

Digital Transformation and the Enterprise of Things

MARK WILSON

Chief Marketing Officer, BlackBerry



**EMPOWERING THE SECURELY
CONNECTED WORKFORCE**

BlackBerry® Secure™

**WORLD
TOUR**

BlackBerry Highlights

STRATEGY

Leveraging our DNA in security, mobile-first, embedded systems to win in the EoT market

Pivot from hardware to software is complete

INNOVATION

23%
of revenue invested in R&D

37,500
Patents

18
Major development centers in 7 countries

FINANCIAL PERFORMANCE (Non-GAAP)

\$1.08B
FY18 revenue

81%
Of total FY18 software and services revenue

8
consecutive quarters of operating profit

\$2.4B
In cash as of February 28, 2018

RECOGNITION

Recognized market leadership by



FORRESTER™

Gartner



STRATEGY ANALYTICS
Research, Experts, and Analytics

VDC|Research
Insights for the Connected World

CUSTOMERS

9/10
of Largest Commercial Banks and Insurance Companies

8/10
of Largest Healthcare and Aerospace/Defense Companies

All 7
of the G7 Governments

60M
Vehicles from leading auto manufacturers

SECURITY DIFFERENTIATORS

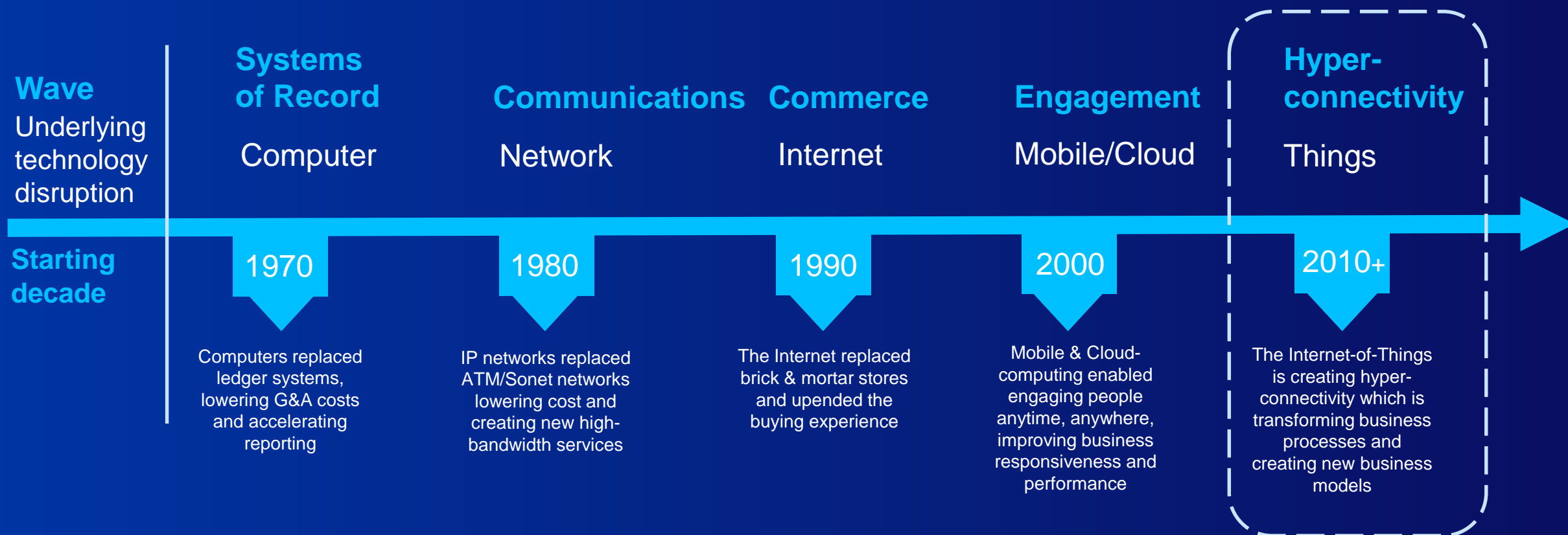
80+
Security Certifications

Cybersecurity Operations Center

Only ISO 26262 Certified

Elliptical Curve Cryptography

The “Enterprise of Things” (EoT) is the 5th wave of enterprise productivity



BlackBerry enables EoT

What is the “Enterprise of Things”

