ivanti

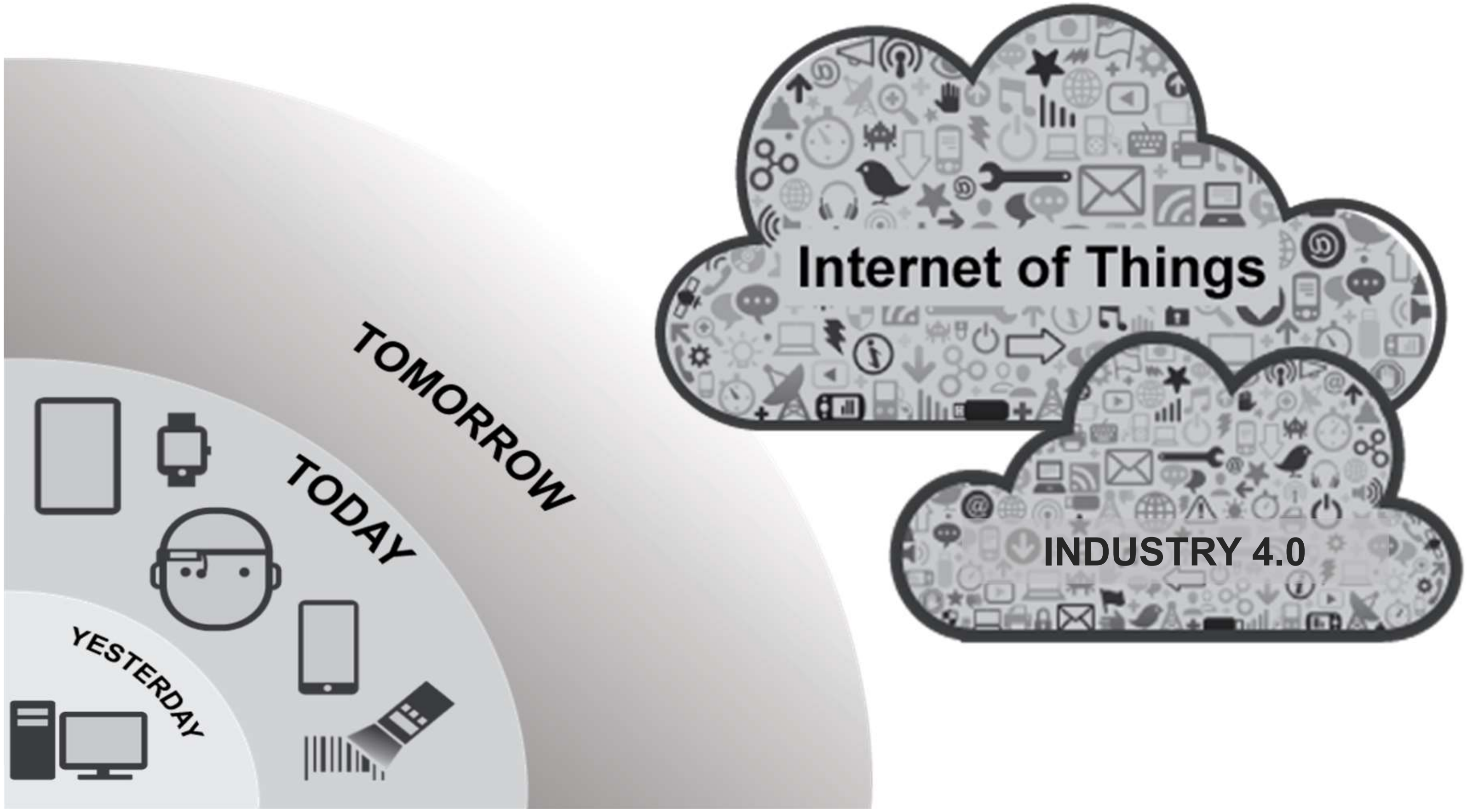
Endpoint Security in industry 4.0 era

Marek WODA, PhD

Senior Technical Consultant

Industry 4.0 Era – pains & gains

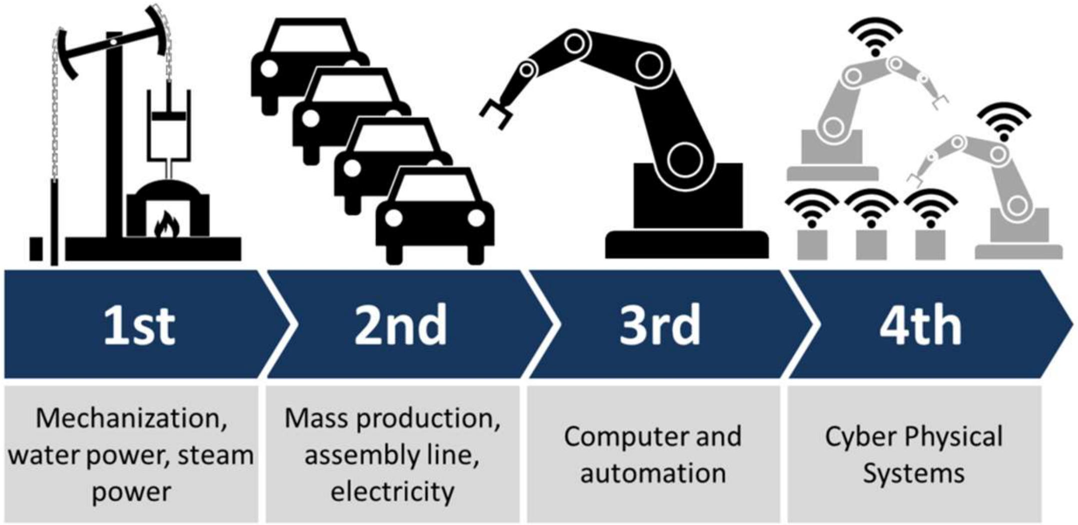
Evolution of the Workplace



