

Integrated Cyber May 2 & 3, 2019

TRUST IN AUTOMATION AND AUTONOMY



Aubrey Merchant-Dest
Federal CTO



Geoff Hancock
Chief Cybersecurity Executive

ADVANCED CYBERSECURITY
GROUP



Juhee Bae
Product Manager

GENERAL DYNAMICS
Mission Systems



Jennifer Ockerman
Cognitive Systems
Engineer

APL JOHNS HOPKINS
APPLIED PHYSICS LABORATORY



The Evolution of Cyber Security Automation

Definitions



Trust

- Firm belief in the reliability, truth, ability, or strength of someone or something *(Oxford)*

Reliance

- The act of relying -> being dependent or having confidence based on experience *(Merriam-Webster)*

Automation

- A system that works by itself with some amount of human intervention *(Bae, 2019)*

Autonomy

- A self-governing system acting independently without intervention from a human at any point in time *(Bae, 2019)*

IACD Trust in Automation Framework



Farid Ahmed

Gill Brown

Rose Daley

Jennifer Ockerman, PhD

Willie Stewart

Jennifer Ockerman, PhD



- **IACD Trust Initiative Lead**
- **Principal Cognitive Systems Engineer**
- **Johns Hopkins University Applied Physics Laboratory**

- **Focus on the human element of cognitive systems - joint human and technology efforts to complete cognitive tasks**
 - **Decision making**
 - **Human performance measures**
 - **UI design**

- **Domains**
 - **Cybersecurity**
 - **Military command and control**
 - **Homeland security**
 - **Law enforcement and corrections**
 - **Healthcare**



IACD Trust Framework: Putting It All Together



- **IACD encourages the use of automation to meet the pressing needs of cybersecurity**
- **Some reluctance to automation is due to lack of trust**
- **Trust in automation**
 - What is trust in automation?
 - What do we know about it?
 - How might it impact cybersecurity and IACD efforts?
 - Can it be measured?
 - What are the gaps? What additional work is needed?
- **Created a trust framework from**
 - Academic literature
 - Reports from previous IACD efforts and financial pilot
 - Focus group with non-cyber automation designers, developers, and deployers

TRUST IN AUTOMATION

A necessary component to realizing automation's potential

Trust in automation is a multi-dimensional, interdependent problem space involving automation trustworthiness, human trust, and human reliance shaping automation's contribution to cyber operations.

PERSPECTIVES

AUTOMATION LIFECYCLE

PRE-IMPLEMENTATION

IMPLEMENTATION

INITIAL USE

SUSTAINED USE

ROLES/ PERSONAS

CISOs

SECURITY ARCHITECTS

OPERATION MANAGERS

ANALYSTS

SOURCES OF (MIS)TRUST

SECURITY

AUTOMATION ALGORITHMS

COMMUNICATION (HM & MM)

INFORMATION

OPERATIONAL FIT

TYPES OF AUTOMATION

SENSING

SENSE-MAKING

DECISION MAKING

ACTING

CONTROL & MANAGEMENT

SCOPE OF AUTOMATION / AUTONOMY

NO AUTOMATION

SINGLE FUNCTION AUTOMATION

COMBINED FUNCTION AUTOMATION

PARTIAL AUTONOMY

FULL AUTONOMY

CONDITION

ATTITUDE

LEVEL OF TRUST

NO TRUST

LIMITED TRUST

CALIBRATED TRUST

EXCESSIVE TRUST

CONDITION

BEHAVIOR

LEVEL OF RELIANCE

NO RELIANCE

UNDER RELIANCE

CALIBRATED RELIANCE

OVER RELIANCE

INFLUENCERS

HUMAN

PERCEIVED LEVEL OF CONTROL

PERCEIVED ACCOUNTABILITY

UNDERSTANDING OF AUTOMATION

PERCEIVED SELF SKILL LEVEL

SELF CONFIDENCE

PERCEPTION OF UTILITY

TECHNOLOGY

AUDITABILITY/ MEASURABILITY

TRANSPARENCY

SIMPLICITY/ CERTAINTY

REPUTATION

RELIABILITY

TIMELINESS

RESILIENCY/ REVERSIBILITY

SUSTAINABILITY

ENVIRONMENT

THREAT LEVEL

WORKPLACE CULTURE

TASK COMPLEXITY

SITUATION AWARENESS

WORKLOAD

TASK DIFFICULTY

RESULT

AUTOMATION

LEVEL OF CONTRIBUTION

NO CONTRIBUTION

LIMITED CONTRIBUTION

VALUABLE CONTRIBUTION

EXCESSIVE CONTRIBUTION

SPEED AT SCALE

OPERATIONAL CONSISTENCY

RISK REDUCTION

GREATER HUMAN IMPACT

CONDITION

PERCEPTION

LEVEL OF TRUSTWORTHINESS

NO TRUSTWORTHINESS

LIMITED TRUSTWORTHINESS

ENABLING TRUSTWORTHINESS

DECEPTIVE TRUSTWORTHINESS

Maximizing Mission Assurance with Autonomous Platforms




Juhee Bae

Product Manager, Trust in Autonomy
General Dynamics Mission Systems

Questions? Email me at: Juhee.Bae@gd-ms.com

Exterior View

A night-time exterior view of a road with white lane markings, illuminated by streetlights. The text "Exterior View" is overlaid in red.

