Industrial Cybersecurity in a Cloud and Mobile First World

Presented by: Saadi Kermani

Life Is On

A little history

- Security was not a priority at the time of introduction for Industrial Control Systems (ICS)

- Originally optimized to help automate simplistic production tasks to produce product and increase yield

- Everything was bounded (fixed) and was physically connected

However, things changed

- The PC revolution hit
- Windows became a standard IT stack used in ICS systems
- The internet happened
- Wireless devices and wireless communication became the norm

However, things changed

- Ethernet connected devices became the norm
- Virtualization became a de-facto standard (leading to software defined resources a.k.a. “SDx”)
- Mobile devices including in the broader sense Laptops, USB sticks, mobile phones and most recently, wearable devices became the norm

However, things changed

- Cloud services are everywhere, easy to leverage and consume

- IoT is the next big thing – an evolving story

Suddenly …

Assumptions that were held about accessing and potentially controlling ICS systems became outdated

- Isolated physically bounded systems became a set of interoperable boundless virtual systems (software defined, logically contained)

Suddenly …

- Security, CyberSecurity and Cyber-Physical security concepts was thrust into the spotlight and became a top (US national) priority following the 2010 Stuxnet attack

- Proprietary systems and protocols became blurred. (Common protocols based on TCIP/IP, or Ethernet connected, Common IT infrastructure based on Windows/COTS – the IT/OT convergence)

Initial cybersecurity defensive posture

- As ICS Systems became (permanently) connected (intentionally or not) we added firewalls to reinforce control

- Between air gapped networks and firewalls, both of these approaches were based on the assumption that if nothing got in – we were “safe” (from the inside too right?)

- It also helped by coincidence that the ICS world – at first – was distinctly different from most other IT solutions at the time both in terms of protocols and systems and technology.

▶ FIVE MYTHS OF INDUSTRIAL CONTROL SYSTEMS SECURITY

Despite growing awareness of cyber-based attacks on industrial control systems, many IT security models continue to adhere to the outdated belief that physically isolating systems and 'security by obscurity' is enough. It's not. Here's why.

KASPERSKY lab

Life Is On | Schneider Electric

Kaspersky Labs Data Sheet – 5 myths

1. **Myth -** Industrial control systems are not connected to the outside world.

2. **Myth -** We are safe because we have a firewall.
3. **Myth -** Hackers don't understand SCADA.
4. **Myth -** We are not a target.
5. **Myth -** Our safety systems will protect us.

Kaspersky Labs Data Sheet – 5 myths

1. **Fact:** Most industrial control systems have eleven connections to the Internet.

2. **Fact:** Most firewalls allow "any" service on inbound rules.
3. **Fact:** More and more hackers are specifically investigating this area.
4. **Fact:** Stuxnet proved ICS are targets. <u>note:</u> Stuxnet defeated “air gap”
5. **Fact:** Safety and control likely using same O/S with the same vulnerabilities.

Best Practices

- Network Segregation
    - Demilitarized Zone (DMZ), Bastion Host, Proxy Host

- Electronic Access Point Access Controls (port hardening, ingress/egress)

- User Access Controls (Role Based Access Control - RBAC via MS AD and even extend to Azure AD or similar IAM)
    - With complex passwords policy
    - Multi-factor Authentication
    - Least Privilege

Best Practices

- Malicious Software Prevention | Anti-Virus
- Device Control/ Inventory
- Patching Server, Back ups
- Logging Server (SIEM - Security information and event management)
- System Hardening (least required)

Best Practices

- Intrusion Prevention/ Detection (IPS/IDS)
  - Deep Packet Inspections
  - Implement "Next Generation Firewalls" (NGFW)
- Anti-malware
- Performance Monitoring and Alerting
  - Switch Performance, HD Performance
- Centralized Cyber Management
  - Management Server

Best Practices

- Well documented system/network architecture
- Patching Server / Patching Plan
- Backups / Tested and Documented Recovery Plan
- Standardized Systems
- Knowledge of System Baseline
- Malicious Software Prevention - Anti-Virus / Whitelisting
- Device Control / Inventory
- System Hardening (least required)
- Cyber Security Training and Awareness Program

Where to get guidance – Old Friends

- DHS and NIST ICS
- NERC/ CIP
- ISA/IEC 62443
- ISO 27001/2

ISA™

IEC

U.S. DEPARTMENT OF HOMELAND SECURITY

Information Security Management System ISO 27001 Certified

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Where to get guidance – New Friends

CSA cloud security alliance SM

FedRAMP

AICPA Service Organization Control Reports
AICPA
SERVICE ORGANIZATIONS
SOC
aicpa.org/soc
Formerly SAS 70 Reports ®

HIPAA

PCI

Where to get guidance – General Tools

- Shared Assessments

  Complete organizational risk assessment

  https://sharedassessments.org/

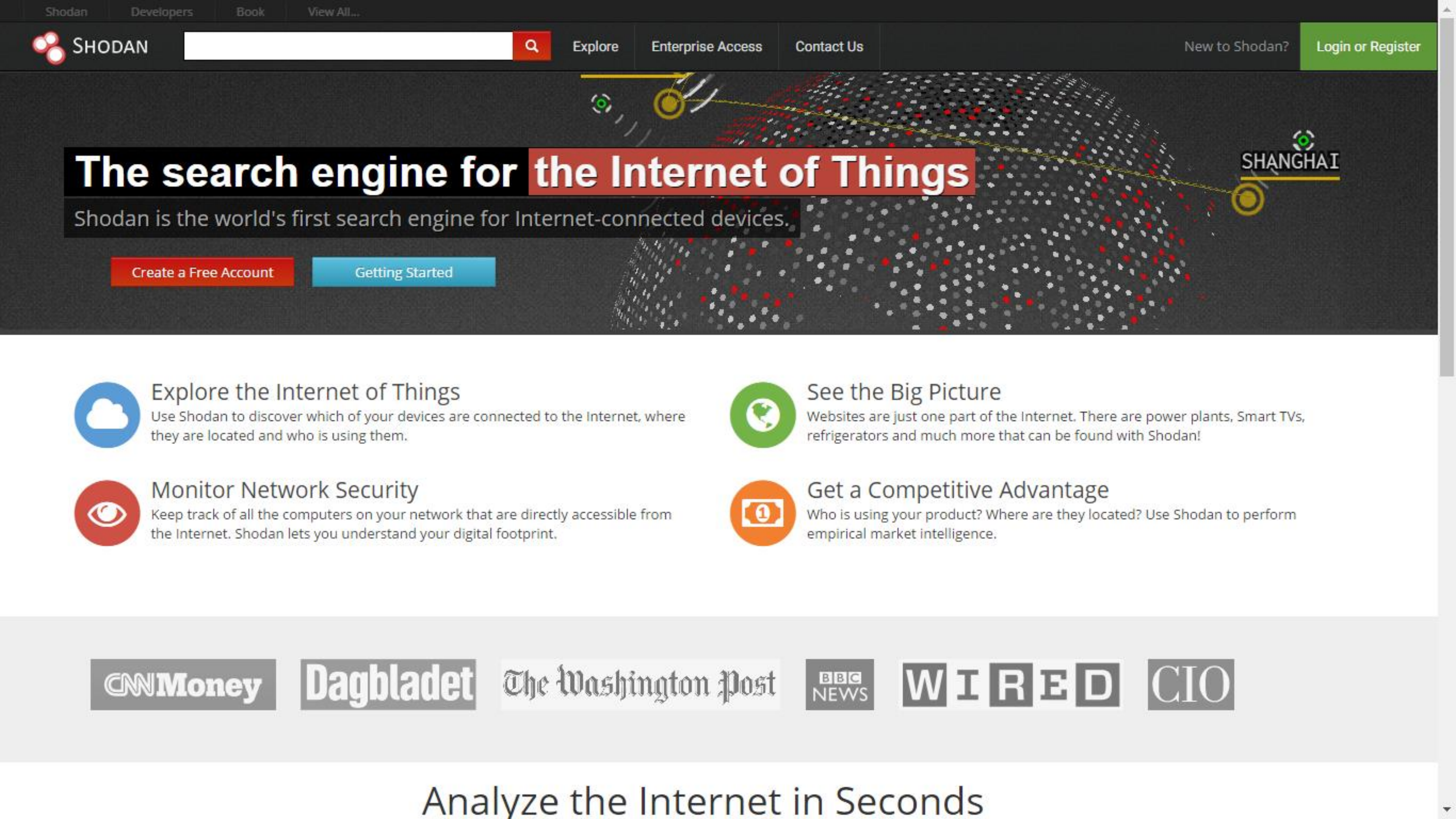
- Open Security Architecture

  SP-023: Industrial Control Systems

  http://www.opensecurityarchitecture.org

Where to get guidance – Google for ICS

- Shodan “IoT” public search engine
- RISI database of public ICS attacks



The search engine for the Internet of Things

Shodan is the world's first search engine for Internet-connected devices.

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

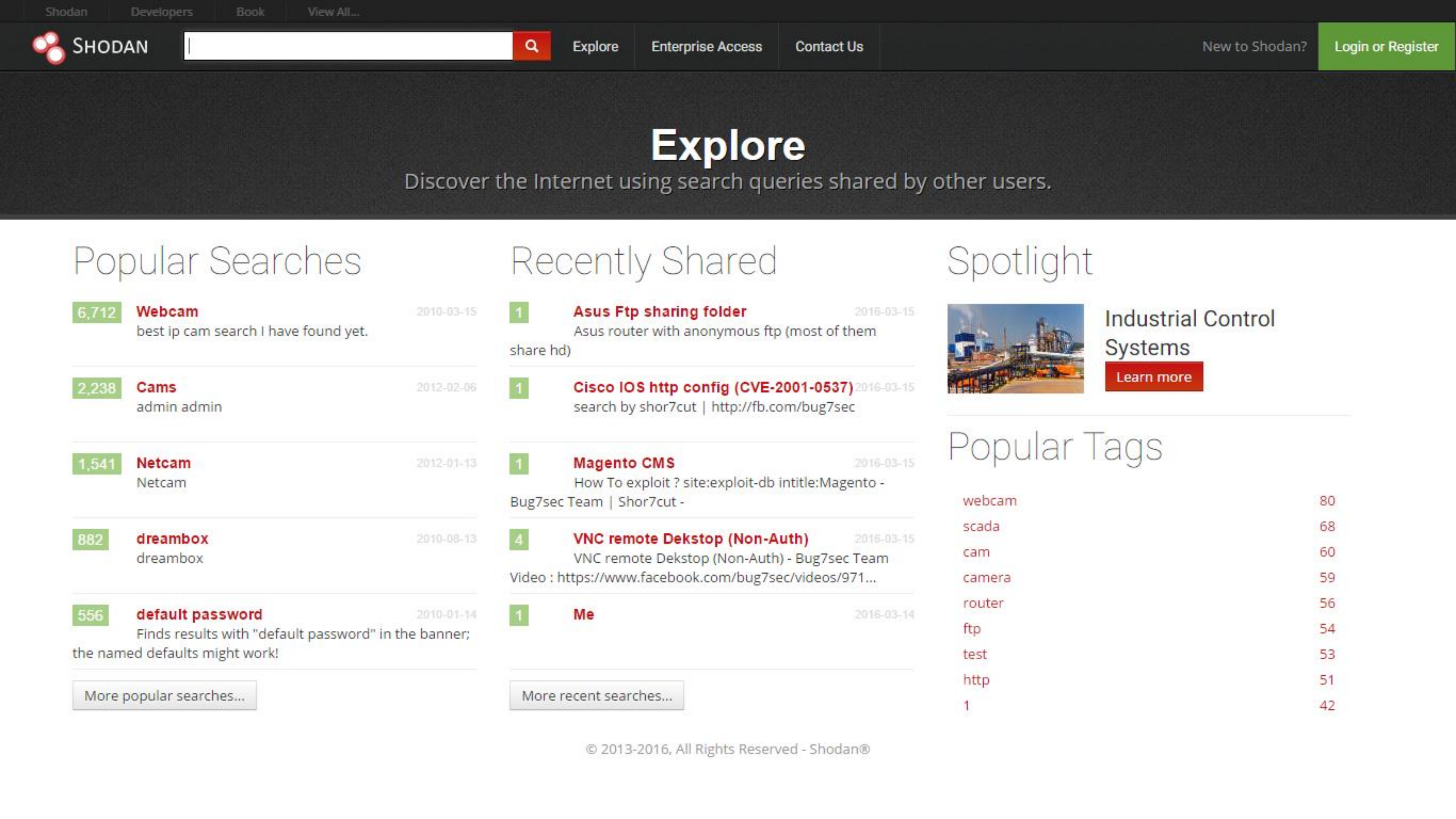
Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

Analyze the Internet in Seconds



Explore

Discover the Internet using search queries shared by other users.

Popular Searches

6,712 **Webcam** 2010-03-15
best ip cam search I have found yet.

2,238 **Cams** 2012-02-06
admin admin

1,541 **Netcam** 2012-01-13
Netcam

882 **dreambox** 2010-08-13
dreambox

556 **default password** 2010-01-14
Finds results with "default password" in the banner; the named defaults might work!

Recently Shared

1 **Asus Ftp sharing folder** 2016-03-15
Asus router with anonymous ftp (most of them share hd)

1 **Cisco IOS http config (CVE-2001-0537)** 2016-03-15
search by shor7cut | http://fb.com/bug7sec

1 **Magento CMS** 2016-03-15
How To exploit ? site:exploit-db intitle:Magento - Bug7sec Team | Shor7cut -

4 **VNC remote Dekstop (Non-Auth)** 2016-03-15
VNC remote Dekstop (Non-Auth) - Bug7sec Team Video : https://www.facebook.com/bug7sec/videos/971...

