SEAGATE | GOVERNMENT SOLUTIONS

MAXIMIZING DATA'S POTENTIAL

2019 March 14th MSPCMG Meeting
Storage – The Final Frontier of Innovation

Cybersecurity and Risk Management and World-wide Standards

Henry Newman CTO Seagate Government Solutions hsn@seagategov.com

SEAGATE

Agenda

- Digital Disruption
  - Global Data Explosion
  - Market Transition to Security

- Product Cybersecurity Scope

- Security Certification and Standards

- Manage / Mitigate Risks
  - Compliance and Certification Management
  - Product Security Operations

- Summary

> “To understand where we are going,
> it’s important to understand how we got here.”

Digital Disruption

10 million users

1.0 1960 - 1970

Mainframe

Centralized

2 billion users

2.0 1980 - 2000

Client-Server

Distributed

7 billion users

3.0 2005 - 2020

Mobile-Cloud

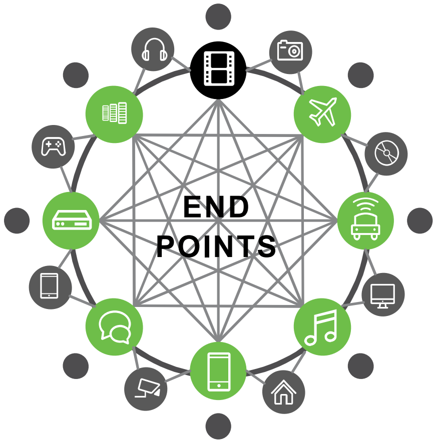
Centralized

1+ trillion users

4.0 2020 -

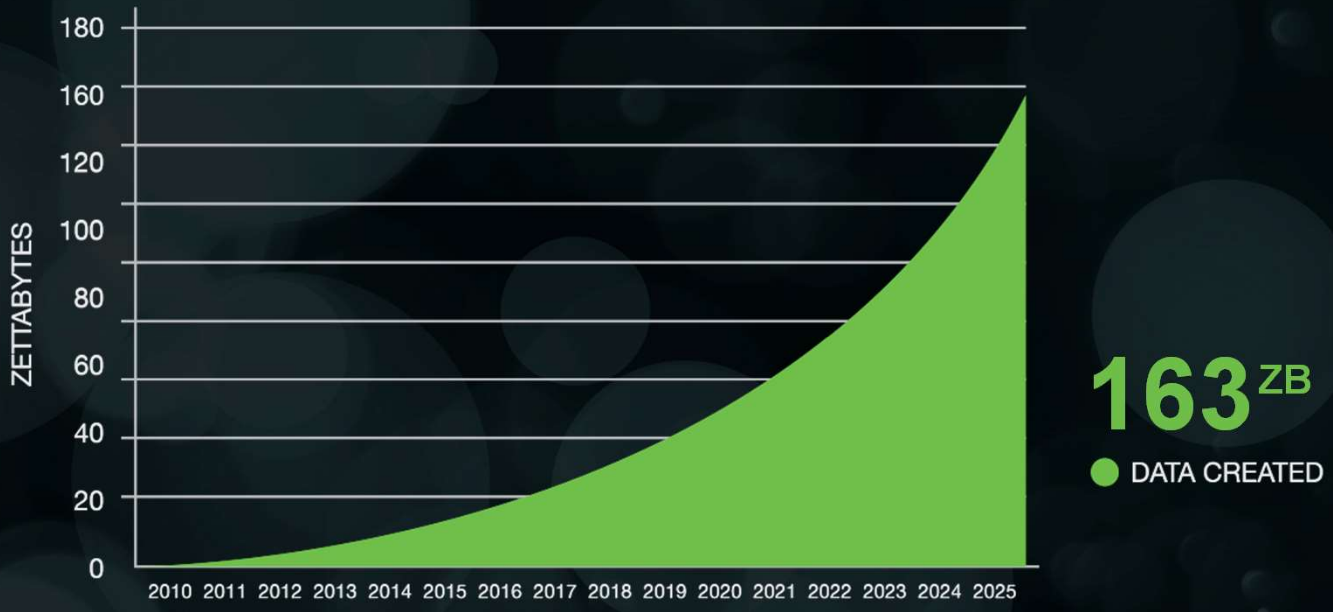
Rise of the Edge

Distributed



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.

