Intelligent and Connected Enterprises

Mark J. Barrenechea | Vice Chair, CEO and CTO
mark@opentext.com

April 12, 2018
We are The Information Company.

Enabling intelligent and connected enterprises.

Inspiring a new way to work.
Our Vision for Intelligent and Connected Enterprises

- Digital Applications
- Digital Information Platform
- Customer Experience
- Employee Engagement
- Asset Utilization
- Supplier Efficiency
- Developer
- Cloud Platform
- Security
- Business Network
- IoT

EIM Suite
OpenText inspires a new way to work

#1 in EIM
Top 10 Software Company

Helping the world cure cancer

Advancing women in technology

27%

Helping the world be a better place
Computing has changed

- Always ON, Connected, Real Time
- Visual and has sensors
- Workforce is fluid and global
- Takes ONE finger to use
- Users are changing the way IT works
- Wicked smart

Mainframes
- Monolithic

Client server
- Calculation

Internet
- Automation

Cloud
- Digital

Webservices

Microservices
- Cognitive

AI
Finding the opportunity in a disruptive time

- **4 Billion Connected Humans**
- **65% Gen Z/Y Workforce**
  - 2000: Gen X 31%, Gen Y 34%, Gen Z 9%, Baby Boomers 25%
  - 2020: Gen X 27%, Gen Y 34%, Gen Z 31%, Baby Boomers 8%
- **1 Trillion Machines**
  - Industrial
  - Commerce
  - Towns & Cities
  - Homes
  - Vehicles
  - People
- **25 Million Developers**
  - Worldwide developer population to Top 25 million by 2020
Business is very complex today …

- Changing workforce (Gen Y/Z)
- New business models (Gig-economy)
- We are all software companies
- Data scientists (the new job)
- Corporate social responsibility (CSR)
- AI
- Regulation (GDPR)
- Digital (got to go faster)
- Robots (going to lose my job)
- Machines and IoT (raining data)
- Security
- Mobile is eating the world (PC’s are gone)
- Cutting costs, increasing revenue
Comfort + Complexity = Calamity
Job #1 today:

- **Security** is the digital platform
- **Insight** through AI
Amazing things are happening

3D printed organs. No human hands.

No check out lines. No human hands.

5 million cars a year. No human hands.
So are bad things

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Largest breach in the history of the internet</td>
<td>Bankrupt after hackers extracted trade secrets</td>
<td>Credit Card Readers listened to from Parking Lot</td>
<td>Target of a data breach where 21.5 million records were stolen</td>
</tr>
</tbody>
</table>

**YAHOO!**  **NORTEL**  **LUCKY**  **UNITED STATES OFFICE OF PERSONNEL MANAGEMENT**
And so are “stranger things”…

When your social data determines your social status and when your social data can no longer be trusted at the same time.
No, Emma González did not rip up the U.S. Constitution!

https://www.teenvogue.com/story/emma-gonzalez-parkland-gun-control-cover

And the activity is growing

- **Dropbox**: 68 million
- **US Office of Personnel Management**: 22 million
- **Yahoo**: 145 million
- **Yahoo**: 3 Billion
- **eBay**: 145 million
- **Target Stores**: 110 million
- **LinkedIn**: 165 million
- **JP Morgan Chase**: 76 million
- **Adult Friend Finder**: 412.2 million
- **Equifax**: 145 million
- **FedEx**: Undisclosed
- **Heartland Payment Systems**: 134 million
- **Stuxnet**: Undisclosed
- **Uber**: 57 million
- **Anthem**: 69 million
- **Maersk**: 200 million
- **Boeing**: Too soon to tell

Bubble size represents impact of breach
How do hackers work?

- Test Perimeters
- Spam & Phish
- 3rd Party Data
- Penetrate and Lurk
- Find weak “information” policies, procedures and systems
- Go lateral inside your network
- Drip or Pour information out
- Time from “Penetration to actual Breach” can be weeks
- Reasons vary: crime, espionage, hacktivism, conflict, war
Just one event can take down your business

- Personal data of 143 million Americans
- Names, Social Security numbers, birth dates, addresses, driver's license, credit card numbers, tax identification numbers and email addresses
- The company took six weeks to notify the public after finding out about the breach
- 90 day breach
- Patches where available
- Data did not show up on the dark web

Massive data breach hits 143 million Americans
Or take down your business for months

Shamoon - 2012

- Saudi Aramco is Saudi Arabia’s state owned national oil company
- **August 15, 2012:** an attack is launched through an opened scam email; **infecting 30,000** workstations
- **75% of infected PC’s had their data erased** [documents, spreadsheets, emails, files]
- **200 day breach**
Or take down an eco-system