1 **Me** 2016-03-14

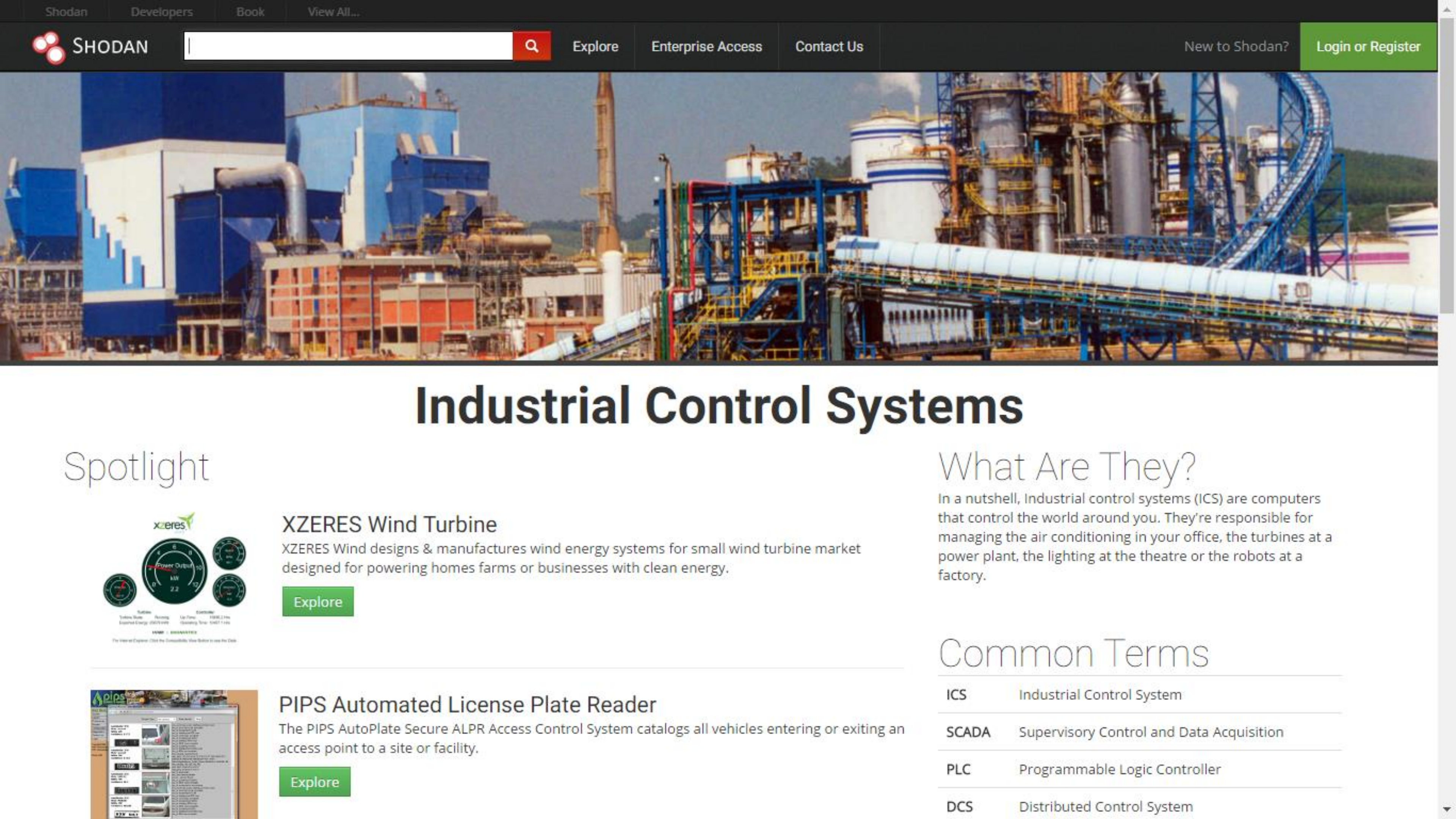
Spotlight

Industrial Control Systems

Popular Tags

webcam	80
scada	68
cam	60
camera	59
router	56
ftp	54
test	53
http	51
1	42

© 2013-2016, All Rights Reserved - Shodan®



Industrial Control Systems

Spotlight

XZERES Wind Turbine

XZERES Wind designs & manufactures wind energy systems for small wind turbine market designed for powering homes farms or businesses with clean energy.

PIPS Automated License Plate Reader

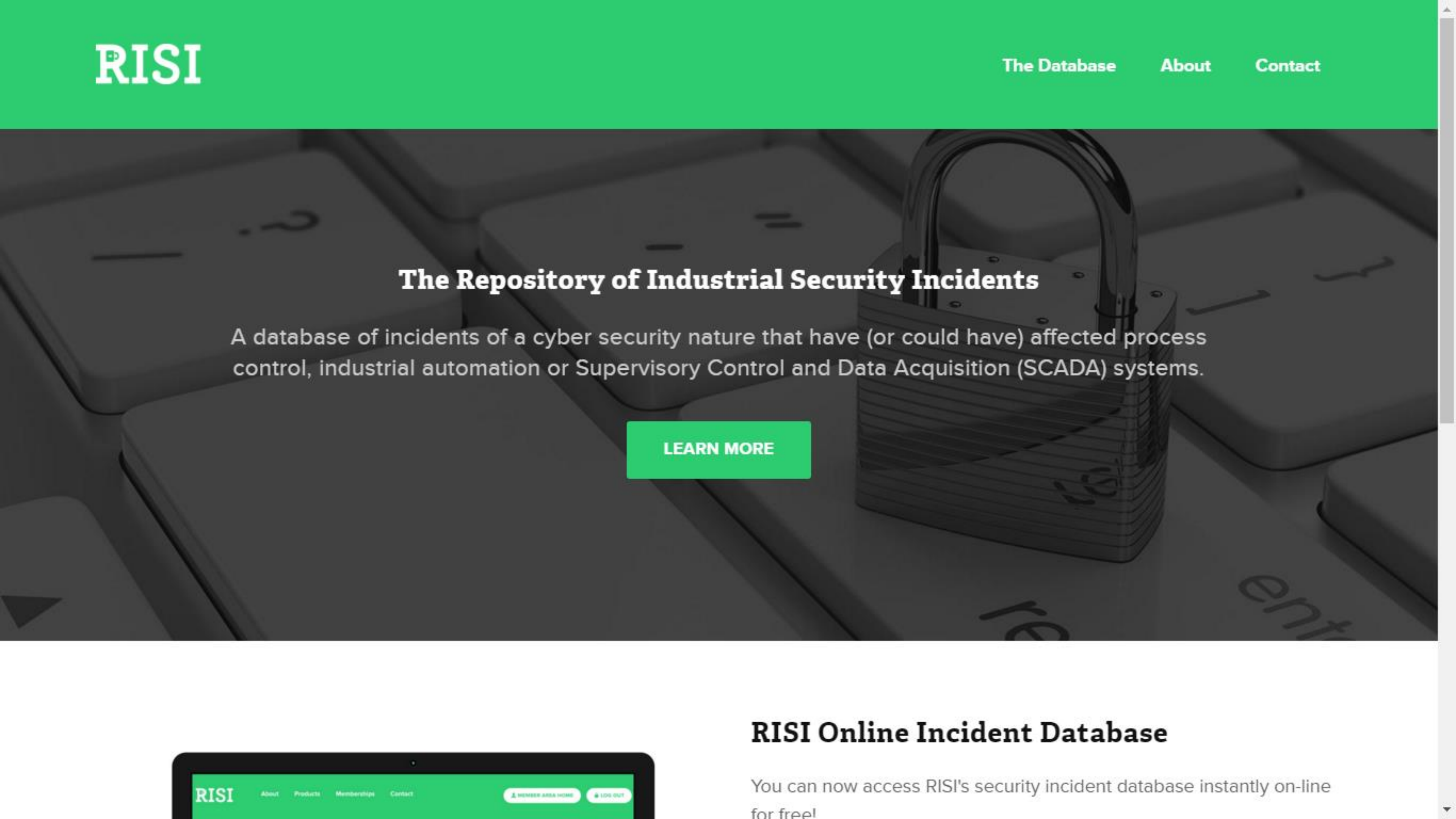
The PIPS AutoPlate Secure ALPR Access Control System catalogs all vehicles entering or exiting an access point to a site or facility.

What Are They?

In a nutshell, Industrial control systems (ICS) are computers that control the world around you. They're responsible for managing the air conditioning in your office, the turbines at a power plant, the lighting at the theatre or the robots at a factory.

Common Terms

ICS	Industrial Control System
SCADA	Supervisory Control and Data Acquisition
PLC	Programmable Logic Controller
DCS	Distributed Control System

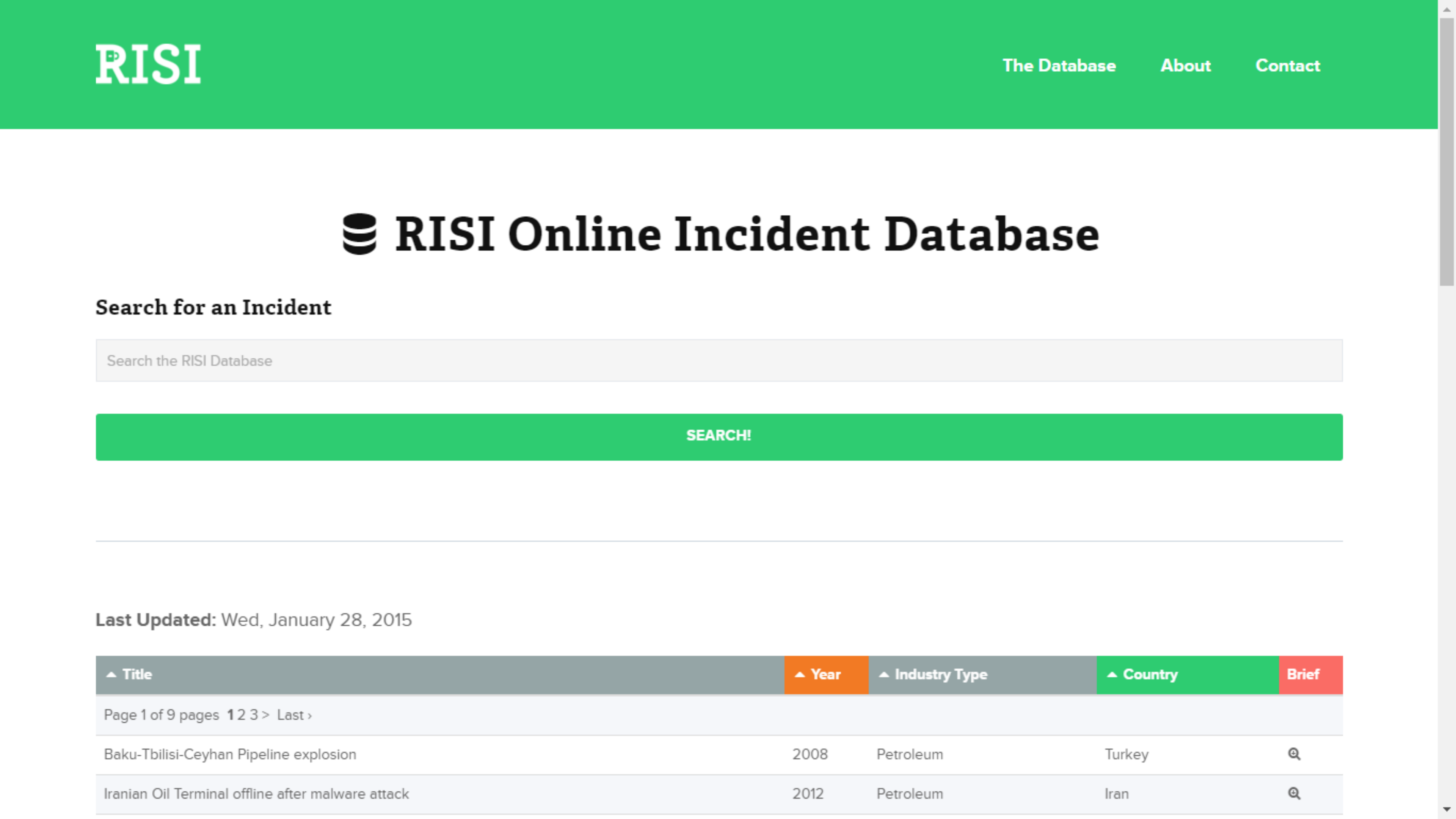


The Repository of Industrial Security Incidents

A database of incidents of a cyber security nature that have (or could have) affected process control, industrial automation or Supervisory Control and Data Acquisition (SCADA) systems.

RISI Online Incident Database

You can now access RISI's security incident database instantly on-line for free!



RISI

The Database About Contact

RISI Online Incident Database

Search for an Incident

Search the RISI Database

SEARCH!

