February 6th-7th

NIC

20/20 VISION

Oslo Spektrum

Security in the Cloud with Cisco Security Architecture

Øyvind Dahl
Senior Solution Architect
Conscia

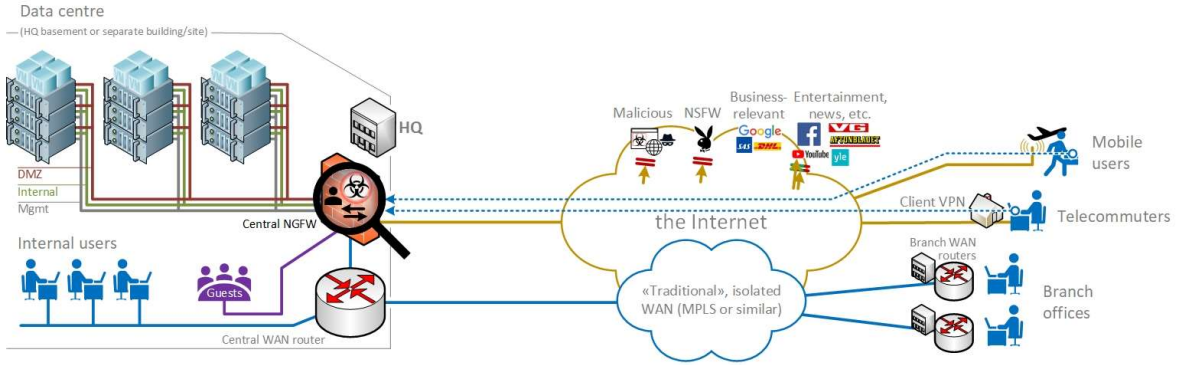
Slides and demos from the conference will be available at

https://github.com/nordicinfrastructureconference/2020

The Cloud and the changing threat environment

Traditional network security

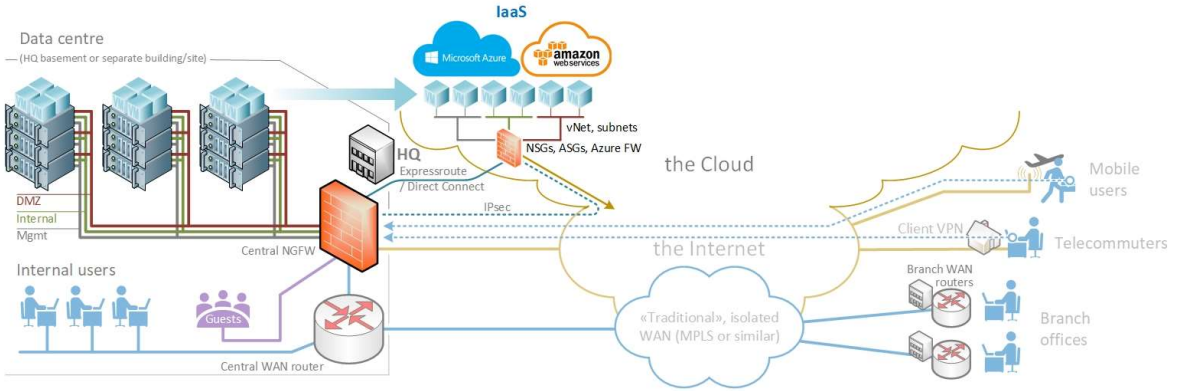
- Perimeter security, with a central firewall separating
  - Inside users (at HQ, branch sites, and client VPN users)
  - Data centre (possibly segmented … and probably virtualized)
  - Outside zones, including the Internet and guest networks
- Some level of Internet access needed for business purposes…
  …possibly calling for a Next-Generation Firewall (NGFW) capable of layer 7 inspection:
  - URL filtering
  - Application recognition
  - IDS / IPS
  - Anti-Virus / Anti-Malware
  - Identity-based filtering



The Cloud and the changing threat environment

The Cloud – Infrastructure as a Service (IaaS)

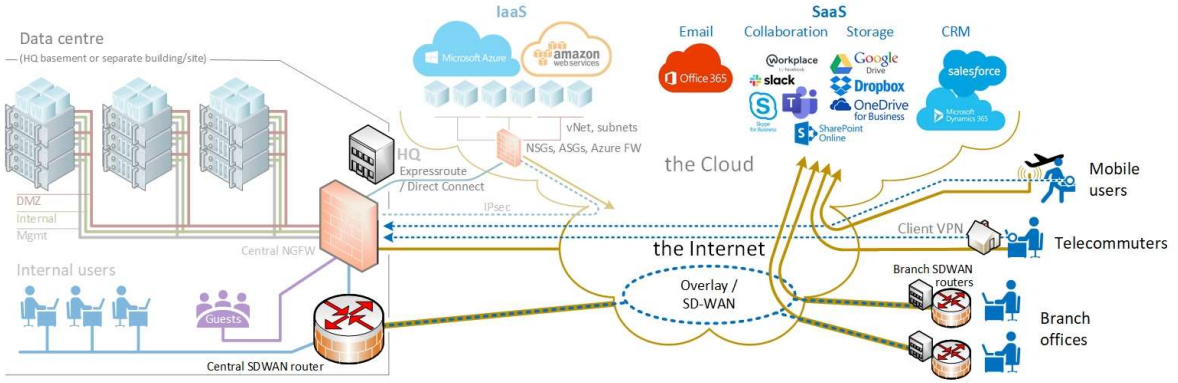
- The Cloud – Some principally different categories
  - IaaS: InfraStructure as a Service
  - SaaS: Software as a Service
  - PaaS: Platform as a Service
- IaaS (e.g. Azure or AWS)
  - Self-service data centres
  - Virtual network (vNet)
  - Internet connectivity
- Secure connection to your network
  - IPsec tunnels across the Internet
  - Azure Expressroute / AWS Direct Connect
- Native security (Layer 3-4)
  - Subnets
  - Network Security Groups (NSGs)
  - Application Security Groups (ASGs)
  - Azure firewall



The Cloud and the changing threat environment

The Cloud – Software as a Service (SaaS)

