opengear
A DIGI COMPANY

OOB Network

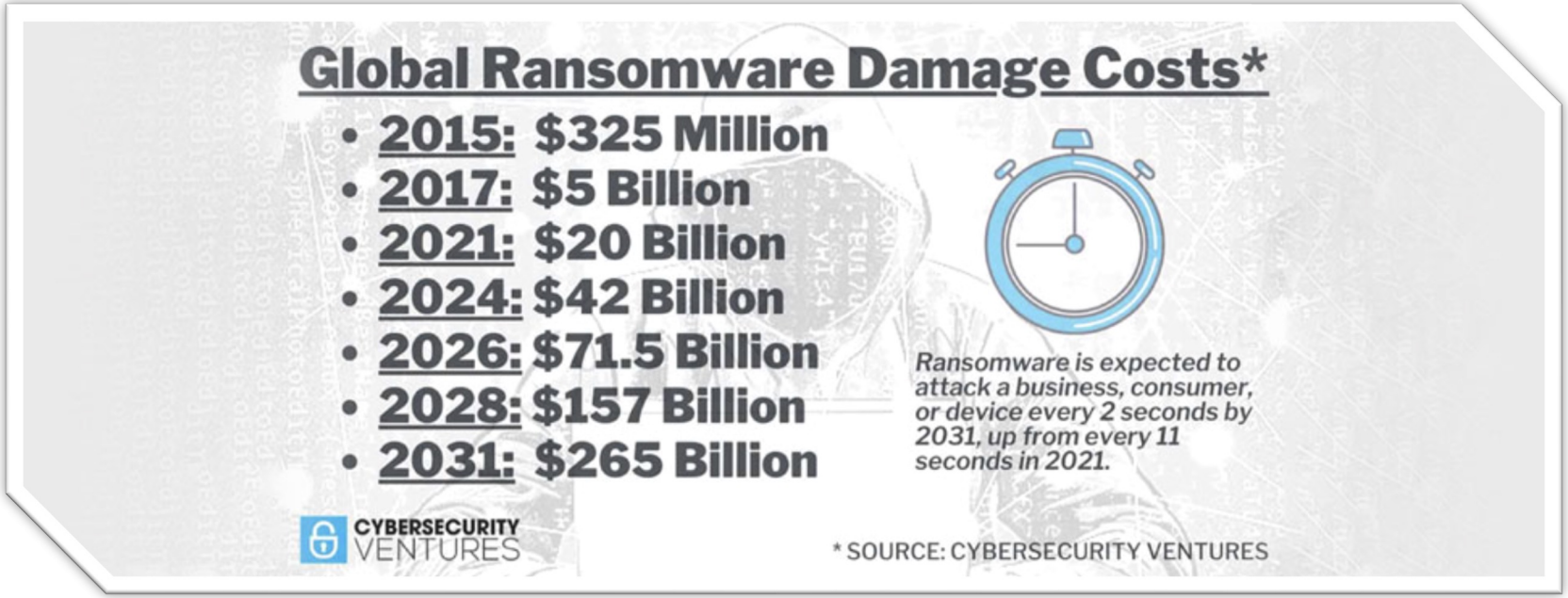
Fortify Your Management Network Against Security Threats