Last Updated: Wed, January 28, 2015

▲ Title	▲ Year	▲ Industry Type	▲ Country	Brief
Page 1 of 9 pages **1** 2 3 > Last ›				
Baku-Tbilisi-Ceyhan Pipeline explosion	2008	Petroleum	Turkey	🔍
Iranian Oil Terminal offline after malware attack	2012	Petroleum	Iran	🔍

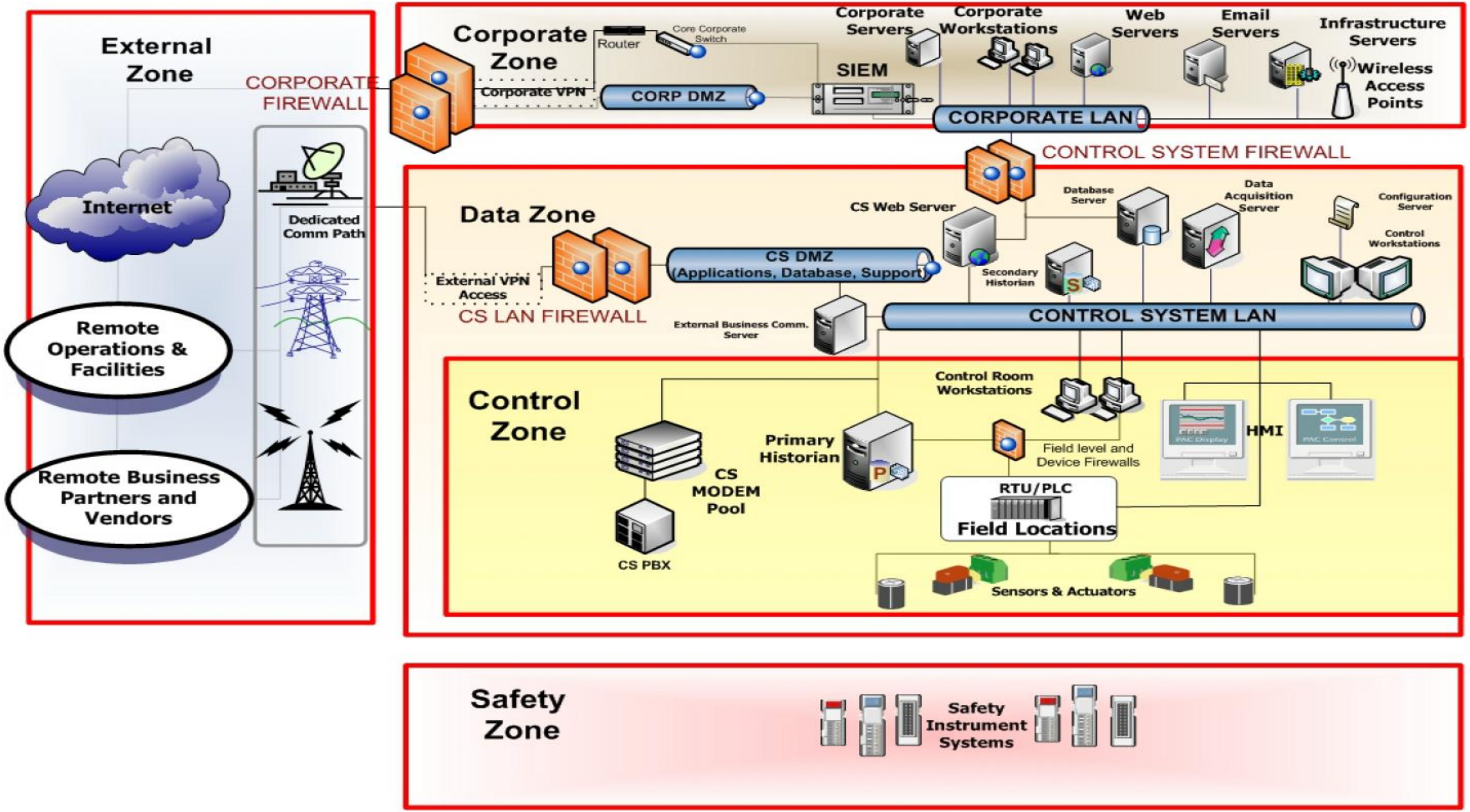
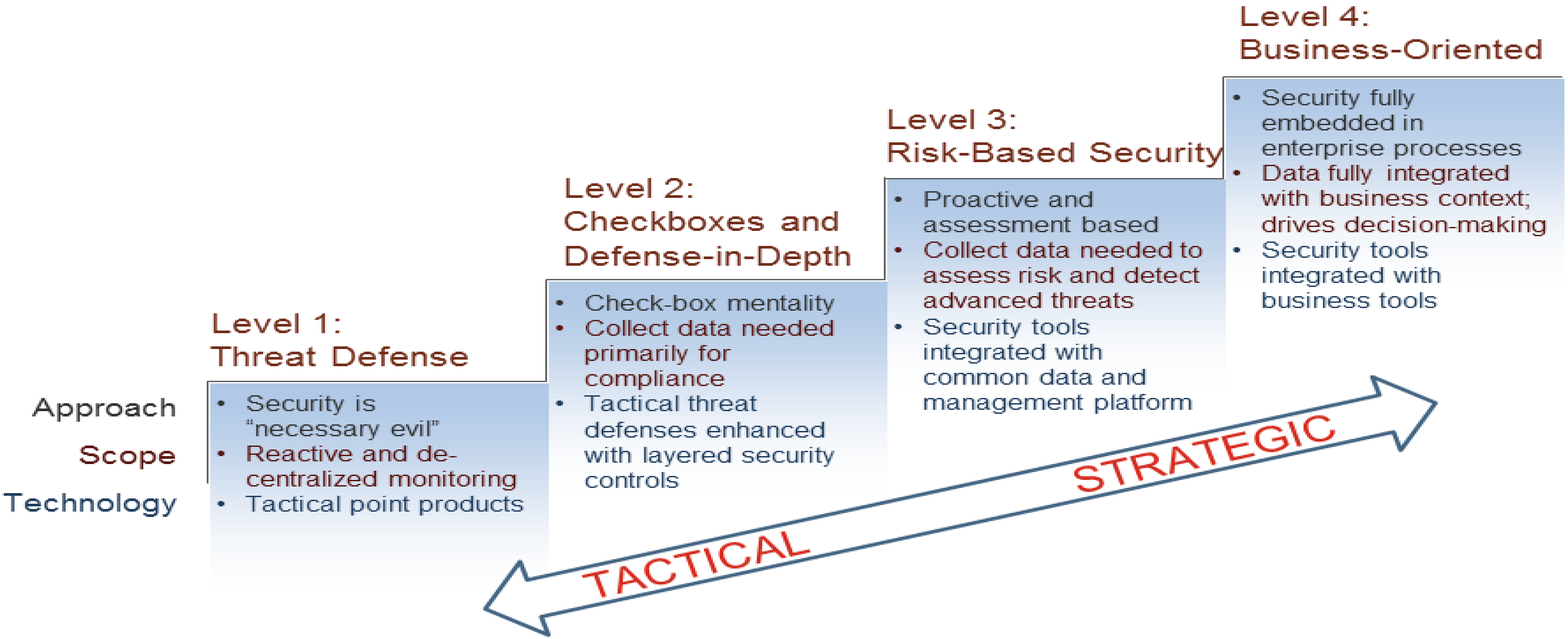


Figure 10. Complete defense-in-depth strategy with the intrusion detection system and SIEM.

Technology Risk Management Maturity Model



Approach

Scope

Technology

Level 1: Threat Defense

- Security is "necessary evil"
- Reactive and de-centralized monitoring
- Tactical point products

Level 2: Checkboxes and Defense-in-Depth

- Check-box mentality
- Collect data needed primarily for compliance
- Tactical threat defenses enhanced with layered security controls

Level 3: Risk-Based Security

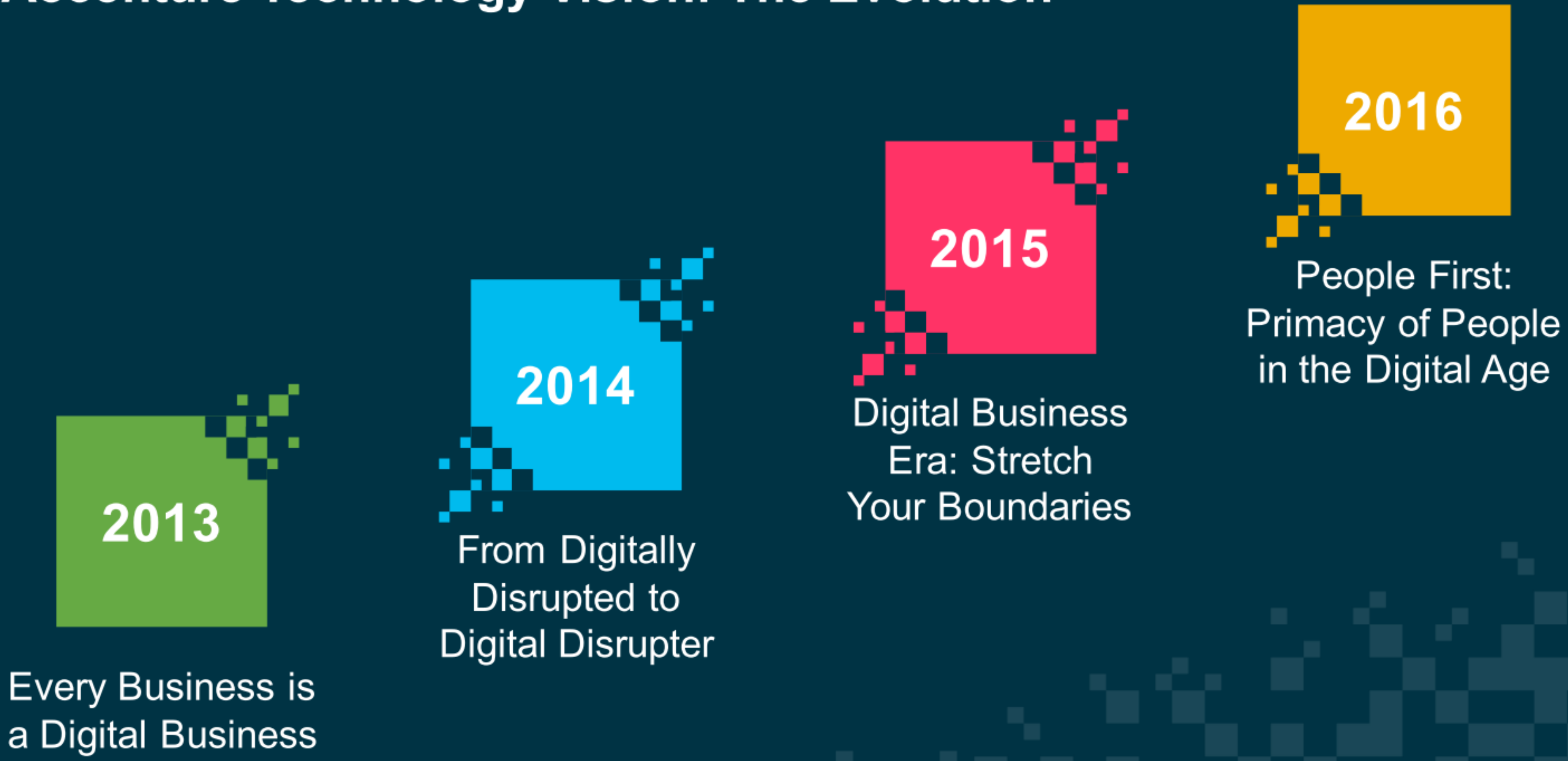
- Proactive and assessment based
- Collect data needed to assess risk and detect advanced threats
- Security tools integrated with common data and management platform

Level 4: Business-Oriented

- Security fully embedded in enterprise processes
- Data fully integrated with business context; drives decision-making
- Security tools integrated with business tools

Credit: Alexander Open Systems (AOS)

Accenture Technology Vision: The Evolution



2013

Every Business is a Digital Business

2014

From Digitally Disrupted to Digital Disrupter

2015

Digital Business Era: Stretch Your Boundaries

2016

People First: Primacy of People in the Digital Age

People First: The Primacy of People in the Digital Age

The Accenture Technology Vision 2016 identifies five technology trends fueled by the *people first* principle and that are essential to business success in the digital economy.

