



Securing the journey to DORA Fortinet Zero Trust Fabric

Paulo Rodrigues - Senior Solutions Architect Fortinet UK&I

DORA Fundamentals

- **Risk Management**

- set up and maintain resilient ICT systems and tools to identify and minimize ICT risk on a continuous basis, set up protection and prevention measures

- **Digital operational resilience testing**

- test the operational resilience of capabilities and functions included in the ICT risk management framework to identify weaknesses, deficiencies or gaps

- **ICT third-party risk**

- critical ICT third-party service providers in the financial sectors to adhere to an oversight framework.

- **Incident reporting**

- establish and implement a management process to monitor, classify and report major ICT-related incidents to competent authorities

- **Intelligence sharing**

- financial entities to set up arrangements to exchange cyber threat information and intelligence amongst themselves.



NIST Cyber Framework



Zero Trust is a Journey Not a Product



Best of Breed ??

Or Weakest Link ?

Gartner.

Licensed for Distribution

The Future of Network Security Is in the Cloud

Published 30 August 2019 - ID G00441737 - 32 min read

By Analysts [Neil MacDonald](#), [Lawrence Orans](#), [Joe Skorupa](#)

10/8/2019

Gartner Reprint

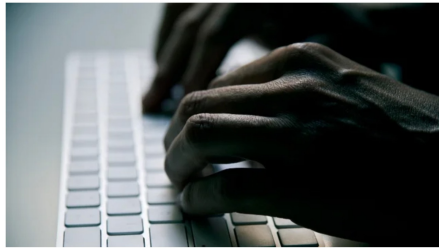
- Reduce complexity now on the network security side by moving to ideally one vendor for secure web gateway (SWG), cloud access security broker (CASB), DNS, zero trust network access (ZTNA), and remote browser isolation capabilities.



AXA insurance subsidiary group hit by ransomware attack in multiple Asian countries

BY MAGGIE MILLER - 05/17/21 02:16 PM EDT

SHARE TWEET



Most Popular

- 1 **Manchin blasts McConnell for...**
→ 511 SHARES
- 2 **Biden to propose \$6T budget...**
→ 370 SHARES
- 3 **Extinct giant bird claw with the...**
→ 331 SHARES

CYBER SECURITY NEWS · 4 MIN READ

Cyber Insurance Firm Suffers Sophisticated Ransomware Cyber Attack; Data Obtained May Help Hackers Better Target Firm's Customers

ALICIA HOPE · APRIL 5, 2021



A cyberattack struck the computer networks at New Orleans-based Pan-American Life Insurance Group last month, crippling communications ever since, according to a report by *The Times-Picayune*.

Liberty Mutual Scam: Insurance website used to file false unemployment insurance claims

carmellebruchesi · March 29, 2021

Department of Labor

Unemployment Benefits Jobs & Careers Business Support Workforce Protections Labor Data Resources

File a New Unemployment Insurance Claim

Our online system has been improved to better serve New Yorkers. You may file any day of the week from 7:30 AM to 7:30 PM.

HOW TO FILE APPLY ONLINE NOW

Click here to chat with our Virtual Assistant

Insurance Broker Gallagher Reports Ransomware Attack

September 29, 2020

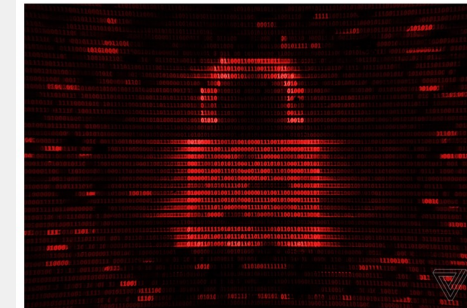


One of the US's largest insurance companies reportedly paid \$40 million to ransomware hackers

The ransom demands are rising

By Mitchell Clark | May 20, 2021, 6:06pm EDT

SHARE



verge deals

Subscribe to get the best Verge-approved tech deals of the week

Email (required)

By signing up, you agree to our Privacy Notice and European users agree to the data transfer policy.

SUBSCRIBE



Fortinet Security Fabric

Broad

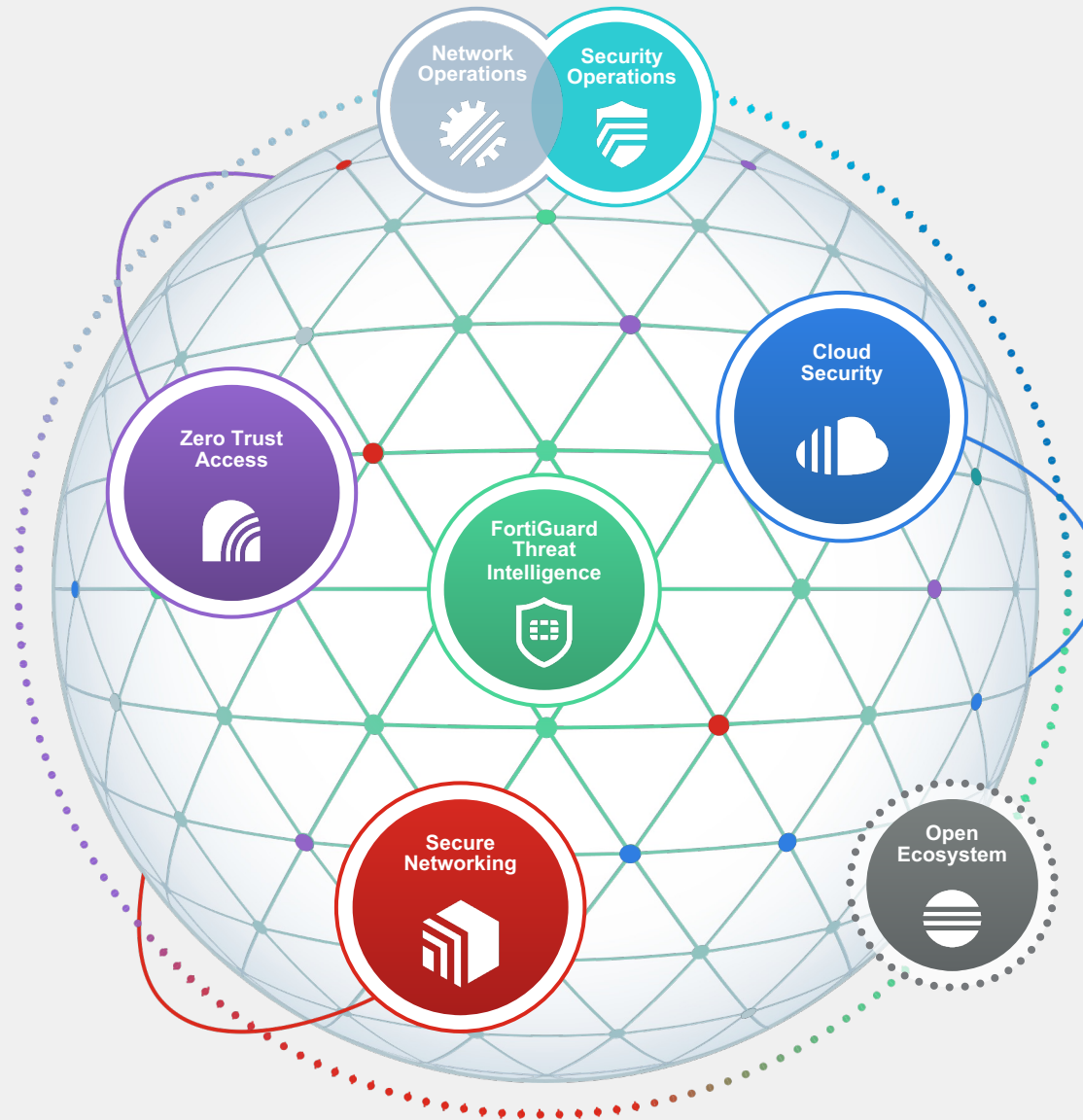
visibility and protection of the entire digital attack surface to better manage risk