EoT enables digital
transformation using
hyper-connected “things”
that are highly secure



Source: McKinsey & Company, Gartner, Ericsson Mobility Report,
2016 Verizon Data Breach Investigations Report

1. Things - Enables transformation

Digital things

52 billion exabytes of data by 2020 -
51% CAGR

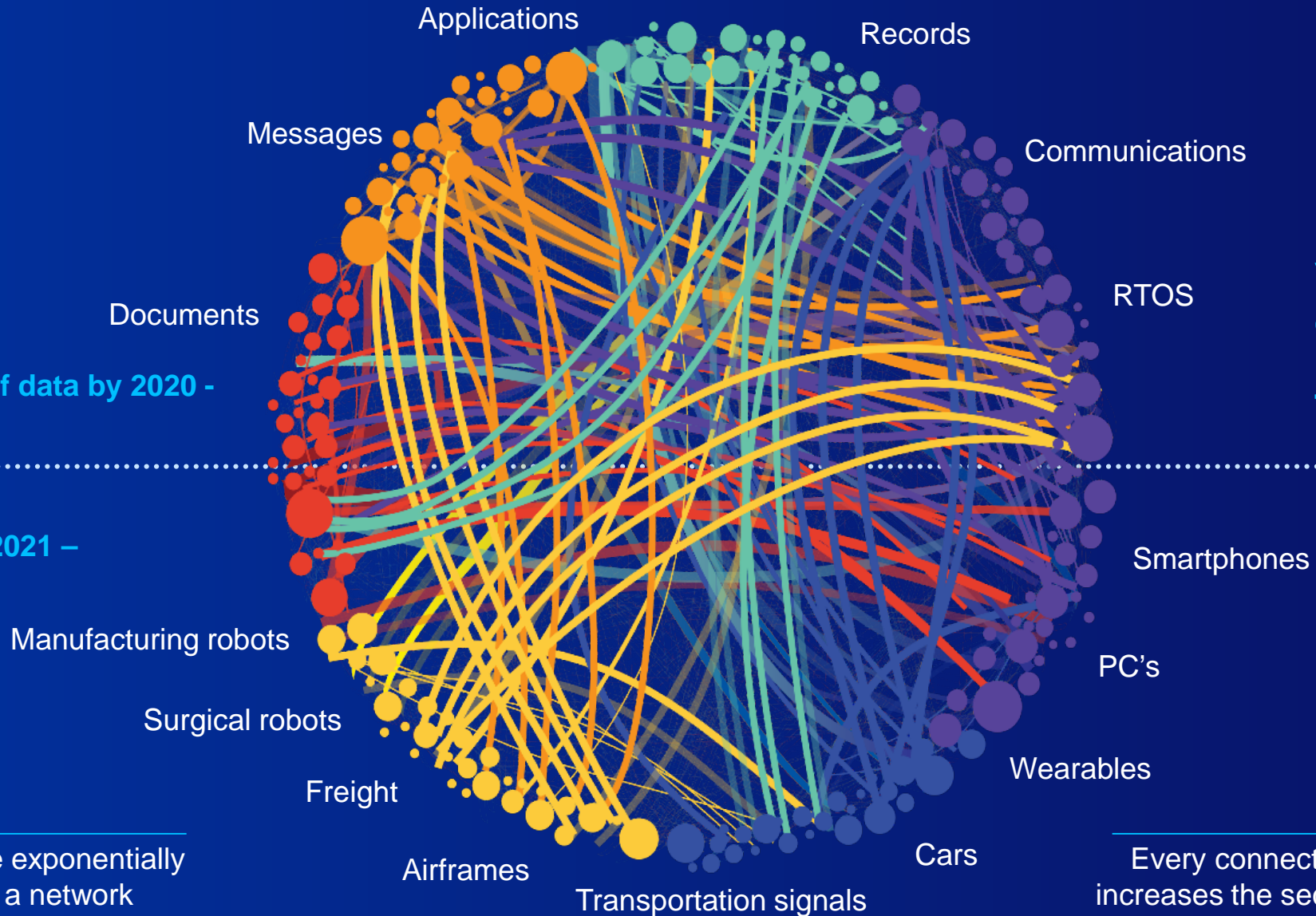
Physical things