Intelligent Automation

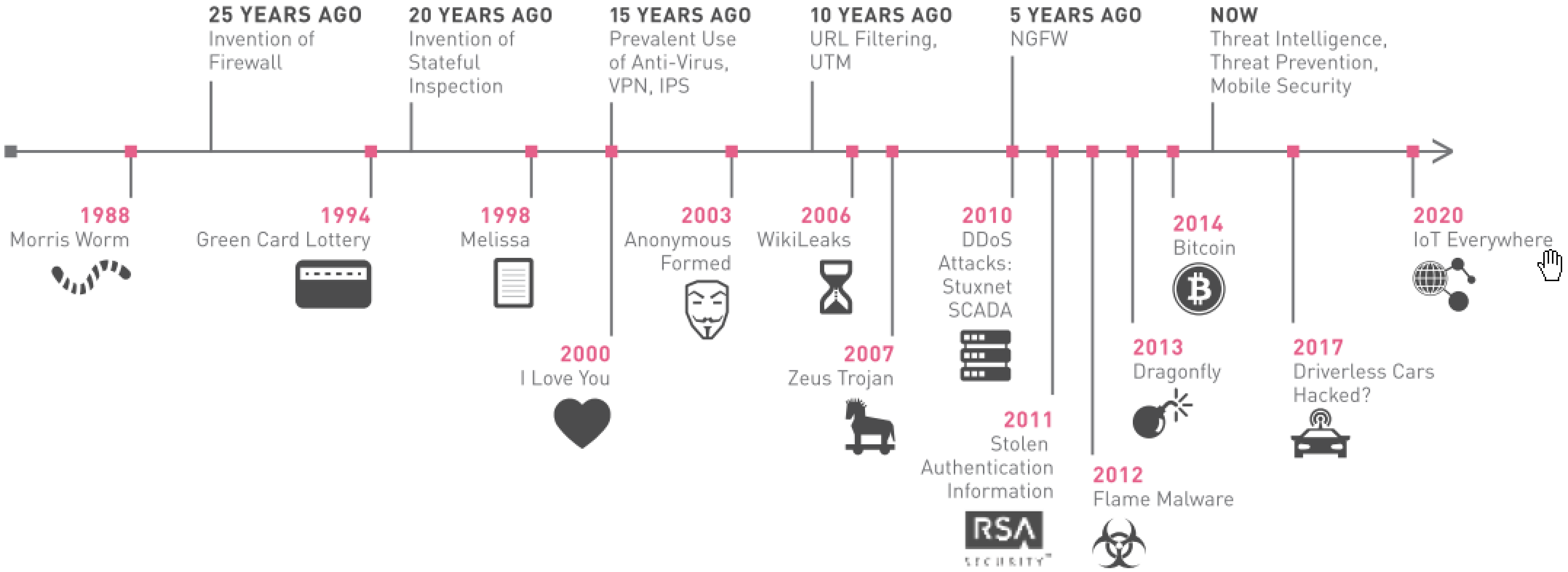
Liquid Workforce

Platform Economy

Predictable Disruption

Digital Trust

THE EVOLUTION OF MALWARE



25 YEARS AGO
Invention of Firewall

20 YEARS AGO
Invention of Stateful Inspection

15 YEARS AGO
Prevalent Use of Anti-Virus, VPN, IPS

10 YEARS AGO
URL Filtering, UTM

5 YEARS AGO
NGFW

NOW
Threat Intelligence, Threat Prevention, Mobile Security

1988
Morris Worm

1994
Green Card Lottery

1998
Melissa

2000
I Love You

2003
Anonymous Formed

2006
WikiLeaks

2007
Zeus Trojan

2010
DDoS Attacks: Stuxnet SCADA

2011
Stolen Authentication Information

2012
Flame Malware

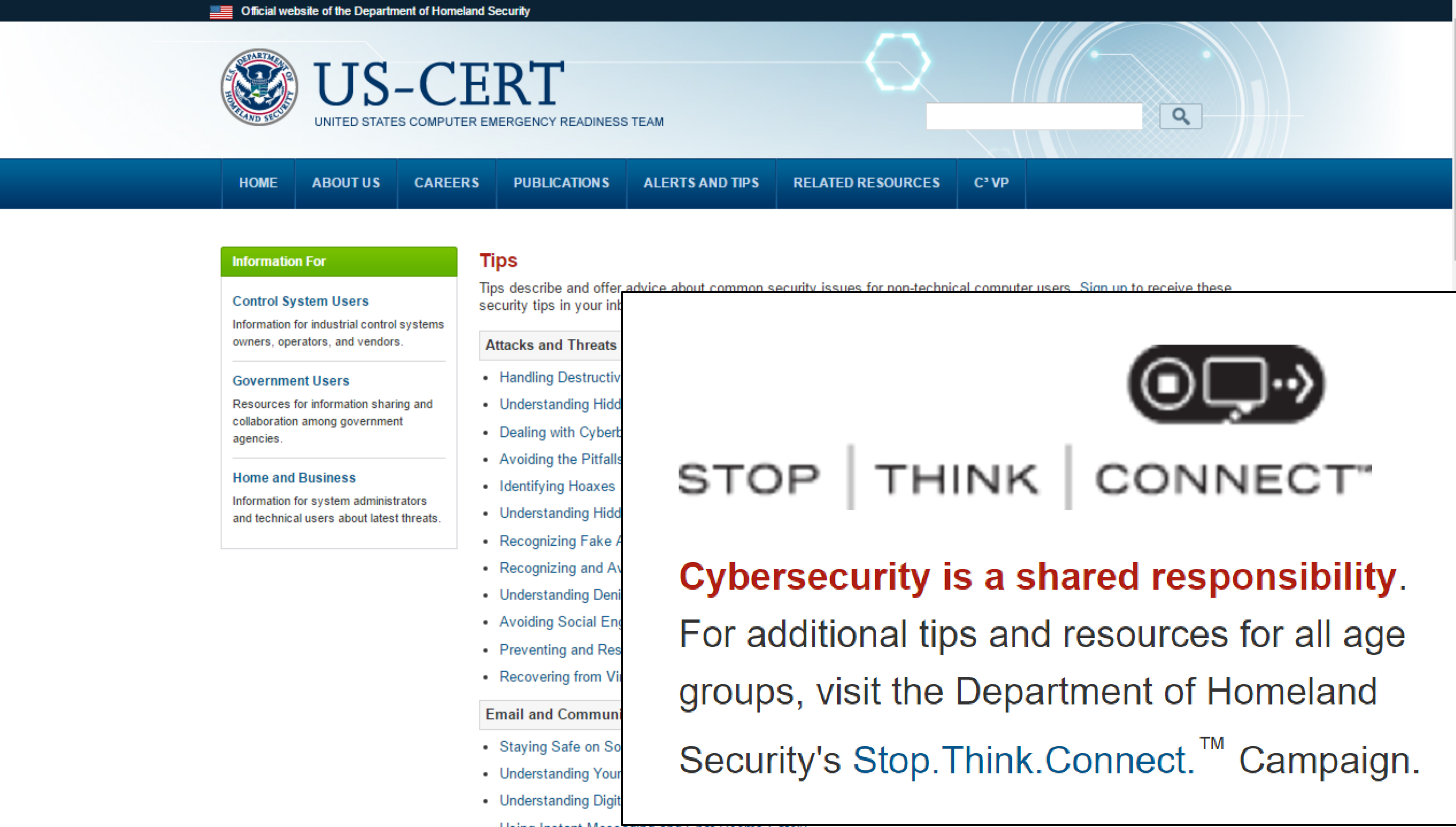
2013
Dragonfly

2014
Bitcoin

2017
Driverless Cars Hacked?

2020
IoT Everywhere

Source: Check Point Software Technologies – Security Report 2015



Official website of the Department of Homeland Security

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Information For

Control System Users
Information for industrial control systems owners, operators, and vendors.

Government Users
Resources for information sharing and collaboration among government agencies.

Home and Business
Information for system administrators and technical users about latest threats.

Tips

Tips describe and offer advice about common security issues for non-technical computer users. Sign up to receive these security tips in your inb

Attacks and Threats

- Handling Destructiv
- Understanding Hidd
- Dealing with Cyberb
- Avoiding the Pitfalls
- Identifying Hoaxes
- Understanding Hidd
- Recognizing Fake A
- Recognizing and Av
- Understanding Deni
- Avoiding Social Eng
- Preventing and Res
- Recovering from Vi

Email and Communi

- Staying Safe on So
- Understanding Your
- Understanding Digit

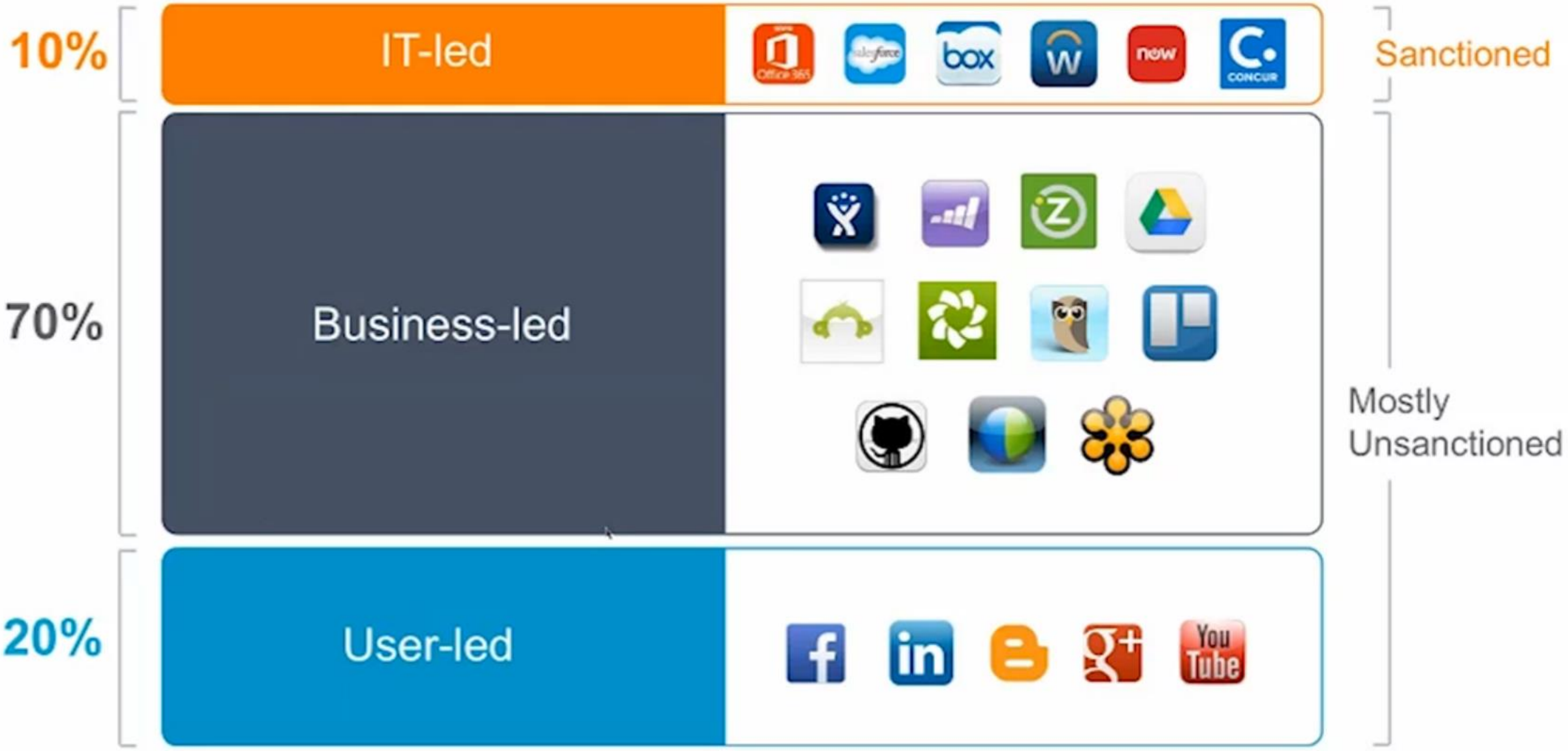
STOP | THINK | CONNECT™

Cybersecurity is a shared responsibility. For additional tips and resources for all age groups, visit the Department of Homeland Security's Stop.Think.Connect.™ Campaign.

There are 22,000 enterprise apps today (and growing).

netskope

755 cloud apps per enterprise - how do they get in?

