endpoint Solutions – Features

- Fabric Connector
- Vulnerability Scanning
- Secure Access (VPN)
- Antimalware
- Web Filter
- Sandbox Connector
- Data Loss Prevention
- EDR / UEBA Components
- Identity Integration
- Host Firewall
- Application Firewall
- Host Intrusion Detection
- File Integrity Monitoring
- Network Access Control

Web – Directory – Database – Email – File Services

Endpoint Solutions Reference Architecture

Operations Center (NOC) (SOC)

- SIEM
- Analytics
- Log Collection
- Automated Response
- IOC
- Treat Feed

Network Access Control

- Captivity/Quarantine
- Security Posture
- Identity
- Compliance
- BYOD

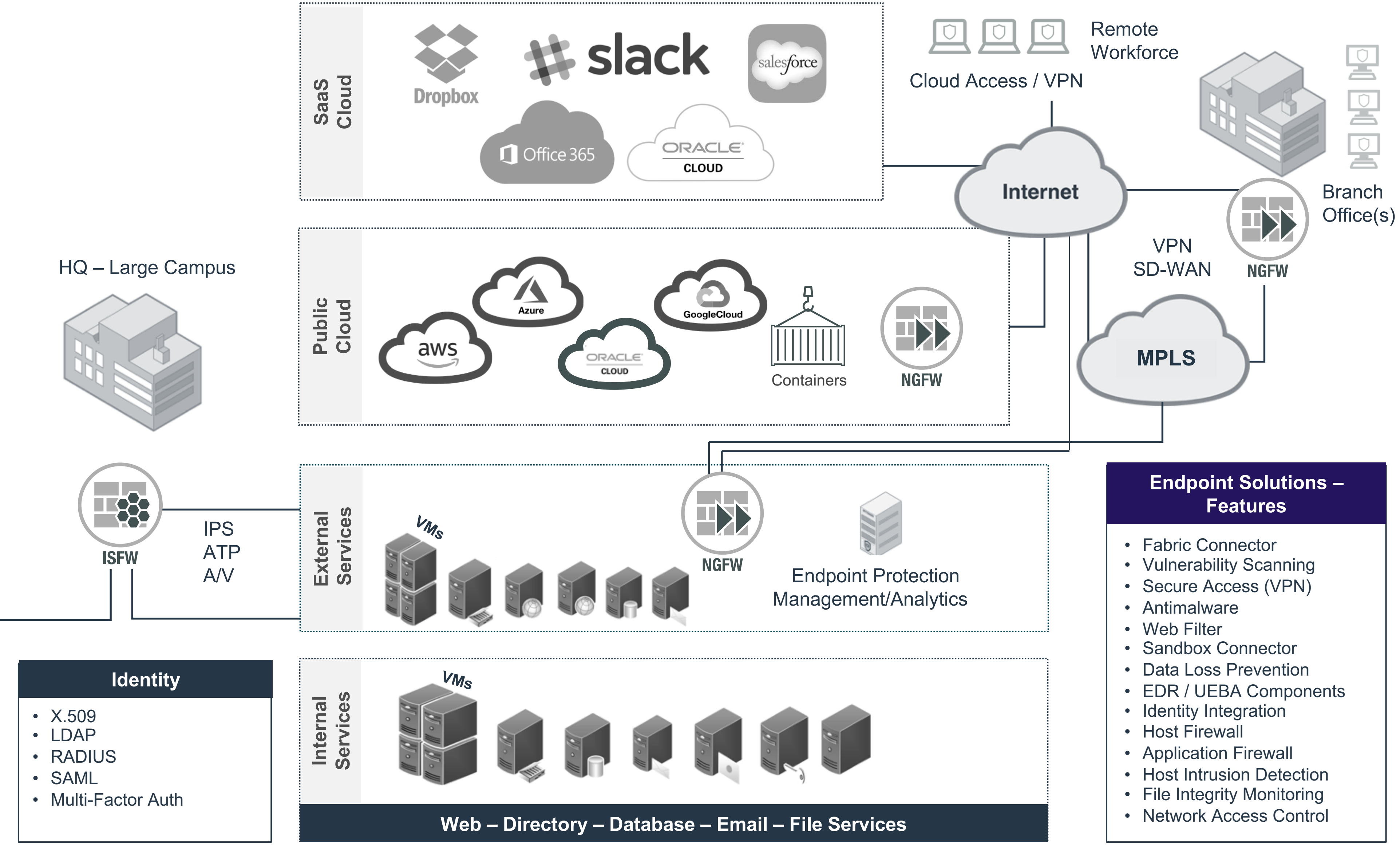
Policy / Governance

- Managed A/V
- Acceptable Use
- Access Control
- Data Security

Access Layer

- Wireless
  Access Points
- WLAN Controllers
- Switch Infrastructure

People & Devices



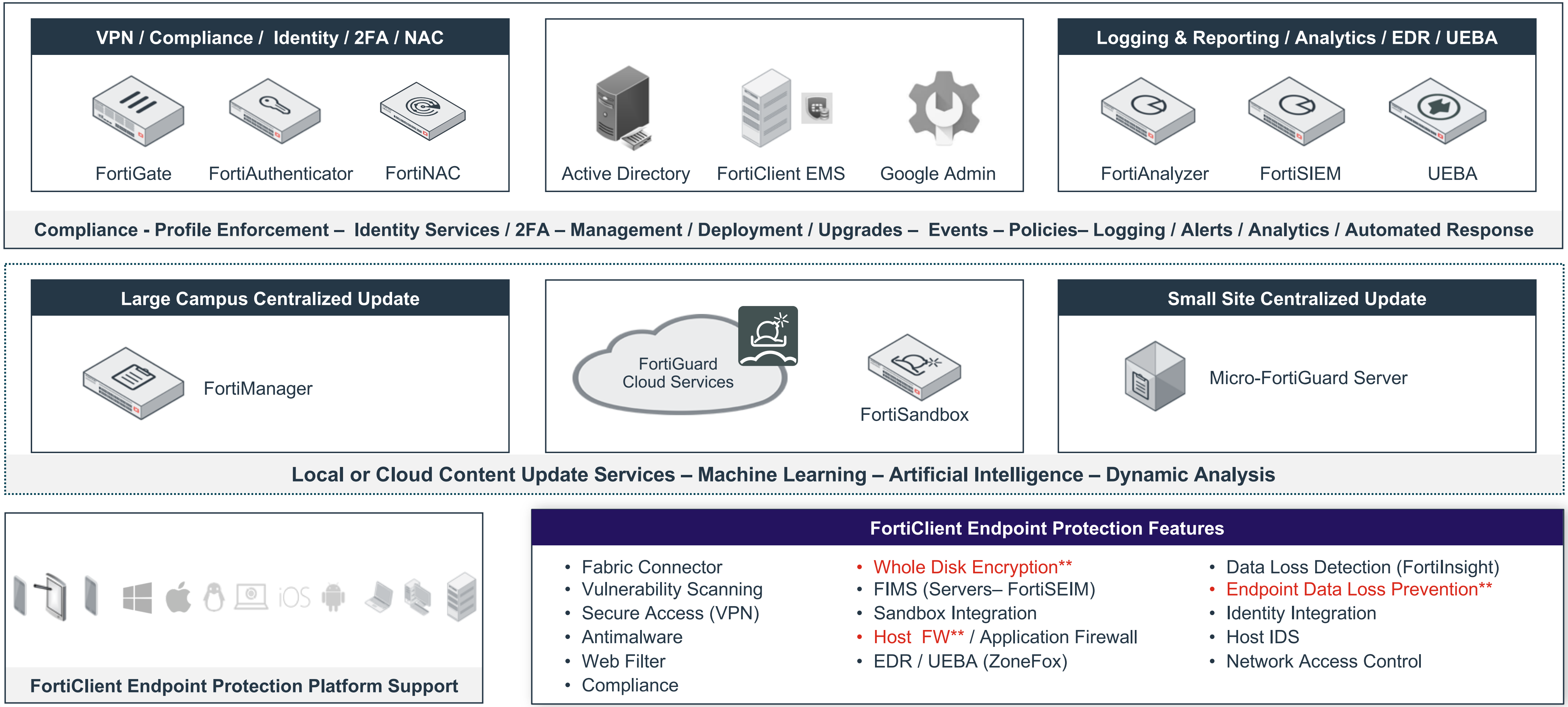
Identity

- X.509
- LDAP
- RADIUS
- SAML
- Multi-Factor Auth

Endpoint Solutions – Features

- Fabric Connector
- Vulnerability Scanning
- Secure Access (VPN)
- Antimalware
- Web Filter
- Sandbox Connector
- Data Loss Prevention
- EDR / UEBA Components
- Identity Integration
- Host Firewall
- Application Firewall
- Host Intrusion Detection
- File Integrity Monitoring
- Network Access Control

Fortinet Endpoint Solutions Architecture Components



VPN / Compliance / Identity / 2FA / NAC

FortiGate FortiAuthenticator FortiNAC

Active Directory FortiClient EMS Google Admin

Logging & Reporting / Analytics / EDR / UEBA

FortiAnalyzer FortiSIEM UEBA

Compliance - Profile Enforcement – Identity Services / 2FA – Management / Deployment / Upgrades – Events – Policies– Logging / Alerts / Analytics / Automated Response

Large Campus Centralized Update

FortiManager

FortiGuard Cloud Services

FortiSandbox

Small Site Centralized Update

Micro-FortiGuard Server

Local or Cloud Content Update Services – Machine Learning – Artificial Intelligence – Dynamic Analysis

