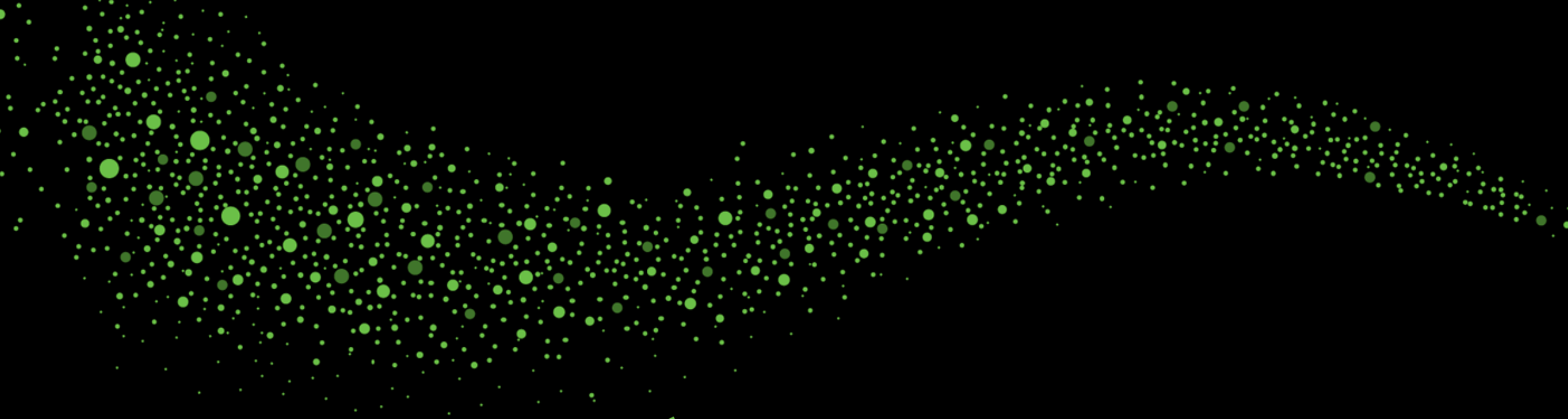


Securing the Datasphere

Standards-Based Trust for Global Leverage

Bangkok, Thailand — November 2019

Monty A. Forehand, Product Security Officer — Seagate

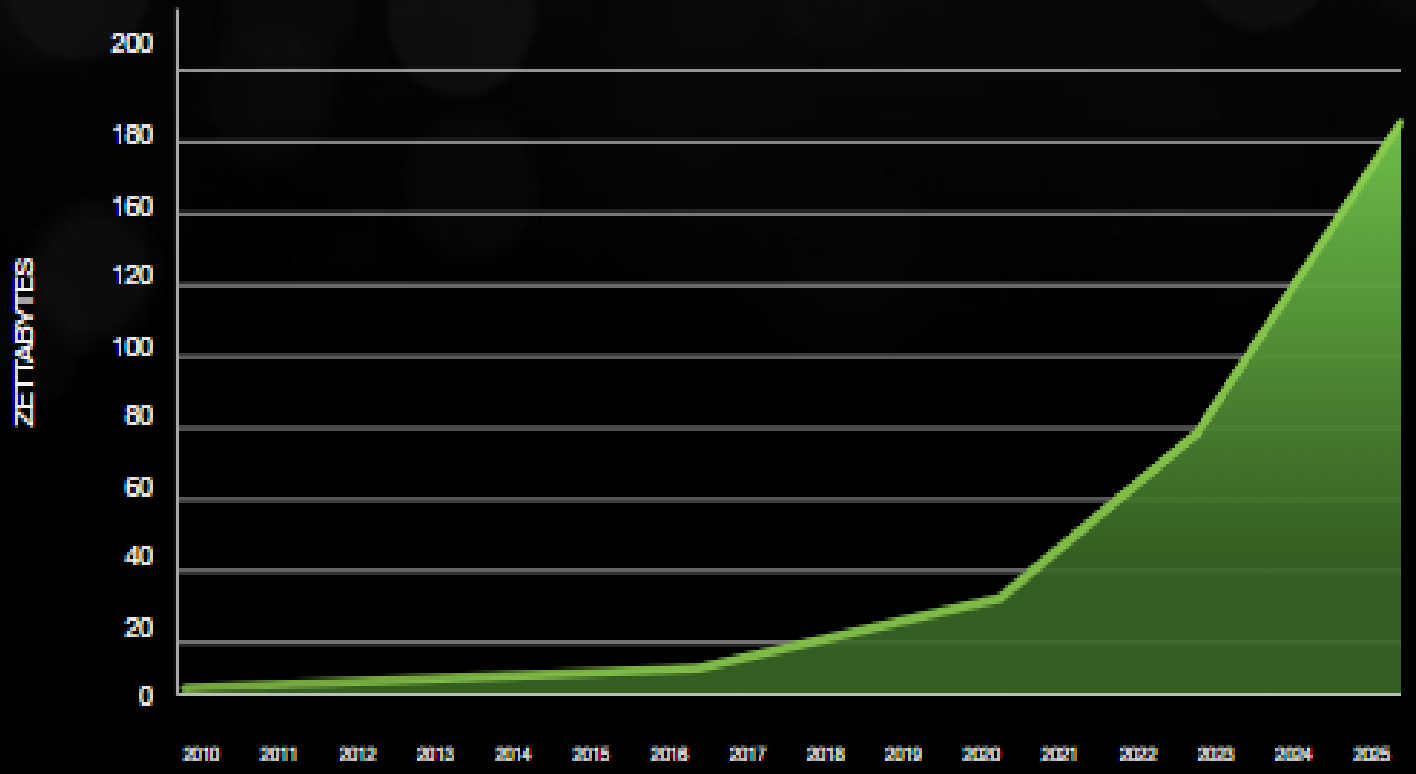
Our Global Presence

Crafting the Datasphere

Seagate was founded on the belief that **Data is Potential.** Our mission is to continuously craft a datasphere that maximizes data potential for everyone.

Global Data Explosion

The IDC Data Age 2025 report predicts massive volumes of data creation and a convergence of every industry utilizing the value of data