Sachin Mhankal – Sales Engineer, India

Predictions and Priorities CIO/CTO

AI	Automation	CyberSecurity

The Number and Sophistication of Cyber Attacks Will Increase

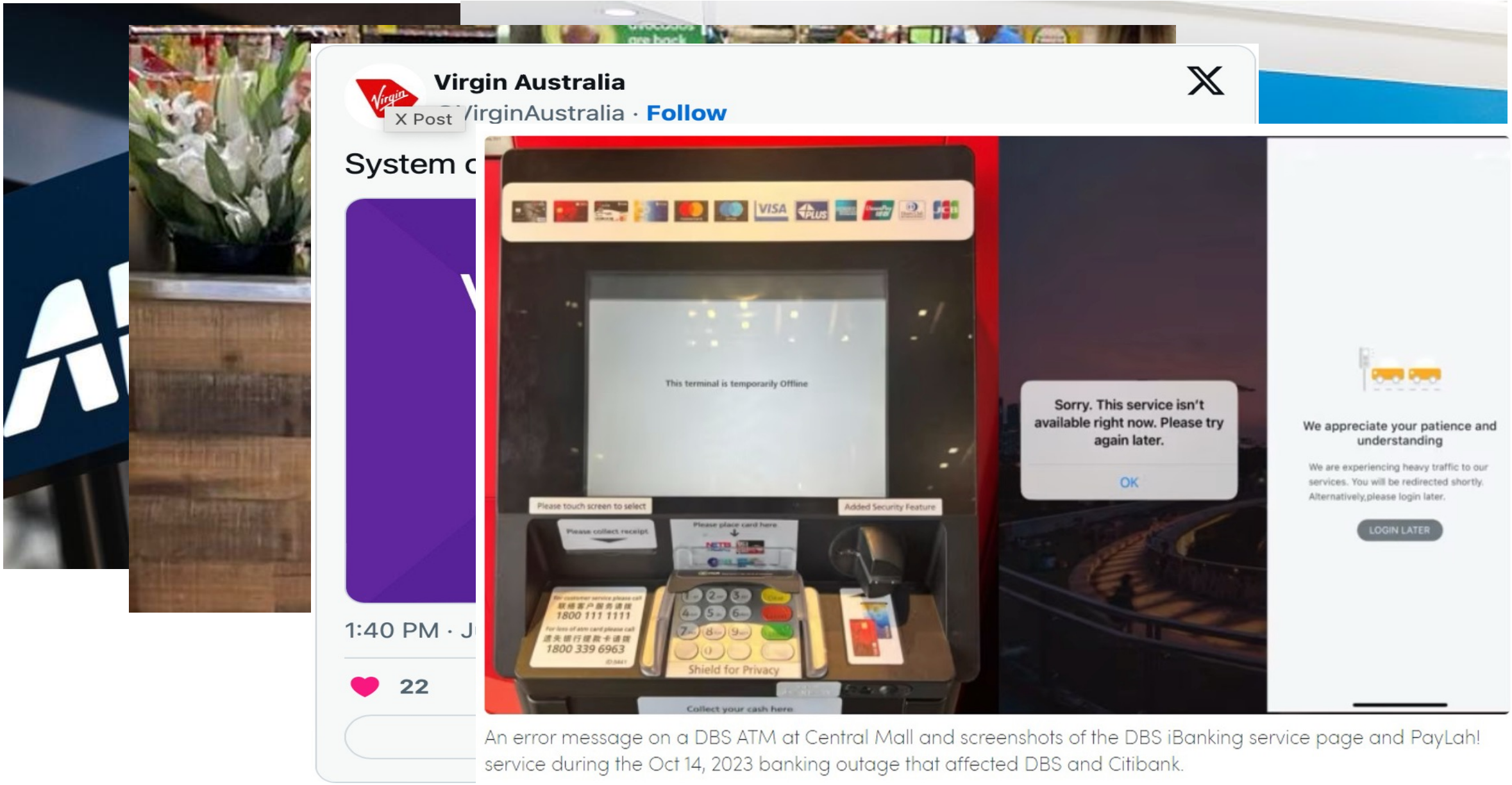


Top 10 Cybersecurity Threats in 2024

Extract from https://www.embroker.com/blog/top-cybersecurity-threats/

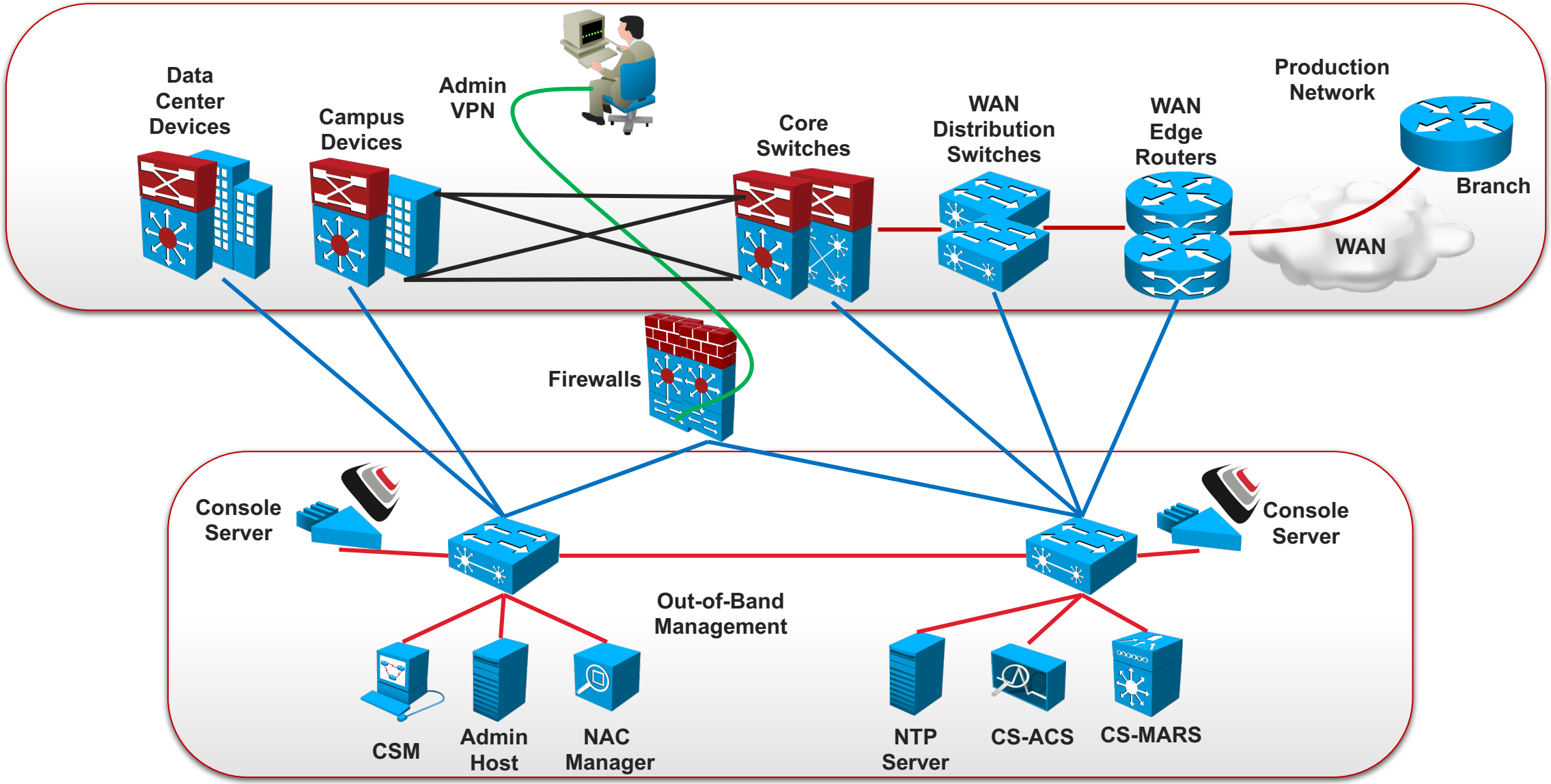
- We're likely to see security threats become more sophisticated and therefore more expensive over time: experts predict that the global costs of cybercrime will reach $10.5 trillion by 2025, up 15% from $3 trillion in 2015.

Challenges during Cyber Security Attacks