46 billion things by 2021 -
56% CAGR

Metcalf's Law

Every connected node exponentially increases the value of a network

Source: Juniper Research, 2015, *McKinsey Global Institute "The Internet of Things, Mapping the Value Beyond the Hype, 2015.



**“40% of IoT
value requires
connectivity”**

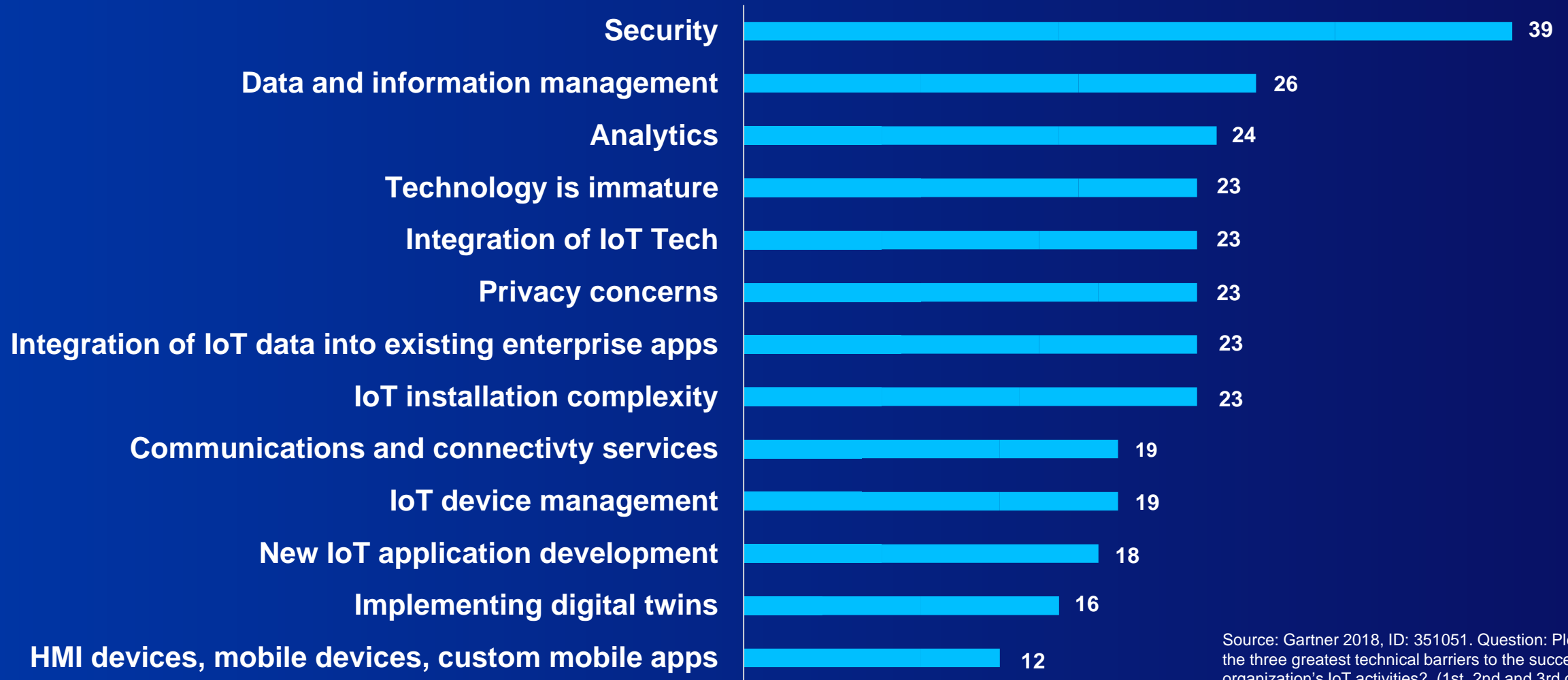
- McKinsey & Co.