1 Zettabyte Printed

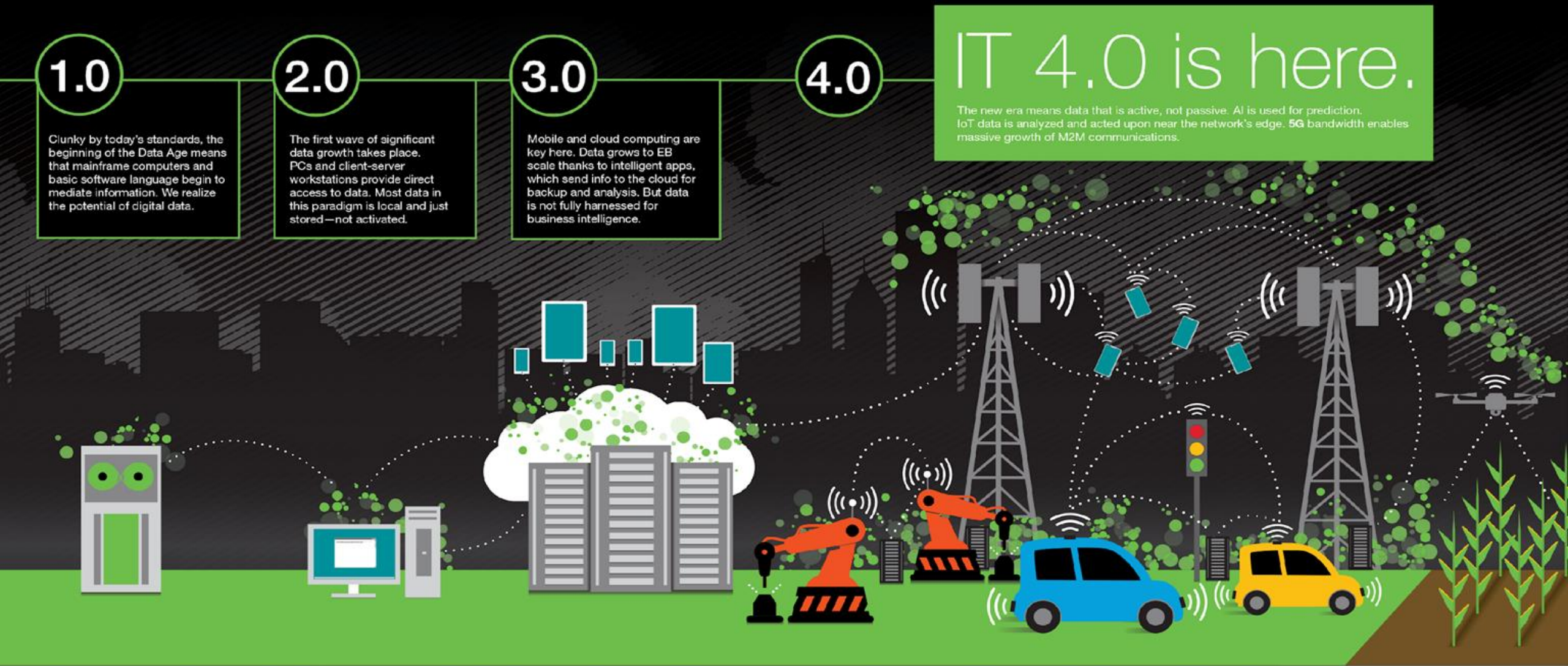
Covers Earth's Surface 2 Times

175 Zettabytes = 175,000,000,000,000,000,000,000 Bytes

https://www.live-counter.com/how-big-is-the-internet/

Evolution of The Datasphere

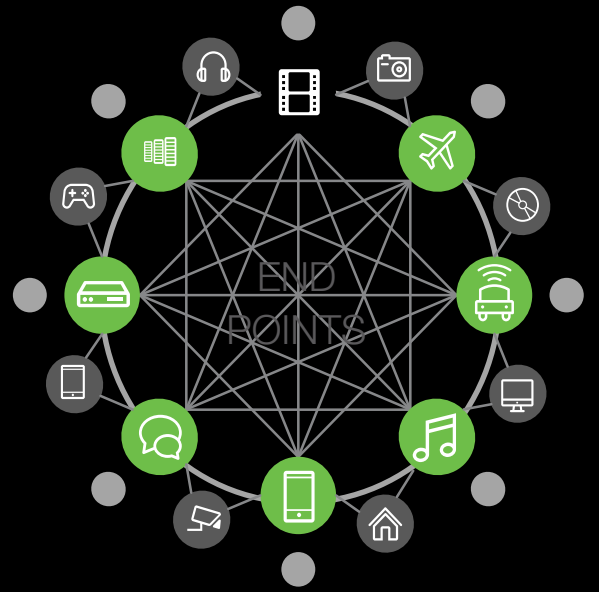
The Storage Market Continues to Transform



DIGITAL DISRUPTION

4.0

The Edge



Data 2025 Report

True Mobile and Real-Time Data

- 75% of the world's population will be connected by 2025.
- Increase in connectivity requires parallel leaps in real-time and mobile data access.
- By 2025, almost 30% of data created will be real-time in nature.