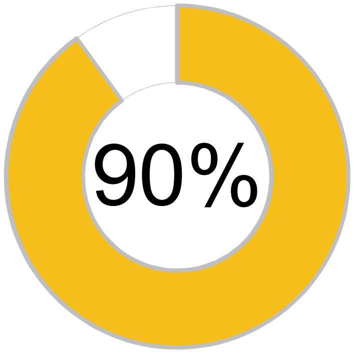


SOURCE: IDC's Data Age 2025 study, sponsored by Seagate, April 2017

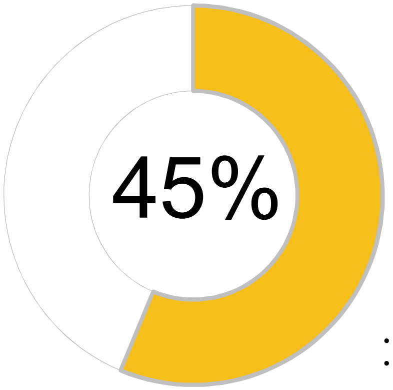
Market Transition to Security is Occurring

7.9M*

GDPR: 2-4% Annual Revenue



Data created in 2025 that should be protected



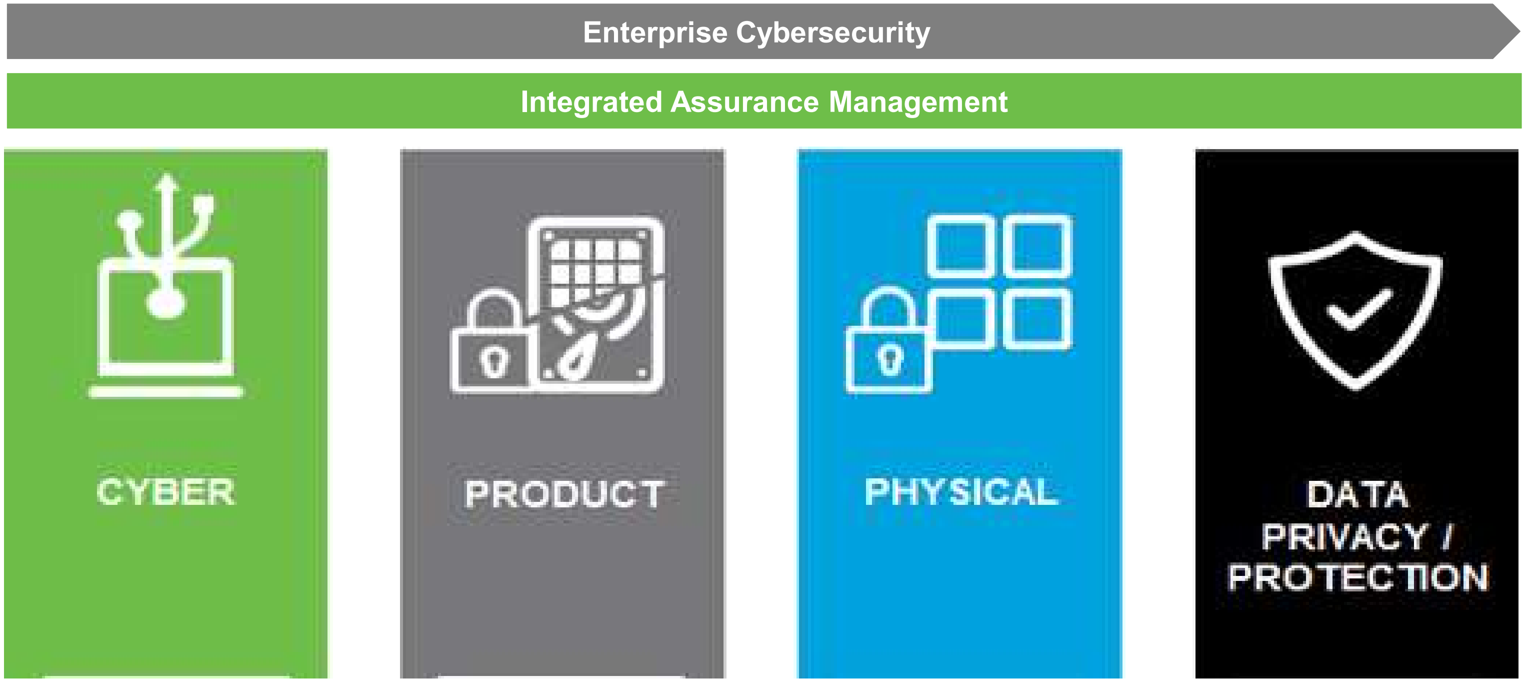
Amount that will actually be protected

- Majority of data requires at least some form of protection
- Actual amount of data protection falls far short
- This gap presents an increasing industry need for security and privacy technologies, systems, and processes to address it
- Substantial penalties for non-compliance

- https://www.pcmag.com/news/362543/how-much-does-a-data-breach-cost
- Average Cost of Data Breach in US from IBM and Ponemon study.

Cybersecurity Scope

Lines of Protection



Enterprise Cybersecurity