Integrated

solution that reduces management complexity and shares threat intelligence

Automated

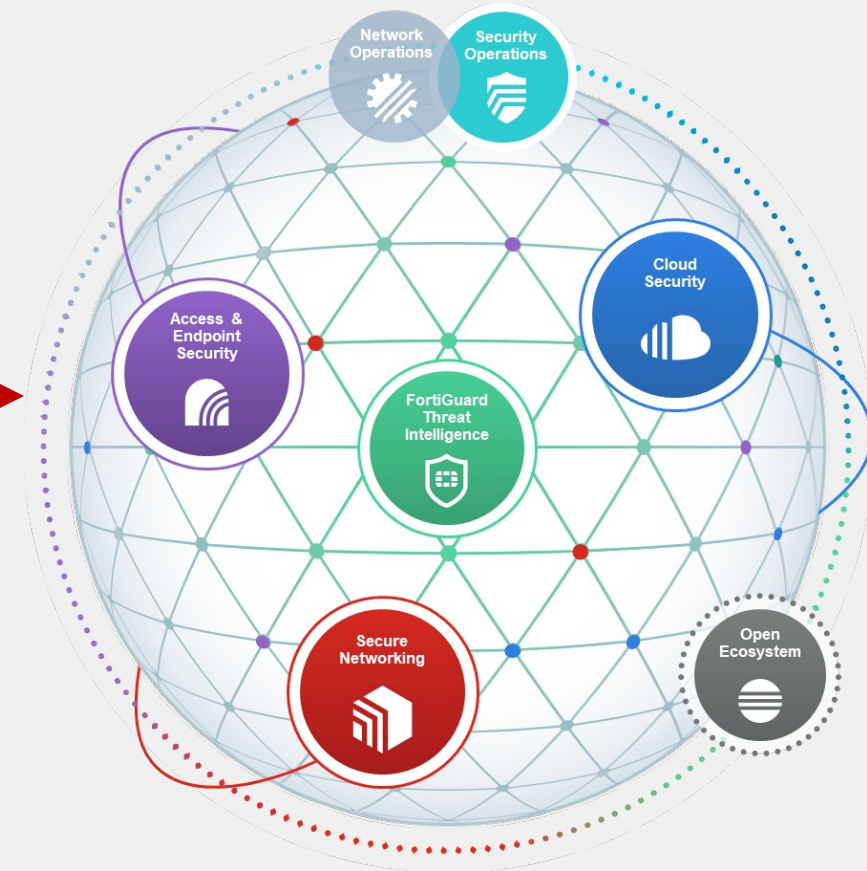
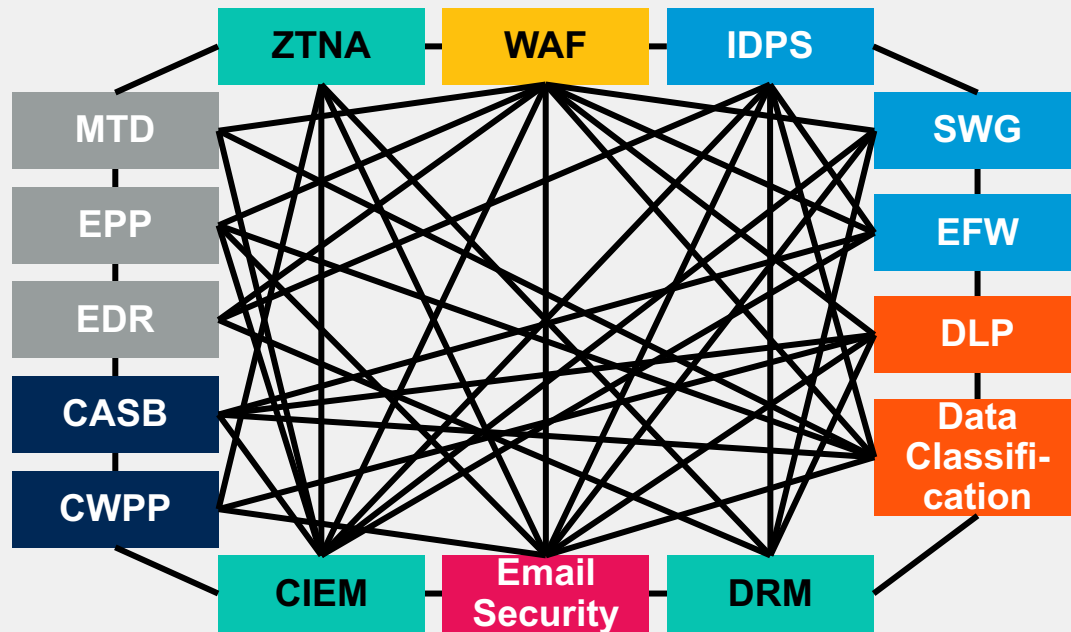
self-healing networks with AI-driven security for fast and efficient operations



Gartner Cybersecurity Mesh Architecture

Gartner®

FORTINET®



- Appliance
- Virtual
- Hosted
- Cloud
- Agent
- Container

Executive Guide to Cybersecurity Mesh, 2022

Felix Gaehtgens, James Hoover, Henrique Teixeira, Claudio Neiva, Michael Kelley, Mary Ruddy, Patrick Hevesi. As of October 2021

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Fortinet.



GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.


