Integrated Risk Management in the Maritime Environment

American Association of Port Authorities
Security Seminar & Expo
July 2019

UNISYS | Securing Your Tomorrow®

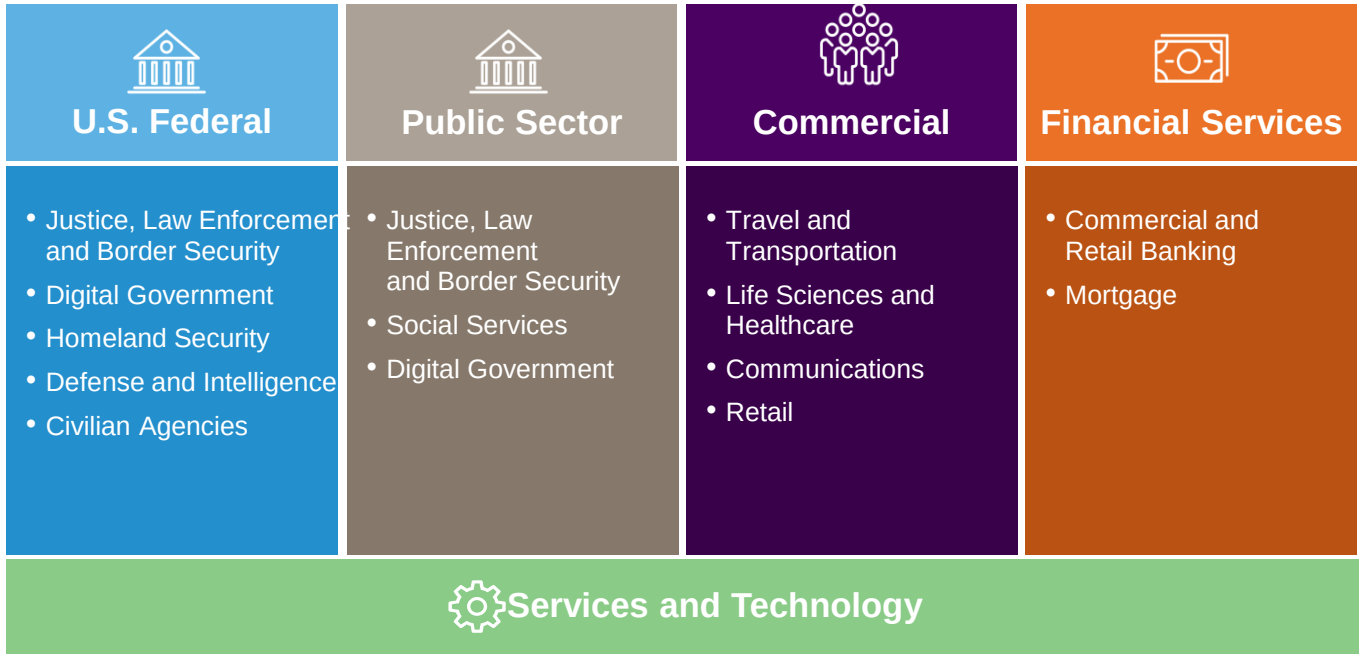
Agenda

- Who is Unisys?
- Maritime Security Challenges
  - Increasing security responsibilities with limited resources
  - Combatting new, emerging threats
- How can I manage risk and protect my systems and data?
  - Traditional approaches
  - A better approach thru Zero Trust Microsegmentation
  - A Zero Trust strategy using Unisys Stealth™
- How do I know who to trust when using a Zero Trust strategy?
  - Fresh Haystack trust assessment

About Unisys

Unisys is a global information technology company that builds high-performance security-centric solutions for the most demanding businesses and governments on Earth. We offer security software, solutions and services; consulting and innovative digital transformation services; and industry applications, workplace services and operating environments that build better outcomes for our clients securely.

- Headquartered in Blue Bell, PA, with offices in more than **25 countries**
- **275 government agencies** worldwide use Unisys solutions (including the City of Philadelphia)
- **9 of the top 10 airlines** depend on Unisys solutions
- Providing services to Government, Commercial, Transportation and Financial Services clients in all 50 states
- A leader in securing mission-critical operations in demanding environments



About Unisys

- Providing IT and Physical Security solutions to the maritime community and associated industries for more than 20 years including:
  - Security consulting
  - Video surveillance, access control and TWIC solution implementation
  - Secure cloud computing
  - TrustCheck™ Cyber Risk Management
  - Stealth™ Security
- Current or recent clients include:

Lifting Global Trade
APM TERMINALS

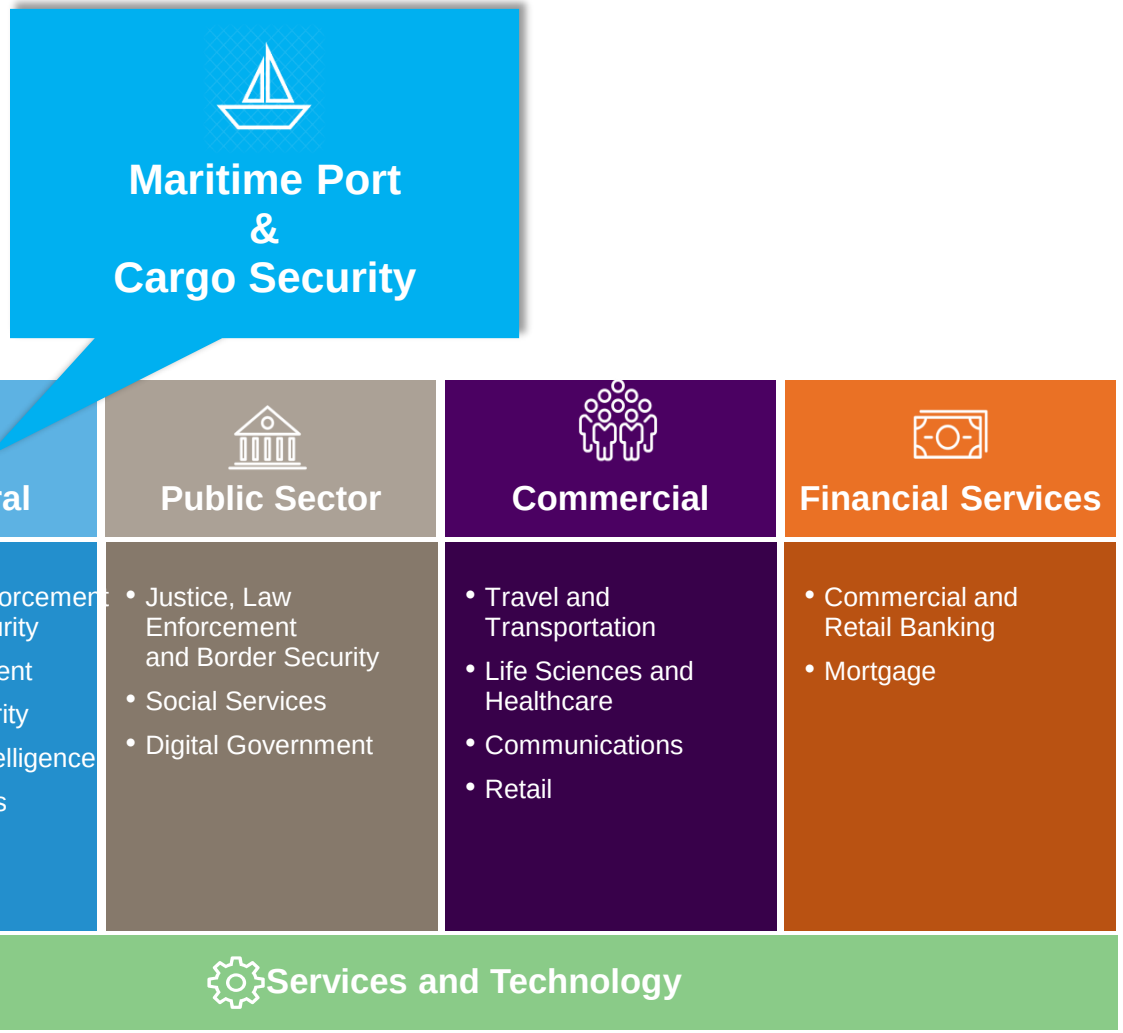
U.S. Customs and Border Protection

WBCT

Transportation Security Administration

Carnival

THE PORT OF LOS ANGELES



Maritime Security Challenges

Security and IT organizations are being asked to…

- Do more with less (fewer employees, lower budgets)
- Secure people, assets, physical locations, information systems and data
- Protect against increasingly sophisticated adversaries and new threats
- Maintain a competent, trained staff that manages an increasingly complex environment of systems and technologies
- Comply with local, state and Federal regulations

UNISYS

Maritime Security Challenges

Security and IT organizations are being asked to…

- Do more with less (fewer employees, lower budgets)
- Secure people, assets, physical locations, information systems and data
- Protect against increasingly sophisticated adversaries and new threats
- Maintain a competent, trained staff that manages an increasingly complex environment of systems and technologies
- Comply with local, state and Federal regulations

"Protect everything we have against everything that's out there….but make sure we're flexible and easy to do business with!"

Maritime Security Challenges

Internal Threats…

- Intentional – A “rogue Admin” or disgruntled employee
- Unintentional – A vendor unknowingly using a contaminated USB stick to update a truck gate control system

External Threats….