Integrated Assurance Management

CYBER

PRODUCT

PHYSICAL

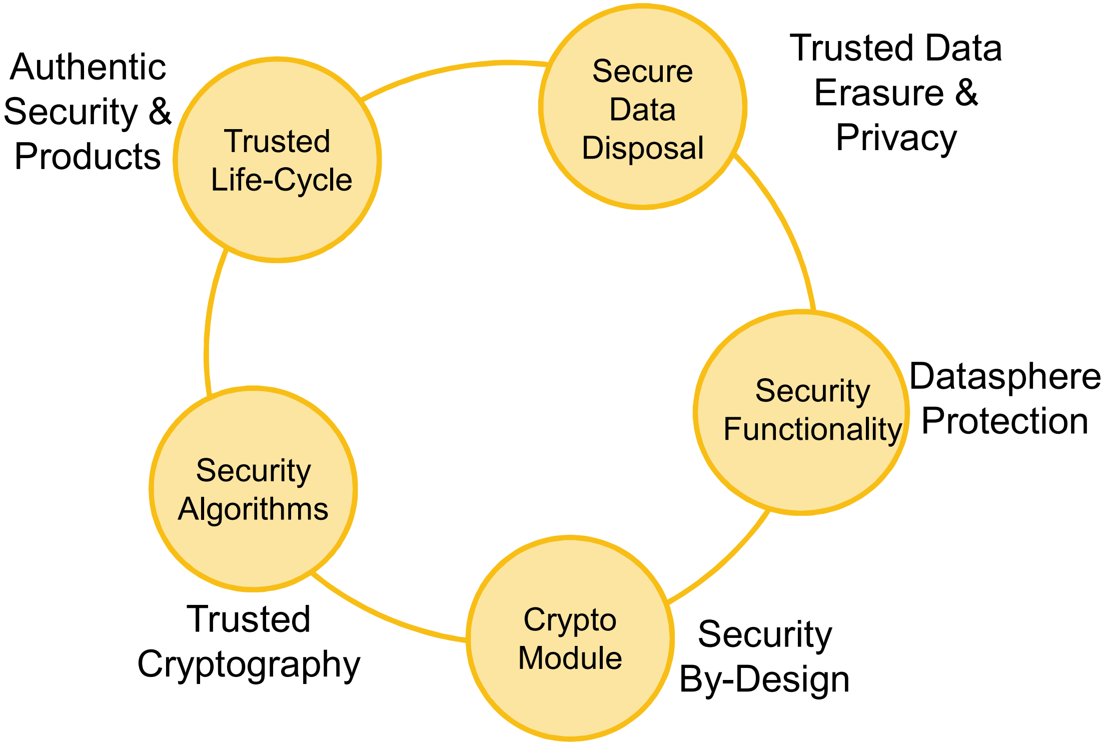
DATA PRIVACY / PROTECTION

Cybersecurity Scope

Enabling a Full Lifecycle Data Security Model

Manage Risk

Security Certification and Standards



Authentic Security & Products

Trusted Life-Cycle

Secure Data Disposal

Trusted Data Erasure & Privacy

Security Functionality

Datasphere Protection

Crypto Module

Security By-Design

Security Algorithms

Trusted Cryptography

NIST

ISO

THE Open GROUP

FIPS VALIDATED 140-2

Common Criteria

Security Algorithm Certifications

Security Algorithms

Trusted Cryptography

- Standard and Trusted Security Algorithms
- Certifications of all algorithms
  - Data Encryption
  - Integrity & Signatures
  - Random # Generation
  - Key Derivation…
- Required for FIPS 140-2 & Common Criteria Certs

