WAVESTONE

WHAT IS THE NEXT GENERATION CYBERSECURITY MODEL?

CLOUD-BASED SERVICES, DIGITAL TRANSFORMATION AND OPEN SYSTEMS ARE PLACING EVER GREATER DEMANDS ON CYBERSECURITY PROFESSIONALS. AS A RESULT, WE NEED TO EVOLVE BEYOND TRADITIONAL MODELS (USUALLY REFERRED TO AS “CASTLE/FORTRESS” AND “AIRPORT”) TOWARDS A NEW AGILE CYBERSECURITY MODEL REFERRED TO AS THE "AIRLINE” MODEL. IT IS BASED ON A DECENTRALISED INFORMATION SYSTEM DESIGNED TO PREVENT ADVANCED THREATS AND DELIVER EFFECTIVE CYBERSECURITY.

INSIGHT

1 THE EVOLUTION OF CYBERSECURITY MODEL

1.1 THE CASTLE/ FORTRESS – A CENTRALISED INFORMATION SYSTEM

Previously, information systems were protected by a strong security wall, based on a traditional castle/ fortress model. This was based on only one entry point. Once inside, users could circulate freely. However, this centralised information system can no longer deal with the scale of change in data and connections, as users have multiple access options across a variety of devices. These developments exposed the constraints of the fortress model.

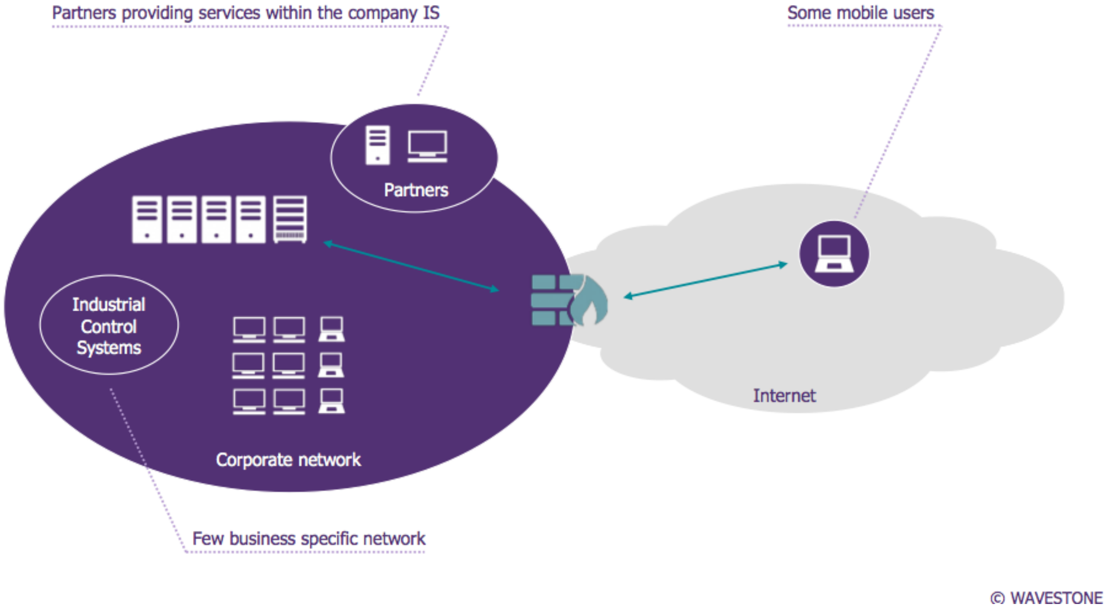

Partners providing services within the company IS
Some mobile users
Partners
Industrial Control Systems
Internet
Corporate network
Few business specific network
© WAVESTONE

Figure 1: The "Castle/Fortress" cyberecurity model

1.2 THE AIRPORT – AN INCREASINGLY OPEN INFORMATION SYSTEM

The next evolution in security was the “Airport” model, based on an increasingly open information system, consisting of different zones with different levels of security, similar to an airport.