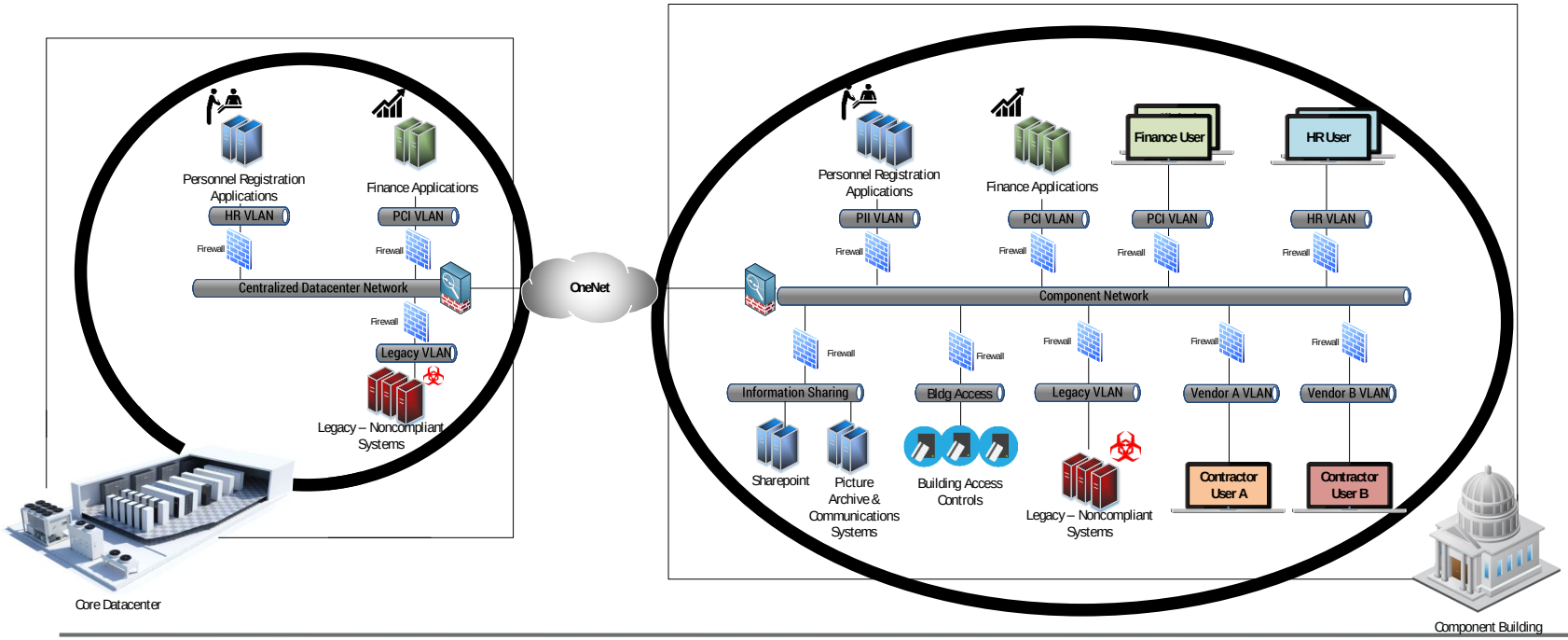
- Criminal enterprises seeking monetary gain through ransomware
- Hacker groups backed by nation states intent on disruption/destruction

UNISYS

Risk Management and Cyber Defense

Traditional approaches….

- *Require managing multiple security platforms and infrastructure which is inefficient*
- *Use firewalls, VLANS and other traditional segmentation approaches to create network boundaries results in exponential complexity*
- *Are costly, can require new hardware, modifications to IT architecture, IP addresses, etc.*
- *Count on employees to not make mistakes because they've gone through Security Training*



UNISYS

Risk Management and Cyber Defense

A better approach…

Zero Trust software-based Microsegmentation

A new approach to security designed to provide containment in a hyper-connected world. It accepts that ***users are human and make mistakes****, that* ***technology is constantly evolving*** *and that the* ***bad guys are just as clever and resourceful*** *as the good guys.*

- *Software based and can be easily loaded/imaged onto new computers, servers, mobile/edge devices, etc.*
- *Does not require new hardware, network architecture changes, modifications to firewalls, IP address schemes, etc.*
- *Cost-effective and flexible – Protect everything or select specific systems, functions (ex. Finance) or locations*

What is a Zero Trust Security Model?