BlackBerry Law

Every connected node exponentially increases the security risk of a network

2. Security – Safeguards “Things” from attacks

Security is the #1 technical barrier to EoT success



Source: Gartner 2018, ID: 351051. Question: Please rank the three greatest technical barriers to the success of your organization's IoT activities?. (1st, 2nd and 3rd choice rankings of technical barrier to EoT success)

2. Security – Safeguards “Things” from attacks

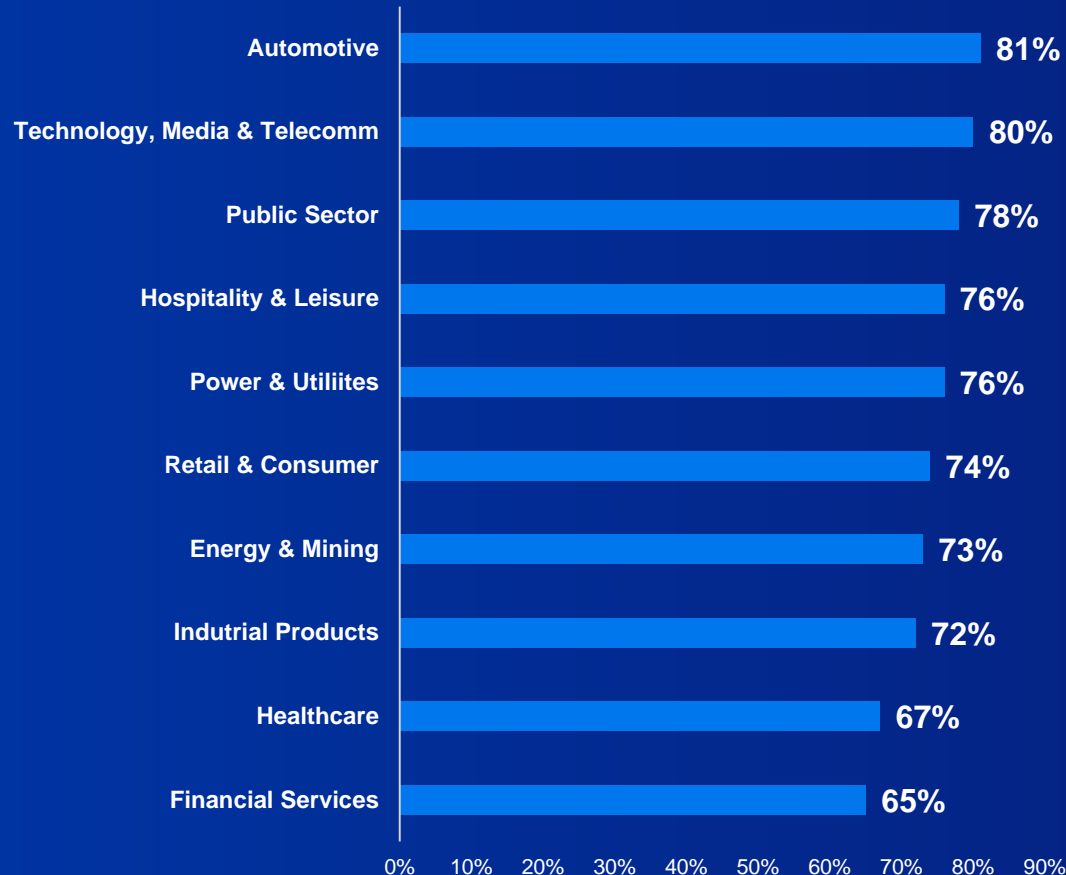
New security requirements for EoT

- Attack surface has grown exponentially
- Employees and endpoints are emerging vulnerabilities
- Need to ensure network of suppliers and distributors are secure
- New standards for customer data privacy
- AI assessments needed to identify emerging vulnerabilities

3. Transformation – Creates business value

Industries are investing in EoT ...