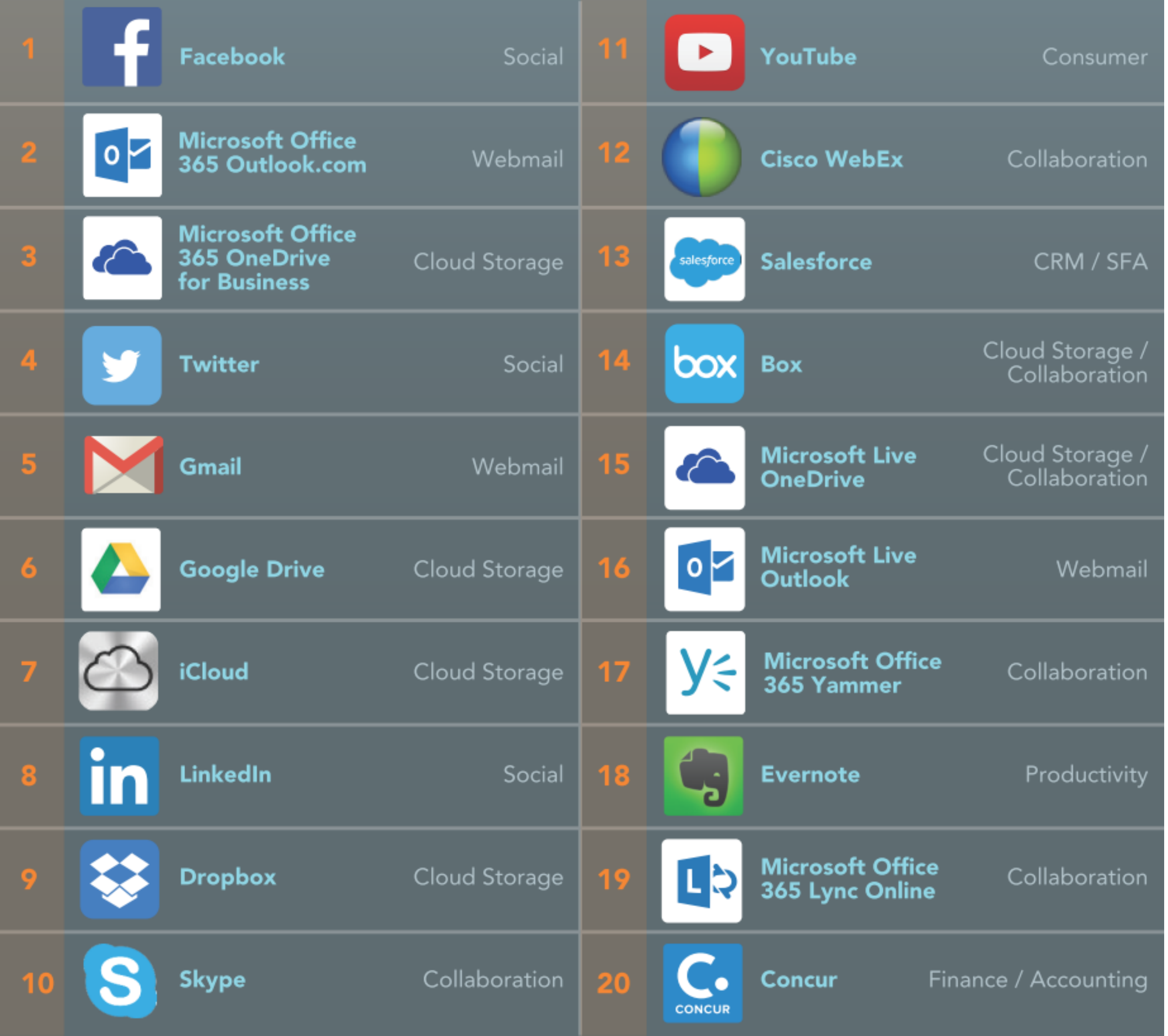


10% IT-led — Sanctioned

70% Business-led — Mostly Unsanctioned

20% User-led

Top used cloud apps in enterprise networks



1	Facebook	Social
2	Microsoft Office 365 Outlook.com	Webmail
3	Microsoft Office 365 OneDrive for Business	Cloud Storage
4	Twitter	Social
5	Gmail	Webmail
6	Google Drive	Cloud Storage
7	iCloud	Cloud Storage
8	LinkedIn	Social
9	Dropbox	Cloud Storage
10	Skype	Collaboration
11	YouTube	Consumer
12	Cisco WebEx	Collaboration
13	Salesforce	CRM / SFA
14	Box	Cloud Storage / Collaboration
15	Microsoft Live OneDrive	Cloud Storage / Collaboration
16	Microsoft Live Outlook	Webmail
17	Microsoft Office 365 Yammer	Collaboration
18	Evernote	Productivity
19	Microsoft Office 365 Lync Online	Collaboration
20	Concur	Finance / Accounting

Source: netskope

Key cyber-concepts relevant today

- **Layered architecture techniques**
  - Cover all the reasonable bases
- **Defense in Depth – a holistic view**
  - Not just a technology problem
  - Need to include people (culture) and process (continuous habits)
- **Mobile Device Management (MDM)**

Cybersecurity Organizational Commitment

- CyberSecurity Officer (CSO)
- First in our space to achieve SDLA certification (x3)
- Dedicated Industrial Control Systems Cybersecurity Incident Response Team (CSIRT)
- Professional Services group for ICS Consulting
- Appointed CyberSecurity Advisors to support R&D Cybersecurity practices

Secure Development Practices Commitment

- Adherence to the Microsoft Security Development LifeCycle (SDL)
- Penetration Testing, OWASP Scoring, Fuzz testing, Application Threat Modeling, Surface Attack Vector analysis
- Internal audits by Cybersecurity auditors
- Adoption of Agile, DevOps practices with capacity for rapid release

Third-party validation Commitment

- Periodic engagement with third-party professional services company’s for external cybersecurity audits with specialization in Industrial Control Systems (ICS) and Critical Infrastructure and Key Resource (CIKR) security.

- Gold Certified Microsoft ISV Partner with regular architectural review and design sessions surrounding cybersecurity principles for managed solutions.

Industry Standards Commitment

- RESTful, secured APIs over TCP/IP
- XML data structures where applicable
- oData interface for secure data retrieval
- OpenID Connect , oAuth 2.0 Authentication end points
- SSL/TLS encryption for all channels on the well known Port 443
- Native support for modern browsers based on HTML5
- Native mobile O/S for our mobile apps
- Transparent Data Privacy, Data Ownership and Data Protection policies
- Support for Hybrid deployment models (ex: on-premises to cloud)

Industry Best Practices Commitment

- Encryption for Data in Motion (SSL/TLS)
- Encryption for Data at Rest
- Defense in Depth architectural layers based on least privilege
- Support for federated Active Directory (Azure Active Directory)
- Embedded Privacy Controls
- Secured APIs
- Status Dashboard for critical and transparent incident reporting (https://status.wonderware.com)
- Planned support for:
  - 2-Factor Authentication (2FA)/ Multi-factor Authentication (MFA)
    - something you know ; something you have; something you are
  - Audit Logs

Industry Best in Class Commitment

- Enterprise partner with Microsoft as our Cloud Service Provider (CSP) based on the Microsoft Azure platform.
- Microsoft Azure has 24 data centers deployed globally with 20+ compliance certifications availability across their cloud services and data centers (including HIPPA, PCI, ISO/IEC 27018:2014)
- Cloud Security Alliance (CSA) STAR Registrant
- Capacity to respond to Data Residency laws in geo-political zones
  - United States | Canada
  - Australia
  - European Union
  - India | China

Compliance audits and certifications for Azure

GLOBAL

- ISO/IEC 27001
- SOC 1
- SOC 2
- PCI DSS L1 version 3
- Cloud Security Alliance Cloud Security Matrix
- ISO / IEC 27018

UNITED STATES

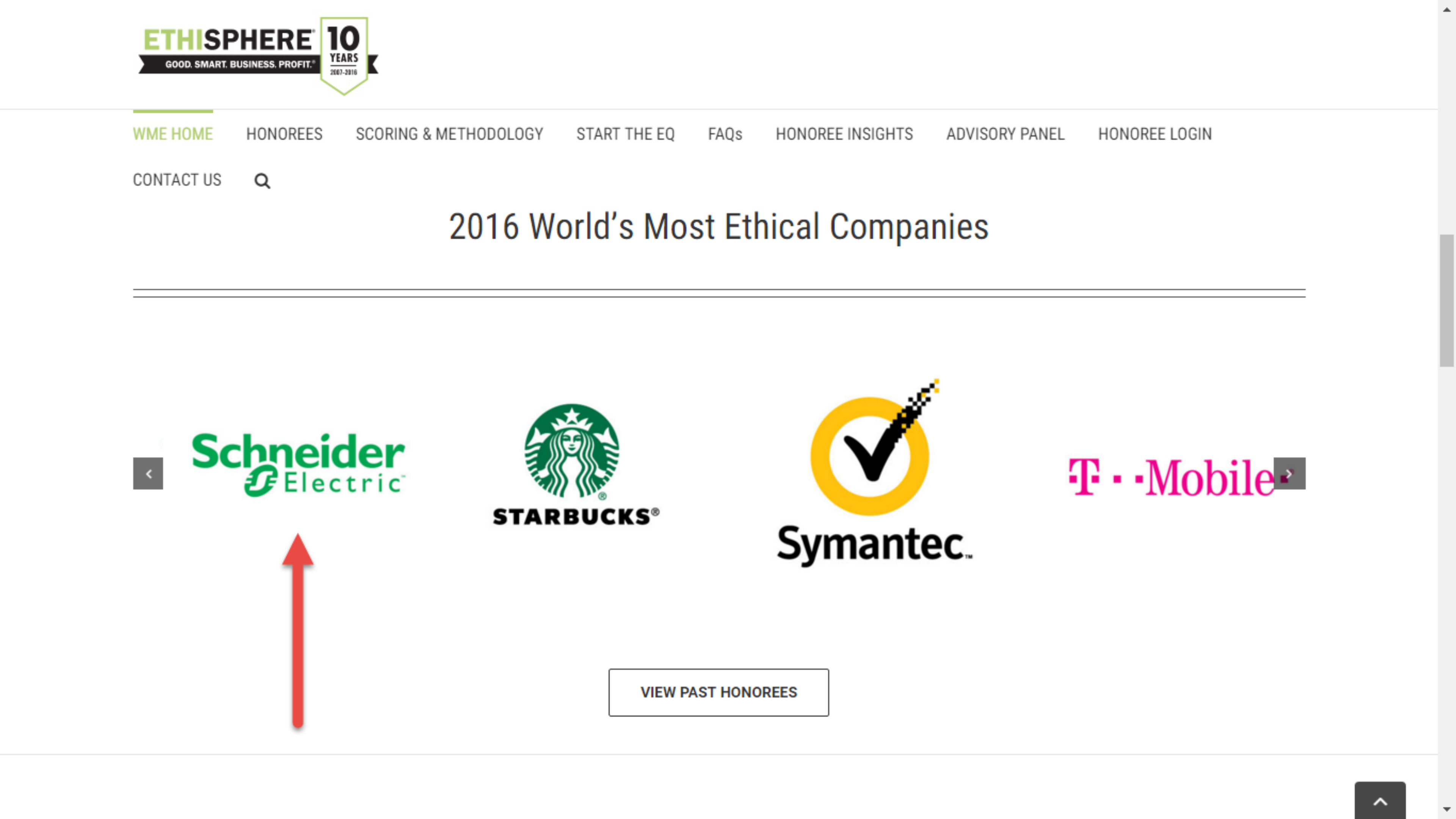
- FedRAMP
- HIPAA (Healthcare)
- FIPS 140-2
- Life Sciences GxP
- Family Educational Rights & Privacy Act

REGIONAL

- European Union Model Clause
- United Kingdom G-Cloud
- China Multi Layer Protection Scheme
- China CCCPPF
- Singapore Multi-Tier Cloud Security
- Australian Signals Directorate I-RAP Assessment

COMING SOON

- Sarbanes Oxley
- Criminal Justice Information System
- Defense Information Systems Agency L2
- ITAR
- Defense Information Systems Agency L3-5



2016 World's Most Ethical Companies

Domain Expertise Commitment

- Schneider Electric and its associated power brands including Wonderware, Foxboro and Avantis bring over 175 years of Industrial Automation experience.
- Schneider Electric and the Wonderware software portfolio offer customers the industry’s most advanced industrial software platform with available modules covering most industries
- NERC/CIP requirements experience for Power and Energy verticals
- NIST aligned architecture
- ISA/IEC 62443 voting board member

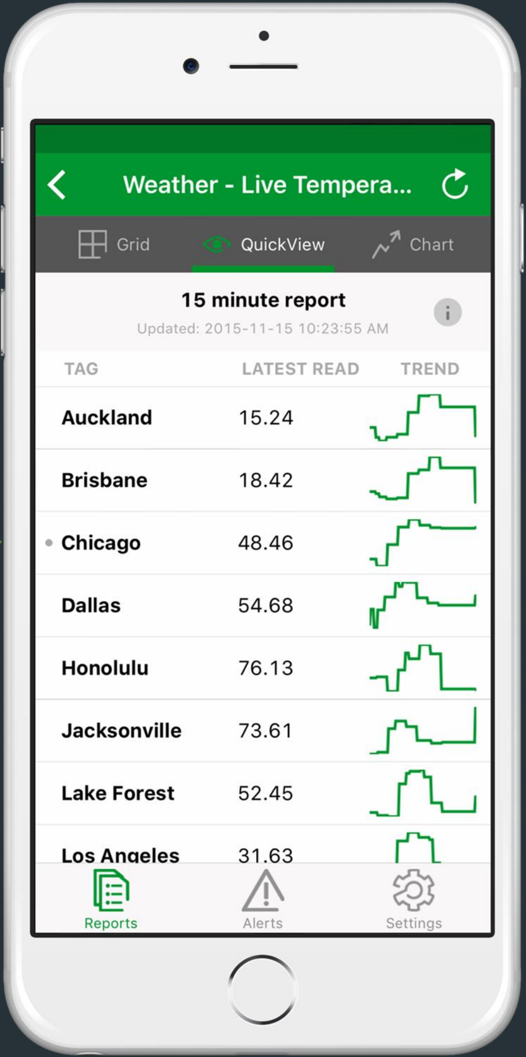
Wonderware SmartGlance

Monitor asset and production metrics from any source on any mobile device

What is it?

- A mobile app to trend, analyze and consume Industrial data provided as a hosted, managed service.