Pillars of Safe and Effective Use = TRUST

Safe and Effective Use
of Autonomous Platforms

Cybersecurity and
Assured Control

Trustworthiness

Action
Recommendations

1

Protecting your system from cyber attack, insider threat, user error, and malfunction...

2

But no system will ever be perfectly protected, nor perfectly trained for any and all scenarios, so the user must have an understanding of how trustworthy the platform is at any one point in time...

3

So now that the user knows when their system is not trustworthy, the user must be informed of what they need to do to mitigate



Maximizing Incident Response at the Edge



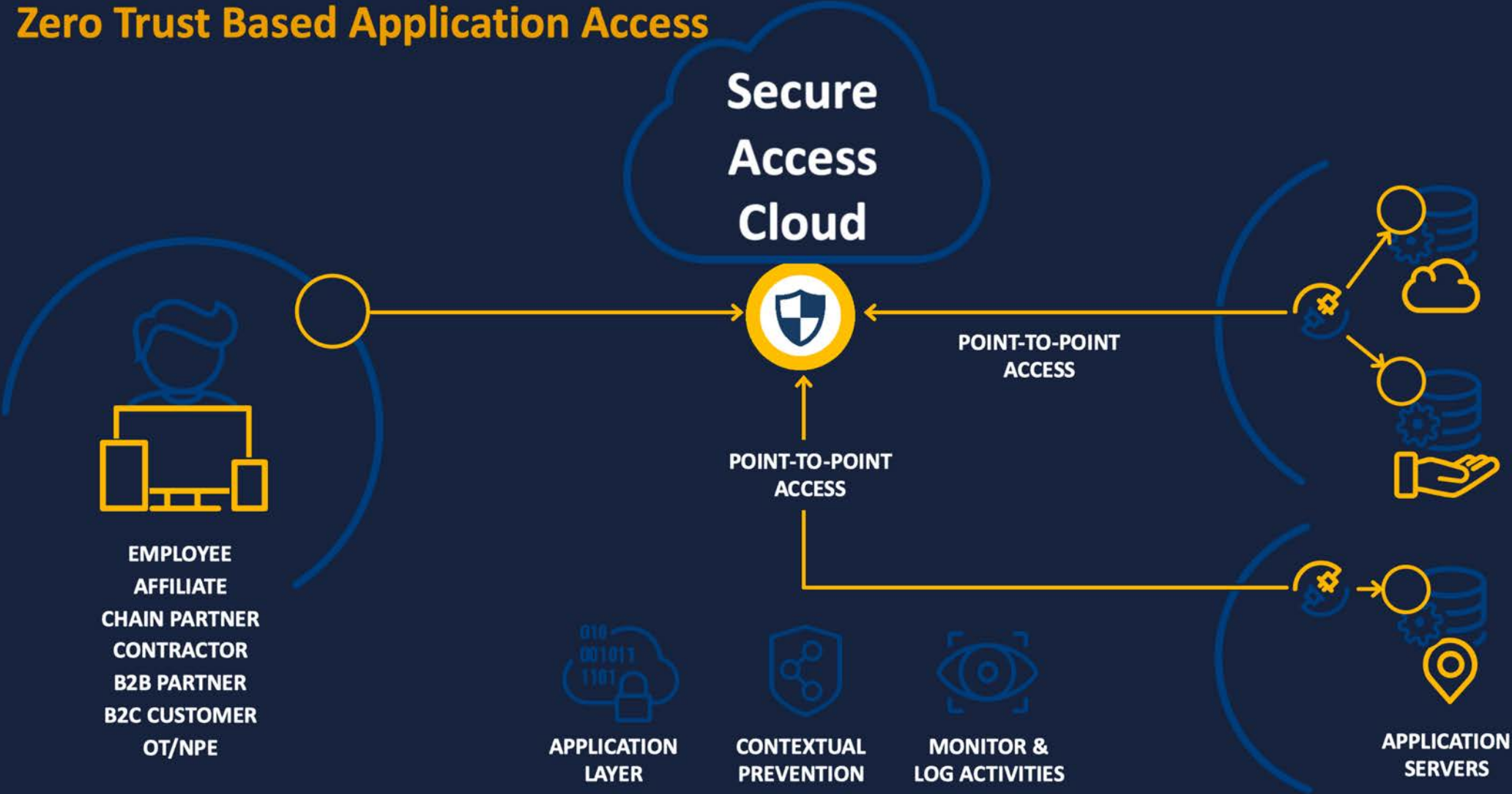
Addressing Massive
Change in Security and
Compliance Architectures



Secure Access Cloud: How It Works



Zero Trust Based Application Access



Anyone/Anything to Anywhere – Simple and Secure App Access

Secure Access Cloud



Within Symantec's Cloud Network Protection Portfolio



Integrated Cyber May 2 & 3, 2019

TRUST IN AUTOMATION AND AUTONOMY



Geoff Hancock

Chief Cybersecurity Executive

ADVANCED CYBERSECURITY
— GROUP —



The Evolution of Cyber Security Automation