An error message on a DBS ATM at Central Mall and screenshots of the DBS iBanking service page and PayLah! service during the Oct 14, 2023 banking outage that affected DBS and Citibank.

Legacy Network, Legacy Out-of-Band Management Network



The problem(s)

Limitations

A major pain point associated with traditional management network is that it does not extend well to remote locations with IT infrastructure. It does not enable proper “bootstrapping” of remote IT infrastructure.

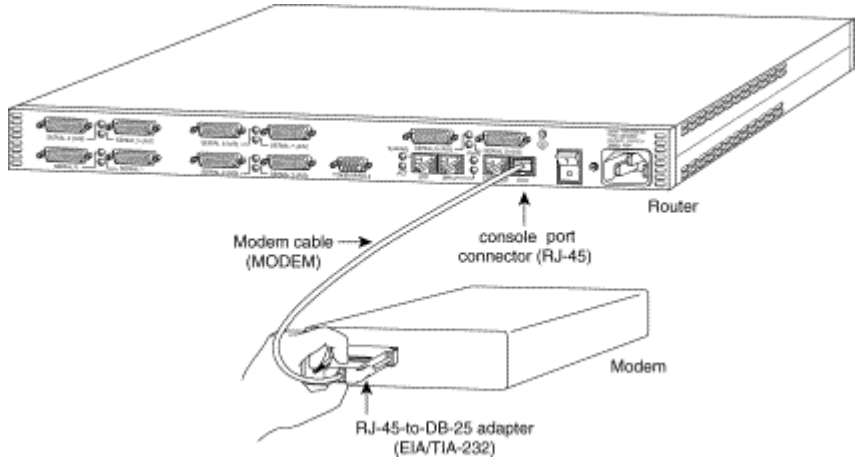
When it does, it is often times limited to serial connectivity or static methods to reach IP endpoints.