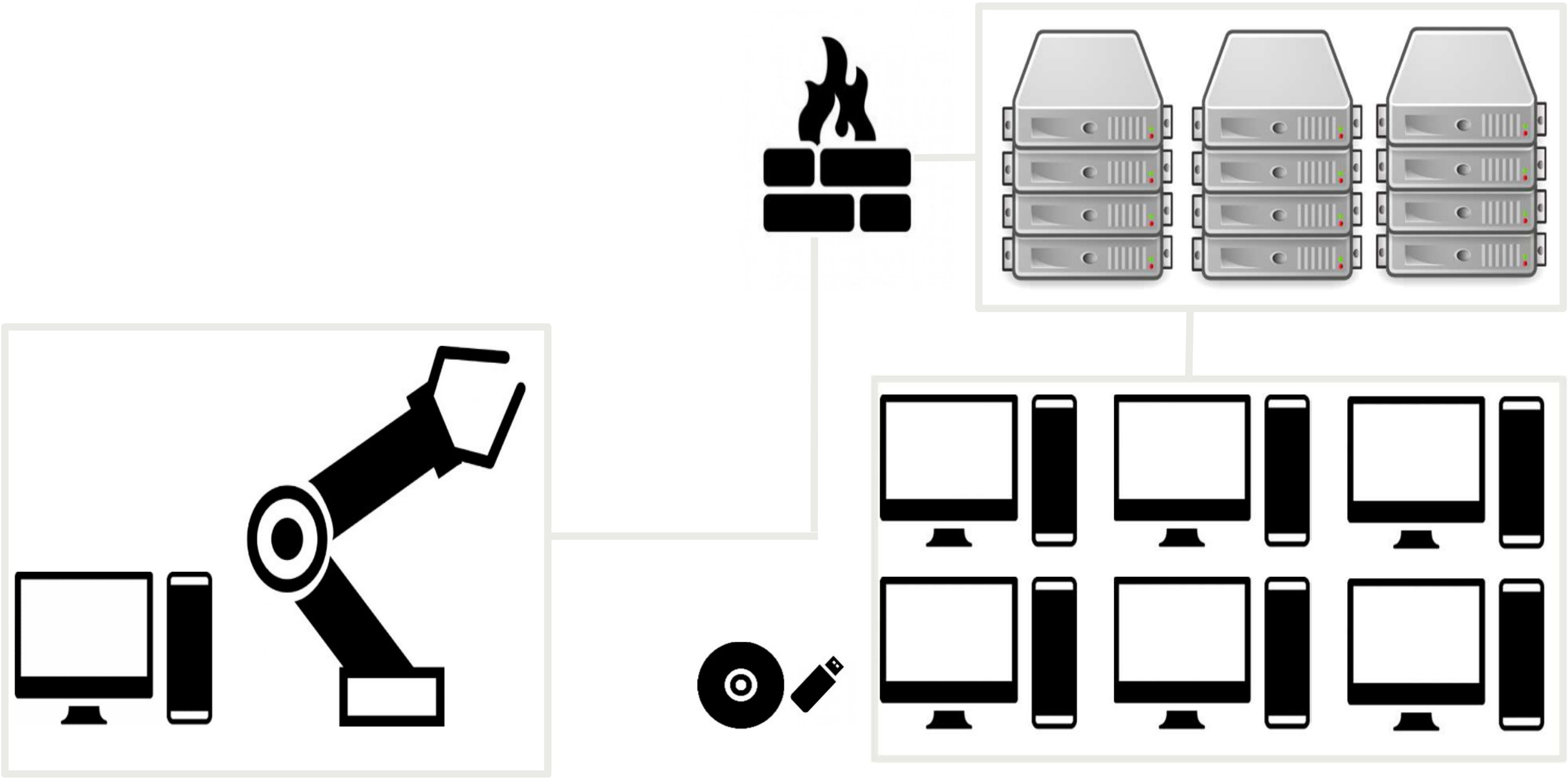
Industry 4.0 – Definition

Current trend of automation and data exchange in manufacturing technologies. It includes cyber-physical systems, the *Internet of Things* and *Cloud Computing*