$81M stolen and evidence erased through SWIFT

1. Attackers gain access and install malware
2. Malware decrypts config file containing search terms to scan within SWIFT messages
3. Malware identifies and exploits host’s SWIFT application to bypass validity check within Oracle DLL
4. Confirmation messages from the SWIFT network and now monitored by the malware. Functionality continues in loop until 06:00 6th Feb 2016
5. SWIFT messages sent to printer are tampered with in real time
6. PRC and FAL files are scanned for attacker defined terms. On match with extract transfer reference and sender address to form a SQL DELETE statement to delete a transaction
7. Messages that contain attacker defined terms will be used to form SQL statements to query Convertible Currency availability and then update transfer amounts
8. Checks the “Login/Logout” status of the Journal table every hour and sends result to attacker domain over HTTP
Or take down a nation

JSF family of aircraft

- Air-frame designs
- Engine designs
- Take off and landing specifications
- Communication systems
- Weapon systems
- ALL stolen
Windows of exposure need to shrink

Today's Reality is broken

Resolution: average breach resolution
Detection: 35 days

Attack: 206 days to detection

Tomorrow is machine vs. machine

Resolution: Go shorter
Detection: Go smarter
Learn: seconds
Go faster: minutes
And corporate information is sprawling everywhere

Information is everywhere

Security is nowhere!
Information is at the heart of your business, and at the heart of attacks.
Introducing OpenText Release 16, EP4

The secure digital platform for intelligent and connected enterprises
Security as the digital platform

Access and Organize

Application Security, Data Security

Sensitive information

Content Intelligence

100% secure work spaces

Create, share and collaborate

Sharing with confidence

OpenText Confidential. ©2018 All Rights Reserved.
1. Machines are now attacking humans

2. Humans cannot fight the machines

3. Machines are now fighting machines, with
   - Knowledge (Machine Learning)
   - Insight (AI)
   - Autonomic Action (Autonomous Clouds)
Machine vs. Machine: Over 1,000 Security Related Features in OpenText Release 16 EP4

- Application level security
- Database level security
- User and role base security
- Context, Rights and Time base
- SAML 2.0 and SSO
- AES-256 encryption at-rest & in-transit (SSL)
- Document fragmentation & Document-level security
- Standards: WORM, event-based, SEC 17a4, FIPS 140-2, DOD 5015.2, ITAR, FSTEC, and more
- Audit trails, usage patterns, monitoring and analysis – Content Intelligence
- And hundreds more
We have an endpoint responsibility !!!

- A day in the life of the modern workforce is “connected” and complex
- Working, sharing, social, WiFi jumping, always online
- If it has a signal or an address, it can be found and exploited
- **We have an endpoint responsibility:**
  - On and off our networks
  - From employees to trading partners
Endpoints are smart and critical

Examples of Critical Data on Endpoints

- Software controlled vehicles
- Tunnel plans and access points
- Fighter jet capability specifications
- Employee personal information

What EnCase Does

- Collects without disruption
- Monitors and alerts behaviours
- Uses advanced analytics to detect abnormal behaviours
- Find what is important through Machine Learning
- Automatically redact
- Feeds Magellan for detection, resolution and learning
OpenText protects over 50 Million endpoints today

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
<th>Endpoints</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.S. Army</td>
<td>Forensic &amp; malware analysis</td>
<td>800,000</td>
</tr>
<tr>
<td>Texas Children's Hospital</td>
<td>Detect &amp; respond to threats</td>
<td>25,000</td>
</tr>
<tr>
<td>CERT-UA</td>
<td>Endpoint visibility</td>
<td>50,000</td>
</tr>
<tr>
<td>Cleveland Clinic</td>
<td>WannaCry ransomware</td>
<td>120,000</td>
</tr>
<tr>
<td>Citi</td>
<td>Automated alarm response</td>
<td>300,000</td>
</tr>
</tbody>
</table>
OpenText IoT: machines and trusted eco-systems

- Connected Machines and Humans
- Ready to receive information from smart machines via standards
- Messaging and orchestration
- API accessible, persist information, rules driven
- Integrated Magellan
- Build your own Application
OpenText IoT customers

- Industrial
- Commerce
- Towns & Cities
- Homes
- Vehicles
- People

Knorr-Bremse
Alstom
Brunswick
University of Maine
BMW
Mitsubishi Motors
ICBC
OpenText Secure Supply Chain (GXS)