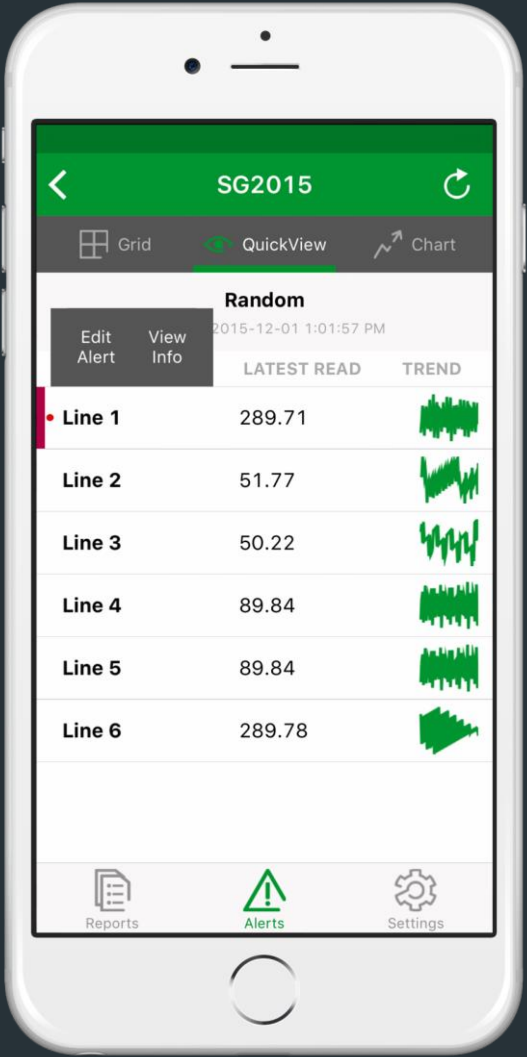
- Remote Access to KPIs, anytime, anywhere, on any device quick summary view



15 minute report

Updated: 2015-11-15 10:23:55 AM

TAG	LATEST READ	TREND
Auckland	15.24	
Brisbane	18.42	
Chicago	48.46	
Dallas	54.68	
Honolulu	76.13	
Jacksonville	73.61	
Lake Forest	52.45	
Los Angeles	31.63	

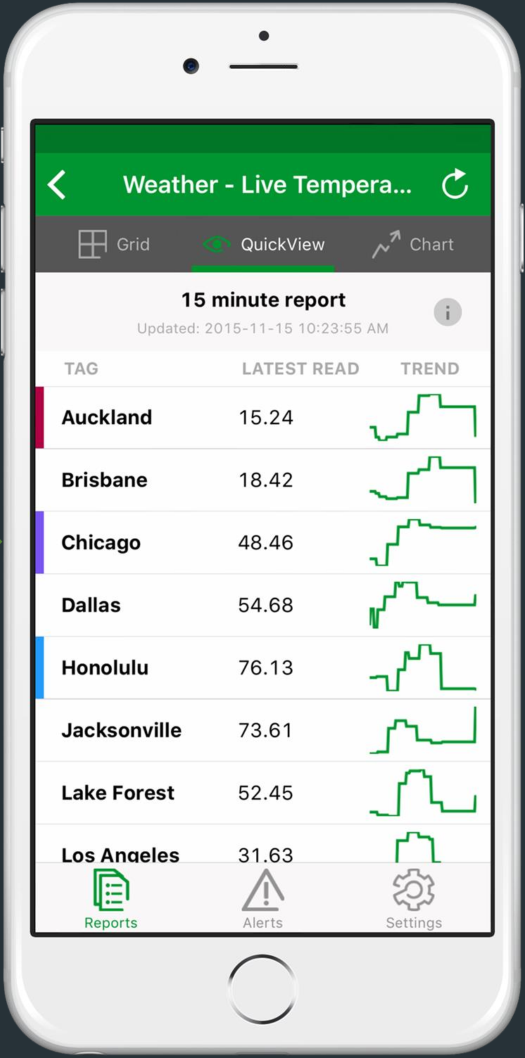


Random

2015-12-01 1:01:57 PM

TAG	LATEST READ	TREND
Line 1	289.71	
Line 2	51.77	
Line 3	50.22	
Line 4	89.84	
Line 5	89.84	
Line 6	289.78	

long-press on any tag to set an alert, view more info plot up to six (6) tags

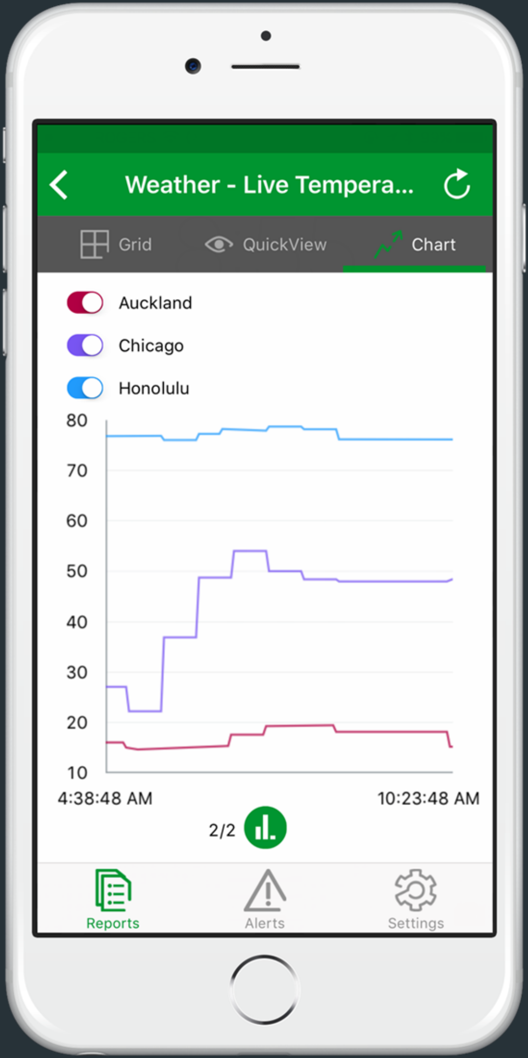


Weather - Live Tempera...

15 minute report

Updated: 2015-11-15 10:23:55 AM

TAG	LATEST READ	TREND
Auckland	15.24	
Brisbane	18.42	
Chicago	48.46	
Dallas	54.68	
Honolulu	76.13	
Jacksonville	73.61	
Lake Forest	52.45	
Los Angeles	31.63	



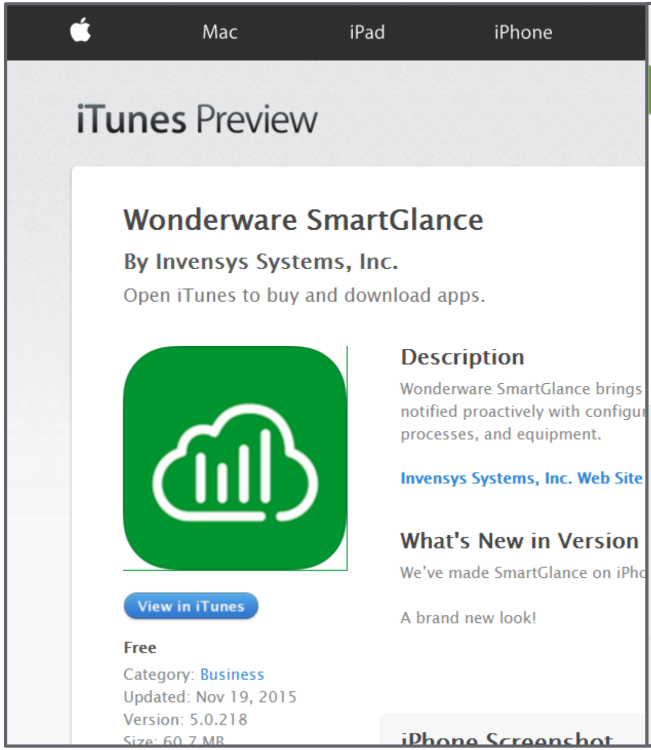
Weather - Live Tempera...

- Auckland
- Chicago
- Honolulu

toggle tags on/off

Life Is On | Schneider Electric

Download Wonderware SmartGlance today!



iTunes Preview

Wonderware SmartGlance

By Invensys Systems, Inc.

Open iTunes to buy and download apps.

Description

Wonderware SmartGlance brings
notified proactively with configu
processes, and equipment.

Invensys Systems, Inc. Web Site

What's New in Version

We've made SmartGlance on iPho

A brand new look!

Free

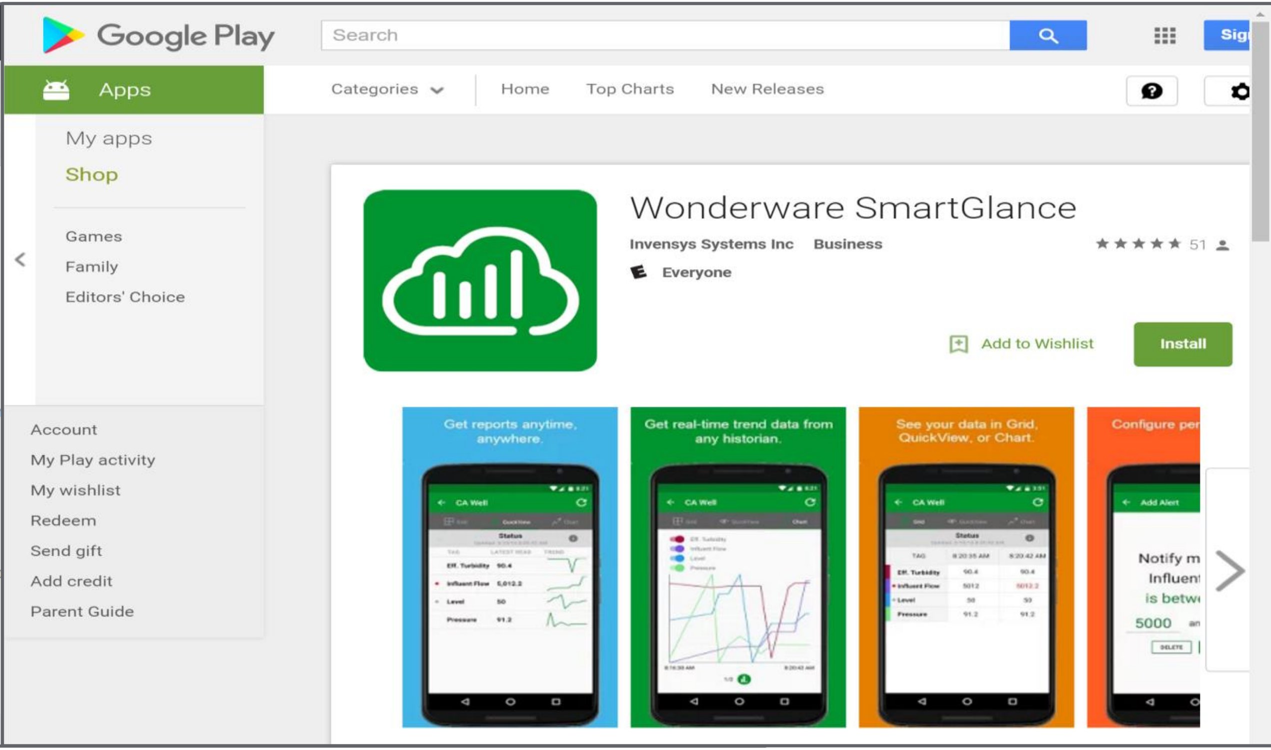
Category: Business

Updated: Nov 19, 2015

Version: 5.0.218

Size: 60.7 MB

iPhone Screenshot



Wonderware SmartGlance

Invensys Systems Inc Business ★★★★★ 51

Everyone

Wonderware Online

Time-series based storage, trend & analysis informational client as a service

Life Is On | Schneider Electric

What is it?

Wonderware Online

High-performance process historian as a service

https://online.wonderware.com

- The Wonderware Historian provided as a hosted, managed service.
- A set of new desktop and mobile clients to easily visualize, interact with and be alerted on plant KPIs, equipment and process data.