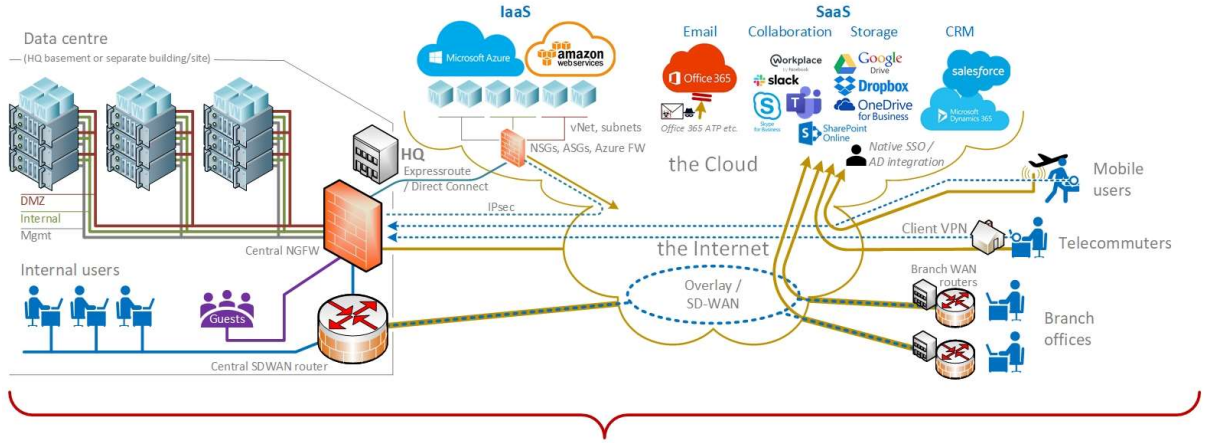
- Traditional “pre-SaaS” architecture
  - Internal services at the data centre
  - Services at the Internet largely for private purposes
- Moving your internal *services* to the cloud
  - You don’t control the VM or OS
  - You don’t control the network
- Internal systems reachable from the Internet
  - Mobile / home users do not need to use VPN clients
  - Local Internet access at branch offices more relevant
  - Firewall-based VPNs, SD-WAN or even Internet-only preferable over traditional WANs



The Cloud and the changing threat environment

The Cloud – Software as a Service (SaaS)

- How can you secure your SaaS services?
  - You don't control the data centre networks where the software runs, not even virtually
  - Most SaaS services integrate with e.g. AD for Single Sign-On
  - Some offer native security, e.g. Office365 ATP for email security
  - NGFW URL and Application filters offer some limited ability to control SaaS accessibility
- End-to-end security needed
  - Native security features often limited compared to on-premise hosted services
  - Multiple admin interfaces and systems increase complexity, workload *and risk*



Source: Clemens Vasters (Flickr)

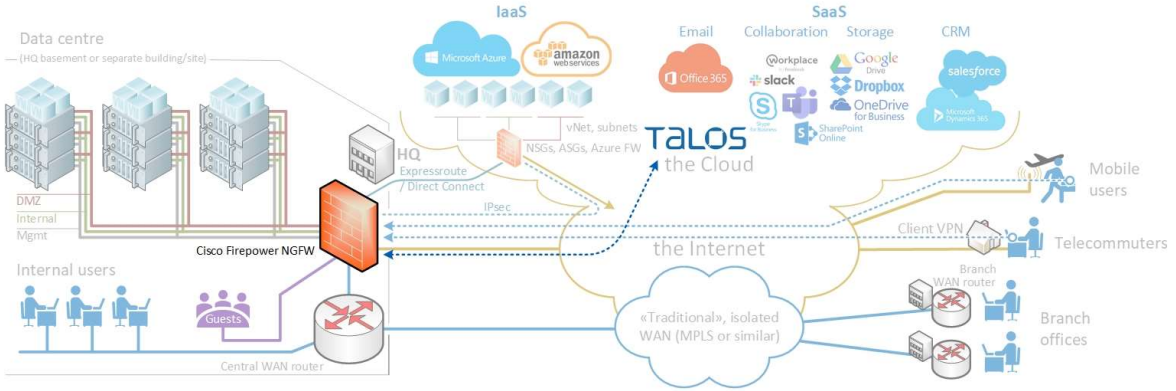
VS

Source: Andrey Belenko (Flickr)

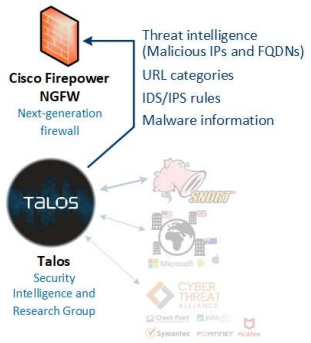
Cisco Security Architecture

Cisco Next Generation Firewalls, Talos, and Supporting Products

- Cisco Firepower NGFW
  - Gartner Leaders quadrant for firewalls 2018 and 2019
  - Advanced NGFW focused on security before, during and after the attack
  - Application rules, IDS/IPS, URL filtering, user-based rules, malware protection, and network visibility



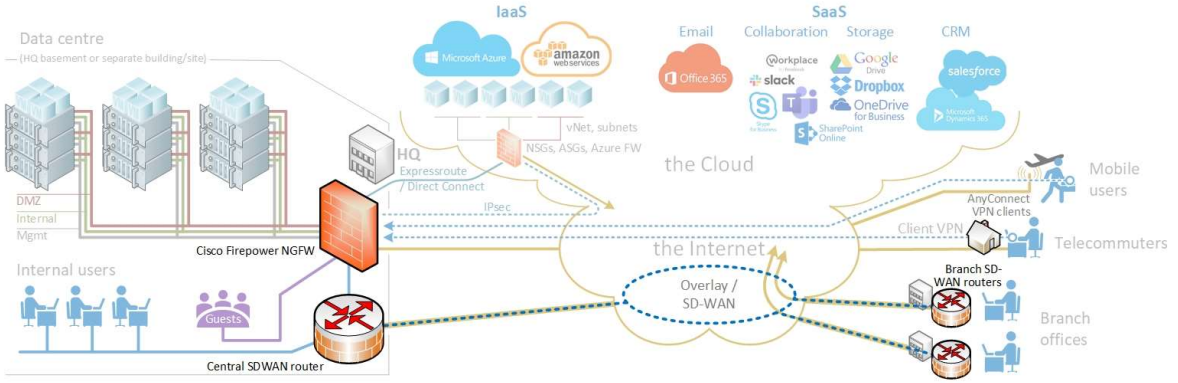
- Talos
  - Security Intelligence and Research Group
  - Provides security and threat information for Cisco security products
  - Threat Intelligence (IP / domain reputation)
  - URL categories
  - IDS/IPS rules
  - Malware verdicts