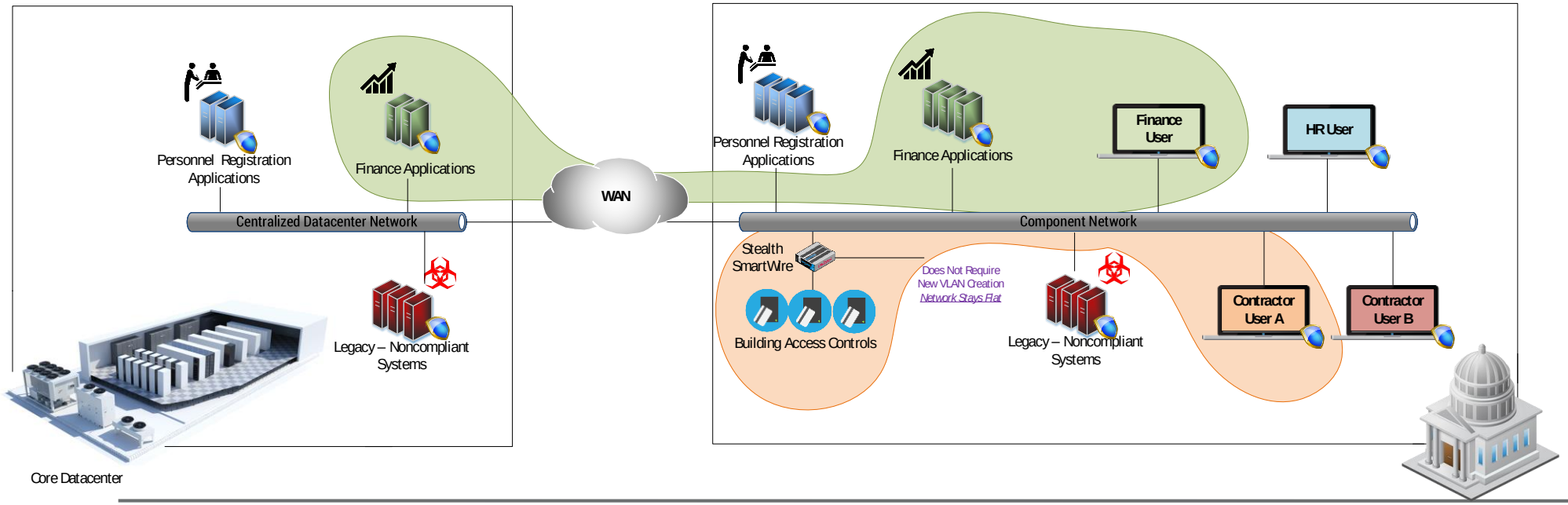
A more identity- and data- centric approach based on network segmentation, data obfuscation, security analytics, and automation that never assumes trust.

UNISYS

Unisys Stealth™

Stealth™ is an example of a zero trust, software-based microsegmentation product being used by governments and the private sector to secure data.

- Every user and device is **authenticated based on its identity** and provided a unique key
- Irrespective of device location — mobile, corporate LAN, cloud, **communication is only allowed between the end points which have matching keys** — together forming Communities of Interest (CoI)
- Upon authentication Stealth™ enables least privileged access — **on a need to know basis only** — as defined by security policies.



Unisys Stealth™

Stealth™ enables a Zero Trust strategy where…

- Secure sensitive and valuable data on **existing infrastructure**
- **Non-compliant and legacy systems can be compartmentalized** with simple to deploy software
- Security boundaries can be created that can traverse any part of the enterprise, regardless of who owns or manages the underlying hardware
- Implementation can be done **incrementally**. Can scale from One User to One Application to an Entire Domain within a Classification.
- Data-in-Motion is protected with **Encryption** (Point-to-Point), while providing Security Operations the ability to conduct Continuous Diagnostics, Monitoring and Dynamic Quarantine.

Unisys Stealth™

Stealth™ has helped clients achieve meaningful results in complex, mission-critical environments…

State of New York

- Datacenter Consolidation: **50 Datacenters into 1**
- Complexity Reduction : Zero internal Firewalls
- OPEX Savings: **125 Firewall Admins to 25 Stealth Admins**
- Agility: Reduce Change Request Process from 8 Weeks to 1
- Deliver FIPS, HIPAA, PHI, PCI-DSS, IRS-PUB 1075 Compliance Controls for State Agencies

Defense Information Systems Agency (DISA)

- Secure Multiple Classified: Secret Releasability Levels on Converged Platform
- Certified: Protect Data-in-Motion with **NSA accredited** CSFC/NIAP software
- Fight Tonight: Reduce Securing Mission Enclave Provision from Months to Days

Transportation Security Administration

- **Secure all Transportation Security Equipment (TSE)**: Body, Luggage, Passport scanners across all National Airports
- Eliminate need to build new network for segment TSE devices

Federal Aviation Administration

- **Protect Mission Critical Pilot and Aircraft Registration System used by all Airlines**
- Bring Application into **800-53 Compliance** for a High Impact Application: Addressing Transmission Confidentiality, Enforcing Least Privilege, and Segmentation

UNISYS

Risk Management and Cyber Defense

How do I know whether (and how much) to trust the users and systems (potentially external) that I will be including in my Communities of Interest and allowing communication between?