Data 2025 Report

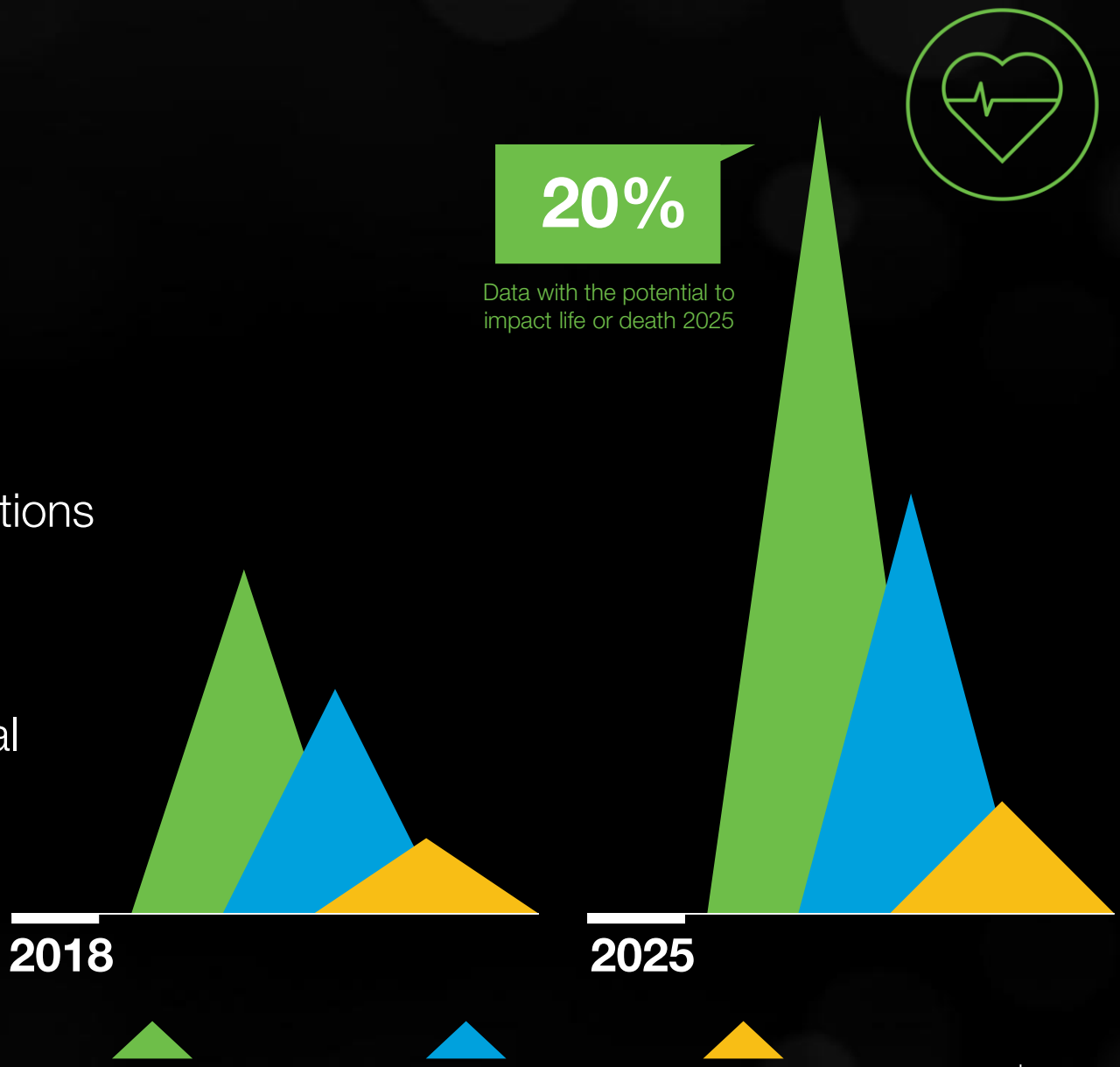
Cognitive/AI Systems Change the Landscape

- Cognitive systems will become proactive drivers of action.
- New technologies make data analysis more frequent, flexible, and important to our lives.
- Machine-to-machine decisions real-time, some critical to life.

Data 2025 Report