Steps to DORA?

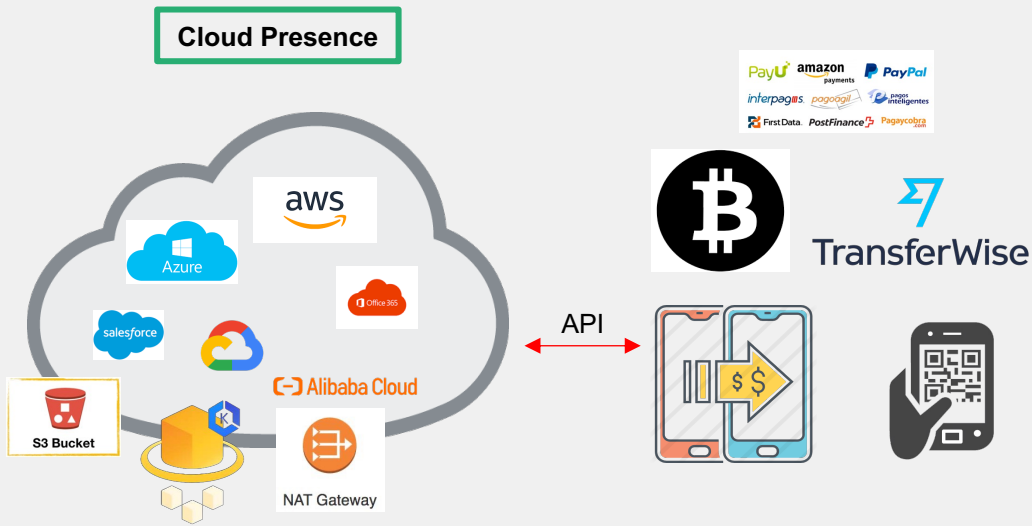




1. Risk Management

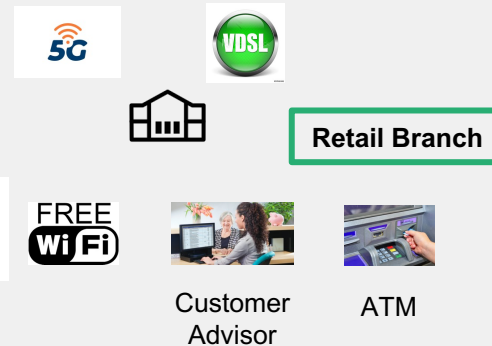
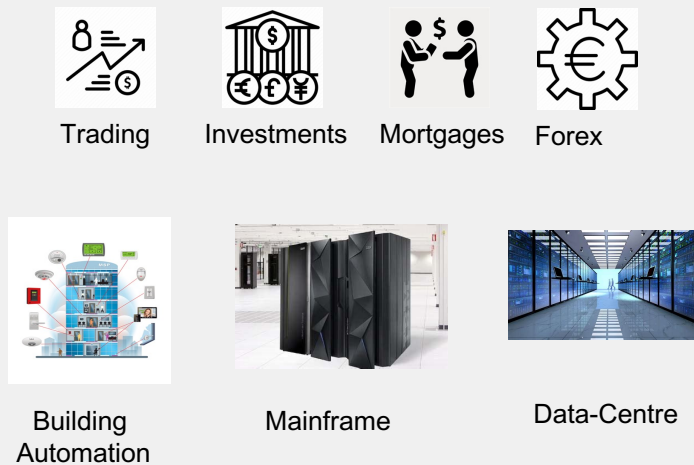
set up and maintain resilient ICT systems and tools to identify and minimize ICT risk on a continuous basis, set up protection and prevention measures



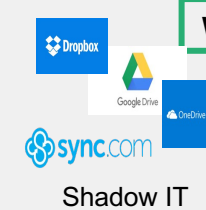
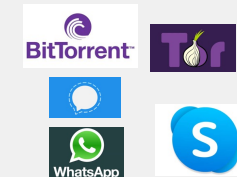


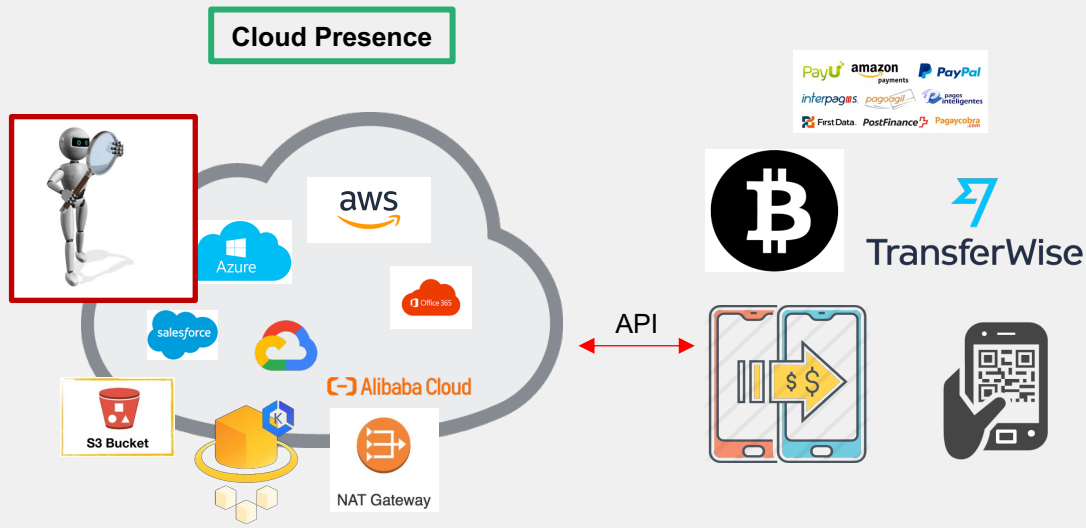
- **Asset Management**
- **Attack Surface Visibility**
 - 5G / SD-WAN adoption
- **3rd Party Risk**
 - Business partners
 - Contractors
- **Cohabitation risk**
 - IOT
 - Shared resource cross contamination
- **Unknown**