Internet of Things investment by Industry*



... to realize key transformational benefits

Six major tasks that benefit from EoT**

1. Enhanced situational awareness
2. Process optimization
3. Optimized resource consumption
4. Sensor-driven decision analytics
5. Tracking behavior for real-time marketing
6. Instantaneous control and response in complex autonomous systems

What this means for a hyper-connected organization

Workplace, either physical or digital, uses things to seamlessly to enable work anytime, across any boundary.



Workflow is optimized using things to securely collect and deliver the right information to the right decisioning endpoint at the right time.

Workforce seamlessly extends across employees, contractors, partners and things. They are enabled to get to better outcomes faster. The result is more agile and effective employees and partners.

TODAY'S DIGITAL WORLD

Disparate security solutions in place to address rising threats



Endpoints not secure

Multiple mobile device management



DISCONNECTED WORKPLACE

CLOSED WORKFORCE

SILOED WORKFLOW

No standard automated process for emergency communications



BYOD and accidental content leakage

Wide variety of file sharing solutions

No standard for EoT and wearables connectivity

Small projects underway for digital transformation

No secure access to corporate systems from outside the office



Multiple logins

Consumer messaging use for company business



Instantaneous control and response in complex autonomous systems

Enterprises are resistant to malicious attack with holistic security solutions

Unified critical communication to connect people, devices and external organizations

Process optimization with semi-autonomous workflows

SMART FUTURE



Secure remote access for any Windows 10 or macOS device

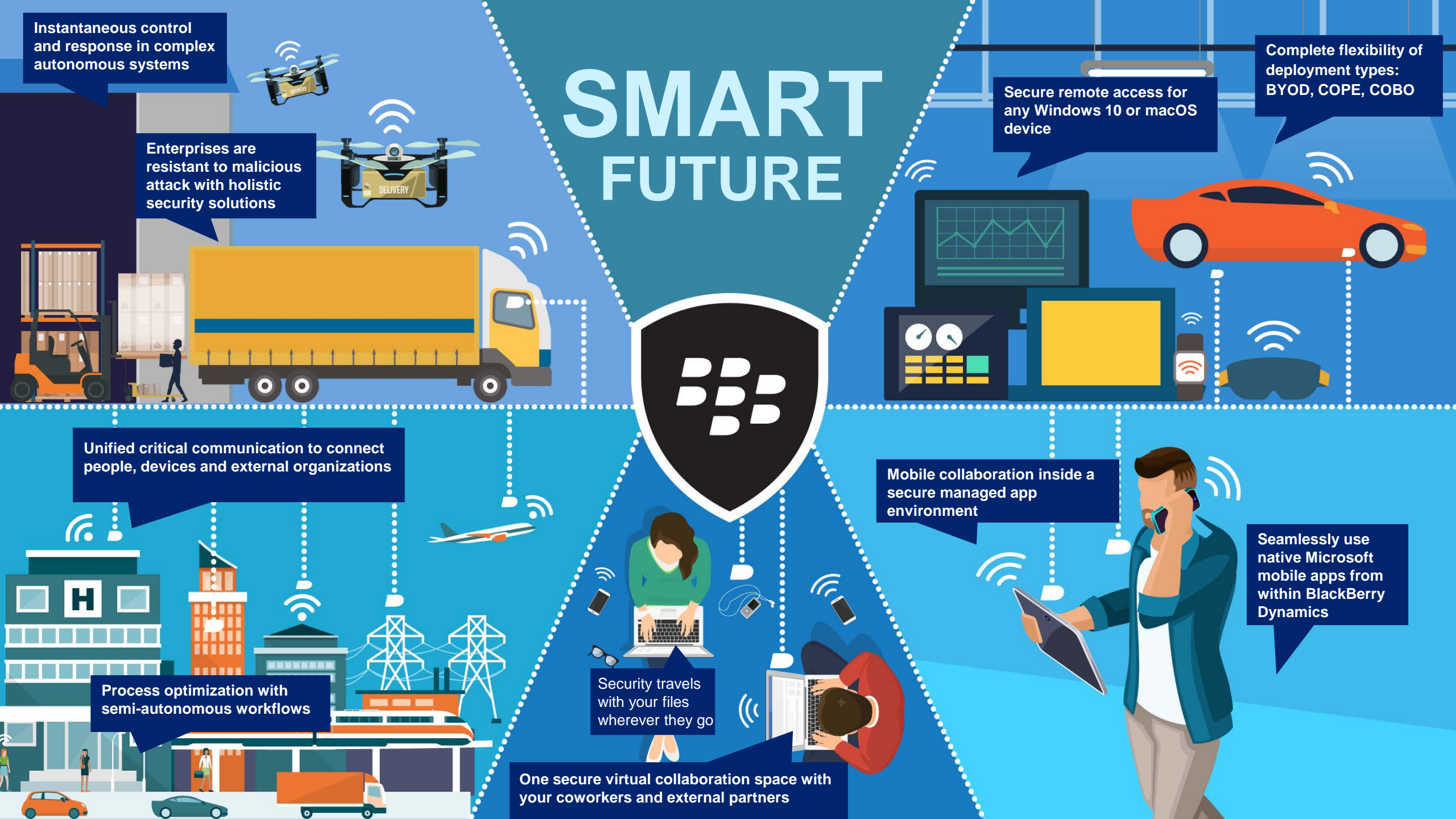
Complete flexibility of deployment types: BYOD, COPE, COBO