NIST National Institute of Standards and Technology

Cryptographic Algorithm Validation Program (CAVP)

Security Module Certifications: FIPS 140-2

Crypto Module

Security By-Design

- Fundamental Security Certification
- Evaluation by Independent Labs
- Required for Information Security Products in Sensitive and Unclassified space in US & Canada
- Value recognized in other geographies

Cryptographic Module Validation Program (CMVP)

Security Module Certifications: Common Criteria (CC)

Security Functionality

Datasphere Protection

- Security Use-Case (Protection Profile) Certification
- Evaluation by Independent Labs
- Certification recognized by 28 member nations globally for Information Security acquisition

Common Criteria for Information Security Evaluation (CC)

Sanitization Standard

Secure Data Disposal

Trusted Data Disposal & Privacy

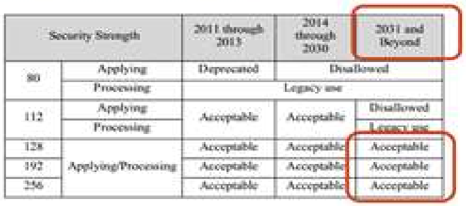
- NIST SP 800-88 (Federal) & ISO 27040 (International) define media sanitization
- NIST SP 800-57 Defines Crypto Algorithm Longevity for erasure assurance.

NIST Special Pub 800-88

NIST Special Pub 800-57

ISO 27040

Crypto Algorithm Longevity*



Security Strength		2011 through 2013	2014 through 2030	2031 and Beyond
80	Applying	Deprecated	Disallowed	
	Processing	Legacy use		
112	Applying	Acceptable	Acceptable	Disallowed
	Processing			Legacy use
128	Applying/Processing	Acceptable	Acceptable	Acceptable
192		Acceptable	Acceptable	Acceptable
256		Acceptable	Acceptable	Acceptable

AES in any key size (128, 192, 256) is acceptable for use to 2031 and Beyond.

Trusted Life-Cycle Standards

Trusted Life-Cycle

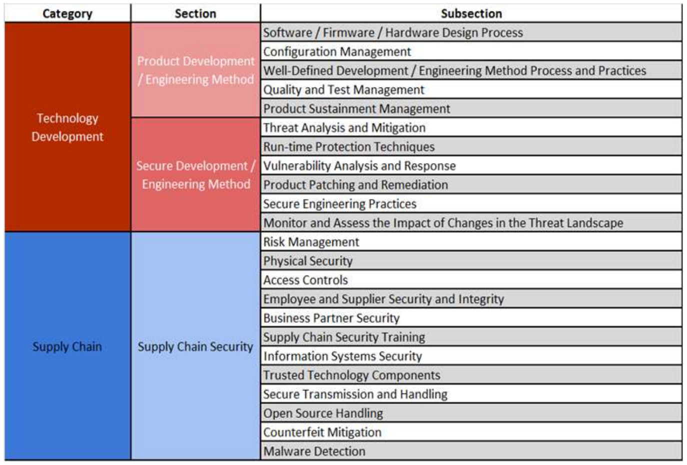
Authentic Security & Products

- The Open Trusted Technology Provider Standard (O-TTPS) is now a sanctioned ISO Standard
- Comprehensive Secure Technology Provider Standard
- Sections for Secure Technology Development and Secure Supply Chain
- The NIST Cybersecurity Framework Provides for common framework and language for managing Cyber Risk