Head Office



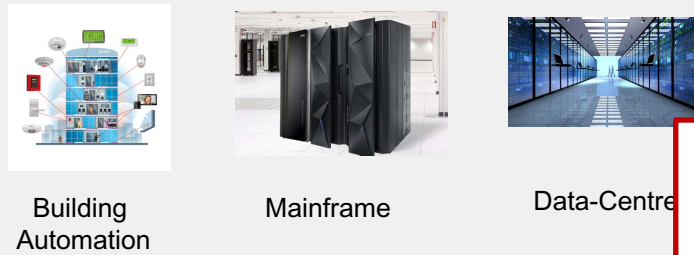
Poor User Hygiene



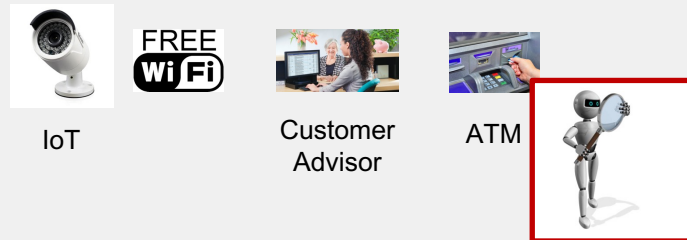


- **What & where is it**
 - **Asset Discovery visibility**
 - **What is it doing**
 - **Has its behaviour or profile changed?**

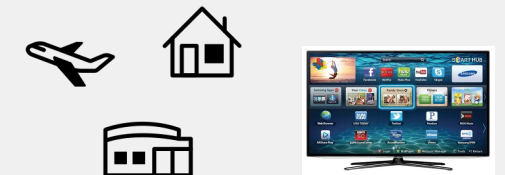
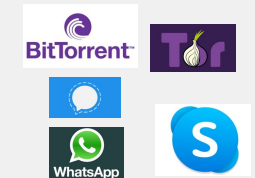
Head Office



Retail Branch



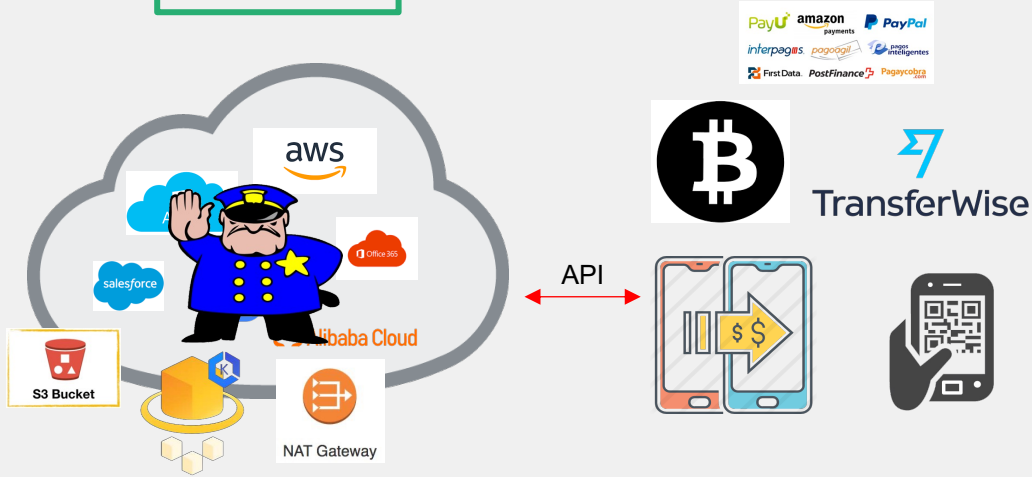
Poor User Hygiene



Work from Anywhere



Cloud Presence



- Who is it & what are they doing
 - Authentication– IAM/Cert?
 - Least privilege access - PAM/RBAC ?
 - Ongoing posture assessment

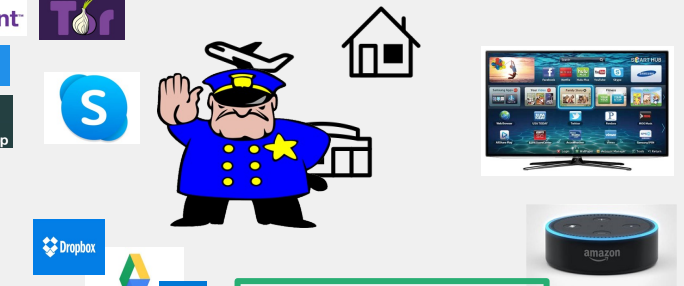
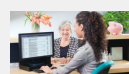
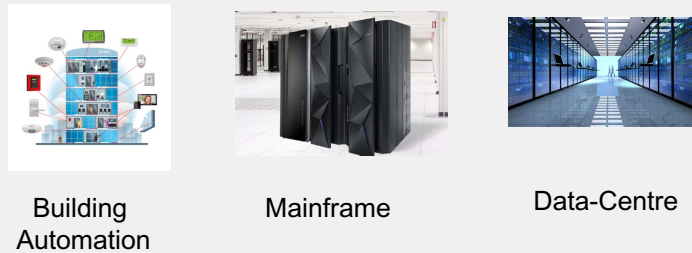
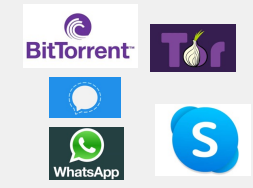
Head Office



