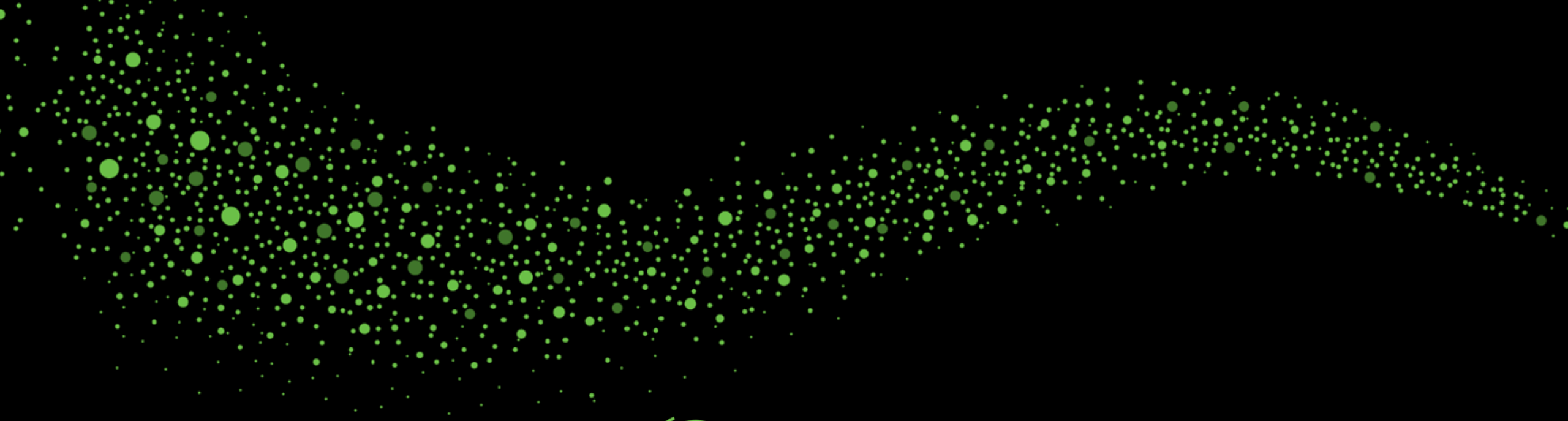
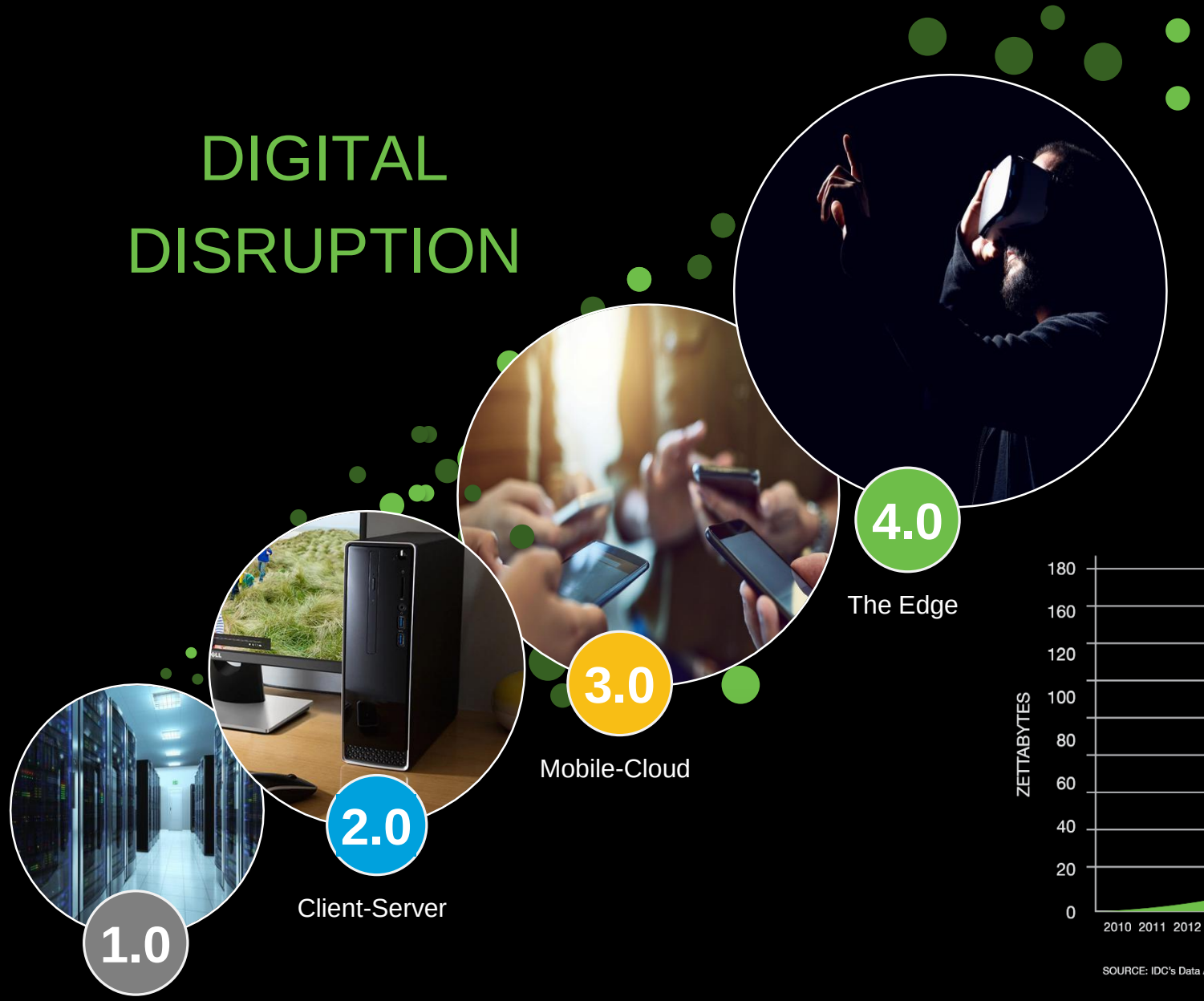
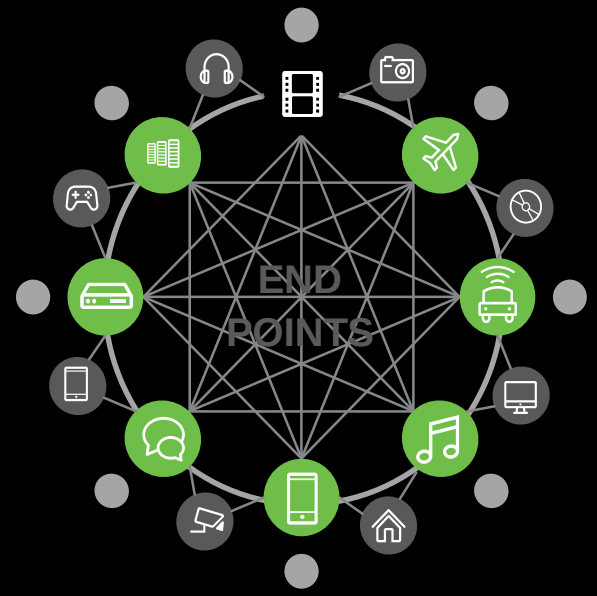