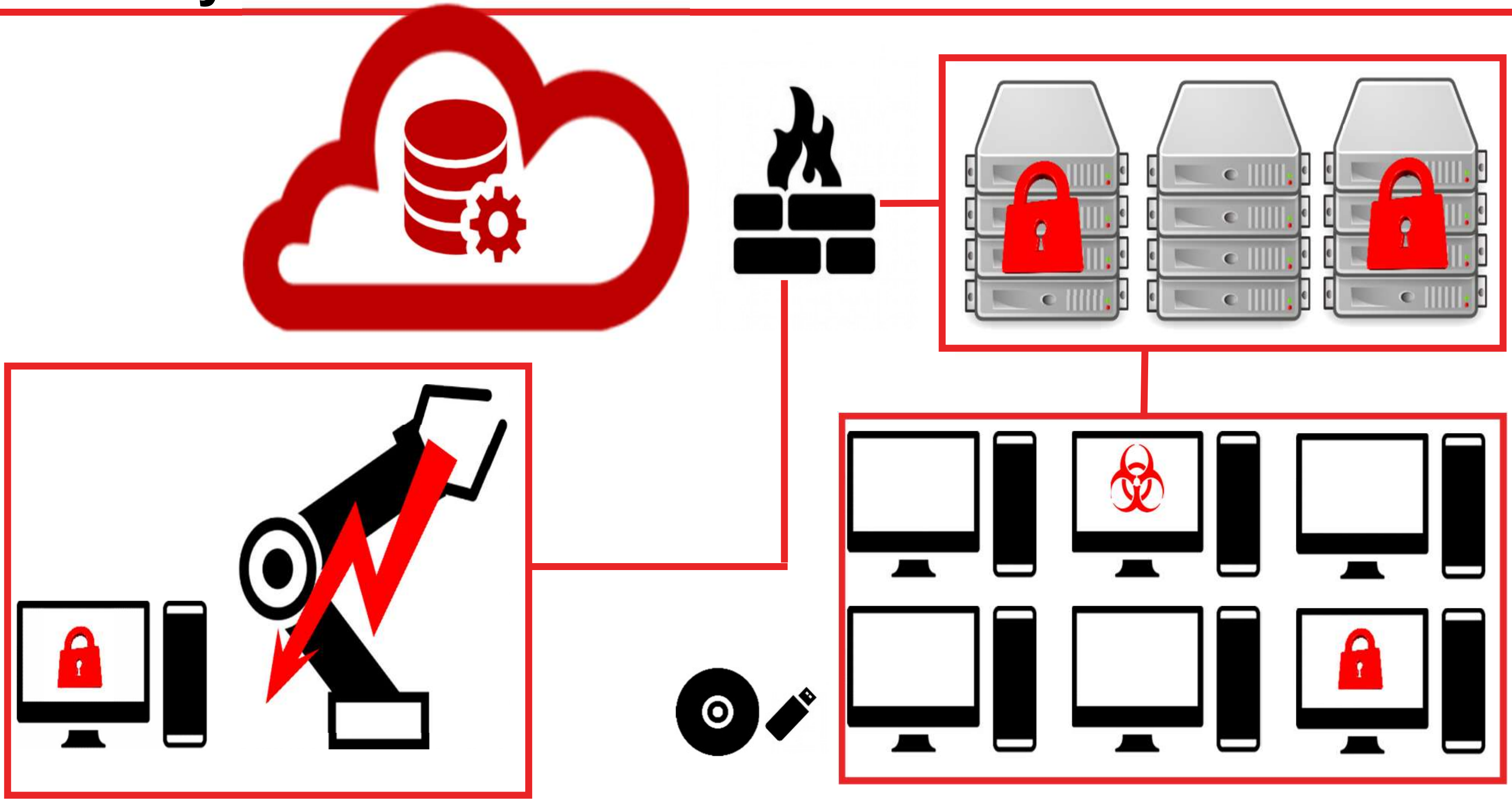
Flexible Low Cost Automation


1st
Mechanization, water power, steam power
2nd
Mass production, assembly line, electricity
3rd
Computer and automation
4th