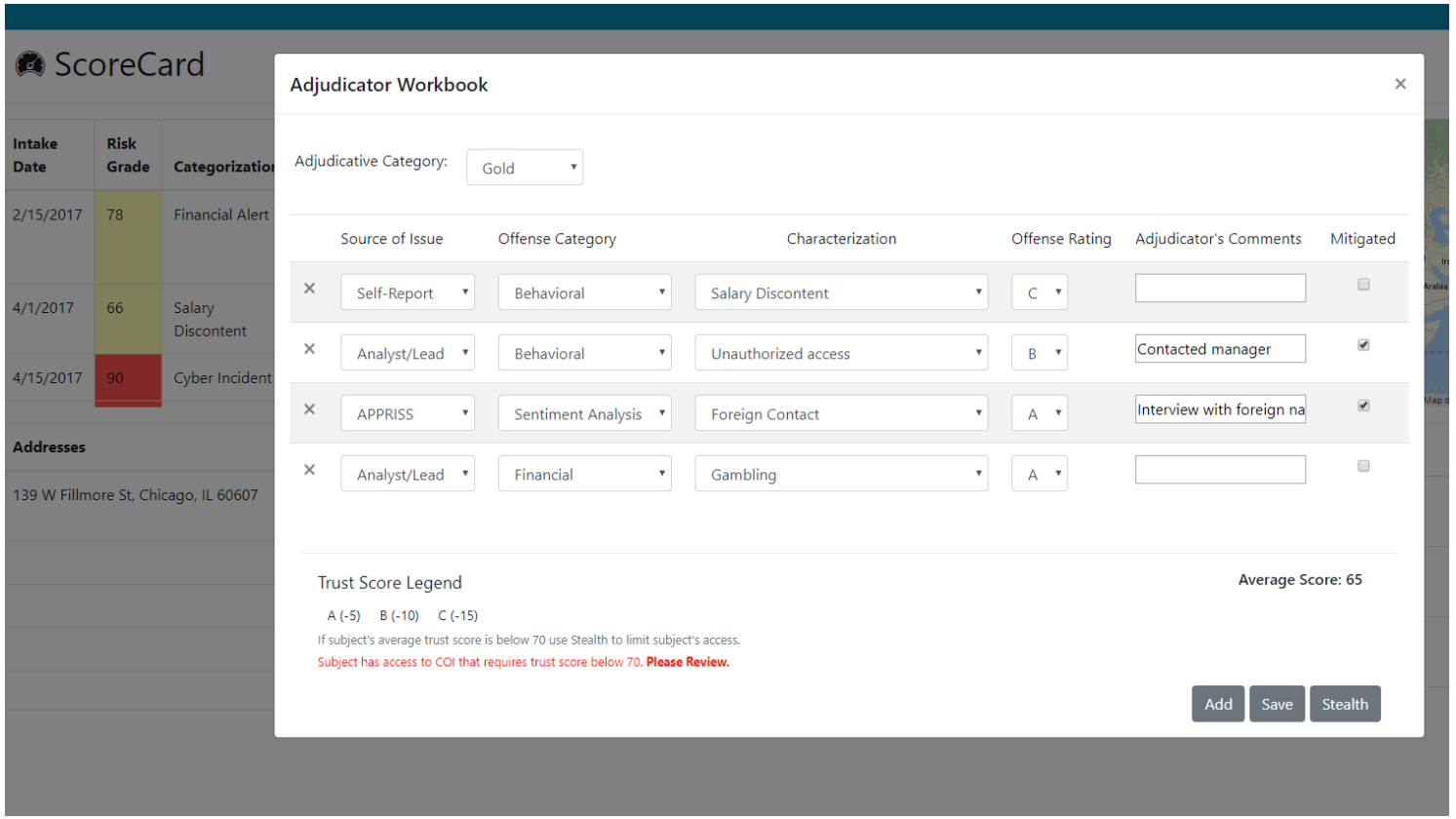
Integrated Risk Management

Evolving to a trusted workforce by bridging the gap between the person, their profiles, access, networks and activity, to continuously deliver trust while minimizing organizational risk exposure.

