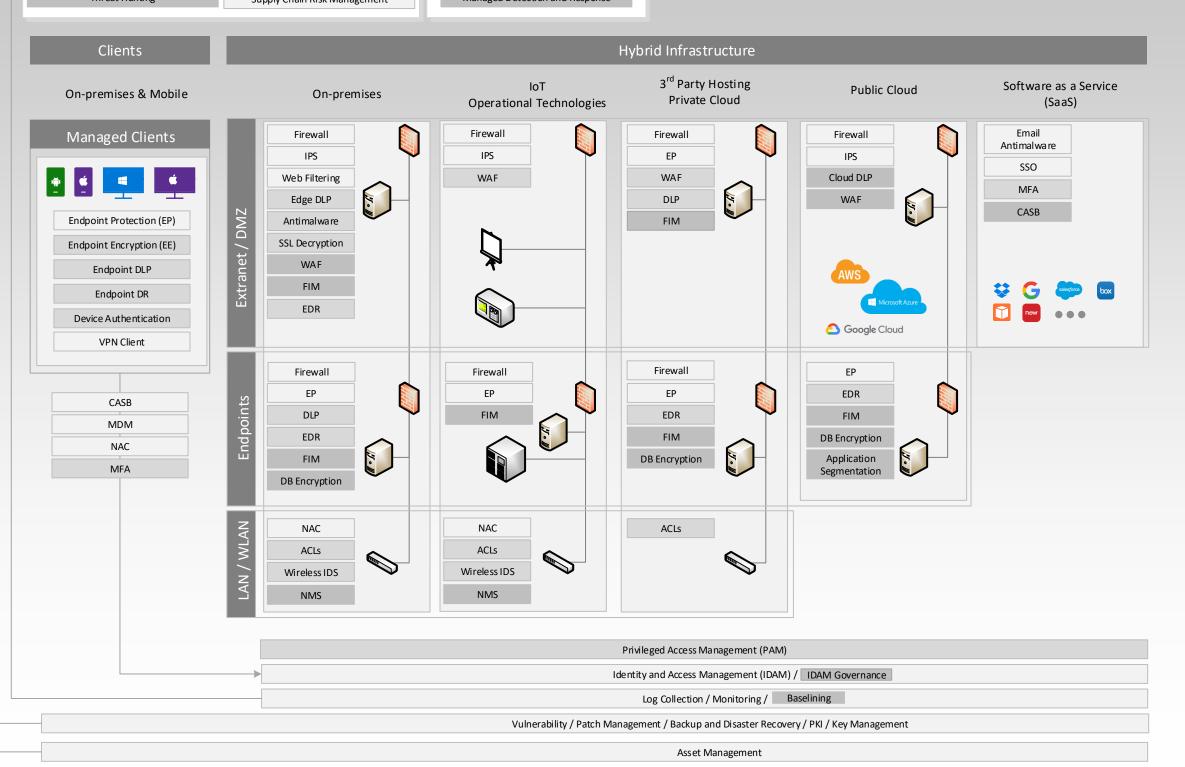
NIST Risk Management Framework – SP 800-18							
	Categorize System	Select Controls	Implement Controls	Assess Controls	Authorize System	Monitor Controls	
		Information S	MSSPs				
	Incident Response and Recovery		Configuration Management		Managed NAC		
	Asset Management		Patch Management		Managed SIEM		
Vulnerability Management		Security Governance		Managed Firewalls/IDS/IPS/Web Filtering			
	SIEM & Analytics		Awareness and Training		Managed IPS/IDS		
	Penetration Testing / Red Teaming		Security Architecture		eDiscovery / Forensics Retainer		
eDiscovery / Forensics			Risk Assessments / Compliance		Threat Hunting		
Threat Hunting			Supply Chain Risk Management		Managed Detection and Response		

Cybersecurity Architecture Roadmap

Version 2.1 – April 2019 © Adrian Grigorof

Currently implemented
2019 implementation
2020 implementation
Not on the roadmap



Identify

Governance

Risk Assessments

Compliance

Configuration Management

Vulnerability Scanning

Penetration Testing

Asset Management

SIE

Firewalls / ACLs

Protect

Remote Access (VPN)

Endpoint Protection (EP)

Email Antimalware

Intrusion Prevention (IPS)

Web Filtering

Identity and Access Management (IDAM)

Single Sign-On (SSO)

Multi-Factor Authentication (MFA)

Privileged Access Management (PAM)

IDAM Governance

Network Access Control (NAC)

Mobile Device Management (MDM)

Endpoint Encryption (EE)

Database Audit Monitoring

Device Authentication

Web Application Firewall (WAF)

Database Encryption

Cloud Access Security Broker (CASB)

Application Segmentation

Public Key Infrastructure (PKI)

Key Management

DDoS Protection

Application Whitelisting

Security Controls vs NIST Cybersecurity Framework



Detect

SIEM & Analytics

Intrusion Detection (IDS/IPS)

Vulnerability Scanning
Wireless IDS

Endpoint EDR / HIDS

Endpoint DLP

Edge DLP

Edge Antimalware

SSL Decryption

NMS

File Integrity Monitoring (FIM)

Baselining

Threat Hunting

Threat Intelligence Feeds

Deception / Honeypots

Code Analysis

Respond

Incident Response and Recovery

Endpoint Detection and Response

eDiscovery / Forensics

Recover

Disaster Recovery Planning

Incident Response and Recovery