THE Open GROUP

ISO 20243

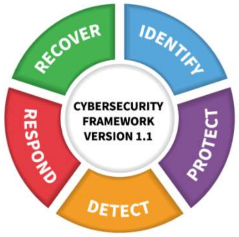
Trusted Tech Provider Standard



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

NIST National Institute of Standards and Technology

Cybersecurity Framework

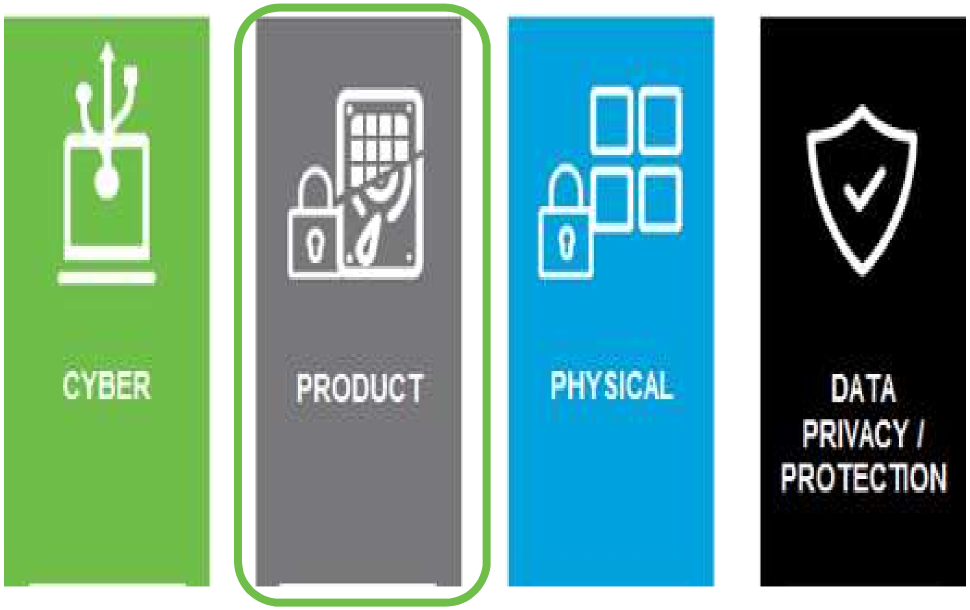


Credit: N. Hanacek/NIST

Product Cybersecurity Scope

Mitigate Risk

Integrated Assurance Management



Policy-based compliance aligned to OTTPS, ISO and the NIST Cybersecurity Framework (CSF)

Identify → Protect → Detect → Respond → Recover

Policies

- Product Development Policy
- Product Development 3rd Parties

Maturity Staircase to Cybersecurity Compliance

- Gap Analysis
- Conformance
- Certification Preparation
- Certification

Transparent Compliance and Incident Response Management

- Product Security Operations Center (PSOC)
- Product Security Incident Response Team (PSIRT)

Scalable to Trusted Product Lifecycle

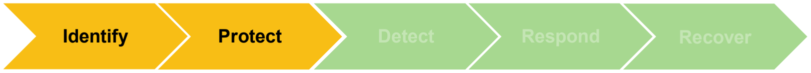
- Design, Source, Manufacture, Deliver, Service