Capitalist forces apply pressures to reduce cost of infrastructure management. Infrastructure management organizations are being asked to do more with less.

“What more can the solution do, since its is already there?”

How Remote Access Starts

- Started off by using an analogue modem and a console cable.



- A **console server** (also referred to as terminal server) is a device or service that provides access to the system console of a computing device via networking technologies.

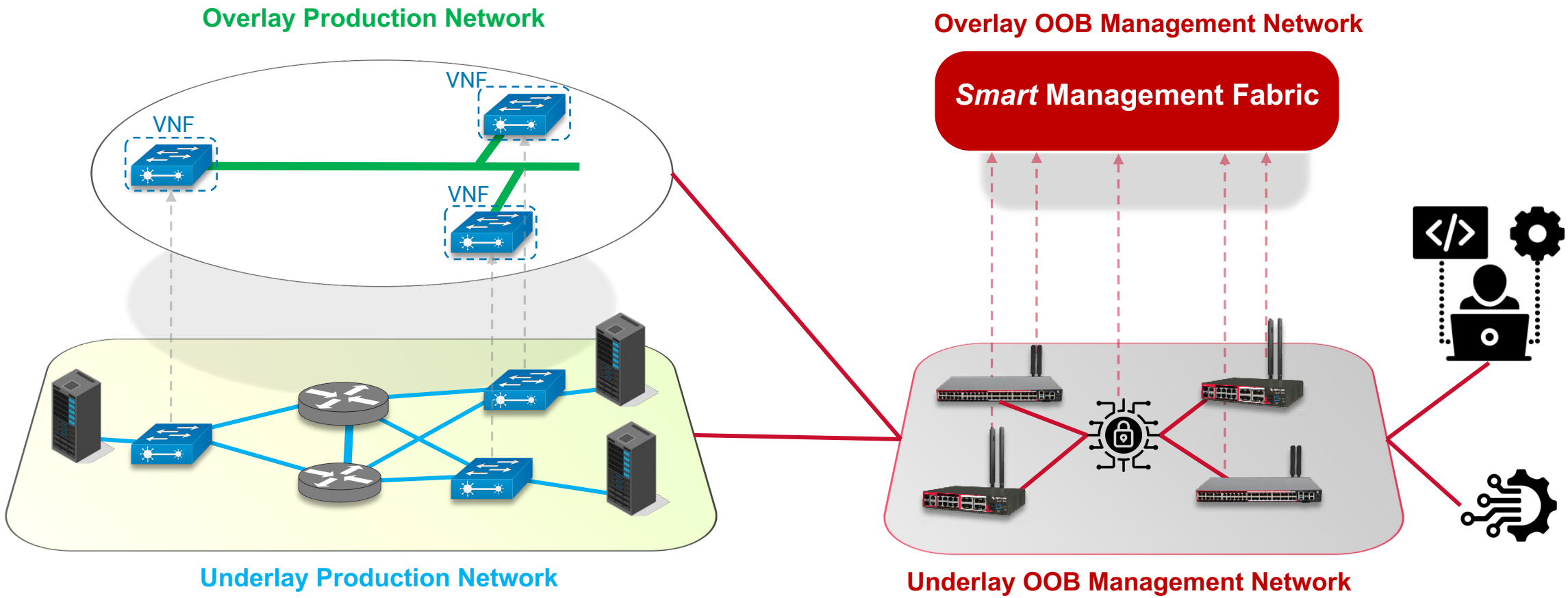
- An **in-band management** involves managing devices through the protocols such as telnet/SSH, RDP/VNC. When network is down and traffic is not flowing, an alternate path is required to reach the network nodes (**especially critical networks**). Here we need a secure remote emergency network access path to manage and troubleshoot the device when network traffic is down. Thus, **out-of-band management** as in-band management tools are **not enough**.

- Most users used in-band management to access to their endpoint devices.

- So how about NOW, where networking had evolved, and security had become a major concern?