Risk Management and Cyber Defense

CARTA (Continuous Adaptive Risk & Trust Assessment

- Continuous Adaptive Trust
- Continuous Identity Verification
- *Is this **still** Joe?*
- *Should we still trust Joe?*

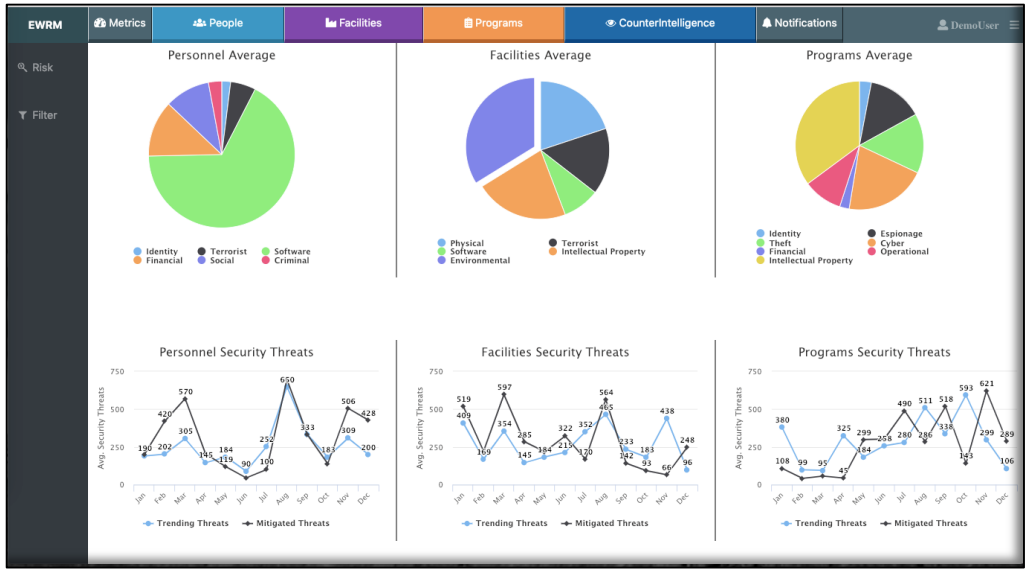


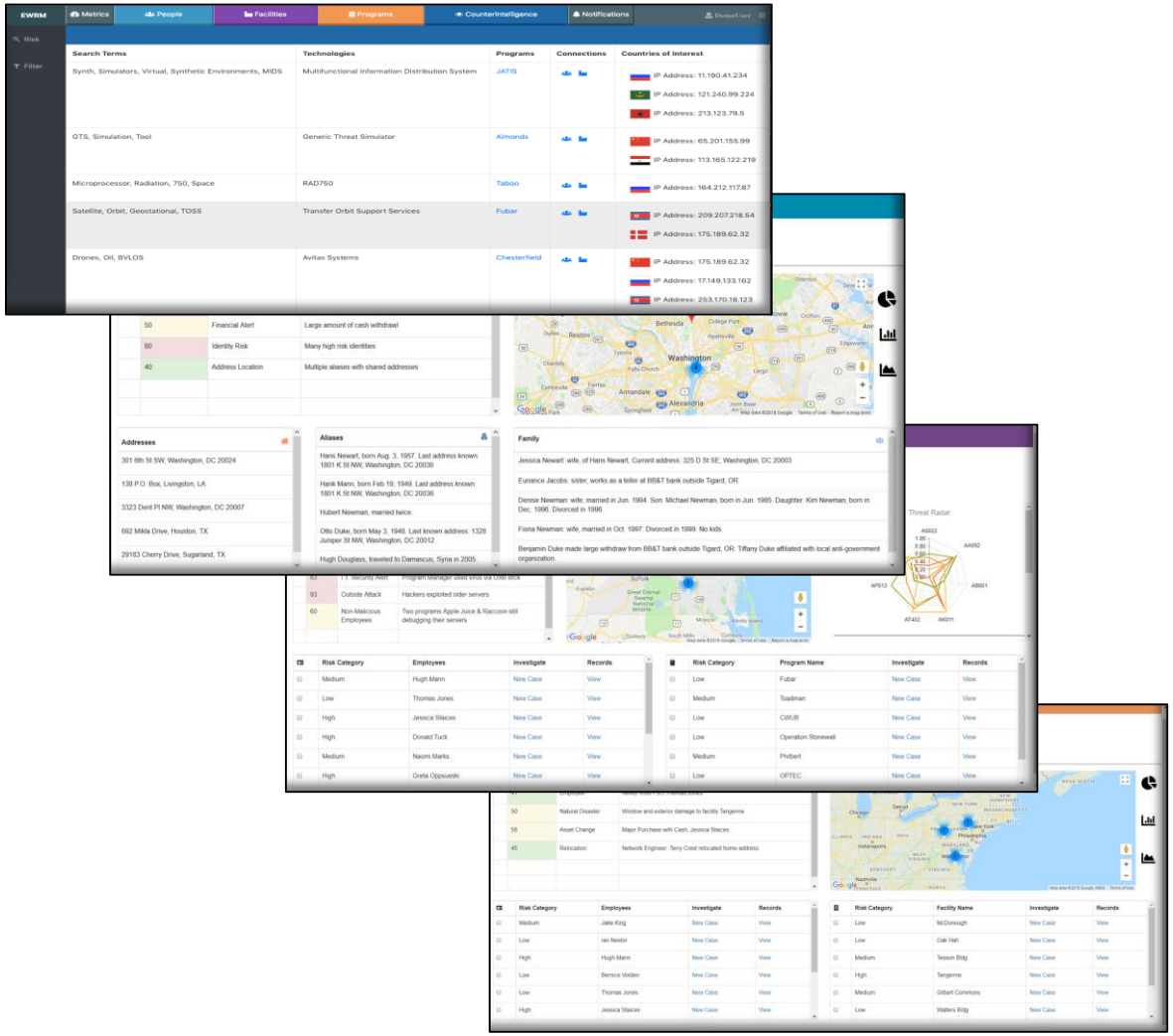
UNISYS

Risk Management and Cyber Defense