From Life-Enhancing to Life-Critical

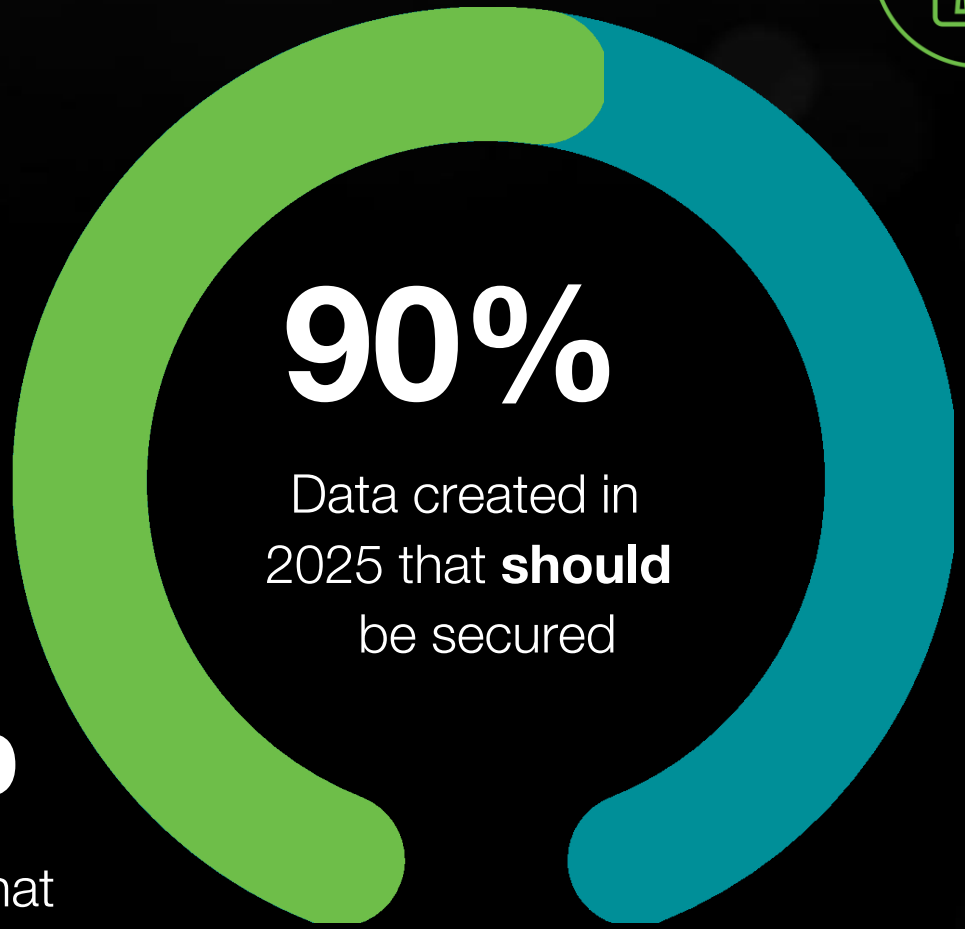
- Data is essential to the optimal operation of our society and our lives.
- If the data flow stopped, our business operations and daily lives would be severely impacted.
- The proportion of data expected to be critical and hypercritical in 2025 illustrates this growing dependency.