Modern Network

Modern Out-of-Band Management Network – *Smart* Management Fabric



Network Isolation & Emergency Access: OOB's Dedicated Pathway

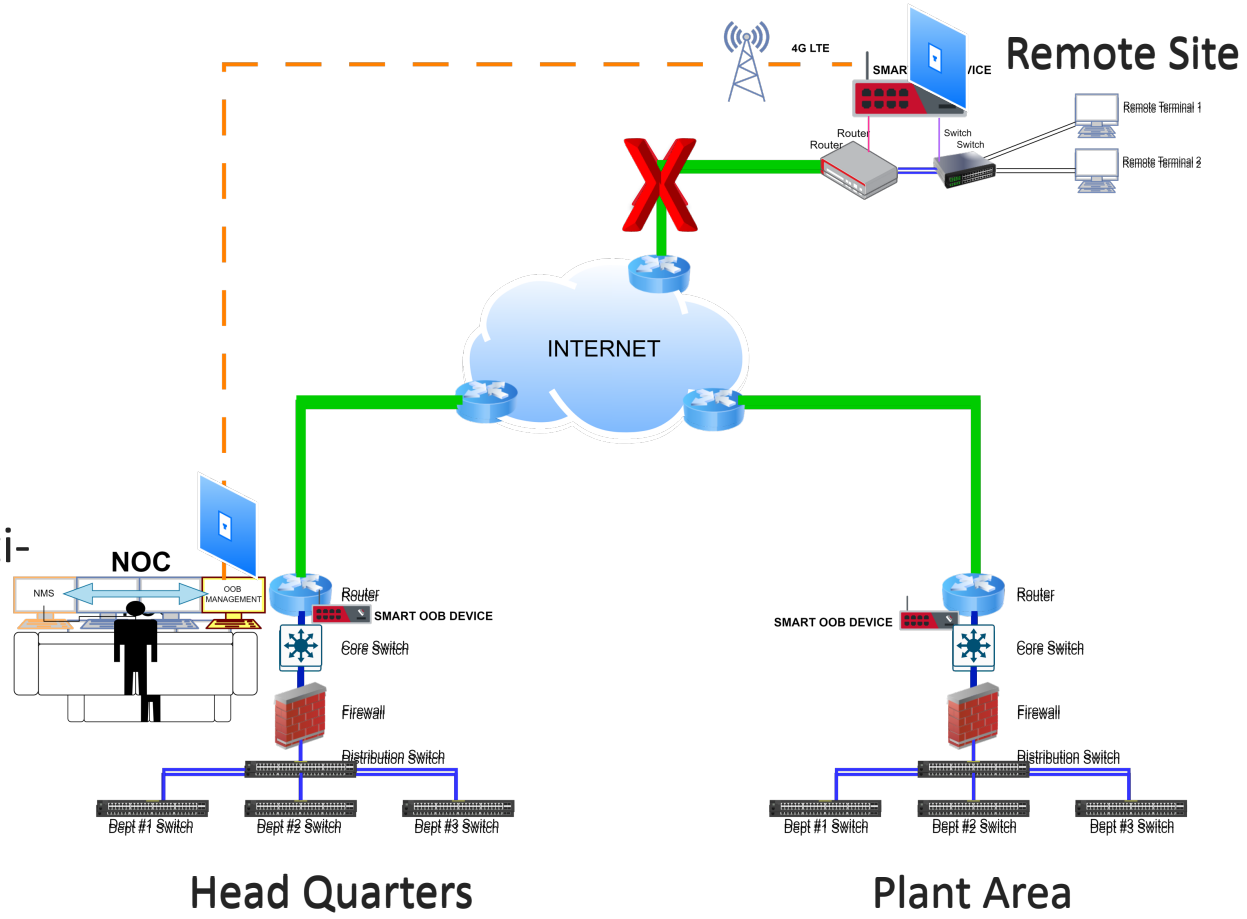
Problem Statement: Networks face threats not just externally but also from within; **reliance on a single network** for management can be a significant vulnerability.

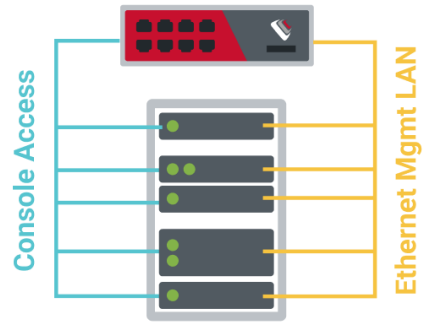
Current Practices: Organizations often use complex, multi-layered security measures, yet some deployments share the same infrastructure for both production and management traffic.

OOB Solution:

Everyday: OOB provides a separate, secure network, enhancing defenses by **isolating management traffic**.

Worst day: Offers a reliable, **alternative access** route with distinct credentials for emergencies, reducing risk.