Retail Branch



Poor User Hygiene

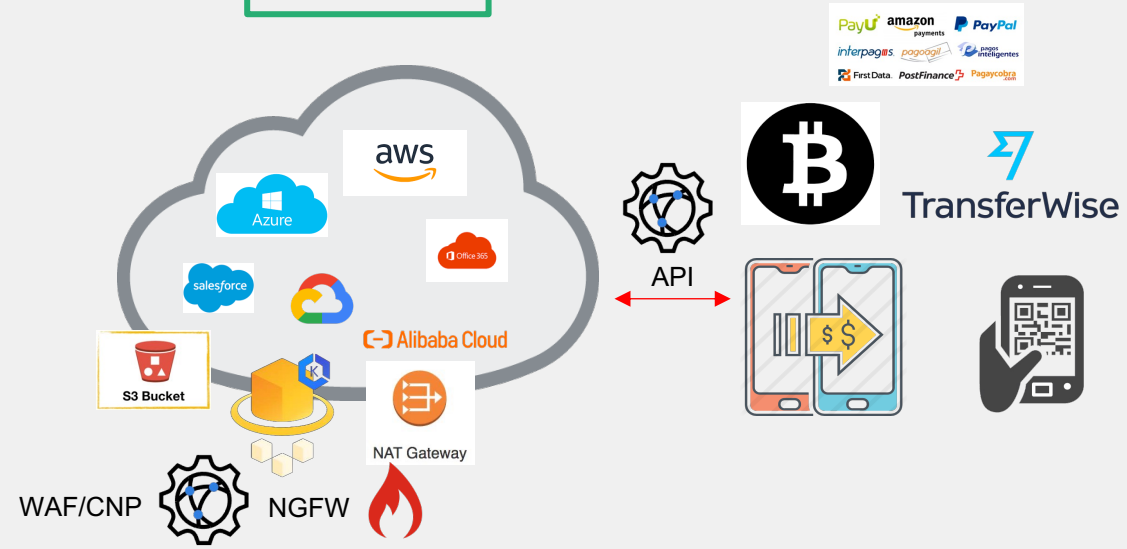


Work from Anywhere

IoT

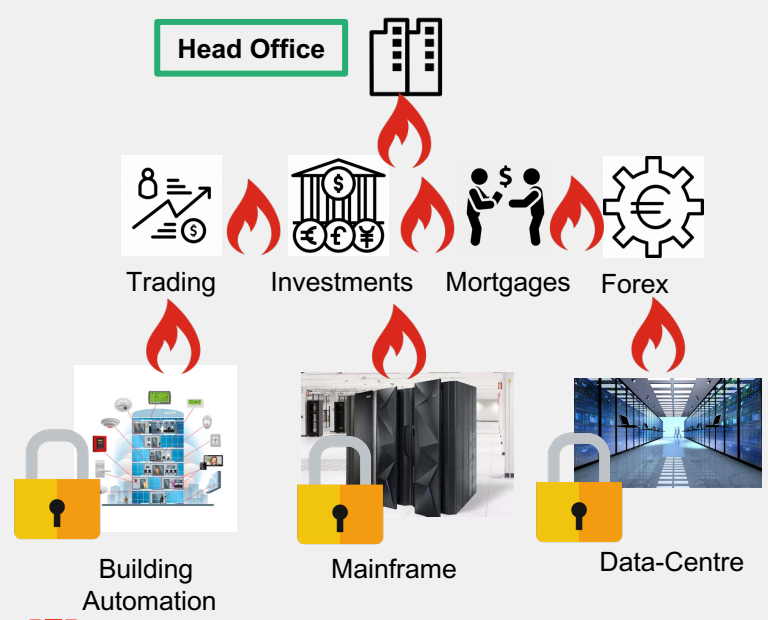


Cloud Presence



- **Segmentation & Isolation**
 - Macro L3-L7
 - Device layer Isolation
 - Nano user based
 - Security by obscurity

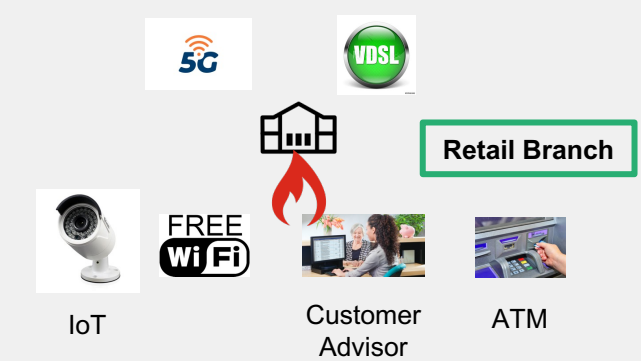
Head Office



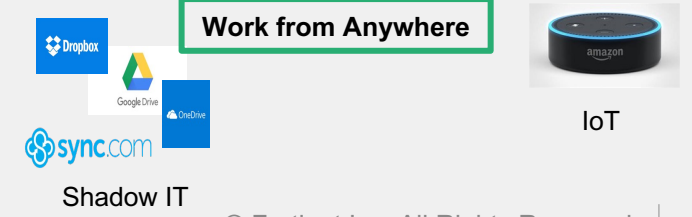
SASE

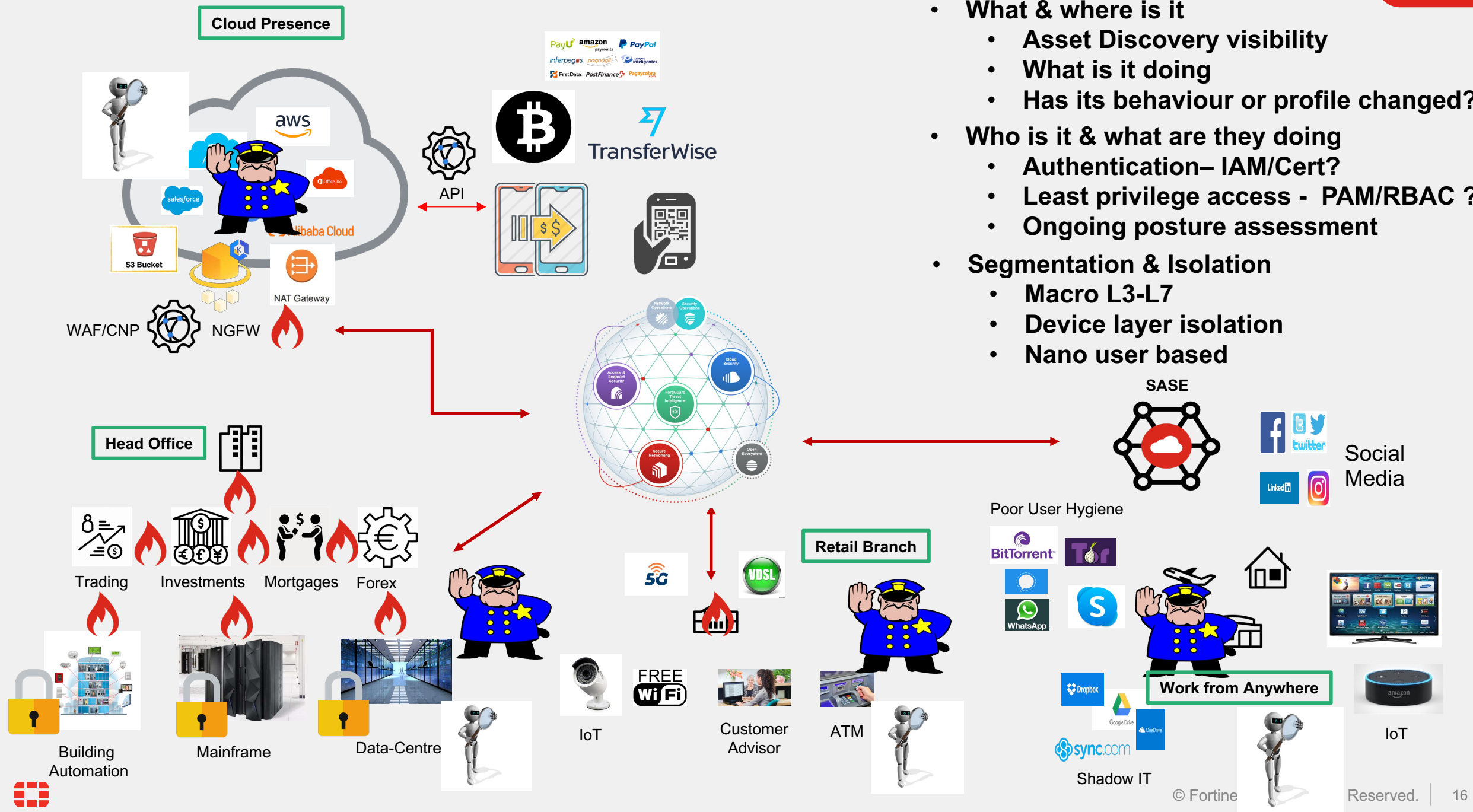


Retail Branch




Work from Anywhere



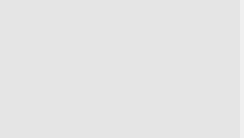
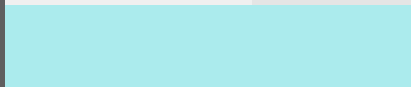