Data 2025 Report

Security as a Critical Foundation

- More data means more vulnerability.
- As the global datasphere explodes in size, so does the gap between secure and unsecure data.



IDC Data Age 2025 study, sponsored by Seagate www.DataAge2025.com

Data Is Valuable

Data Protection Regulations

- EU General Data Protection Regulation (GDPR)
- California Consumer Privacy Act (CCPA)

Data Handling and Delete Regulations

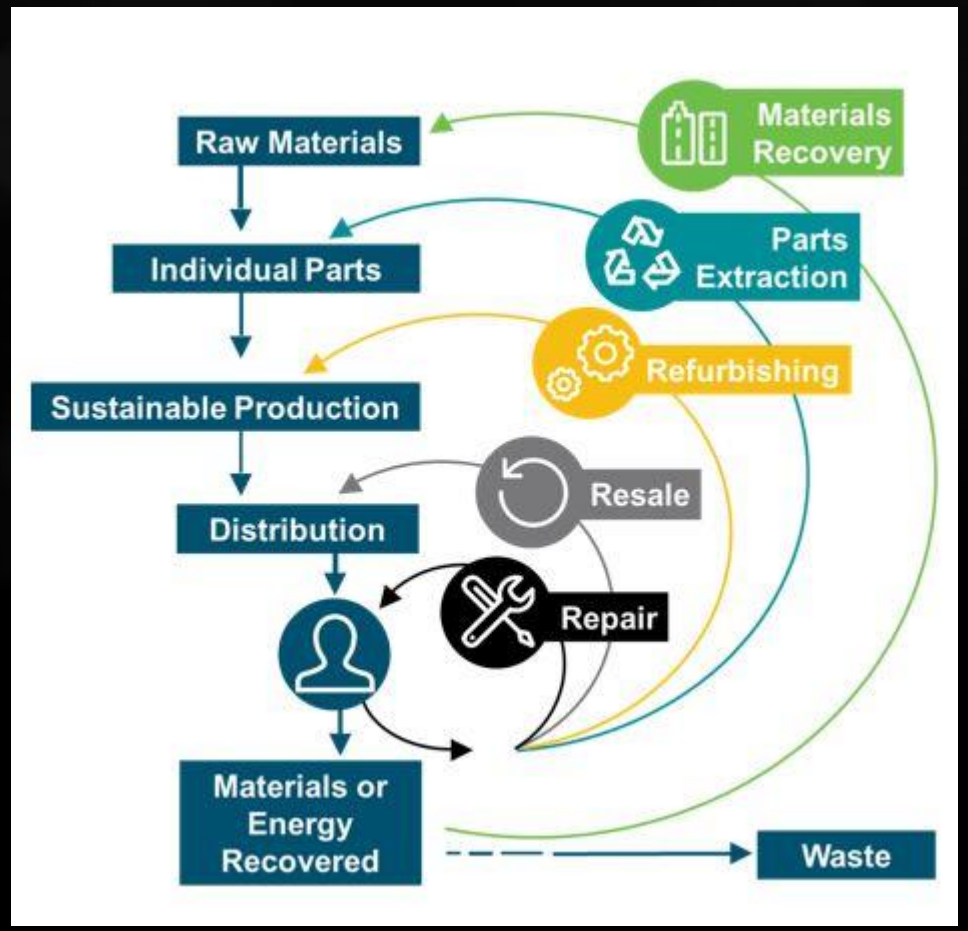
- EU Lot 9 Regulations

Cybersecurity Regulations

- Many countries & regions

Data regionalization and localization laws will influence the solutions

Global Circular Economy



Compliance

Data Privacy Laws: HIPPA, GDPR, CCPA
Cybersecurity Laws: Many Countries/ Regions
Sustainability, Trade, and Fair Labor Regulations