Cisco Security Architecture

Cisco Next Generation Firewalls, Talos, and supporting products

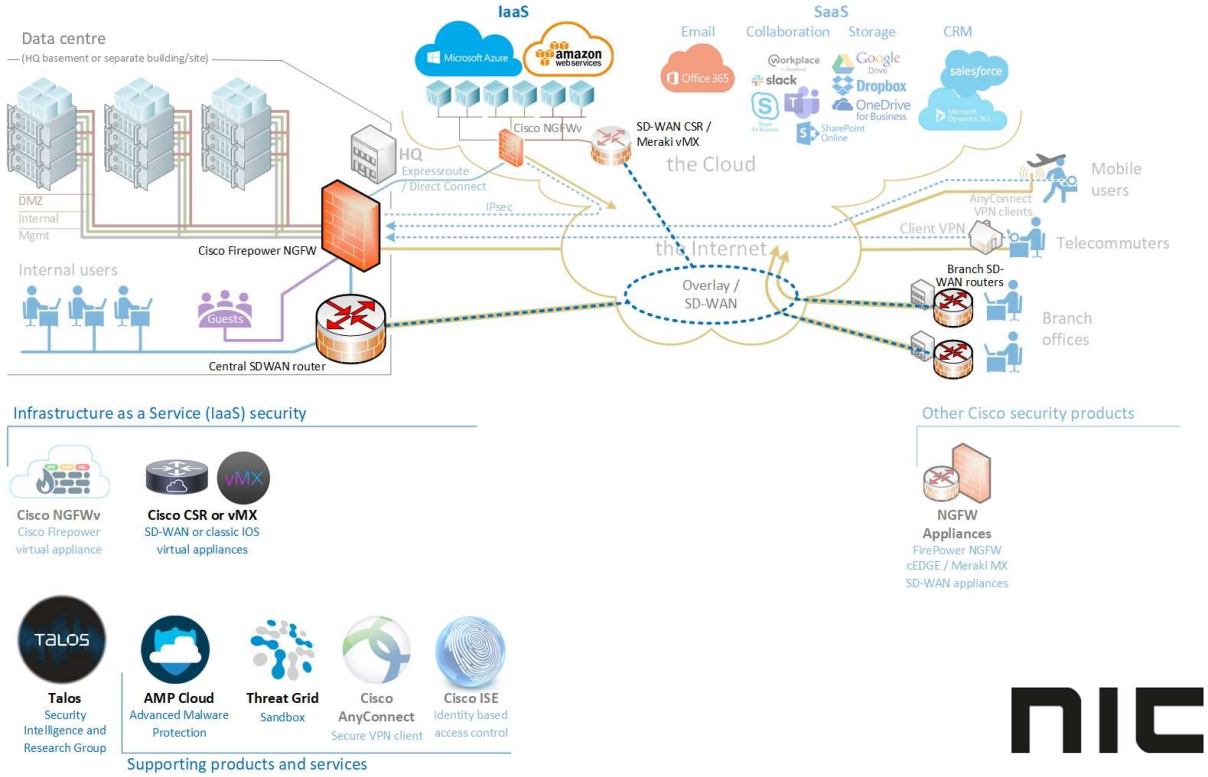
- Advanced Malware Protection (AMP)
- Threat Grid (Sandbox)
- Cisco AnyConnect (Secure VPN client)
- Cisco Identity Services Engine (ISE)
  - Security and access policies for endpoint devices
- SD-WAN with NGFW services
  - Stateful firewalls
  - Application and user-based rules
  - IDS/IPS
  - URL filtering
  - AMP
  - TrheatGrid



Cisco Security Architecture

IaaS Security – Virtual Appliances

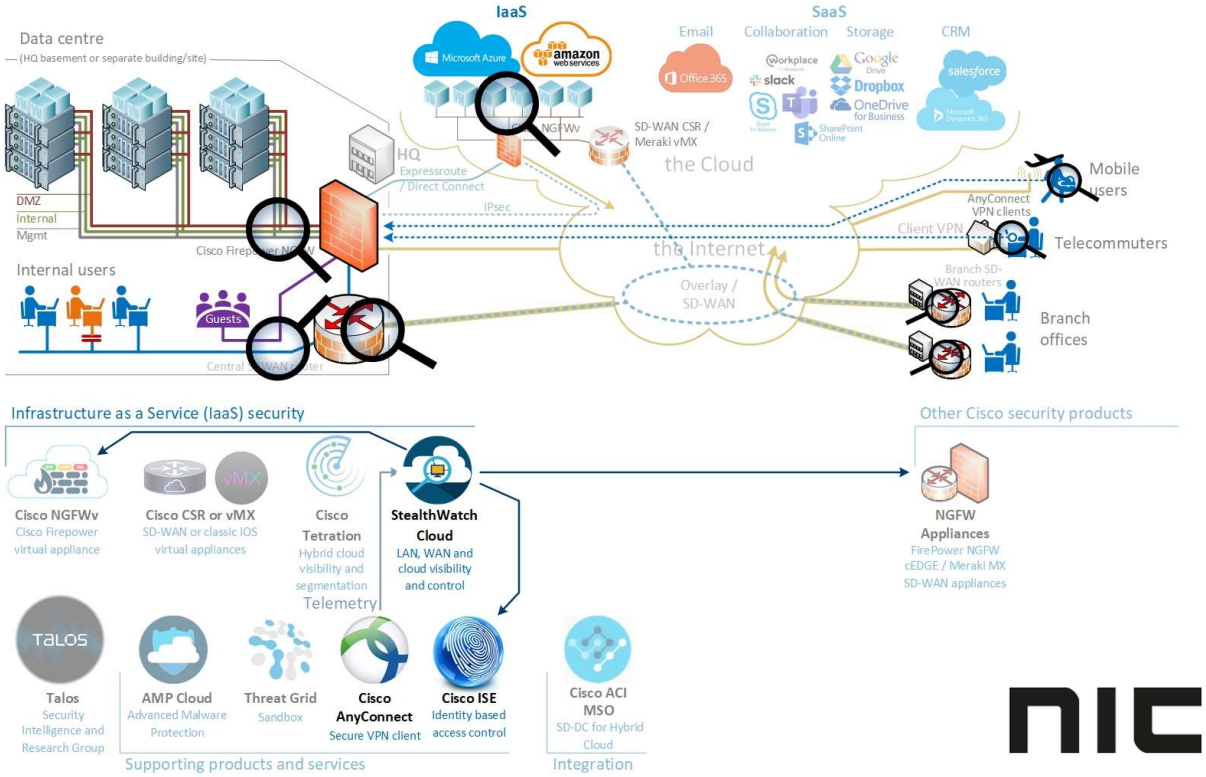
- Azure/AWS Native security
  - NSGs and ASGs, and Azure firewall only provide layer 4 stateful firewalling
  - No layer 7 / NGFW support
  - 3rd party virtual firewalls recommended
  - Inconsistent administration
- Cisco NGFWv virtual appliance
  - Same functionality and administrative interface as physical Firepower NGFW
  - Unified administration using Firepower Management Centre
- Virtual SD-WAN appliances
  - Cisco (Viptela) SD-WAN CSR (cEdge) or Meraki SD-WAN vMX
  - SD-WAN NGFW support
  - Unified administration (vManage or Meraki cloud)