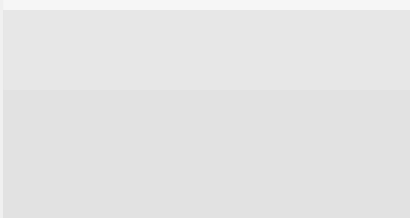


- **What & where is it**
 - **Asset Discovery visibility**
 - **What is it doing**
 - **Has its behaviour or profile changed?**
- **Who is it & what are they doing**
 - **Authentication– IAM/Cert?**
 - **Least privilege access - PAM/RBAC ?**
 - **Ongoing posture assessment**
- **Segmentation & Isolation**
 - **Macro L3-L7**
 - **Device layer isolation**
 - **Nano user based**



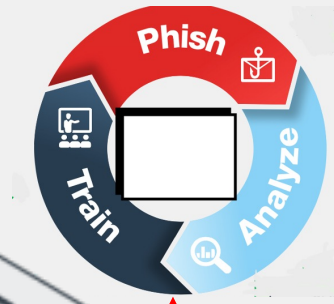
2. Digital operational resilience testing

Test the operational resilience of capabilities and functions included in the ICT risk management framework to identify weaknesses, deficiencies or gaps.





Cyber Education

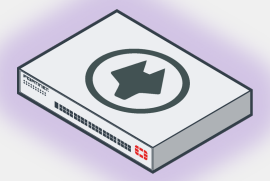


SaaS Pentest Service

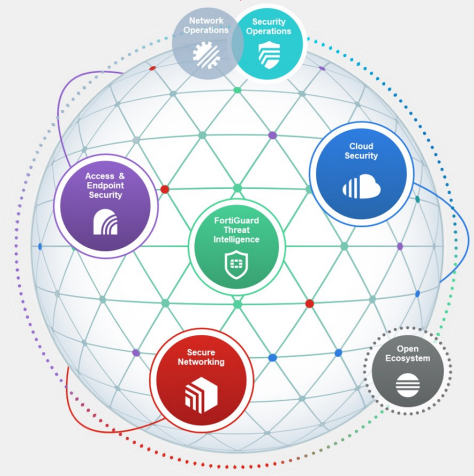
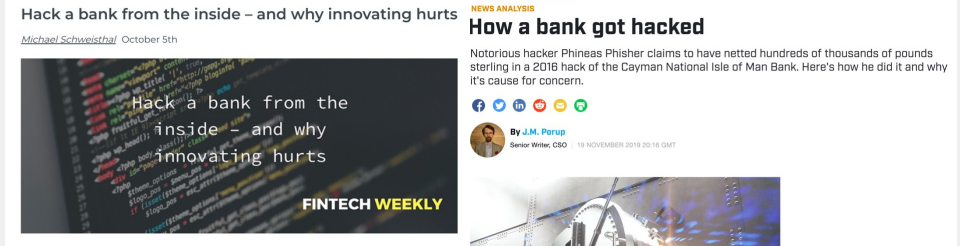


Secure Mail Gateway

Email borne threats & Human naivety

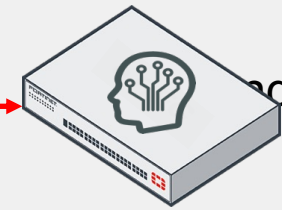
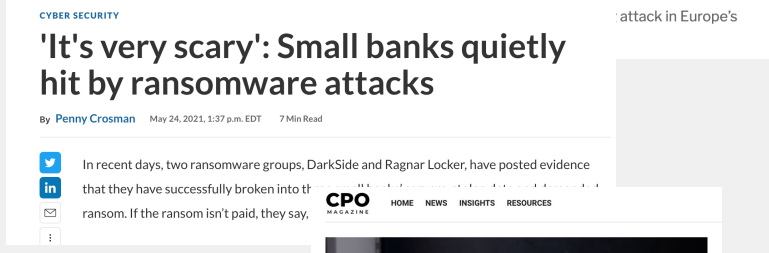


Deceive, Lure, Expose, Terminate



Exposed Network Services

Italy's largest bank HACKED in major security breach as data from 400,000 accounts stolen



AI Engine
Learn, Profile, Normalise, Identify
Terminate

Steal & Spread



Infiltrate & fingerprint





3. ICT third-party risk

Assess, monitor and document ICT third-party risk



Reconnaissance

FortiRecon (SaaS)