Secure Deployment and Recovery with OOB Centralized Management

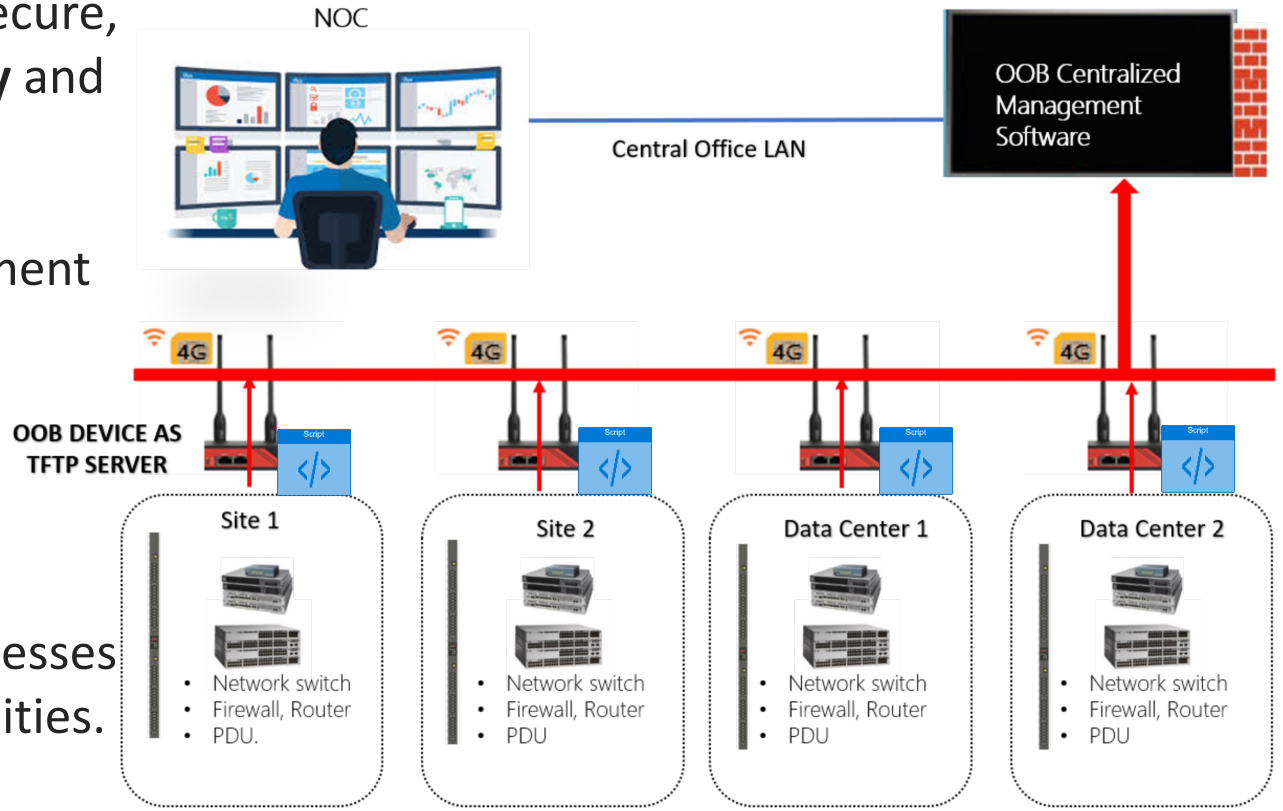
Problem Statement: Cybersecurity threats requires a secure, resilient network architecture capable of rapid **recovery** and secure **redeployment**.

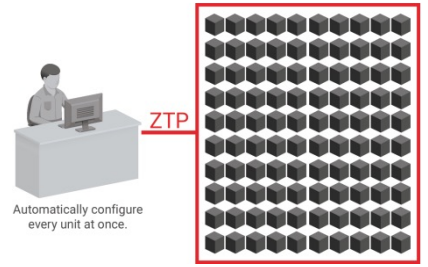
Current Practices: Regular patching and secure deployment practices are essential, but often not enough to quickly recover from sophisticated Cybersecurity attacks.

OOB Advantage:

Everyday: Ensure continuous, secure patching processes via OOB, **unaffected** by primary network vulnerabilities. segregated environment to limit access as needed.

Worst day: **Rebuild** and **re-deploy** your production environment securely through OOB, even during a network compromise.