Cisco Security Architecture

IaaS Security – Segmentation, Visibility and Enforcement

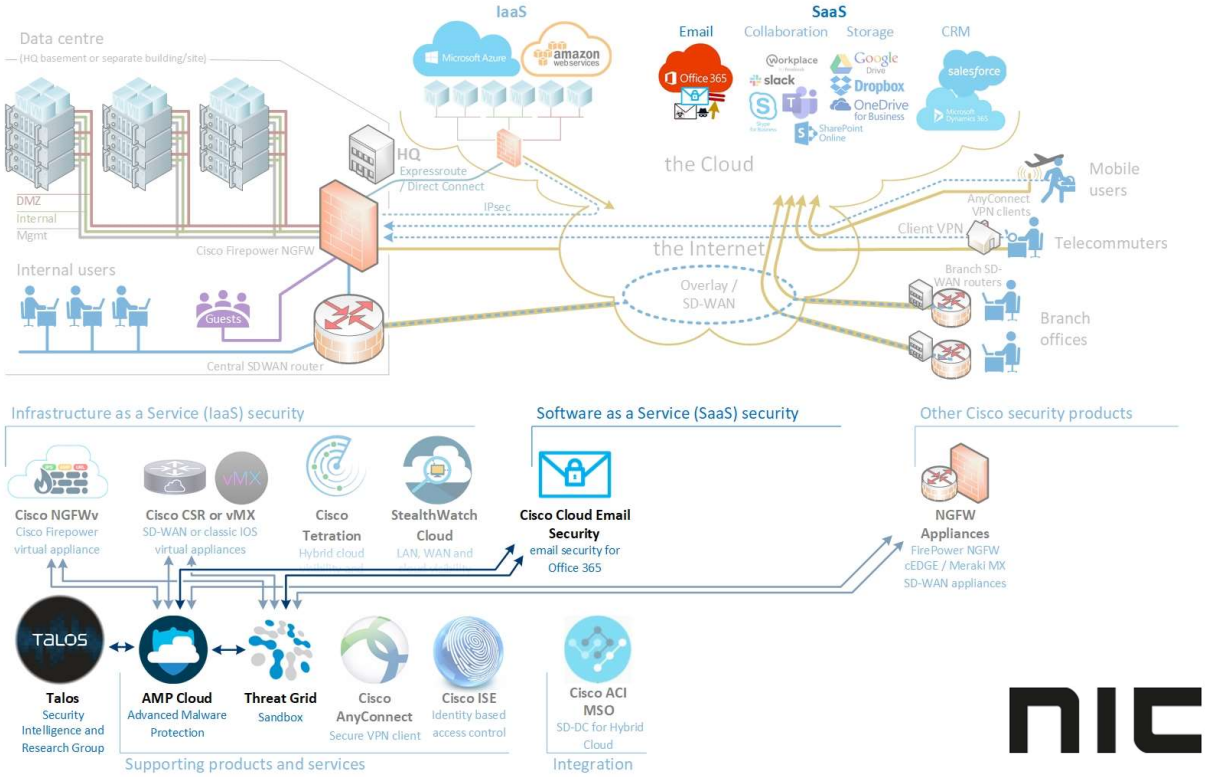
- Cisco ACI
  - Data centre automation and micro segmentation
  - ACI MSO enables hybrid cloud automation and segmentation
- Cisco Tetration
  - Data collection and analysis
  - Organizes and groups traffic and server information
  - Micro segmentation using FW rules, ACLs, NSGs/ASGs, ACI or *Native Enforcement*
- Cisco StealthWatch Cloud
  - Detects anomalies and threats inside LAN, WAN, data centres and public cloud (IaaS)
  - VPN visibility with AnyConnect Network Visibility Module
  - Mitigate threats by blocking compromised users or hosts in Firepower NGFW or ISE