FortiRecon

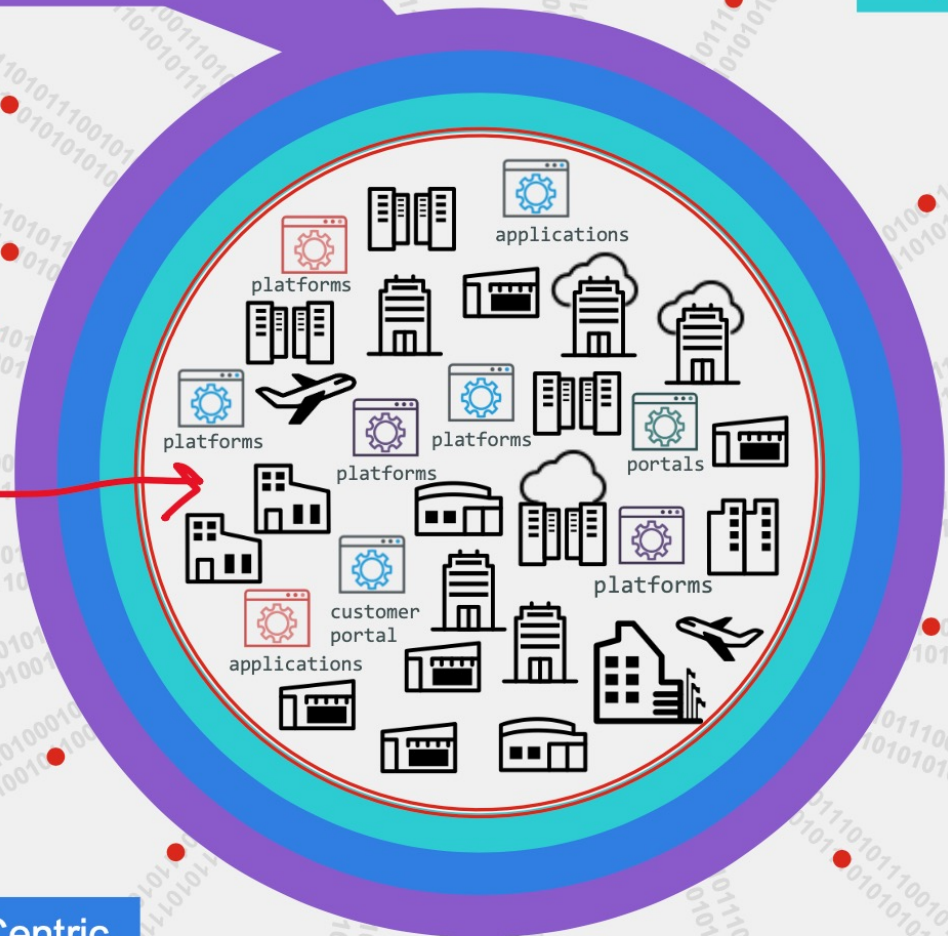


External Attack Surface Management (EASM)

Brand Protection (BP)



Your Business



Adversary Centric Intelligence (ACI)

- View organisation from outside
- Brand & Reputation protection
- Monitors Web & Dark Web
- Impersonation detection
- Detect Credential leaks, Campaigns etc



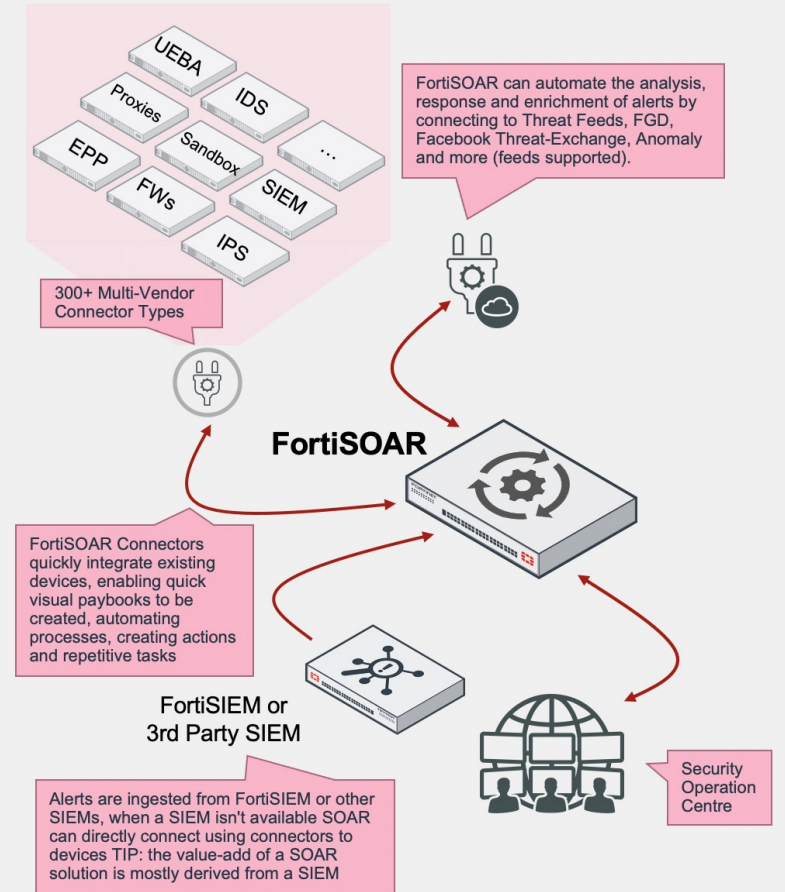
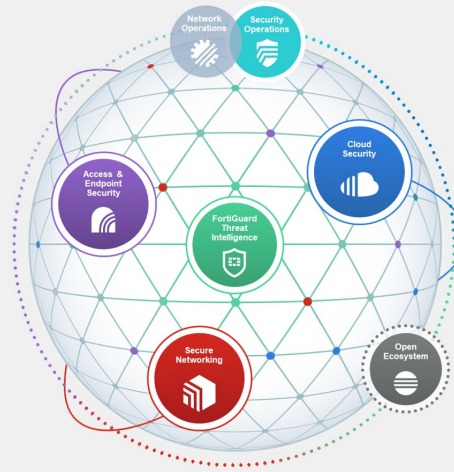
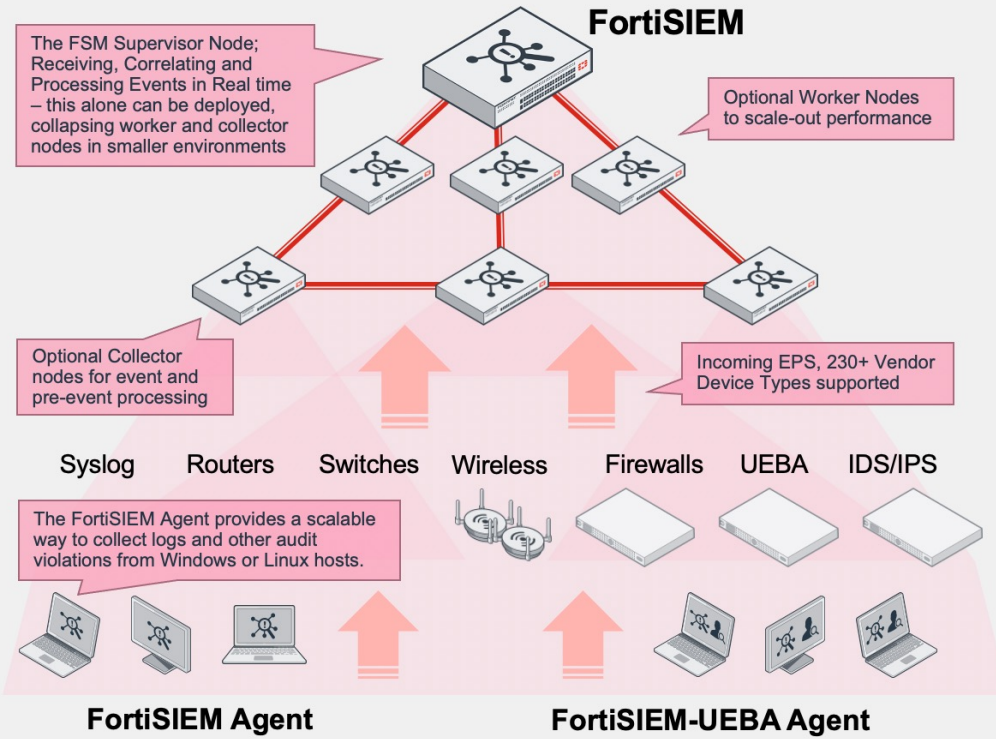