OOB for Enhanced Monitoring, Compliance, and Stealthy Security

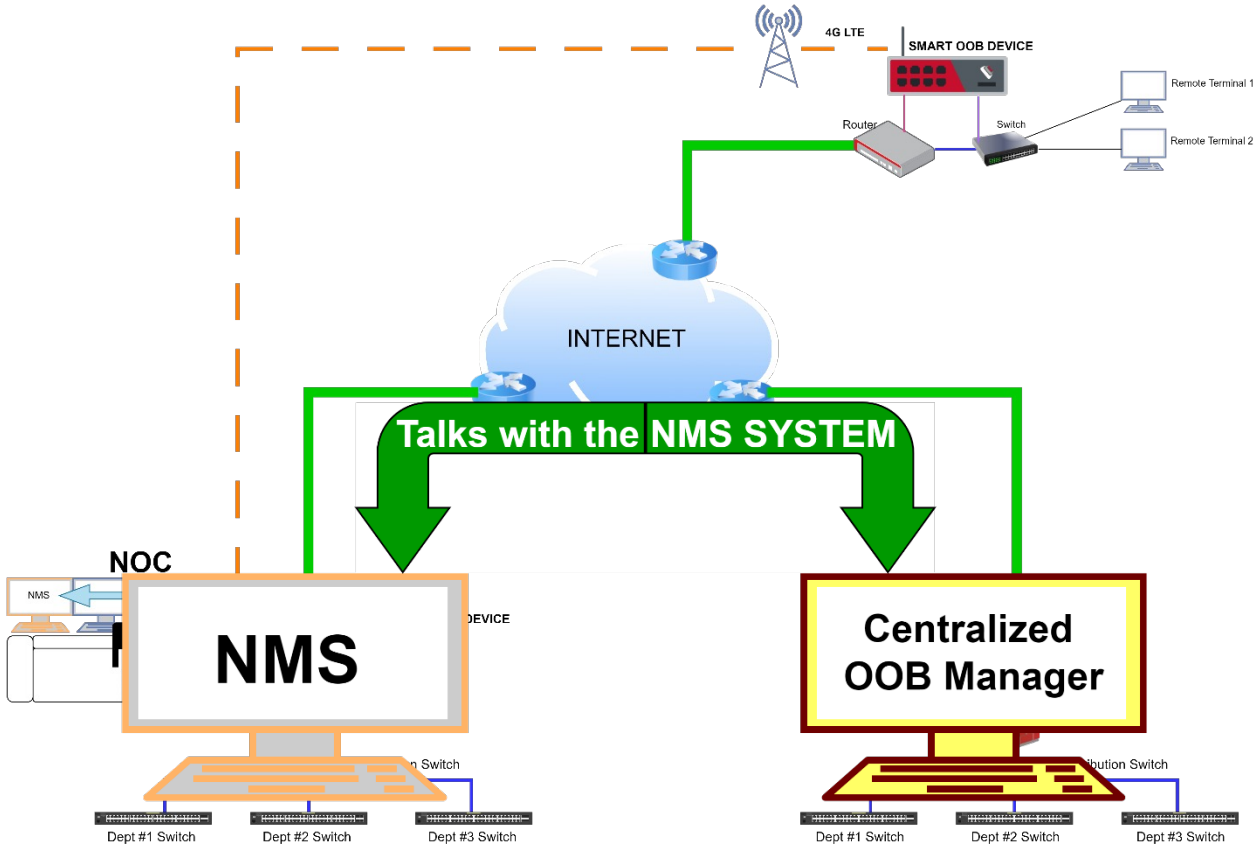
Problem Statement: Continuous monitoring and compliance are crucial, yet **visible security activities** can tip off unauthorized users, including potential attackers.

Current Practices: Security teams implement port logging and maintain playbooks for incident response but typically within the primary network, risking exposure and interference.

OOB Solution:

Everyday: OOB networks offer a **secure**, hidden channel for monitoring and logging, away from prying eyes.

Worst Day: Automated playbooks can **react to incidents** outside the primary network, ensuring responses are discreet and effective.



OOB as the Foundation of Trustworthy Operations

Problem Statement: Maintaining a reliable **source of truth** for network configurations and data integrity is challenging amidst evolving security threats.

Current Practices: Organizations rely on Trusted Platform Modules (TPM), secure copy protocols (scp), and data gathering solutions, yet often within the same network as their operating environments. Encrypting data at rest secures files and documents, ensuring that only those with the key can access them.

OOB Integration:

First day: Establishes OOB as a secure path for **'source of truth**' of configurations and data, independent of the primary network.

Everyday: Enhances data gathering and **secure configuration storage** through isolated, protected pathways.

