STEALTH by UNISYS

Safeguard Sensitive Information Across the Value Chain

Terrorism, cyber-threats, and insider attacks endanger the physical security of passengers, the safe shipment of cargo, and the virtual security of the air transportation industry's critical applications and data. As airports, airlines and government agencies share more mission-critical data to optimize the passenger experience, aviation executives and airport directors are dealing with daunting risks. As airline data moves, it gets stolen. Passenger, flight, baggage, crew, and other data must be protected at all times – only the right personnel should be able to access and manage certain information. Unisys Stealth™ is an innovative approach to data and network security that can help aviation industry executives secure and protect sensitive information as it is shared across the value chain.

Risks to Aviation Data Security Continue to Intensify

Communication and the sharing of highly sensitive flight and passenger information are essential for smooth, efficient aviation industry operations. Information regularly flows across the value chain – to airline and airport personnel, tenants, passengers, check-in agents, ground handlers, vendors, freight forwarders, travel agents, and government agencies. As information gets shared, it gets stolen. At the 2013 Hack in the Box conference, using a flight simulator, a speaker showed off the ability to change the speed, altitude and direction of a virtual airplane by sending radio signals to its flight-management system – claiming that current security systems do not have strong enough authentication methods to make sure the commands are coming from a legitimate source. The potential impact of this data falling into the wrong hands is clear. Protecting highly sensitive aviation information from getting into the hands of cyber criminals and terrorists is something that aviation partners and government agencies are entrusted to do.

How can aviation executives and government officials cost-efficiently protect their commercial information and mission critical systems as they communicate across the value chain?

HIGHLIGHTS

- **Micro-segment your data center based on users. Define and control access to mission-critical airports systems, airline systems, and data communication you are entrusted to protect.**
- **Go dark – conceal communication endpoints.** Make servers, devices, and other communication endpoints undetectable.
- **Secure data in motion.** AES-256 encryption and data dispersal and reconstitution secures data in motion.

Go Dark – Reduce the Attack Surface

Highly sensitive aviation industry information requires extreme security. Airline executives and airport directors know this – and so do their customers and partners. As aviation industry executives deliver more efficient services to passengers, they are adopting new, innovative ways of ensuring their data is secured. In turn, this translates into reduced risk, reduced cost, and safe passengers. Leading aviation industry executives are pursuing the ability to:

- **Limit data exposure** for the airline, airport, partner or government agency and its value chain
- **Segregate data inside the network** so that only those with the right access even know information is being shared, making it undetectable to others
- **Cloak servers and PCs** running sensitive applications in the data center, making servers undetectable to unauthorized users

Unisys Approach – Extreme Security That Protects Airline Data

Unisys Stealth is a leading-edge software security innovation that makes data communication endpoints undetectable on a network, thereby helping to eliminate them as targets for hackers. Stealth's identity-based solution makes communication endpoints "dark" by allowing communications only to authorized members with a defined community of interest such as an airport shared infrastructure or among partners of an airline alliance. Leading aviation industry executives are leveraging Unisys Stealth to:

- **Compartmentalize data centers and networks by reclassifying data based on need-to-know access.** Consumerization of IT, cloud computing, and breach attempts are driving aviation industry executives to micro-segment their networks and data centers. Unisys Stealth is designed to securely segment data centers and protect data and systems by cloaking strategic assets.

> With Unisys Stealth, aviation industry executives can securely share information across the entire transportation industry value chain.

- **Protect local assets within designated regions while controlling access to assets from users in that region.** Unisys Stealth is designed to enable geographically dispersed data centers to obtain secure regional access to the data center, which can protect from untrustworthy governments or other rogue threats.
- **Help ensure the right airport, airline, grounds personnel, and vendors have secure remote access to the enterprise.** Ensuring the right personnel have remote access to the enterprise is a constant challenge. Unisys Stealth is designed to secure point-to-point sessions, helping to avoid data breaches.

Unisys Stealth is an innovative approach to data and network security that empowers aviation industry executives to confidently and cost-efficiently share sensitive information across the value chain.

For more information

contact us at: stealth@unisys.com
or visit us at: www.unisys.com/stealth
or at: www.unisys.com/transportation

STEALTH by UNISYS

Printed in the United States of America 09/15 15-0273