Threats

Data Breach
Alternative Markets
Counterfeit / Fraud
Compromised Products

End-To-End Product and Data Trust

- Components, devices, solutions, and services logically designed to be Secure and Trusted
- Trusted and immutable digital hardware identities and artifacts
- Trust networks for product and data integrity, and provenance proofs

Secure and 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		●

Essential Device Trust

Essential Data Trust

Certified Device & Data Trust

THE Open GROUP

ISO

NIST National Institute of Standards and Technology

Common Criteria

- Globally Recognized Standards
- 3rd Party Evaluation
- Certification
- Public Security Certificates

Global Standards for Leverage

Trusted Digital Products

ISO 15408: Common Criteria
ISO 19790/FIPS-140 Crypto Module Validation Program (CMVP)

Trusted Data Protection and Erasure

ISO 27040: Media Sanitization
NIST 800-88: Media Sanitization
FIPS-197: AES Encryption

Trusted Hardware Identity

ISO 11889: Trusted Platform Module
Emerging TCG DICE, Cerberos, and Titan Standards

Trusted Development and Supply Chain

ISO 20243: Trusted Technology Provider
NIST SP 800-161

Trusted Cryptography

NIST: Crypto Algorithm Validation Program (CAVP)
NIST 800-57: Crypto Strength
NIST: 800-XX Series

Trusted Digital (IT) Infrastructure

NIST Cybersecurity Framework (CSF)
ISO 27001/2: Information Security Management Systems
ISO 27XXX Series

ISO 20243: Open Trusted Technology Provider

Design, Source, Make, Deliver, Service

Category	Section	Subsection
Technology Development	Product Development / Engineering Method	Software / Firmware / Hardware Design Process
		Configuration Management
		Well-Defined Development / Engineering Method Process and Practices
		Quality and Test Management
		Product Sustainment Management
	Secure Development / Engineering Method	Threat Analysis and Mitigation
		Run-time Protection Techniques
		Vulnerability Analysis and Response
		Product Patching and Remediation
		Secure Engineering Practices
		Monitor and Assess the Impact of Changes in the Threat Landscape
Supply Chain	Supply Chain Security	Risk Management
		Physical Security
		Access Controls
		Employee and Supplier Security and Integrity
		Business Partner Security
		Supply Chain Security Training
		Information Systems Security
		Trusted Technology Components
		Secure Transmission and Handling
		Open Source Handling
		Counterfeit Mitigation
		Malware Detection

ISO 15408: Common Criteria Certifications

"Common Criteria for Information Security Evaluation"

Protection Profiles Across Data, Storage, Compute, and Networks

Certified Security


National Information Assurance Partnership

Common Criteria Certificate

is awarded to

Seagate Technology

for

Seagate Secure TCG SSC Self-Encrypting Drives

The IT product identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 3.1) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1). This certificate applies only to the specific version and release of the product in its evaluated configuration. The product's functional and assurance security specifications are contained in its security target. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

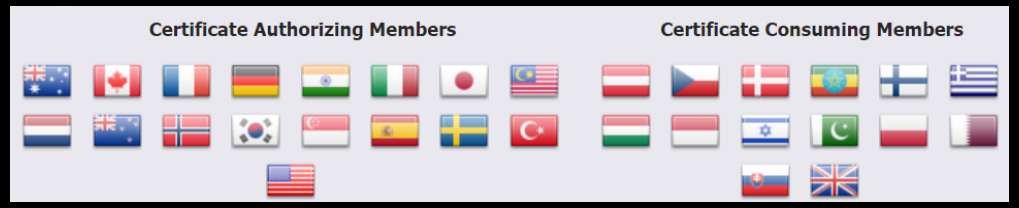
Date Issued: 2018-04-11

Validation Report Number: CCEVS-VR-VID10857-2018

CCTL: Leidos Common Criteria Testing Laboratory

Assurance Level: PP Compliant

Protection Profile Identifier: collaborative Protection Profile for Full Drive Encryption - Encryption Engine Version 2.0