Cisco Security Architecture

SaaS Security – Email Security

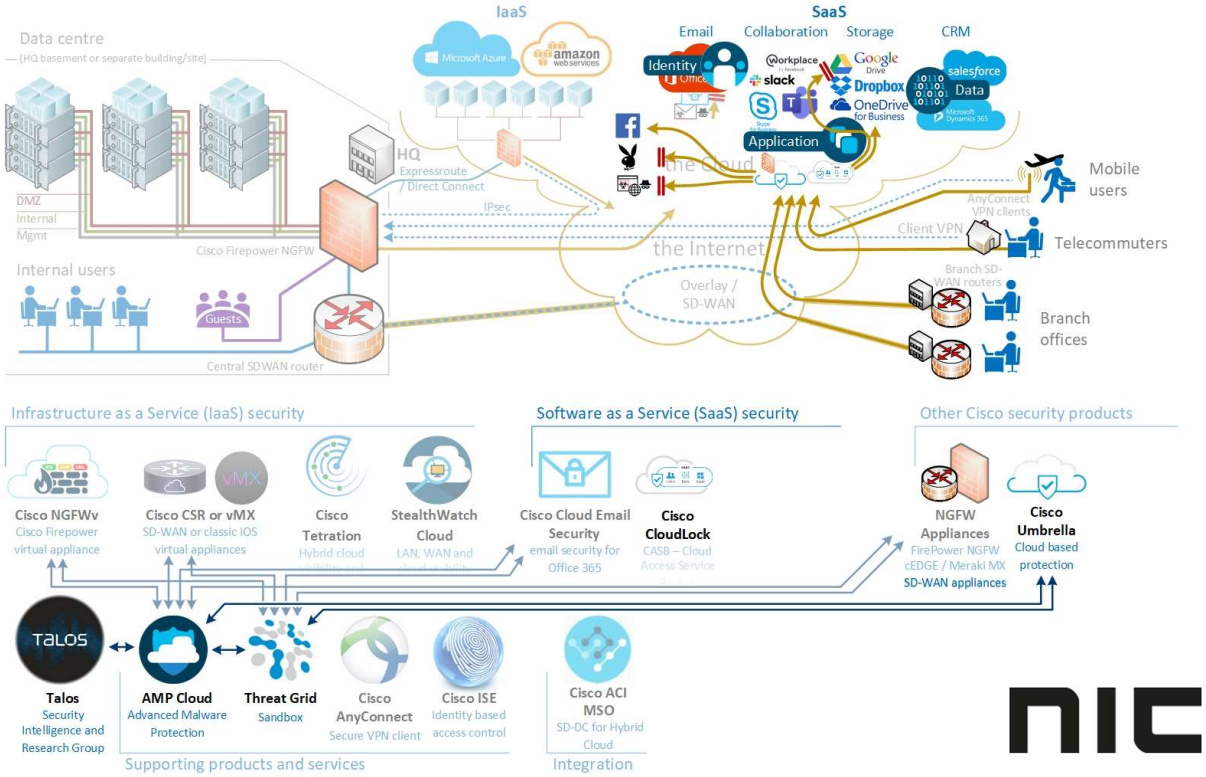
- Cisco Cloud Email Security
  - Cloud equivalent to Cisco Email Security Appliance
  - Provides protection against threats such as spoofed senders, look-alike domains, phising, malicious URLs, and malware
  - Relies on treat intelligence data from Talos
  - Integrates with AMP and Threat Grid



Cisco Security Architecture

SaaS Security – CloudLock and Umbrella

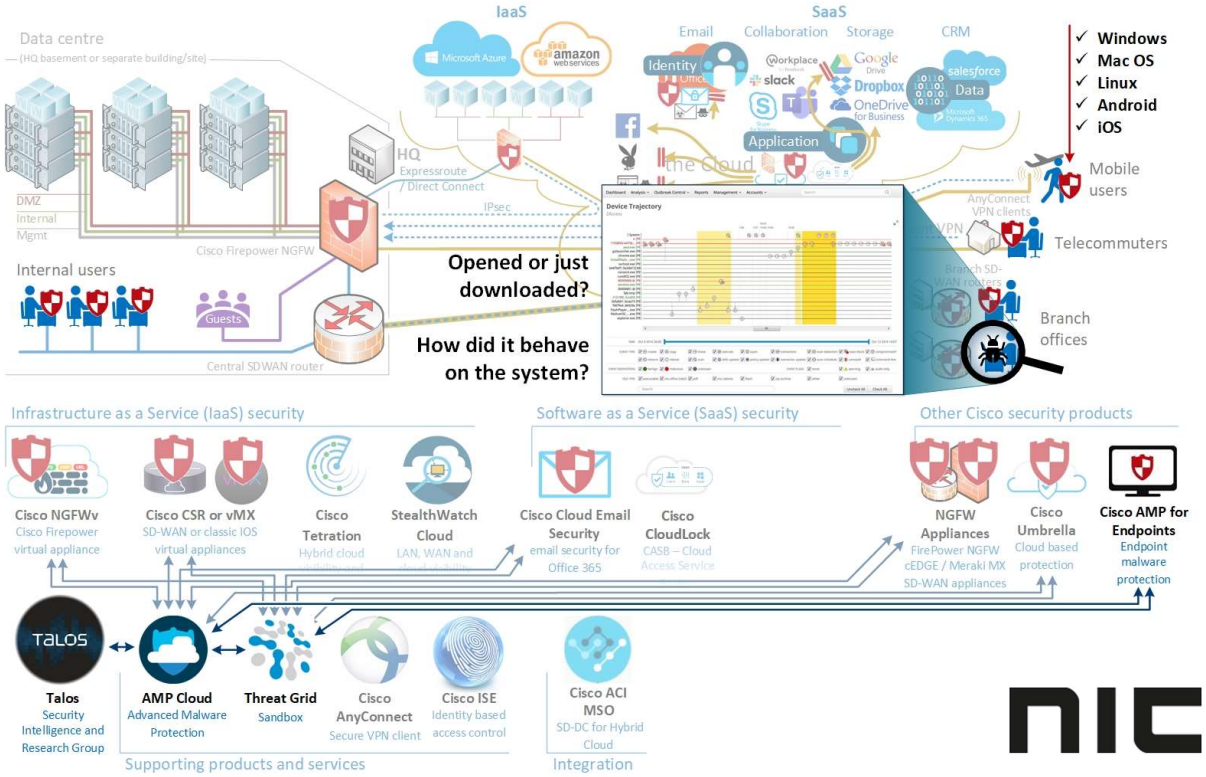
- Cisco CloudLock
  - CASB – Cloud Access Security Broker
  - Application: Discover and control cloud applications. White-/blacklist based on risk
  - Identity: Discover and react to suspicious user activity
  - Data Loss Prevention (DLP)
- Cisco Umbrella
  - Cloud based firewall developed from OpenDNS
  - Discover and control access to malicious or unwanted webpages, cloud apps and IPs
  - Proxy risky domains
  - Equivalent to Firepower URL filter and Threat Intelligence
  - AMP
  - SD-WAN integration