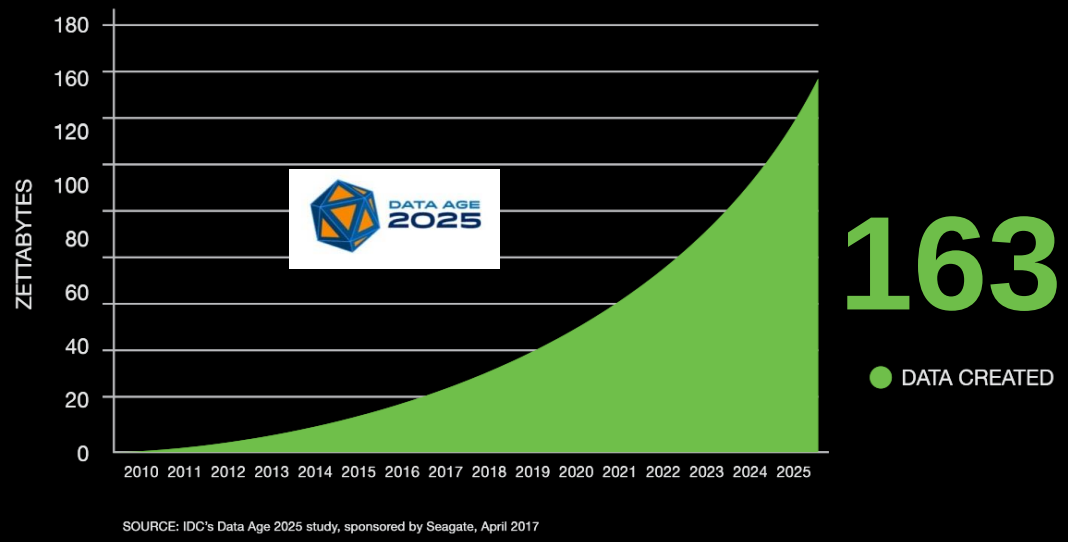
Cyber Supply Chain Assurance

NCCoE Cyber Supply Chain Risk Management (C-SCRM) Workshop
10 Sep 2019, Rockville, MD
Monty A. Forehand, Product Security Officer - Seagate