Everyday: **Expands the reach of security tools** while ensuring their operations are safeguarded from network threats.

End User – Real Life case

Customer A - ransomware attack on one of their sites in the network.

- The Network was built with traditional access to the devices.
- When the attack occurred, the onsite engineer was not able to take any action.
- With no remote access to the device, the admin was unable to take any immediate action.
- They had to run from post to pillar to reach the site and take evasive actions.

After this attack – Introduced Smart OOB solution

- OOB Operates independently from the in-band network (Cellular Connectivity)
- The OOB Solution helps them to access any devices from any site remotely via a secured path.
- The entire network is managed remotely.

Customer B – Preconfigures the OOB device and sends in the racks.

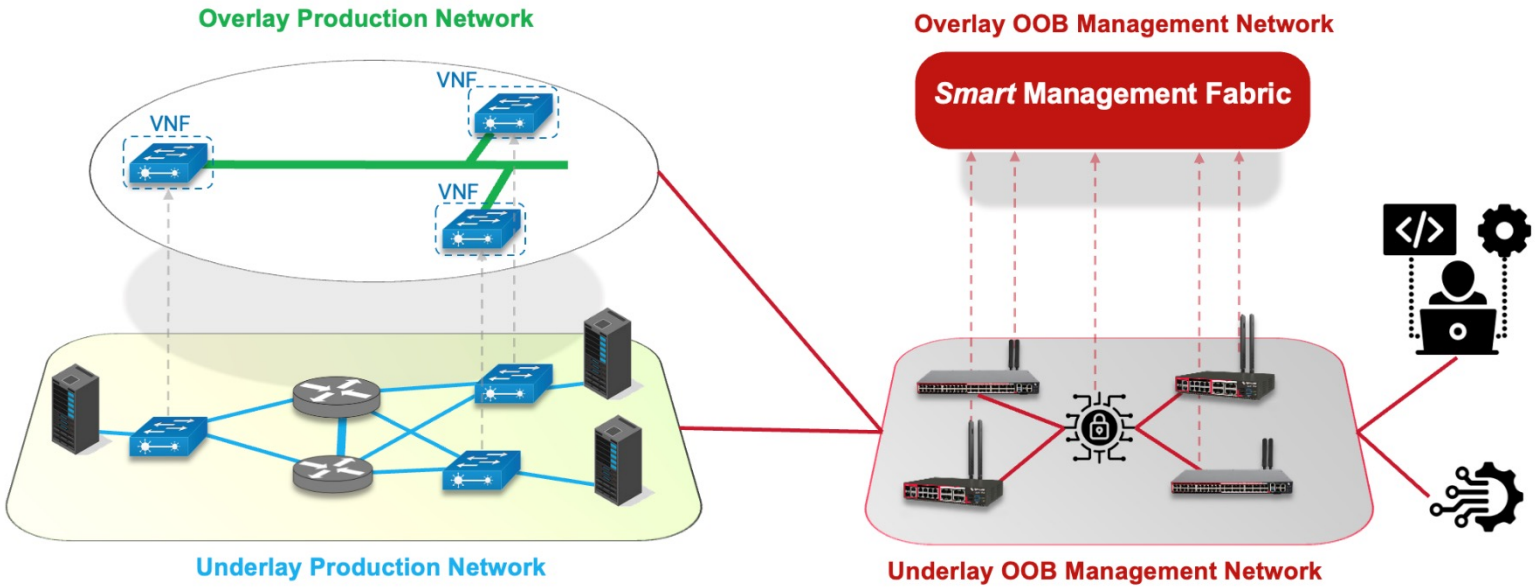
- This is a Multinational customer with lot of remote sites, where they do not have engineers on site.
- Customer pre-configures the OOB device and then fixes the OOB into the rack that is shipped to the remote site.
- Once the rack & devices are mounted and powered on, Admin takes control remotely and configures the site.

With OOB solution

- Necessity of remote site engineer is reduced.
- OOB Operates independently from the in-band network (Cellular Connectivity)
- The OOB Solution helps them to access any devices from any site remotely via a secured path.
- The entire network is managed remotely, and reports are sent to leadership team regularly.

Closing – Smart OOB is must to have for Networks

- Cybersecurity is an **on-going daily** activity
- Organization must have **alternative access** route with distinct credentials for emergencies, reducing risk.
- It applies to all layers of the network infrastructure, from Core to Access.
- **Do not** use your network to manage your network.



opengear
A DIGI COMPANY

Thank You

www.opengear.com