- Access Control Devices and Systems – 2 Protection Profiles
- Biometric Systems and Devices – 2 Protection Profiles
- Boundary Protection Devices and Systems – 11 Protection Profiles
- Data Protection – 12 Protection Profiles
- Databases – 3 Protection Profiles
- ICs, Smart Cards and Smart Card-Related Devices and Systems – 76 Protection Profiles
- Key Management Systems – 4 Protection Profiles
- Mobility – 2 Protection Profiles
- Multi-Function Devices – 2 Protection Profiles
- Network and Network-Related Devices and Systems – 10 Protection Profiles
- Operating Systems – 2 Protection Profiles
- Other Devices and Systems – 53 Protection Profiles
- Products for Digital Signatures – 19 Protection Profiles
- Trusted Computing – 9 Protection Profiles

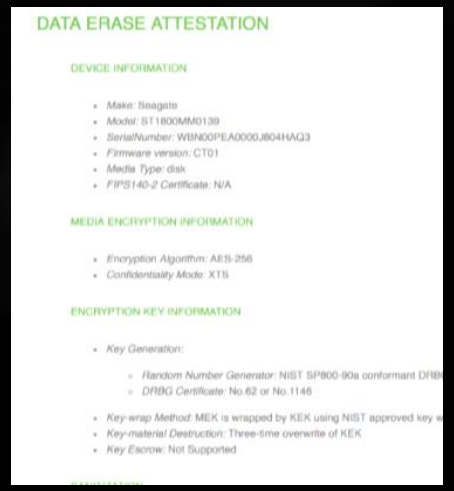
ISO 19790 : FIPS 140

"Cryptographic Module Validation Program"
"Cryptographic Algorithm Validation Program"

Section
Cryptographic Module Specification
Cryptographic Module Interfaces
Roles, Services and Authentication
Software/Firmware Security
Operational Environment
Physical Security
Non-Invasive Security
Sensitive Security Parameter (SSP) Management
Self-Tests
Life-Cycle Assurance
Mitigation of Other Attacks

- Certified Information Security Products
- Certified Cryptography

ISO 27040 / NIST 800-88: Media Sanitization



DATA ERASE ATTESTATION

DEVICE INFORMATION

- Make: Seagate
- Model: ST1800MM0139
- SerialNumber: WBN00PEA0000J804HAQ3
- Firmware version: CT01
- Media Type: disk
- FIPS140-2 Certificate: N/A

MEDIA ENCRYPTION INFORMATION

- Encryption Algorithm: AES-256
- Confidentiality Mode: XTS

ENCRYPTION KEY INFORMATION

- Key Generation:
  - Random Number Generator: NIST SP800-90a conformant DRB
  - DRBG Certificate: No.62 or No.1146
- Key-wrap Method: MEK is wrapped by KEK using NIST approved key w
- Key-material Destruction: Three-time overwrite of KEK
- Key Escrow: Not Supported

"Structure for Certified Erase"

SCSI Solid State Drives (SSDs) *This includes SCSI, SAS, Fibre Channel, etc.*	
Clear:	Overwrite media by using organizationally approved and validated overwriting technologies/methods/tools. The Clear pattern should be at least a single pass with a fixed data value, such as all zeros. Multiple passes or more complex values may alternatively be used.
Purge:	Two options are available: 1. Apply the SCSI sanitize command if supported. One or both of the following options may be available: a. The block erase command. b. If the device supports encryption, the Cryptographic Erase (also known as sanitize crypto scramble) command. *Optionally:* After Cryptographic Erase is successfully applied to a device, use the block erase command (if supported) to block erase the media. If the block erase command is not supported, the Clear procedure could alternatively be applied. 2. Cryptographic Erase through the TCG Opal SSC or Enterprise SSC interface by issuing commands as necessary to cause all MEKs to be changed. Refer to the TCG and vendors shipping TCG Opal or Enterprise storage devices for more information. *Optionally:* After Cryptographic Erase is successfully applied to a device, use the block erase command (if supported) to block erase the media. If the block erase command is not supported, the Clear procedure is an acceptable alternative.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.

- Defines acceptable media sanitization
- Across all media types, from paper to digital
- Data Risk Management Structure

Trust in the Datasphere

DATA IS POTENTIAL

Thank You

SEAGATE