DIGITAL DISRUPTION







SOURCE: IDC's Data Age 2025 study, sponsored by Seagate, April 2017

SEAGATE SECURE

End-To-End Trust Enables Product and Data “Chain of Custody” Proofs

Essential

Certified

Data

Trust

Identity

Data

Trust

Identity

- Components, Devices, and Solutions Logically Designed to be Secure and Trusted
- Trusted and Immutable Digital Hardware Identities and Artifacts
- Enables Trust Networks for Product and Data Integrity and Provenance Proofs

Secure & Trusted Products

SECURE PRODUCT

	Essential	Certified
Secure Supply Chain	●	●
Hardware Root of Trust	●	●
Signed Firmware/Software	●	●
Secure Boot and Update	●	●
Instant Secure Erase	●	●
Self-Encrypting Drive	●	●
FIPS 140-2		●
Common Criteria		●
Trade Agreement Act (TAA)		●

Essential Device Trust

Essential Data Trust

Certified Device and Data Trust

THE Open GROUP

ISO

ISO 20243

Trusted Tech Provider Standard

NIST National Institute of Standards and Technology

Communications Security Establishment Canada

Crypto Module Validation Program (CMVP)

Crypto Algorithm Validation Program (CAVP)

NIAP

Common Criteria

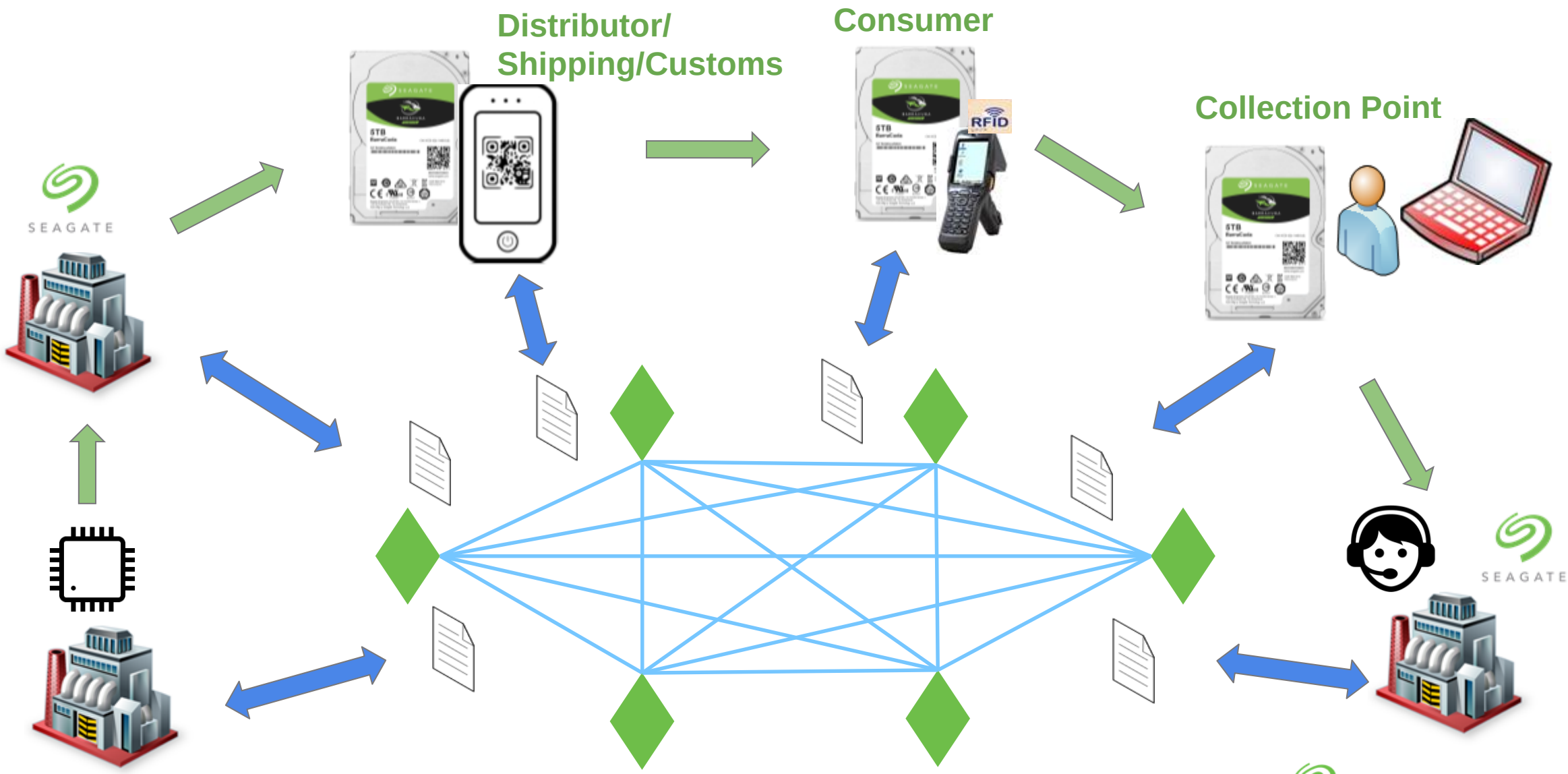
ISO

Common Criteria for Information Security Evaluation (CC)

Trade Agreement Act

U.S. Customs and Border Protection

Trusted Life-Cycle



Move Forward

Standards-based & Certified Product and Data Life-cycles

Hardware Identities & Artifacts for Cryptographic Trust

Ubiquitous Services for Digital Product & Data Trust

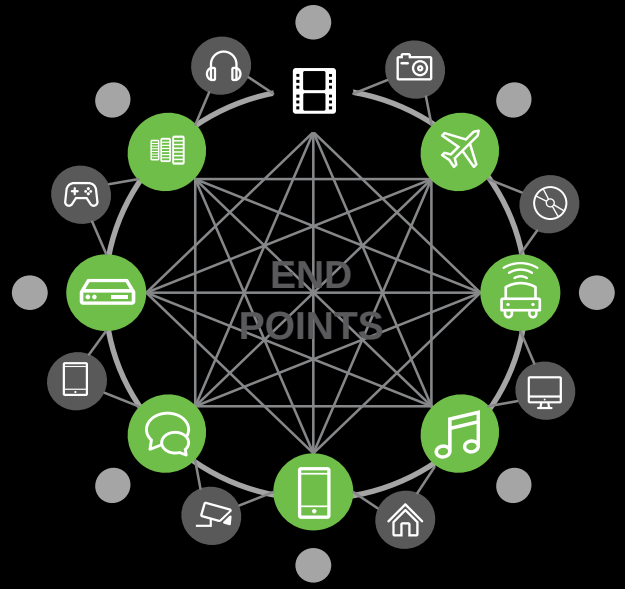
DATA IS POTENTIAL

Back-up

SEAGATE

4.0

The Edge | Distributed | 2020-



- Everything is in the open and vulnerable
- Real-time, Life-critical and Private data