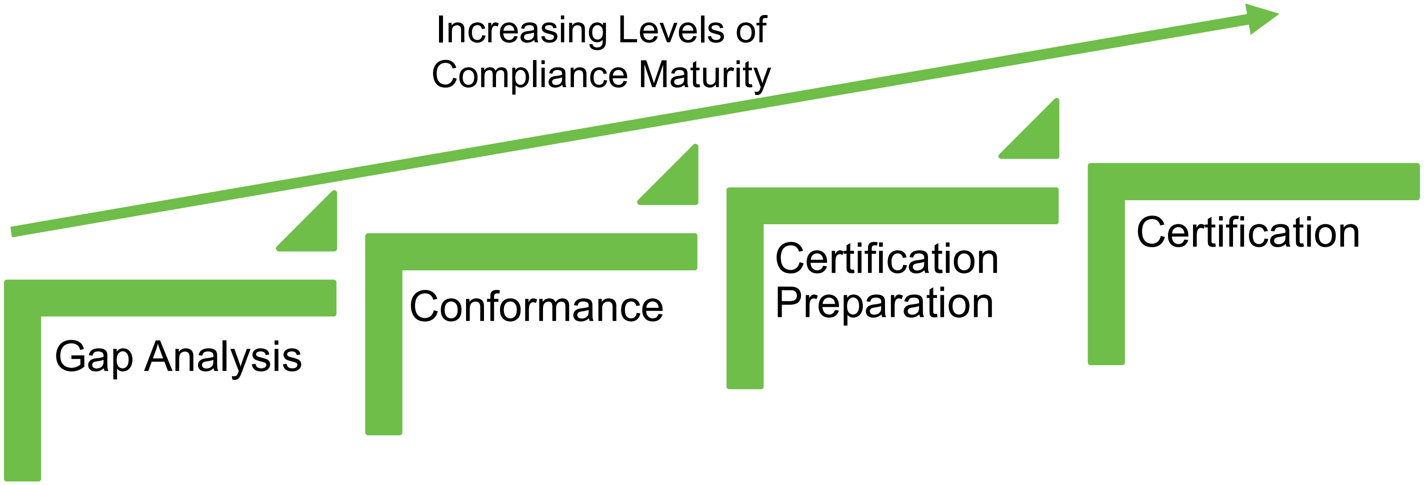
Product Security: Manage Risk

Maturity Staircase Based Policy Compliance

Policies

- Product Development Policy
- Product Development 3rd Parties

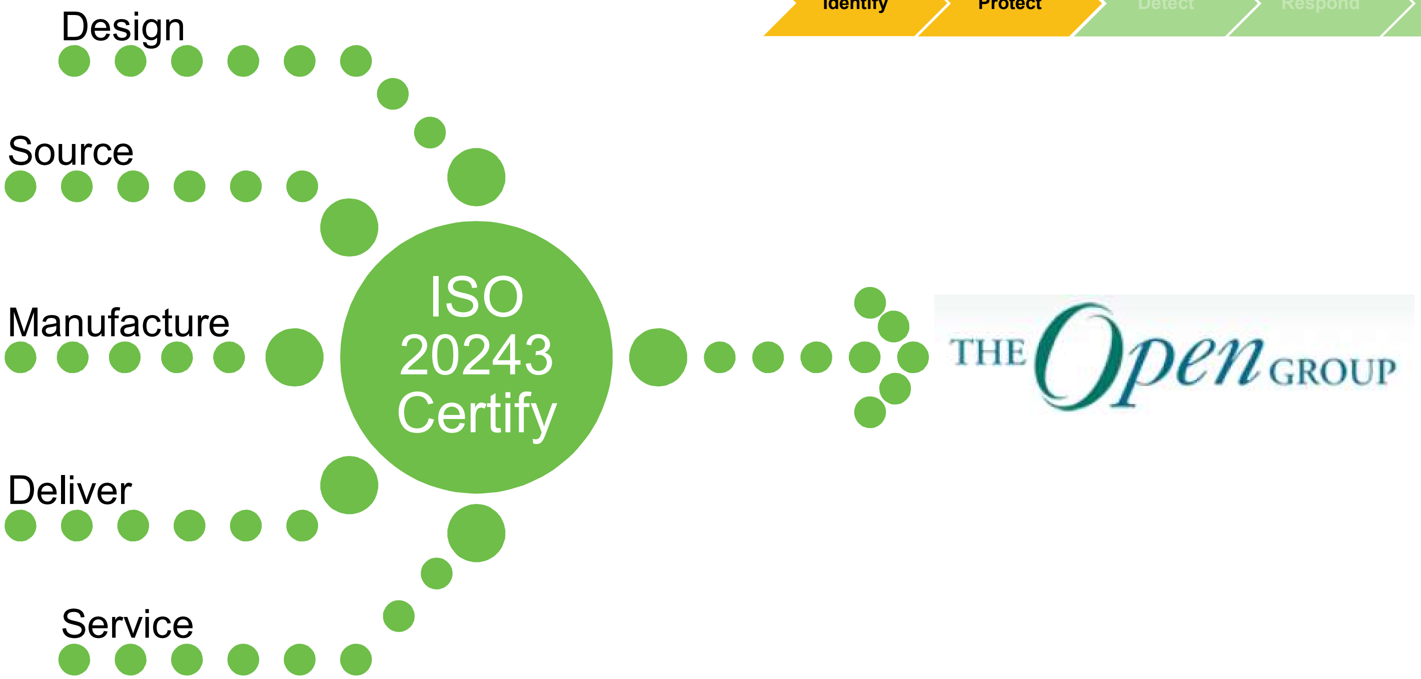



Increasing Levels of Compliance Maturity
Gap Analysis
Conformance
Certification Preparation
Certification