Cisco Security Architecture

SaaS Security – CloudLock and Umbrella

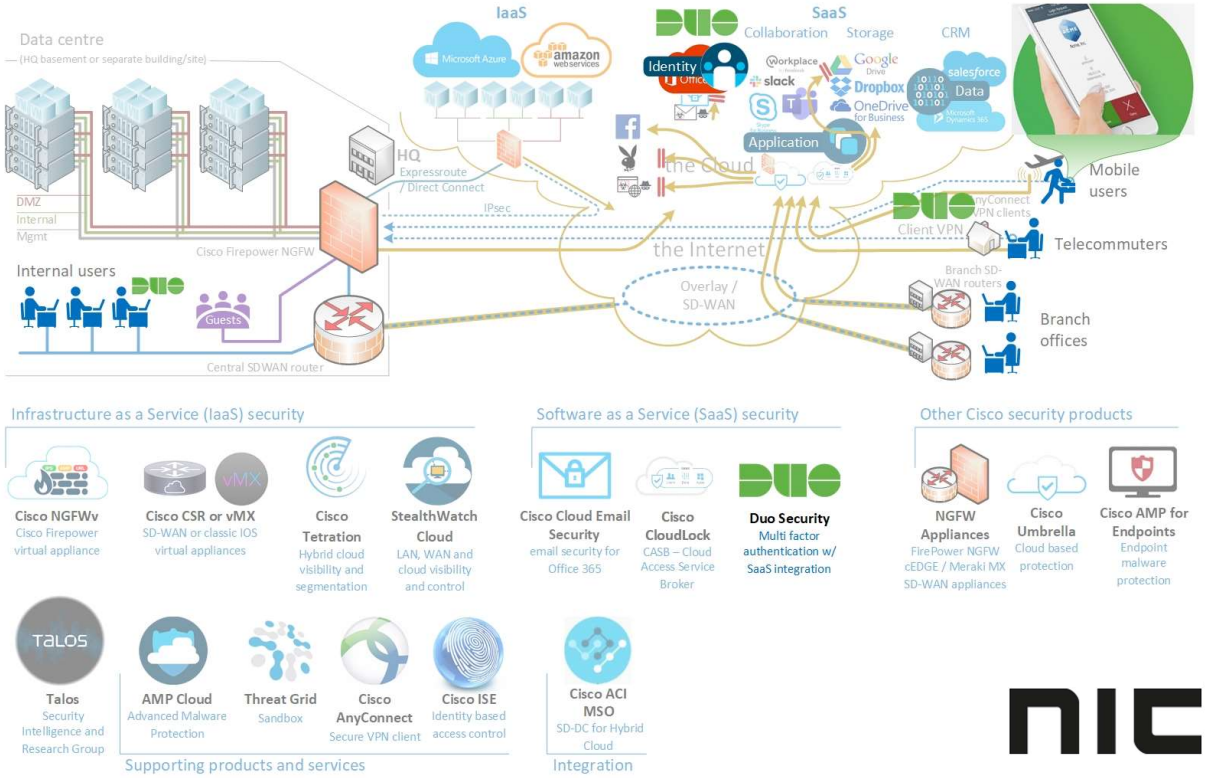
- Cisco CloudLock
  - CASB – Cloud Access Security Broker
  - Application: Discover and control cloud applications. White-/blacklist based on risk
  - Identity: Discover and react to suspicious user activity
  - Data Loss Prevention (DLP)
- Cisco Umbrella
  - Cloud based firewall developed from OpenDNS
  - Discover and control access to malicious or unwanted webpages, cloud apps and IPs
  - Proxy risky domains
  - Equivalent to Firepower URL filter and Threat Intelligence
  - AMP
  - SD-WAN integration



Cisco Security Architecture

SaaS Security – Zero Trust and Duo Security

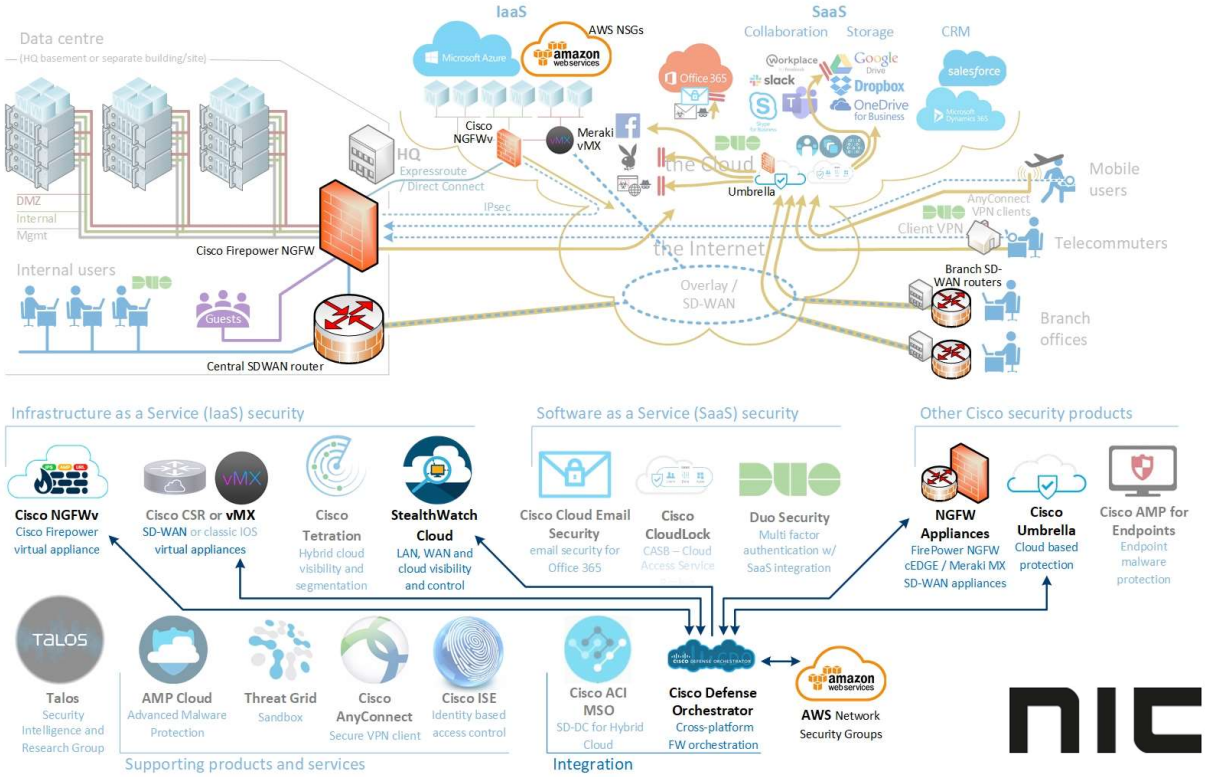
- Traditional security
  - User and device trust established at network connection
  - Traditional trust based on network location
  - Does not apply with users directly on the Internet
- Zero Trust security
  - Establish trust for every access request *regardless of source network location*
- Duo Security
  - Multi-factor authentication
  - Integrates with Windows logon, VPN clients (Cisco and non-Cisco), RADIUS and a wide range of SaaS services
  - Push (mobile app), mobile passcode, phone, SMS, token or U2F/web authentication
  - Device visibility and trust
  - Role, device, location or network based policies