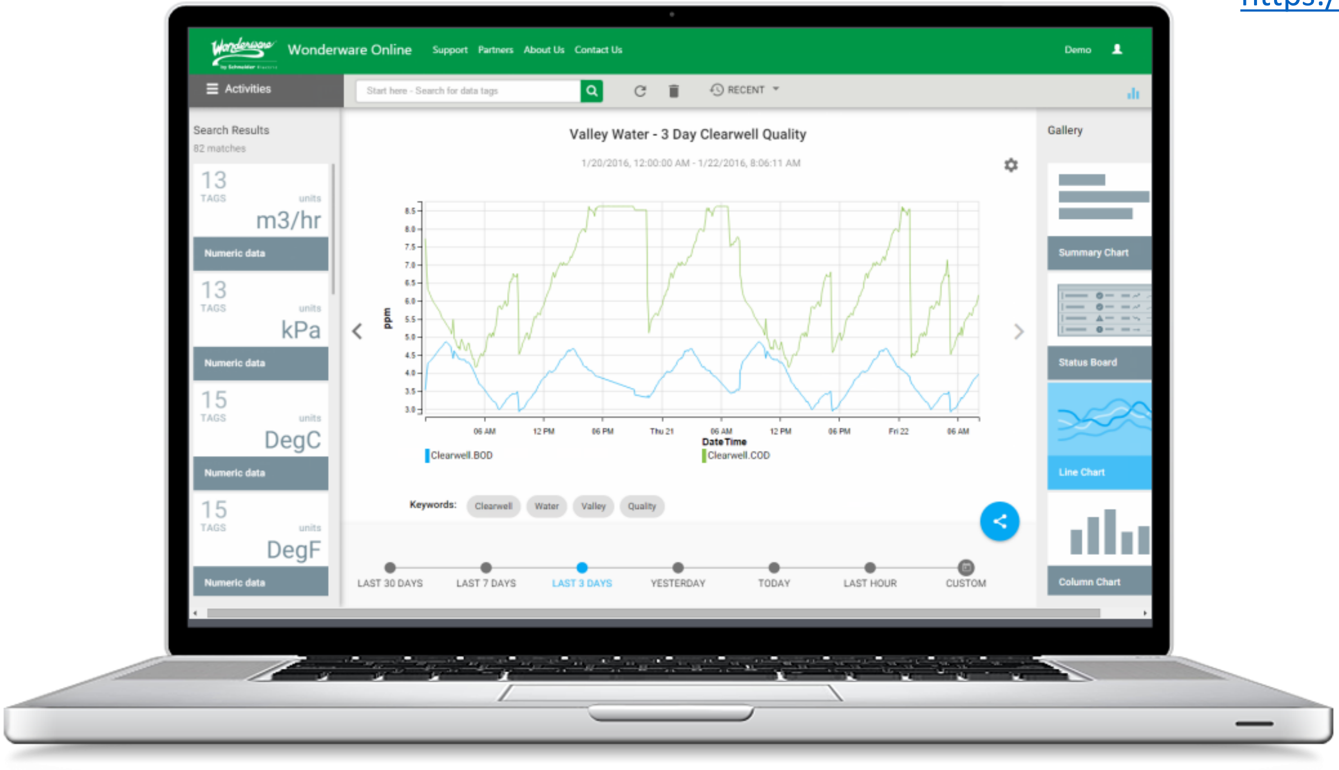
Wonderware by Schneider Electric

Browser Client

Wonderware Online

High-performance process historian as a service

https://online.wonderware.com



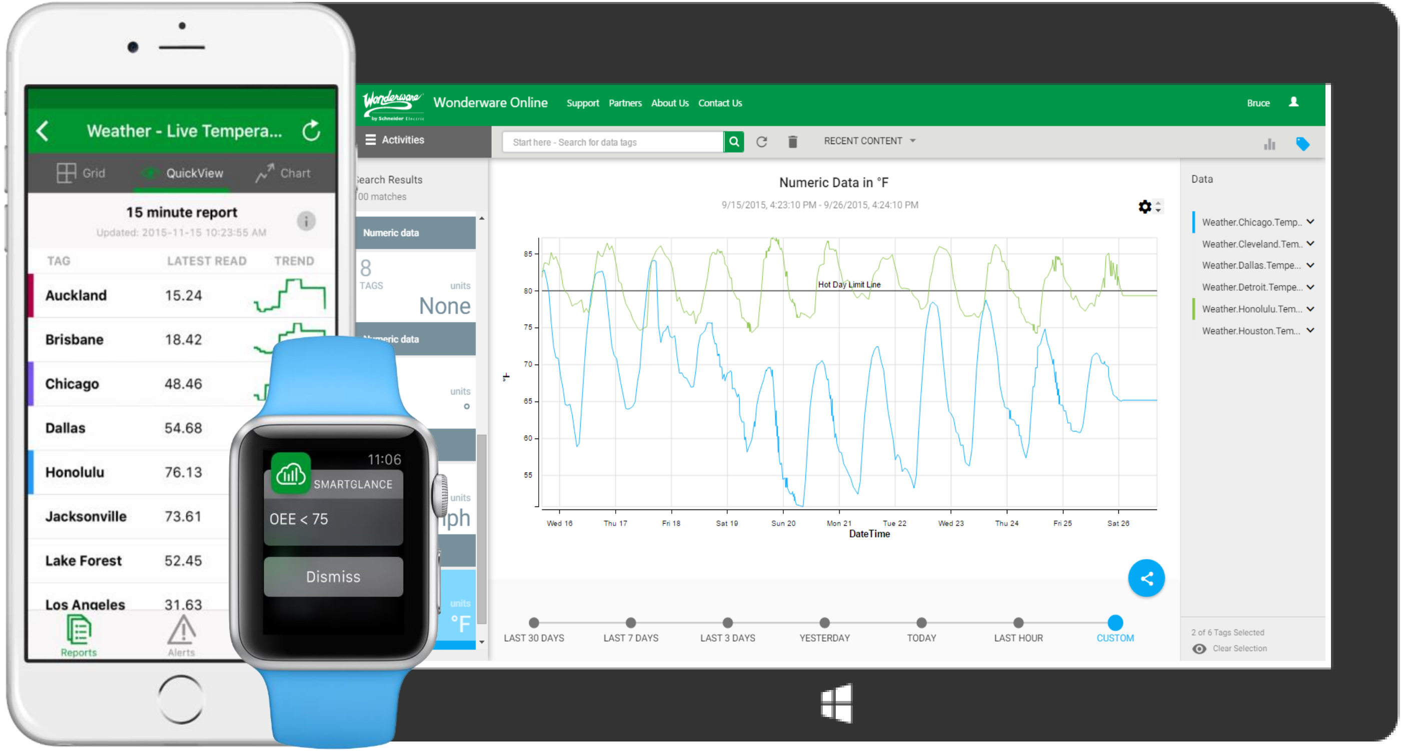
Life Is On | Schneider Electric

Mobile & Wearable Clients

Wonderware Online

High-performance process historian as a service

https://online.wonderware.com



Weather - Live Tempera...

15 minute report

Updated: 2015-11-15 10:23:55 AM

TAG	LATEST READ	TREND
Auckland	15.24	
Brisbane	18.42	
Chicago	48.46	
Dallas	54.68	
Honolulu	76.13	
Jacksonville	73.61	
Lake Forest	52.45	
Los Angeles	31.63	

Numeric Data in °F

9/15/2015, 4:23:10 PM - 9/26/2015, 4:24:10 PM

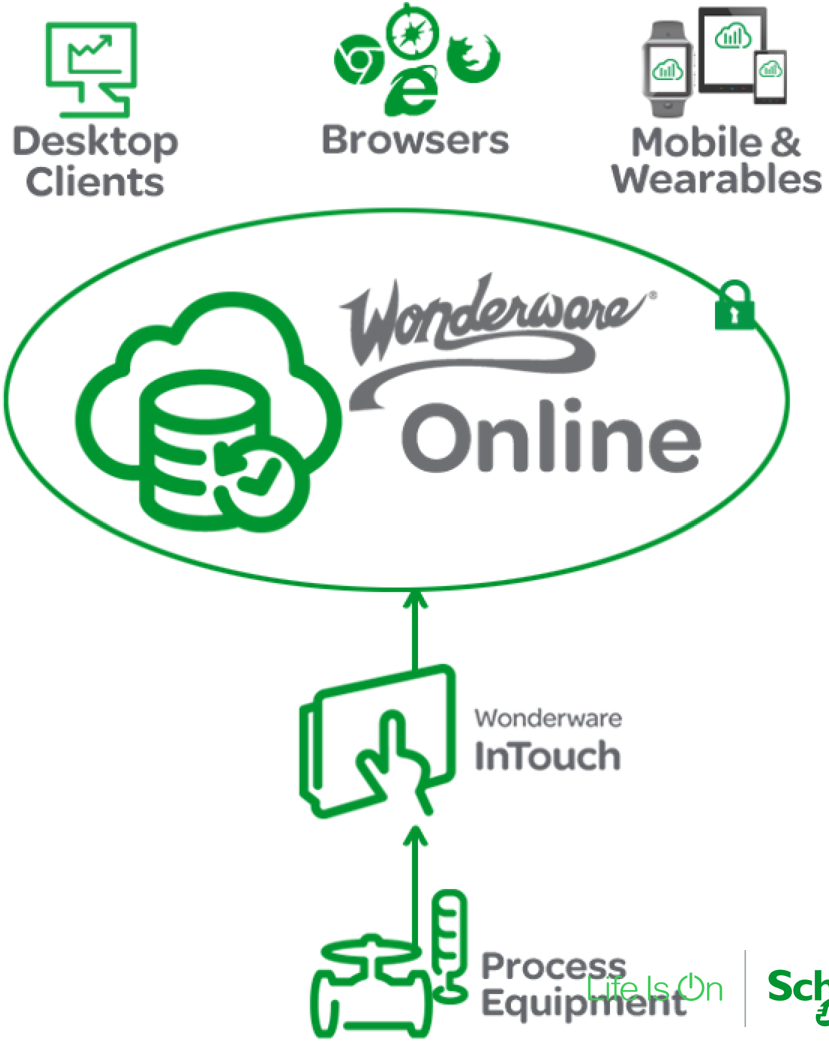
Life Is On

Schneider Electric

Wonderware Online

equipment to historian.

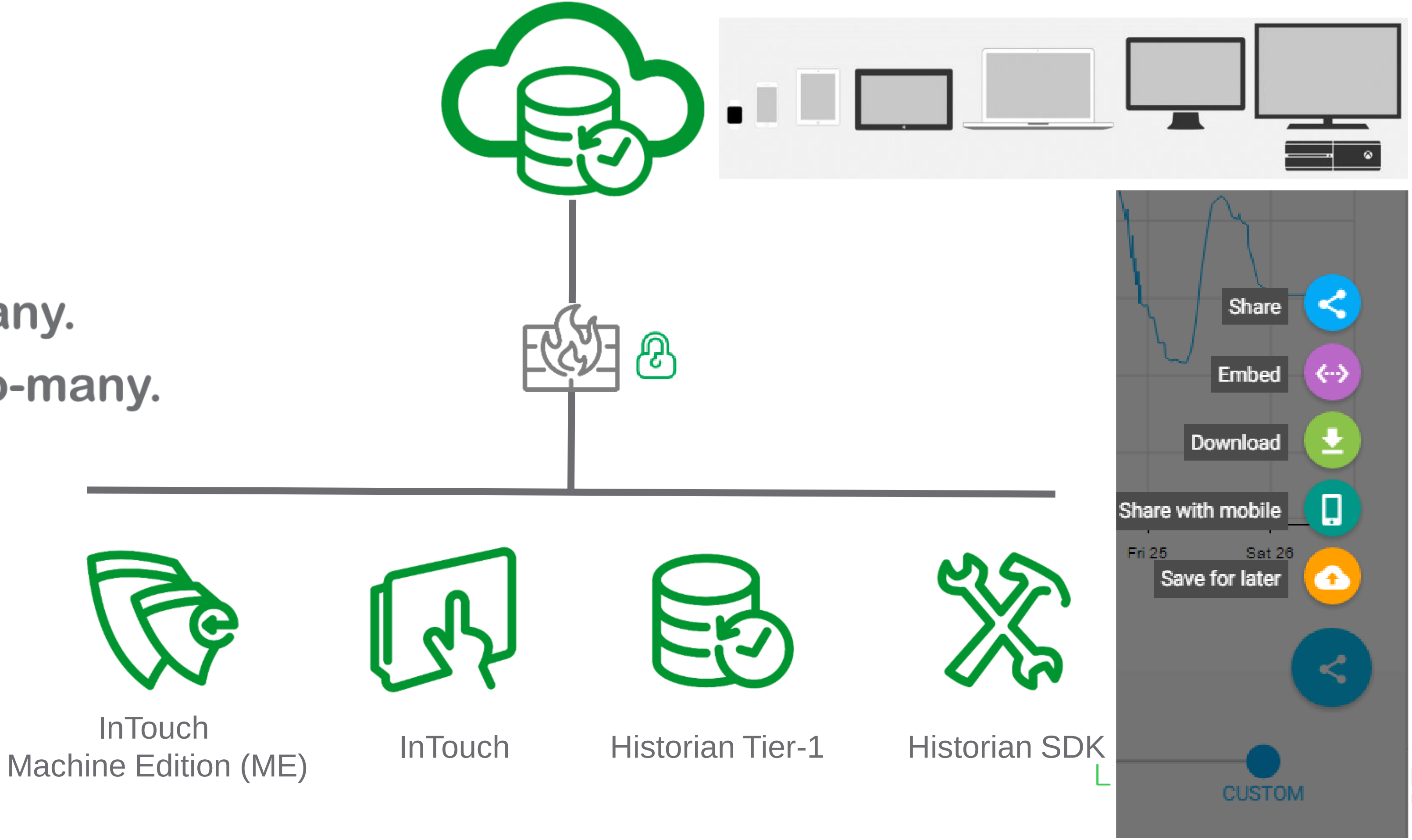
connect, collect, view.

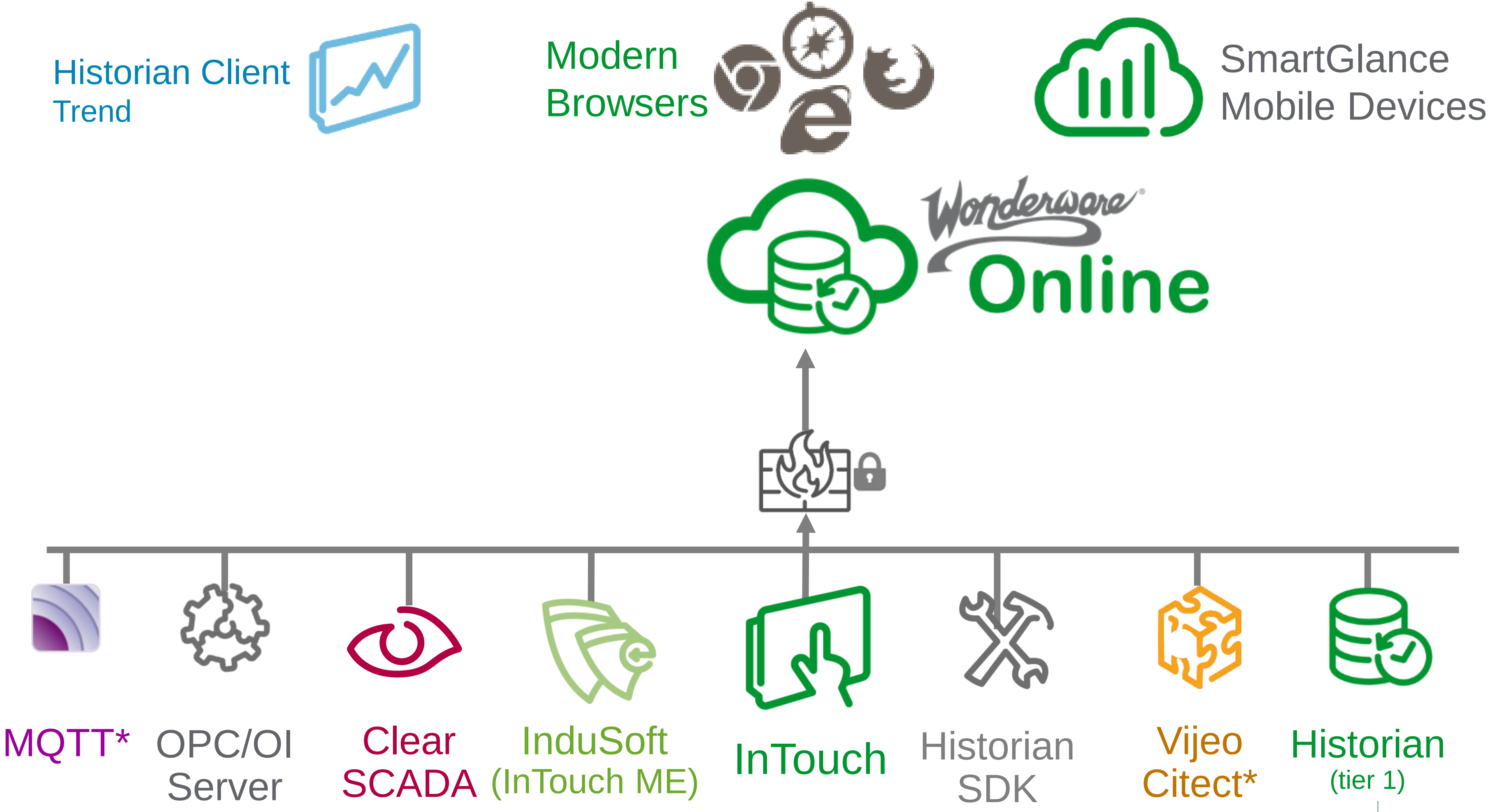


Wonderware Online

any-to-any.

many-to-many.