Product Security: Certification

Trusted Product Life Cycle Certification

Identify | Protect | Detect | Respond | Recover



Design

Source

Manufacture

Deliver

Service

ISO 20243 Certify

THE Open GROUP

Certified Erase - Strong Data Protection Assurance

Trusted Tech Provider Standard

ISO 20243

- ✓ Essential & Certified By Design
- ✓ Trusted Design & Life-cycle
- ✓ Verifiable HW Roots of Trust

NIST Special Pub 800-88

NIST Special Pub 800-57

ISO 27040

- ✓ Defines Strong Media Sanitization
- ✓ Defines Security Requirements
- ✓ Defines Erase Certificate. App. D

Cryptographic Module Validation Program (CMVP)

Cryptographic Algorithm Validation Program (CAVP)

- ✓ Independent Lab Validation
- ✓ Validates 800-88 Security Rqmts
- ✓ Public Online Policy & Certificate

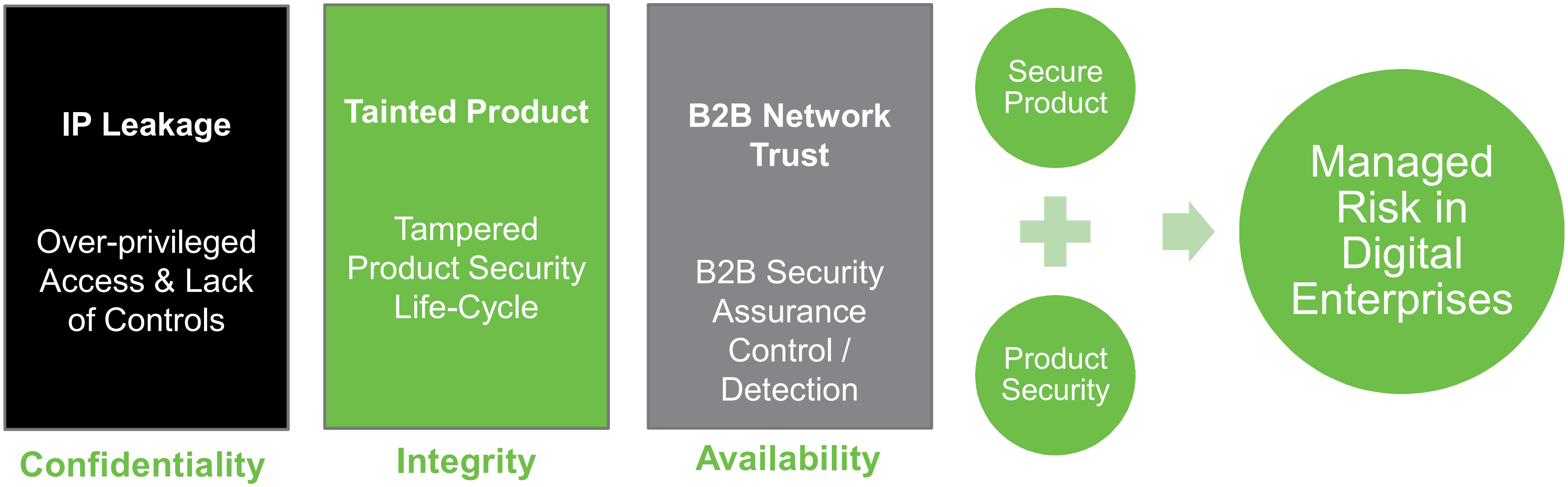
Common Criteria for Information Security Evaluation (CC)

EE – Encryption Engine Profile

AA – Authorization Acquisition Profile

- ✓ Independent Lab Validation
- ✓ Validates 800-88 Data Erasure
- ✓ Public Online Policy & Certificate

Summary



IP Leakage

Over-privileged Access & Lack of Controls

Confidentiality

Tainted Product

Tampered Product Security Life-Cycle

Integrity

B2B Network Trust

B2B Security Assurance Control / Detection

Availability

Secure Product

Product Security

Managed Risk in Digital Enterprises

Thank You