Fresh Haystack Decision Services

A Convolutional Neural Network that uses government adjudication criteria across five tiers of data sources as its initial model for trust evaluation.

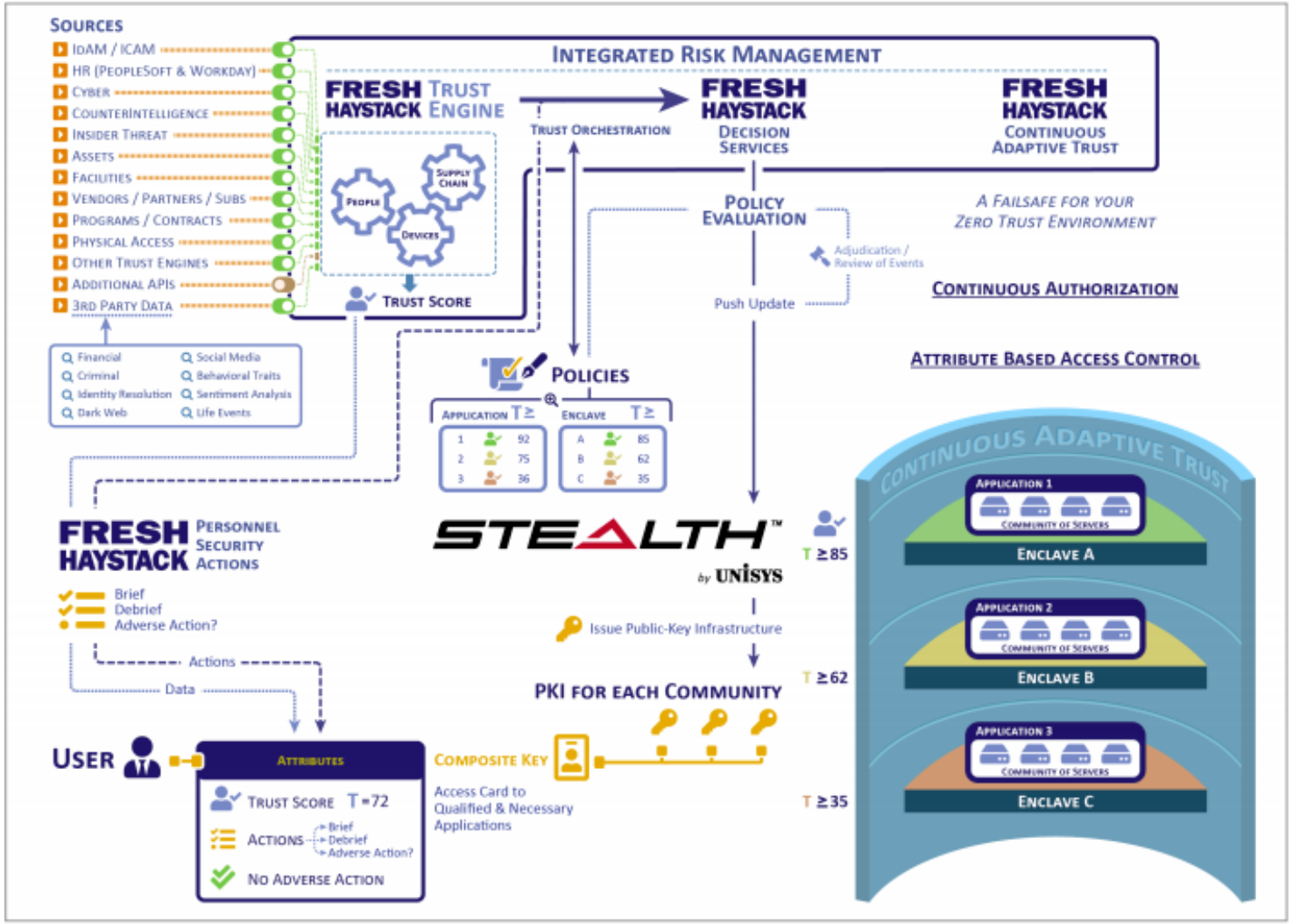




Risk Management and Cyber Defense

Stealth™ and CANDA Solutions' Fresh Haystack capability for Trust Verification enhance security.