Historian Client Trend

Modern Browsers

SmartGlance Mobile Devices

Wonderware Online

MQTT*

OPC/OI Server

Clear SCADA

InduSoft (InTouch ME)

InTouch

Historian SDK

Vijeo Citect*

Historian (tier 1)

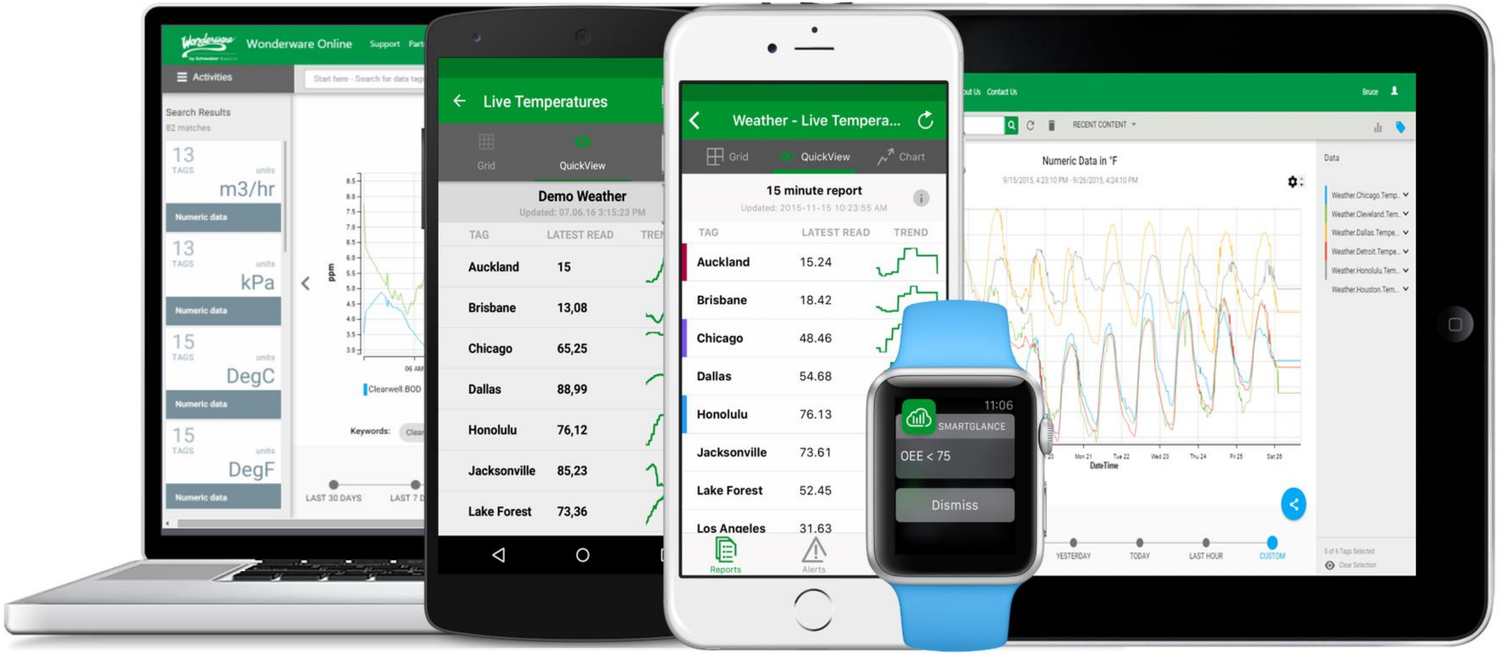
Run on any device

Wonderware

Online

High-performance process historian as a service

https://online.wonderware.com



Demo Weather

Updated: 07.06.16 3:15:23 PM

TAG	LATEST READ
Auckland	15
Brisbane	13,08
Chicago	65,25
Dallas	88,99
Honolulu	76,12
Jacksonville	85,23
Lake Forest	73,36

15 minute report

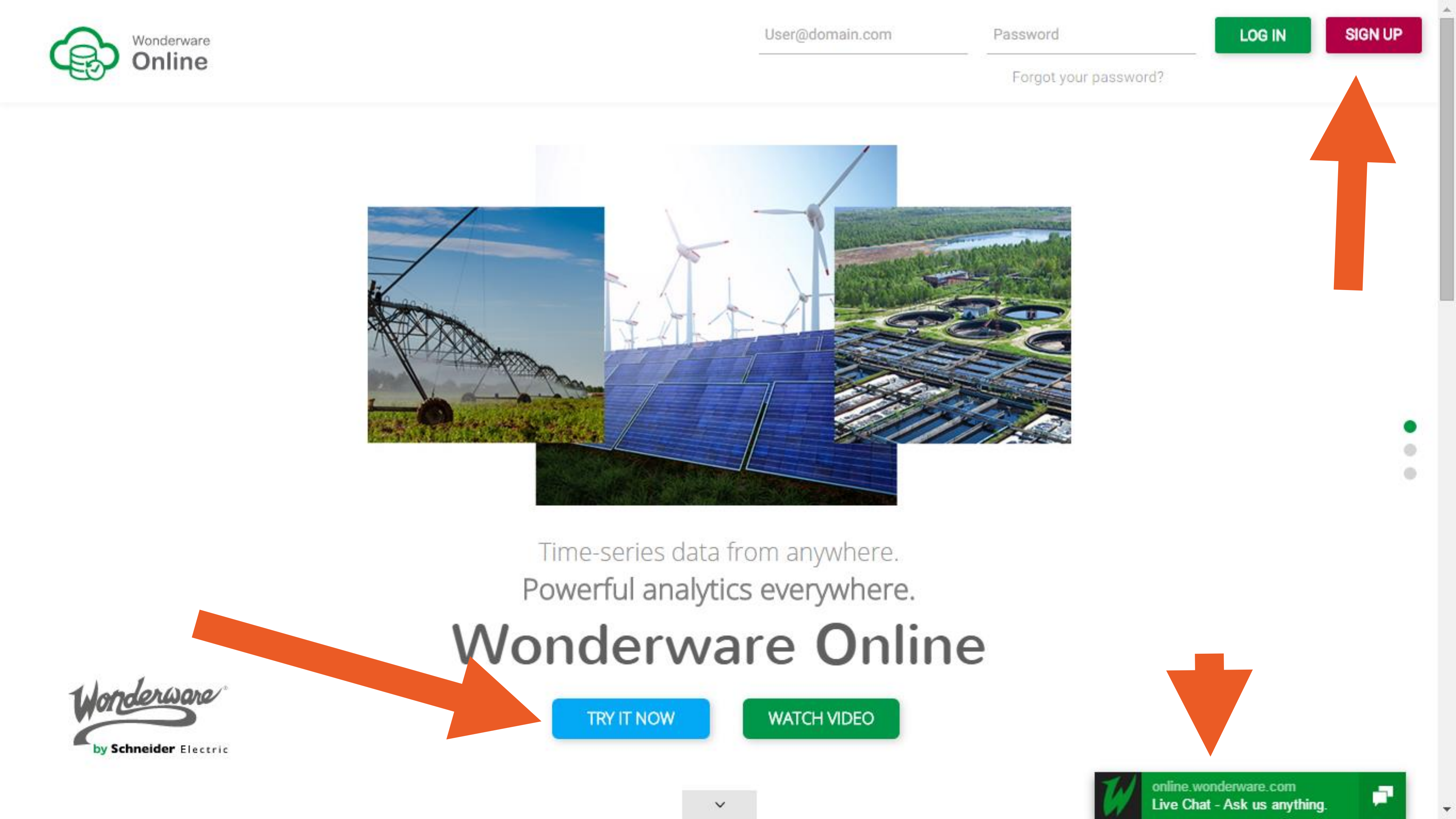
Updated: 2015-11-15 10:23:55 AM

TAG	LATEST READ	TREND
Auckland	15.24	
Brisbane	18.42	
Chicago	48.46	
Dallas	54.68	
Honolulu	76.13	
Jacksonville	73.61	
Lake Forest	52.45	
Los Angeles	31.63	

OEE < 75

Numeric Data in °F

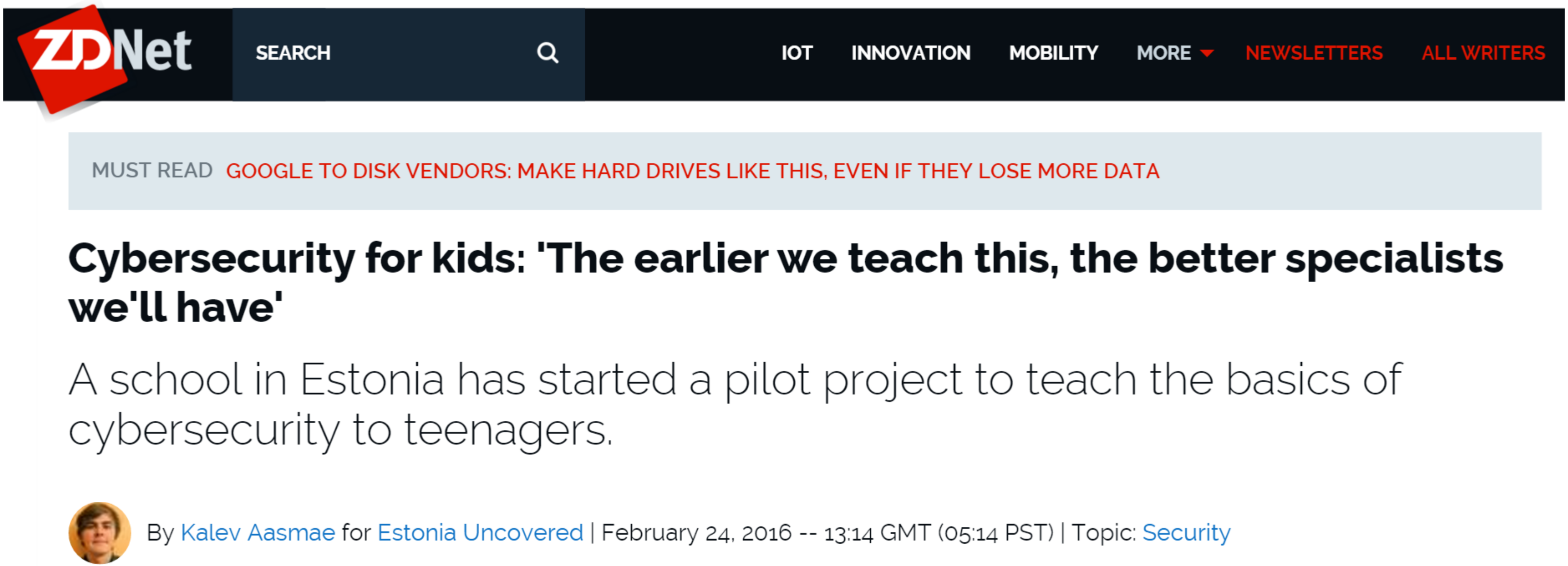
9/15/2015 4:23:10 PM - 9/26/2015 4:24:10 PM



Time-series data from anywhere.

Powerful analytics everywhere.

Wonderware Online



MUST READ GOOGLE TO DISK VENDORS: MAKE HARD DRIVES LIKE THIS, EVEN IF THEY LOSE MORE DATA

Cybersecurity for kids: 'The earlier we teach this, the better specialists we'll have'

A school in Estonia has started a pilot project to teach the basics of cybersecurity to teenagers.

By Kalev Aasmae for Estonia Uncovered | February 24, 2016 -- 13:14 GMT (05:14 PST) | Topic: Security

Contact Info

Saadi Kermani - Product Manager

Wonderware SmartGlance, Wonderware Online

https://ca.linkedin.com/in/skermani

@SaadiKermani

http://blog.wonderware.online

https://www.Wonderware.com

https://online.wonderware.com

Life Is On | Schneider Electric

Thank you.