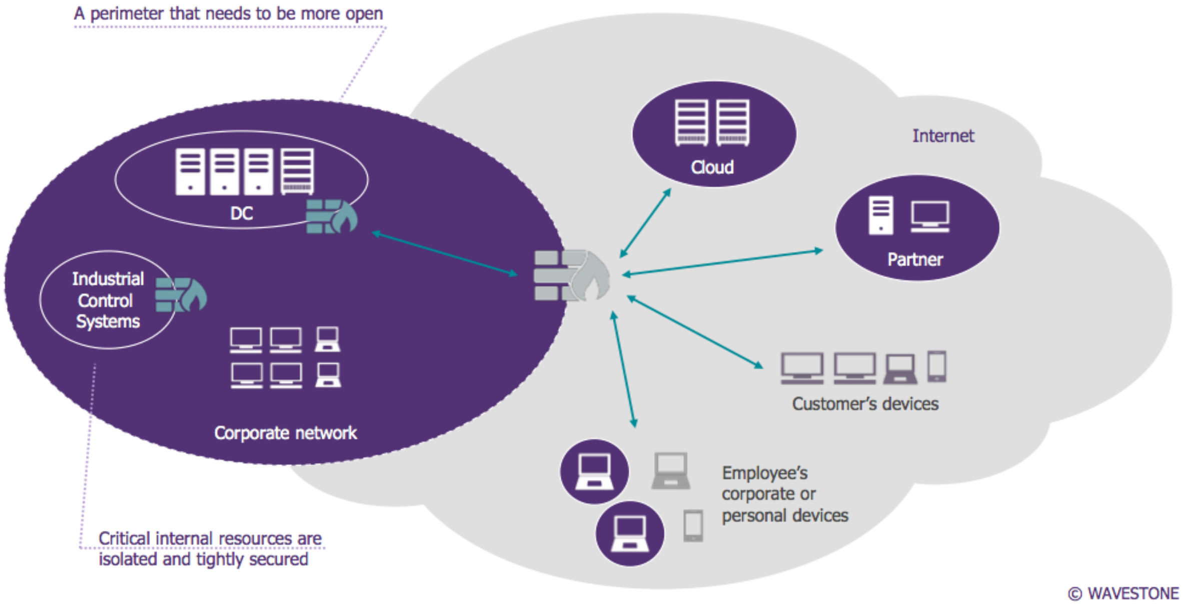
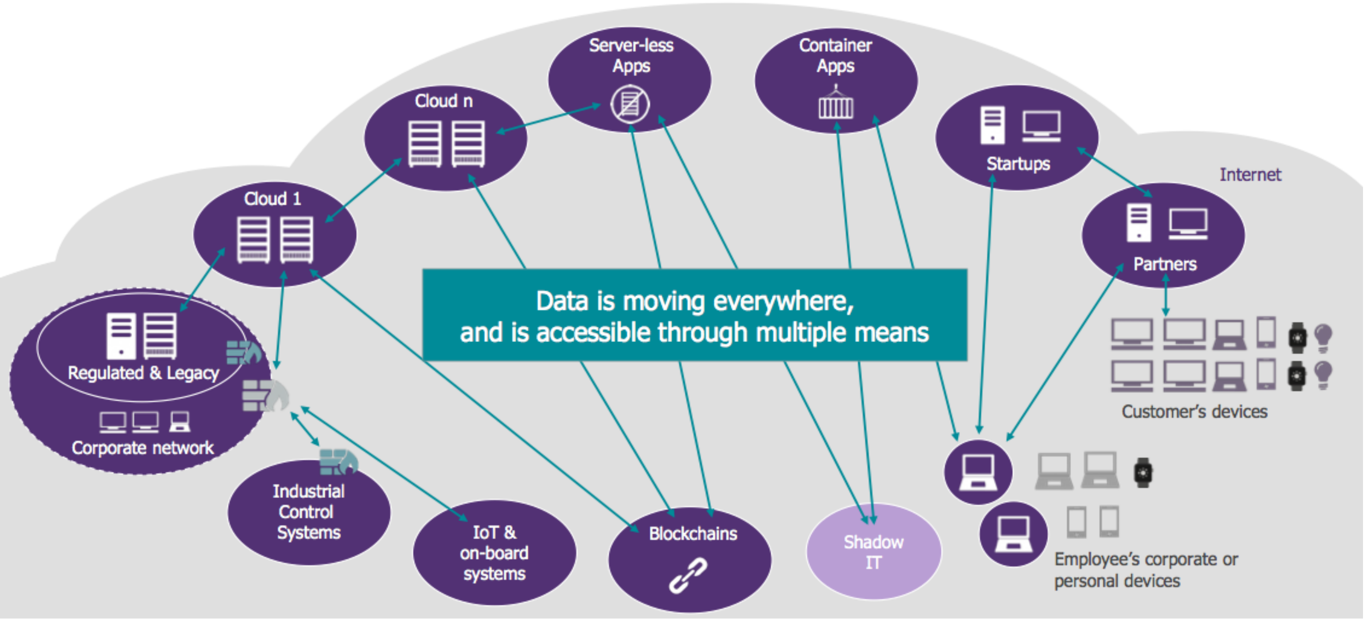

A perimeter that needs to be more open
Cloud
Internet
DC
Partner
Industrial Control Systems
Customer’s devices
Corporate network
Employee’s corporate or personal devices
Critical internal resources are isolated and tightly secured
© WAVESTONE

Figure 2: The "Airport" cybersecurity model

1.3 THE AIRLINE – A DECENTRALISED INFORMATION SYSTEM

Cyber-attacks are increasingly sophisticated and current security practices cannot keep pace with new cloud-based IT operating models for critical business applications. These information systems are typically hosted in multiple locations. This new level of complexity requires organisations to manage this whole environment, which makes it increasingly challenging for the Fortress or Airport models to mitigate the security risks. To respond to this complexity, organisations need to adopt a more innovative cybersecurity model: the "Airline" model.



This concept draws parallels with aircraft and passengers of an airline that are present at multiple destinations. The airline securely transports passengers using trusted airports via secure routes. Its Operations Centre is responsible for monitoring the movement of its fleet and managing incidents or crisis situations.