Mobile collaboration inside a secure managed app environment

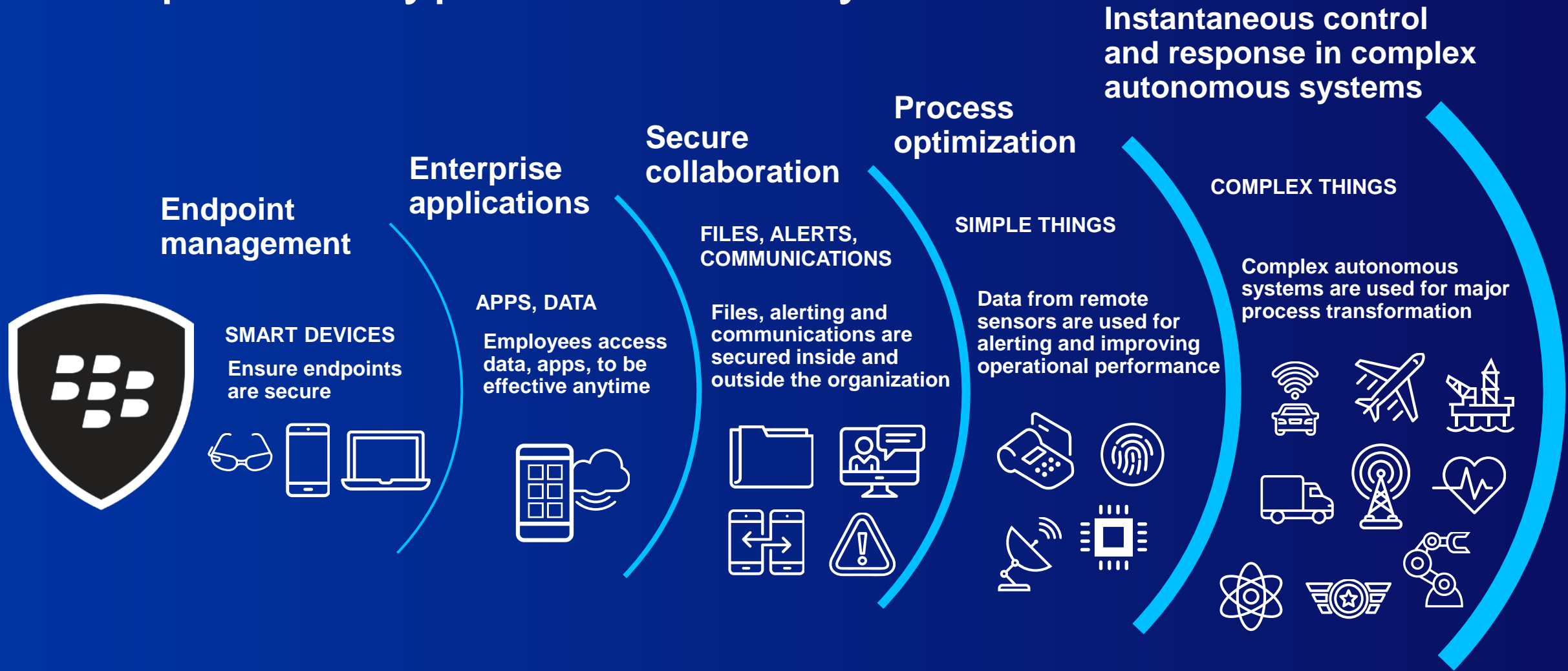
Seamlessly use native Microsoft mobile apps from within BlackBerry Dynamics