Cisco Security Architecture

Integration

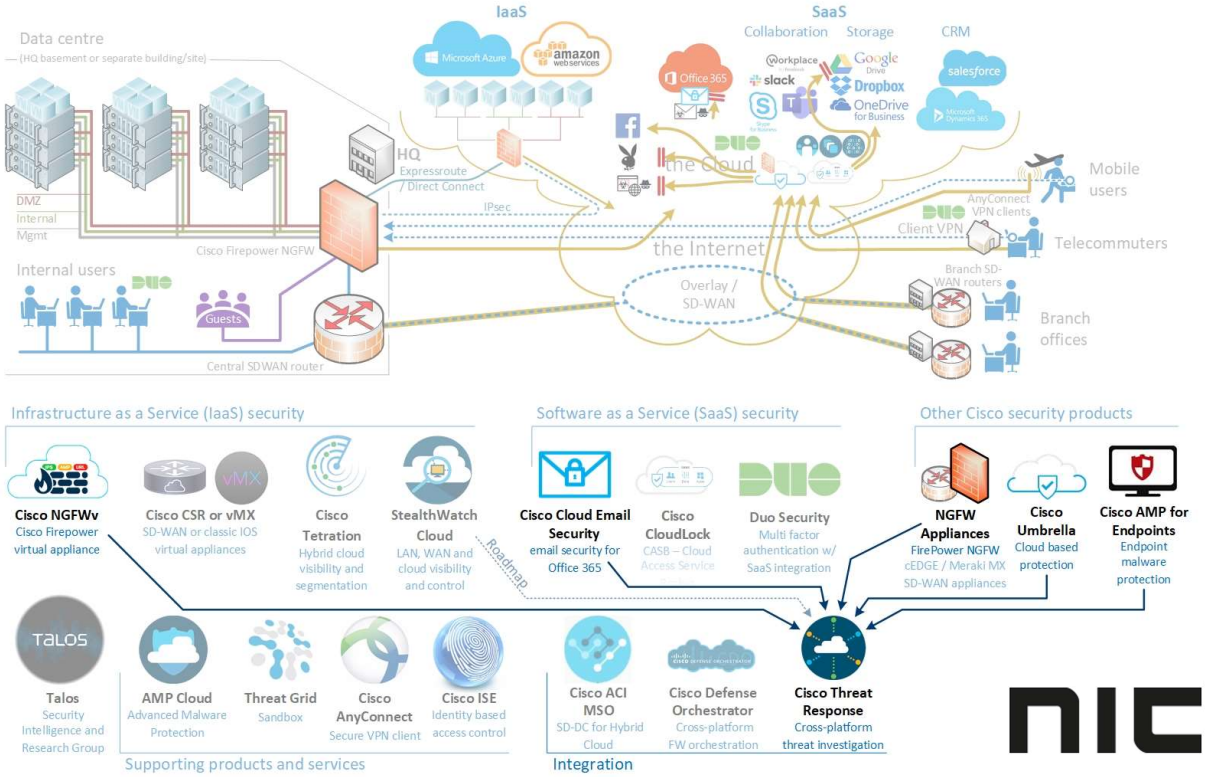
- Cisco Defense Orchestrator (CDO)
  - Cross-platform, cloud, supporting:
    - Cisco Firepower and ASA FWs
    - Cisco Meraki SD-WAN FWs
    - Cisco Umbrella
    - AWS Network Security Groups
  - Efficient cross-platform device and policy management
  - Audit and change management
  - Cloud based logging and analytics integrates with StealthWatch Cloud



Cisco Security Architecture

Integration

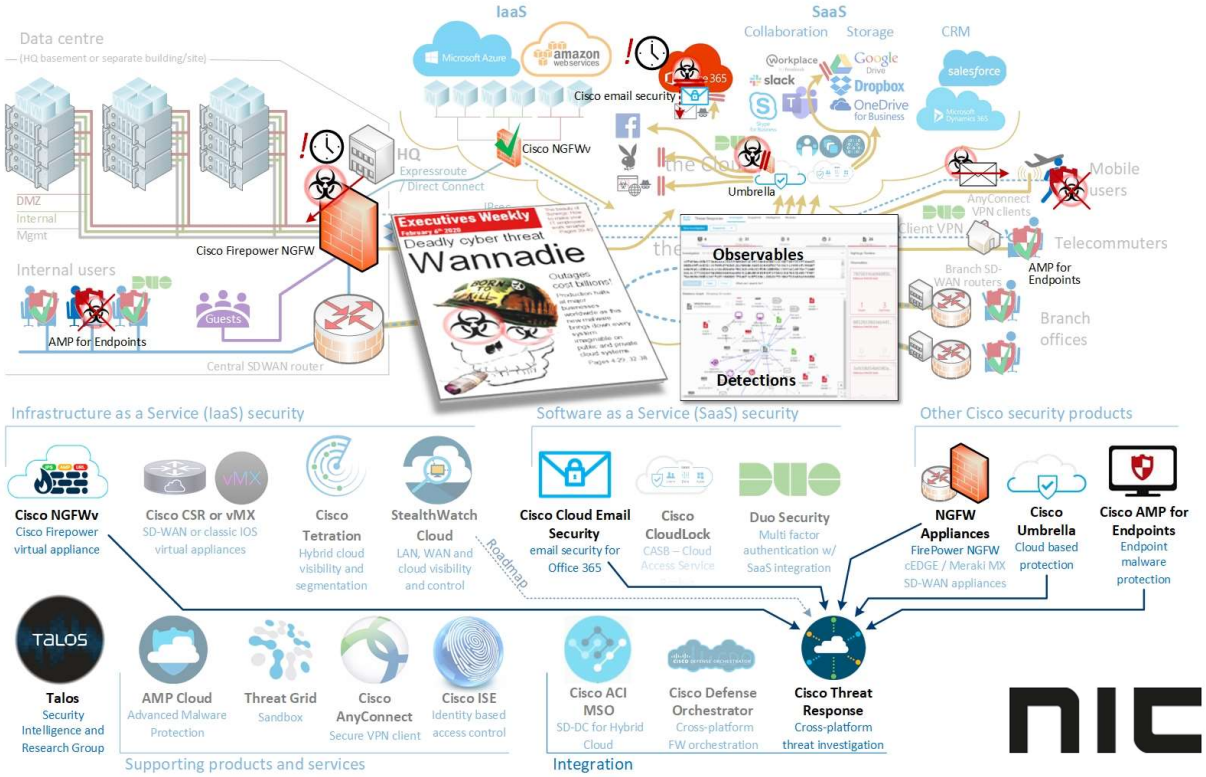
- Cisco Defense Orchestrator (CDO)
  - Cross-platform, cloud, supporting:
    - Cisco Firepower and ASA FWs
    - Cisco Meraki SD-WAN FWs
    - Cisco Umbrella
    - AWS Network Security Groups
  - Efficient cross-platform device and policy management
  - Audit and change management
  - Cloud based logging and analytics integrates with StealthWatch Cloud
- Cisco Threat Response (CTR)
  - Cross-platform threat correlation
    - Firepower NGFW (v6.5 EU)
    - Cisco Email Security
    - Cisco AMP for Endpoints
    - Cisco Umbrella
    - StealthWatch and other products on roadmap
  - Are we impacted?
  - Where was the threat detected?
  - Detect – Investigate – Remediate