FortiClient Endpoint Protection Platform Support

FortiClient Endpoint Protection Features

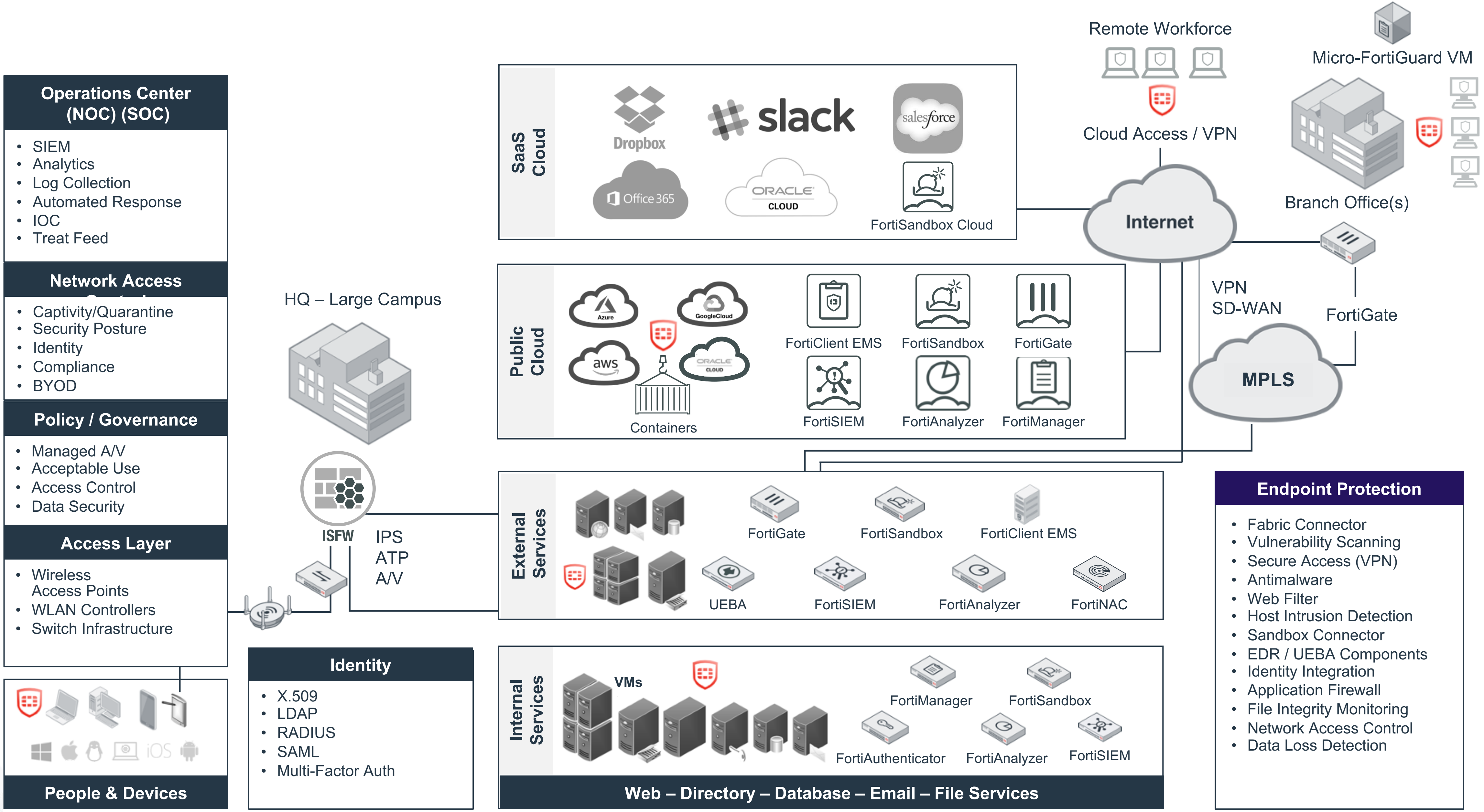
- Fabric Connector
- Vulnerability Scanning
- Secure Access (VPN)
- Antimalware
- Web Filter
- Compliance

- Whole Disk Encryption**
- FIMS (Servers– FortiSEIM)
- Sandbox Integration
- Host FW** / Application Firewall
- EDR / UEBA (ZoneFox)

- Data Loss Detection (FortiInsight)
- Endpoint Data Loss Prevention**
- Identity Integration
- Host IDS
- Network Access Control

** Not currently part of the Fortinet Endpoint Portfolio

Fortinet Endpoint Solutions Reference Architecture



Operations Center (NOC) (SOC)

- SIEM
- Analytics
- Log Collection
- Automated Response
- IOC
- Treat Feed

Network Access

- Captivity/Quarantine
- Security Posture
- Identity
- Compliance
- BYOD

Policy / Governance

- Managed A/V
- Acceptable Use
- Access Control
- Data Security

Access Layer

- Wireless Access Points
- WLAN Controllers
- Switch Infrastructure

People & Devices

Identity

- X.509
- LDAP
- RADIUS
- SAML
- Multi-Factor Auth

Endpoint Protection

- Fabric Connector
- Vulnerability Scanning
- Secure Access (VPN)
- Antimalware
- Web Filter
- Host Intrusion Detection
- Sandbox Connector
- EDR / UEBA Components
- Identity Integration
- Application Firewall
- File Integrity Monitoring
- Network Access Control
- Data Loss Detection