Security travels with your files wherever they go

One secure virtual collaboration space with your coworkers and external partners



The path to hyper-connectivity







#BBSWT



300,000

150



File sharing and the connected workforce

Workplace:
Share files inside
AND outside
your organization



Workflow:

Collaboration through sharing - often confidential and regulated data (intellectual property, business plans, SSN's, credit card info, etc.)

Workforce:

Collaboration with internal peers AND contractors, temps, partners, suppliers, regulators, etc.

The connected workforce

269,000,000,000

Emails are sent every day

2,000,000,000

Files are uploaded to cloud-based file services every day

Source: Radicati

10 Exabytes







File Sharing = Risk

**Email is the #1
file sharing technology**





Cloud based file sharing

File sharing today: Major risk factors



The average organization has 13 file sync applications in use – most not approved or managed by IT



76% of organizations send traffic to Dropbox (2GB/mo. on average)

77%

Of sensitive data stored in the cloud is Microsoft Office or .pdf documents

72%

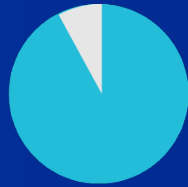
Of cloud DLP violations at FS Firms involve Webmail, Cloud Storage or Collaboration Apps

Source: Netskope, Palo Alto Networks, Gartner, Skyhigh Networks

IT leaders say that their security policies and technology covers file sharing, but they are still susceptible to breaches

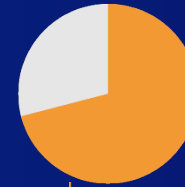
90%

say their security policy covers file sharing*



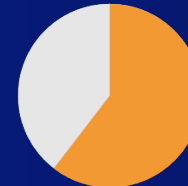
74%

had a breach, or weren't sure if they had or not*



65%

are not certain that their security plan for unstructured data meets regulatory requirements*



*Source: BlackBerry survey 2017

Reported Causes of Breaches



Percentage of respondents reporting breach by type

28%

Accidental sharing

26%

Attacks/hacks

20%

Personal software or devices

20%

Personal email & file sharing

18%

Lost, stolen, or insecure devices

16.5%

Deliberate Internal leaks

14.5%

Consumer services and apps

12.5%

Ransomware

11%

IP Loss

*Source: BlackBerry survey 2017



Secure all your files with BlackBerry Workspaces

File-level
security that
travels
everywhere
your files go



All Files protected with:

- ✓ Encryption at all times
- ✓ Security that travels with the file
- ✓ User authentication
- ✓ Digital rights management (DRM)
- ✓ Tracking and reporting of all file activities



GLOBAL
DIVERSIFIED
ALTERNATIVES

QIC





Legal



Infosec





#BBSWT

VP Inside Sales, BlackBerry



WORLD TOUR

Take-away from the day

We see the future as an exciting one because of the communications and connections possibilities it offers. We intend to make this future a reality and we will make sure it is done right.

JOHN CHEN

CEO and Executive Chairman
of the Board, BlackBerry





 **BlackBerry®**

Please complete
our survey



Join us for a drink
in the experience center!



**Networking Session in
the Experience Center**



**EMPOWERING THE SECURELY
CONNECTED WORKFORCE**

BlackBerry® Secure™

**WORLD
TOUR**