- Real-time Decisions at and between end-points
- Crowd to Machine and Machine to Machine
- Data Regionalization & Strict Data Protection Laws

Adaptive Hardware, Firmware, Software, Gear, & Services Architectures

SEAGATE SECURE

Edge Assurance

Trusted Interactions with Data and Machines

- Secure Data Processing:
  - Secure Localized Data
  - Secure Data in Motion
- Identity & Attestation:
  - Trusted Device Identity
  - Hardware Based Attestations
- Execution Isolation:
  - Certified Transactions
  - Certified Services
- International Data Laws

Standard & Certified Trust

	Essential	Certified	Components	Appliances	Systems	Standard / Spec
Secure Supply Chain	●	●	Product Security Policies and Standards and Compliance Product Provenance			ISO 20243 SP 800-161
Hardware Root of Trust	●	●	SOC Hardware Root of Trust Trusted Platform Module (TPM)			(TPM) ISO/IEC 11889 FIPS 140 Security Policy
Secure Download & Diag	●	●	Digitally Signed Firmware / Software Packages, Protected Diagnostic Interfaces			FIPS 140 Security Policy
Secure Boot	●	●	Secure Boot Process			NIST 800-147
Instant Secure Erase	●	●	Crypto Erase (ATA, Sanitize, TCG) Certified Erase Software, Solutions, and Appliances			NIST SP 800-88 ISO 27040
Self-Encrypting Drive	●	●	TCG Opal & Enterprise Commercial Key Management APIs, Software, and Solutions			KMIP, TCG Standards
FIPS 140-2		●	Cryptographic Algorithm & Module Validation Programs Tamper-Evidence Protection			FIPS 140-2 NIST 800 - XXX Standards
Common Criteria		●	Common Criteria EE & AA Profile Validations			ISO / IEC 15408
Trade Agreement Act (TAA)		●	Trade Agreement Act Country of Origin on Label (USA, SG)			US Customs Rulings