- Exhausted by the inundation of security messaging from a cluttered and confusing security company marketspace
- Focusing on the human aspect of cyber security more than ever. 99.5% of breaches happen because of some aspect of 'touch' with a human, demonstrating how easy it is to hack a human
- Most CISOs agreed that they are in a place where they have board access, executive visibility, and strong leadership roles but not getting enough done



Thank You!

Adam Kiesel

Director, Maritime Port & Cargo Security

Adam.Kiesel@unisys.com

602.412.3240

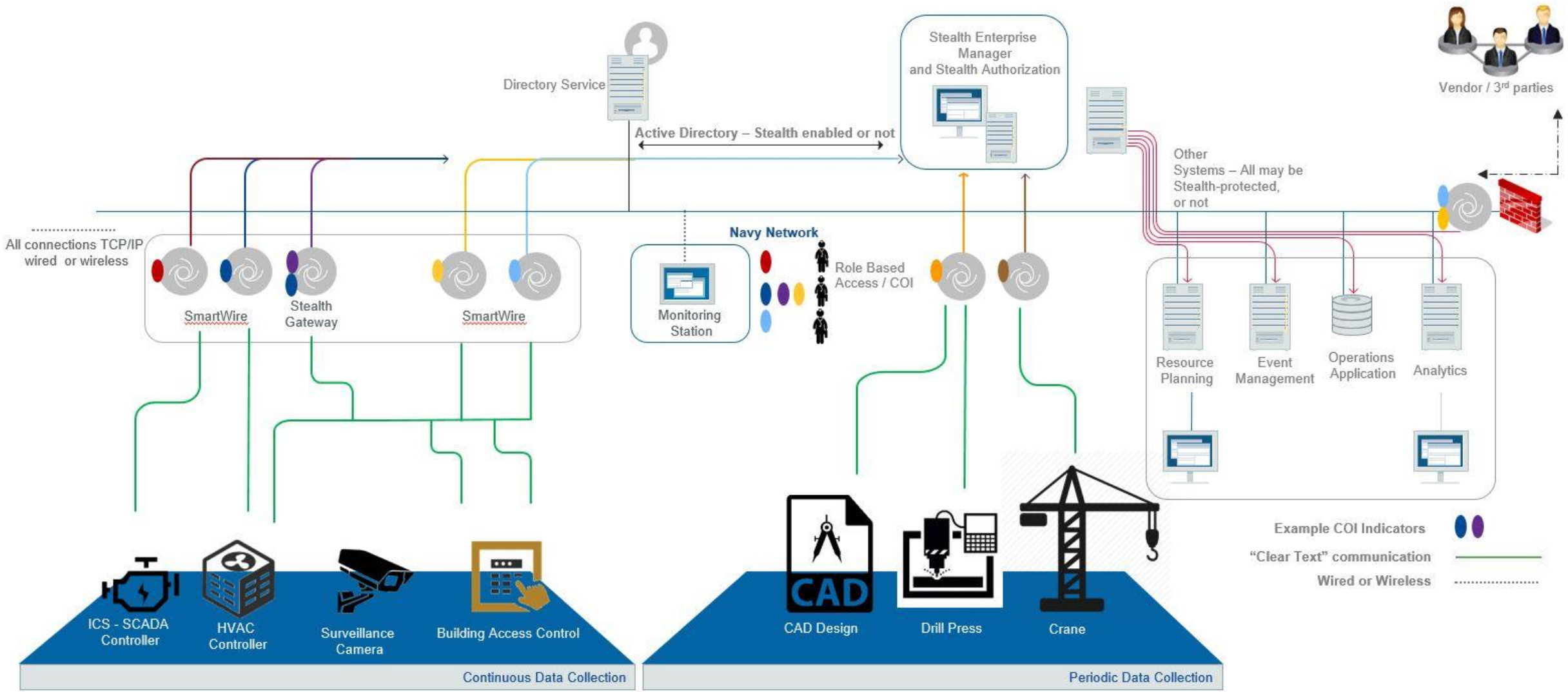
Chris Hagenbuch

Principal

Chris.Hagenbuch@candasolutions.com

301.980.0602

Securing Legacy & Non-traditional Systems



UNISYS