4. Incident Reporting

Establish and implement a management process to monitor, classify and report major ICT-related incidents to competent authorities



Incident Reporting



SIEM: Security Incident & Event Management

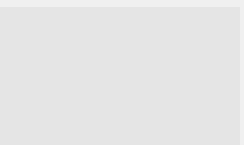
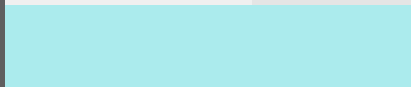




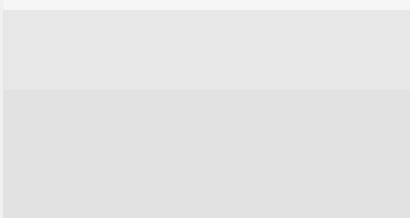
SOAR: Security orchestration, automation and response





5. Intelligence Sharing

Set up arrangements to exchange cyber threat information and intelligence amongst themselves.



FortiGuard Labs Overview

VISIBILITY

Telemetry
 Network
 Web
 Sandbox
 Email
 Endpoint

Enforcement Partnerships

OSINT

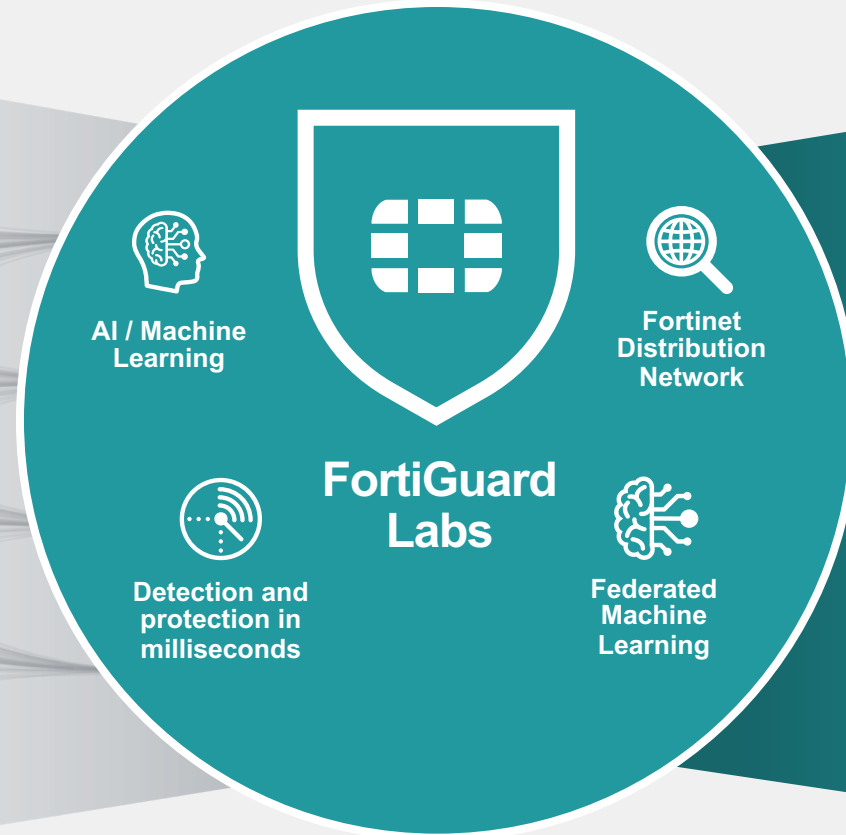
Trusted Partnerships

CERTs

Zero-Day

CYBER THREAT ALLIANCE CTA feeds

INNOVATION



ACTIONABLE THREAT INTELLIGENCE

SECURITY FABRIC PROTECTIONS

- IPS
- Application Control
- Web Filtering
- Anti-Virus
- Anti-Spam
- Endpoint Vulnerability
- Indicators of Compromise (IoCs)

PROACTIVE RESEARCH

- Adversary Playbooks
- Security Blogs
- Threat Intel Briefs
- Threat Signals
- Virtual Patches

THREAT INTELLIGENCE SERVICES
































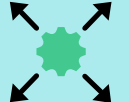





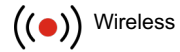



- Penetration Testing
- Phishing Service
- Incident Response
- Detailed Threat Analysis
- Architecture Evaluation
- Cybersecurity Workshops

Fabric Ingest: Mitre ATT&CK Framework, TAXII, STIX, CSV, HTTP
 Fabric export: TAXII, SYSLOG, CSV



Open Ecosystem

480+ Best-in-class integrated solutions for comprehensive protection

 <p>Fabric Connectors</p>	<p>Fortinet-developed deep integration automating security operations and policies</p>	 	 	 	 	
 <p>Fabric APIs</p>	<p>Partner-developed integration using Fabric APIs providing broad visibility with end-to-end solutions</p>	 	 	 	 	 
 <p>Fabric DevOps</p>	<p>Community-driven DevOps scripts automating network and security provisioning, configuration, and orchestration</p>	 	 	 	 	
 <p>Extended Ecosystem</p>	<p>Integrations with threat sharing initiatives and other vendor technologies</p>	 	 	 	 	

Figures as of March 31, 2021
 Note: Logos are a representative subset of the Security Fabric Ecosystem



Fortinet Fabric DORA Summary

Risk Management

- Asset discovery
- Security posture assessment
- Behavioural monitoring
- Identity Management
- Least privilege access
- Posture based segmentation

Digital Operational Resilience testing

- Cyber education + weak link identify
- Email & Content deconstruction
- Deception de-obfuscation
- Exposed asset pen-testing
- AI baselining & anomaly detection

ICT 3rd Party Risk

- External Malicious actor view
- Brand & Reputation protection
- Impersonation detection
- Detect credential leaks
- Monitor Web & Dark Web

Incident Reporting

- Multi-source log collation
- Ingest, normalise, contextualise
- Workflow + playbook
- AUTOMATION !!!
- Threat Response
- Export / Share

Intelligence Sharing

- Global threat intelligence
- Multiple formats – STIX, TAXII, CSV, MITRE
- Import & Export
- Broad Fabric Alliance Integration.





Contact
Paulo Rodrigues
prodrigues@fortinet.com