Cisco Security Architecture

Integration

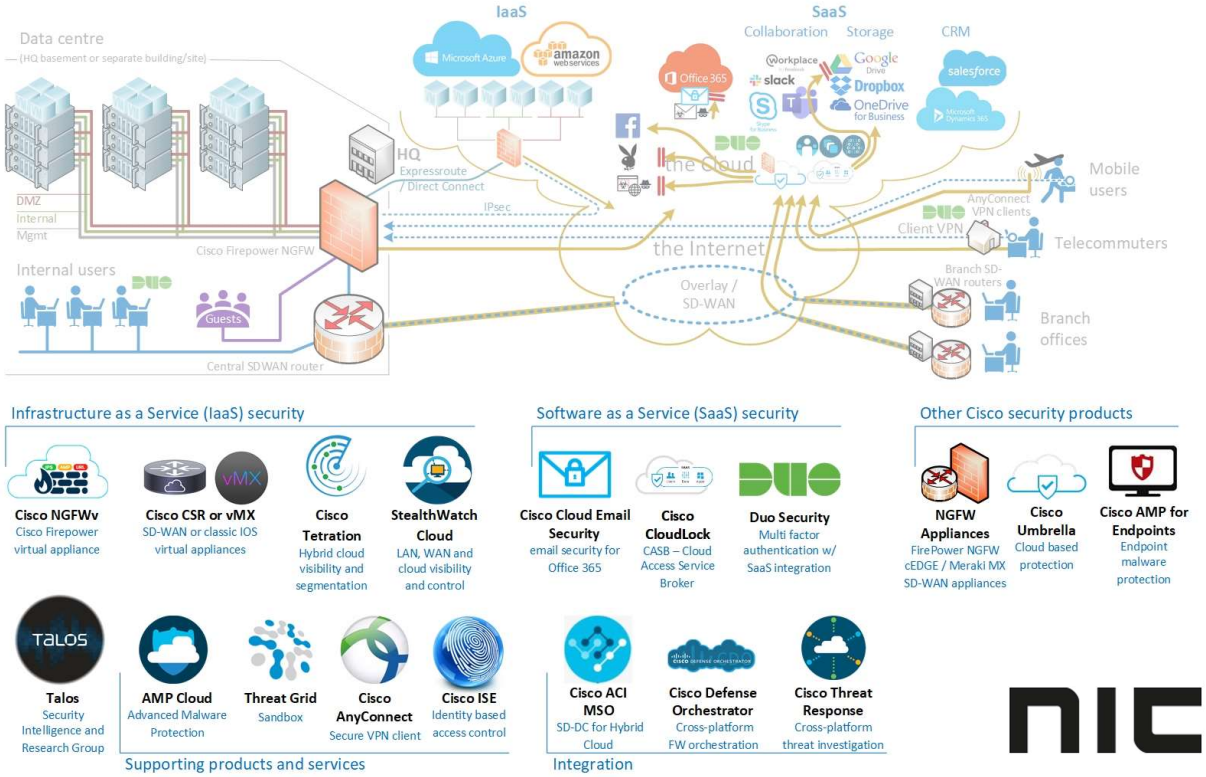
- Cisco Defense Orchestrator (CDO)
  - Cross-platform, cloud, supporting:
    - Cisco Firepower and ASA FWs
    - Cisco Meraki SD-WAN FWs
    - Cisco Umbrella
    - AWS Network Security Groups
  - Efficient cross-platform device and policy management
  - Audit and change management
  - Cloud based logging and analytics integrates with StealthWatch Cloud
- Cisco Threat Response (CTR)
  - Cross-platform threat correlation
    - Firepower NGFW (v6.5 EU)
    - Cisco Email Security
    - Cisco AMP for Endpoints
    - Cisco Umbrella
    - StealthWatch and other products on roadmap
  - Are we impacted?
  - Where was the threat detected?
  - Detect – Investigate – Remediate



Summary

Integrated cloud security

- Infrastructure as a Service (IaaS)
  - Increase and integrate security using NGFWv
  - Integrate with (SD)WAN using virtual CSR or vMX
  - Segmentation and visibility using Tetration / StealthWatch Cloud
- Software as a Service (SaaS)
  - Office365 email security using Cisco Cloud Email Security
  - SaaS visibility and enforcement using Cisco CloudLock
  - MFA / Zero-trust with Duo Security
- Integration
  - Cross-platform firewall integration with Cisco Defense Orchestrator
  - Cross-platform threat investigation with Cisco Threat Response
- End-to-end security architecture
  - Public Cloud (IaaS and SaaS)
  - Private Cloud (“physical” data centre)
  - LAN
  - WAN
  - Endpoints



Slides and demos from the conference will be available at

https://github.com/nordicinfrastructureconference/2020