In the cybersecurity world, this translates into a decentralised information system model. The data moves in multiple directions accessible through various devices and locations, enabling employees to access data remotely. This includes accessing data using applications controlled by third parties. It becomes an organisation's responsibility to ensure that data moves securely across applications from multiple locations using trusted devices. Also similar to an airline, an Operations Centre needs to monitor access to data and manage crisis situations.

2 KEY PRINCIPLES OF THE "AIRLINE" MODEL

2.1 2.1 KNOW YOUR MOST CRITICAL ASSETS (PASSENGERS)

The first principle of the Airline model is knowing the most critical assets that have the highest security requirements. Organisations are continually managing an increasing amount of data accessed from multiple points; it is no longer feasible to maintain similar levels of security effectively across the whole system. So you need to involve the relevant senior executives to identify the most critical assets and apply strict security protocols/ encryption as appropriate. You also need to learn how to manage and share encryption keys through services such as Certificate as a Service (CertaaS), Key Management Service (KMS) and Blockchain trust services.

2.2 CHOOSE TRUSTED CONTEXTS AND BUILD YOUR APPS (TRUSTED AIRPORT/ STOPOVERS)

Since data flows through a variety of access points, the second principle is to develop trusted data applications. Validating your own environment and being clear about your service and security level agreements with cloud providers is critical to ensure that applications/data are protected. Organisations can establish secure environments by assessing the trustworthiness of hosts with standard security metrics. This provides assurance that all applications including third party applications are secure.

On-boarding a security specialist into 'Agile' project teams (so-called 'pizza' teams) enables the prioritisation of risks and critical assets and helps to mitigate the highest threats first. This agile approach brings security controls closer to the developers and reduces time to resolve issues.

This model requires organisations to continuously integrate security in the environment. This could for instance be used for patch management, by releasing security fixes in a continuous and integrated way, as cutting-edge operating systems do. Organisations are encouraged to 'attack themselves' continuously to test for potential gaps in their security systems. To optimise testing efficiency and effectiveness, purple teaming can be used to merge both offensive (red) and defensive (blue) tactics. Organisations can also use bug bounty programmes, encouraging individuals and independent hackers to be rewarded for reporting bugs and vulnerabilities.

2.3 GET YOUR DATA TO MOVE SECURELY (FLY ON A SECURE ROUTE)

The third key principle is to ensure secure movement of data across channels. Despite not being in full control of the applications/data-flow, organisations still need to adopt a dynamic security model. An Operations Centre can identify and allow secure access levels to user devices. Organisations can build reference tables for devices and servers, to validate ownership and security levels statically or dynamically. The checks vary on a case-by-case assessment of trust levels between the device, network and the application. Access is only available to compliant identities and devices.

3 CHALLENGES IN IMPLEMENTING THE "AIRLINE" MODEL

3.1 THE BATTLE AGAINST LEGACY ESTATE

The most common challenge that organisations face is in legacy IT infrastructure. Despite some reservations from CIOs, organisations have started adopting cloud-based models, moving away from legacy IT. Dealing with legacy infrastructure shouldn't hinder the adoption of the "Airline" model. CISOs must acknowledge that they can't initiate a complete migration of the organisation's system for the sole reason of security. So they should find ways to adopt the airline model with the understanding that legacy systems will eventually shrink by themselves. Therefore, security must be kept at the heart of the migration process.

3.2 THE NEED FOR CYBERSECURITY AUTOMATION

A human workforce is no longer capable of keeping up with the volume of cyber threats. Automated security is needed to introduce efficiencies to repetitive tasks. However, the main implementation challenge is the positioning and timing of cybersecurity automation.

Organisations can focus on three areas.

- Introduce automated security roll-outs that scale protection to the evolving Information System needs. This includes deployment of cloud security packages and utilising Software Defined (SD) Security.
- Introduce Automated Detection and Response to enhance and match the detection speeds to that of the attackers. This could include Endpoint Security Automation, Incident Response Automation, and use of Machine/Deep Learning principles to eliminate false positives.
- Introduce enhanced threat intelligence to share threat information for the common good of all, through trusted platforms (authorities, regulators, ISACs, etc.).

3.3 THE SKILLSET OF CYBERSECURITY TEAMS

Successful adoption of the Airline model requires a team with the right skill sets. It is not only about reacting to risk mitigation but also the ability to think innovatively about the defence mechanism. New team structures need to be introduced including new roles such as Data Scientist and Agile Security Champion.

4 CONCLUSION

With organisations adopting cloud-based delivery models and committing to digital transformation, the traditional "Fortress" and "Airport" cybersecurity models are unsustainable. Cyber threats are growing in volume and the nature of the threats is continuously evolving. As a result, it is vital for organisations to adopt the next generation "Airline" model to protect their data, infrastructure and reputation.

ABOUT US

Wavestone is an international consultancy that provides connected thinking, insight and capability to industry leading organisations. We work collaboratively with our clients to plan strategic business transformation and seamlessly turn strategy into action.

FIND OUT MORE

If you'd like to find out more, please contact us by calling at +44 20 7947 4176, or via email at **enquiries@wavestone.com** or visit our website at **www.wavestone.com/uk**

WAVESTONE

www.wavestone-advisors.com