- **One Million Trading Partners**
- **Identity Manager**
  Are you who you say you are
- **Authorization Manager**
  What are you authorized to access
- **Identity Sync, Analysis & Intelligence**
  Analyze and audit information access
- **Identity Event Streaming Engine**
  Integrate all user and ID directories

Every person, device and application needs an identity

Suppliers → Covisint + GXS → Corporate apps

Customers → Covisint + GXS → Cloud apps

Employees → Covisint + GXS → Partner apps
BioTech Customer in Action: Bringing it all Together

End Points
‘connected patients’

- Site
- Lab
- 3rd Party Site
- 3rd Party Lab
- Wearables
- Emerging Technologies

Network
‘connected processes’

- Data Factory
- CTMS
- Safety
- ECG
- SME’s
- Monitors & Investigators
- 3rd Party Monitors & Investigators

- App Marketplace
- Data Model
- Integration
- Event Management
- Service Management

- Data Enrichment
- Alerts & Notifications
- Authorization Management
- Evidence Support
- Transaction Log

- Workflow
- Device Lifecycle Management
- Analytics

Enterprise
‘connected insights’

- Log
- Transaction Log
- Authorization Management
- Workflow
- Data Enrichment
- Alerts & Notifications
- Device Lifecycle Management
- Analytics
- App Marketplace
- Data Model
- Integration
- Event Management
- Service Management

OPENTEXT EIM SUITE

Regulatory
Device Manufacturers
3rd Party Data Providers

OpenText Confidential. ©2018 All Rights Reserved.
When things go wrong …

You need the tools to discover and recover
Discovery is a critical component of EIM

Machine discovery vs Humans

Needle in the haystack

Speed to resolution
OpenText Recommind: Security breach example!

- Preserved Data: 48,431,250 pages (800 GB)
- Collected & Processed: 12,915,000 pages (210 GB)
- Reviewed: 645,750 pages (10 GB)
- Produced: 141,450 pages (2.3 GB)

Data actually used in trial: 142 pages (2.4 MB)

- Collect completely, defensibly
- Cull data volumes
- Minimize human review
- Auto-redact privacy data

Find facts faster
Ransomware brought Atlanta to its knees

SamSam Ransomware
March 22, 2018

- City services have ground to a halt
- City cannot collect revenues and residents cannot pay
- Police databases and judicial systems are compromised
- Completely avoidable!

Population: 472,522
Serious Fraud Office (SFO) Selects OpenText

UK SFO is using OpenText™ Axcelerate as its next-generation investigations platform to:

- Expedite investigations
- Save caseworkers time
- Automated document analysis

“AI technology will help us work smarter, faster and be more effective in prosecuting economic crime.”

— Ben Denison, Chief Technology Officer at the SFO
Meltdown, Spectre, Wannacry. What to do with security nightmares like this?
Outsource to The OpenText Cloud

- 2,000 live customers (Global Examples: Nestle, Citi, Michelin, GM, Toyota)
- OpenText is responsible for security
- 99.99% Uptime
- Never upgrade again
- Based on standards: NIST, ISO, SOC, GDPR
- One contract, on SLA
- 1 Exabyte Under Management
A new narrative:

Data is for the Good
OpenText Artificial Intelligence

Information + Algorithms = Insights

- Magellan = Actuate + Apache Spark + Nstein
- Run standalone or Pre-integrated to OpenText EIM
- Pre-packaged algorithms (via MLIB)
- Write your own algorithms (via R and other languages)
- Pre-certified x86 hardware configurations
- Built on Open Standards
4 Key Ingredients for AI

- Digital Maturity
- Data Ecosystems
- Tools, Techniques
- Use cases, sources of value
Emerging value areas, hundreds of use cases

Financial Services
- Regulatory Filing
- Know Your Customer
- Follow the Money
- Fraud Prevention

Customer Experience
- Product recommendations
- Segmentation

Asset Industries
- Predictive maintenance
- Resource scheduling

Human Resources
- Hiring
- Retention
- Potential
- Case Management

Security
- Behavior
- Logs & events
- Data movement
Using Data for the Good

<table>
<thead>
<tr>
<th>Protecting Marine Life</th>
<th>Reducing Incarceration</th>
<th>Right resources, right location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ocean Conservancy</td>
<td>Calgary Police Service</td>
<td>DRC Danish Refugee Council</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Transparency</th>
<th>Safety</th>
<th>Eliminating Pandemics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Westpac</td>
<td>KNORR-BREMSE</td>
<td>AmerisourceBergen</td>
</tr>
</tbody>
</table>
In Summary

Intelligent and connected enterprises

Security is job #1

Data is for the Good
Thank you