Cyber Physical Systems

Industry 4.0 – Scenario

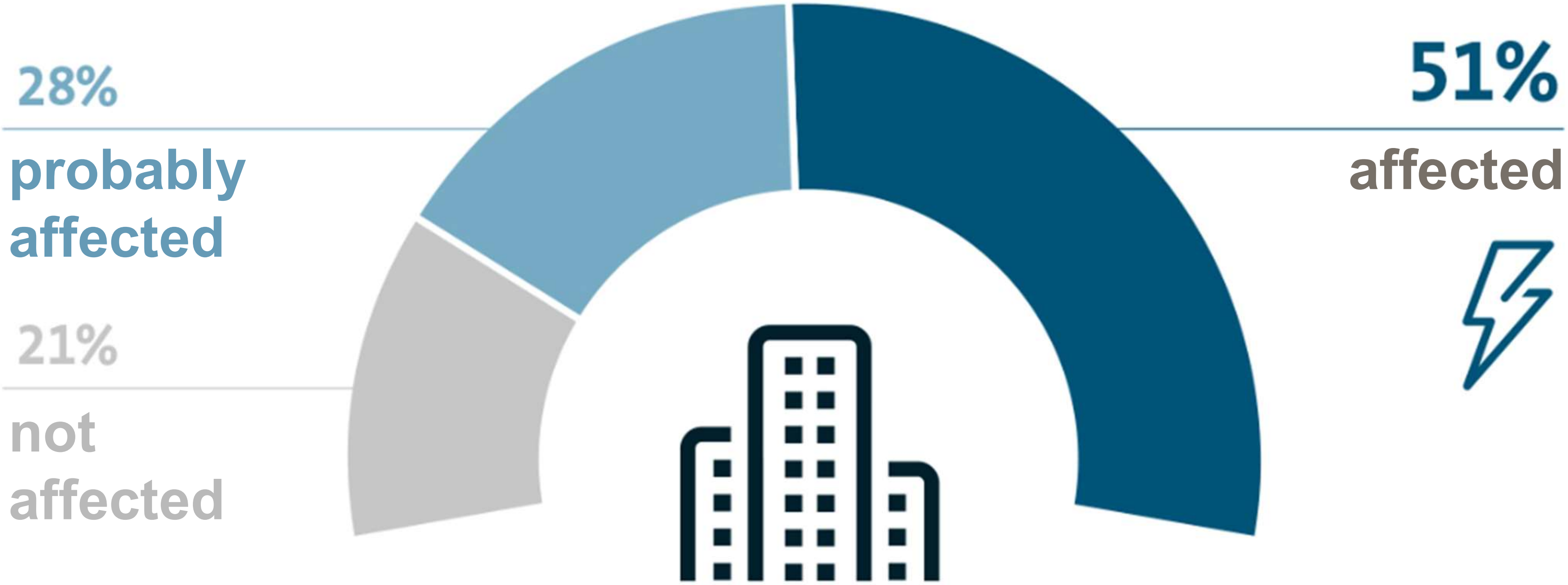


Industry 4.0 – Scenario



Industry 4.0 – Facts

Every second a company is hit by digital attacks



Threat #1

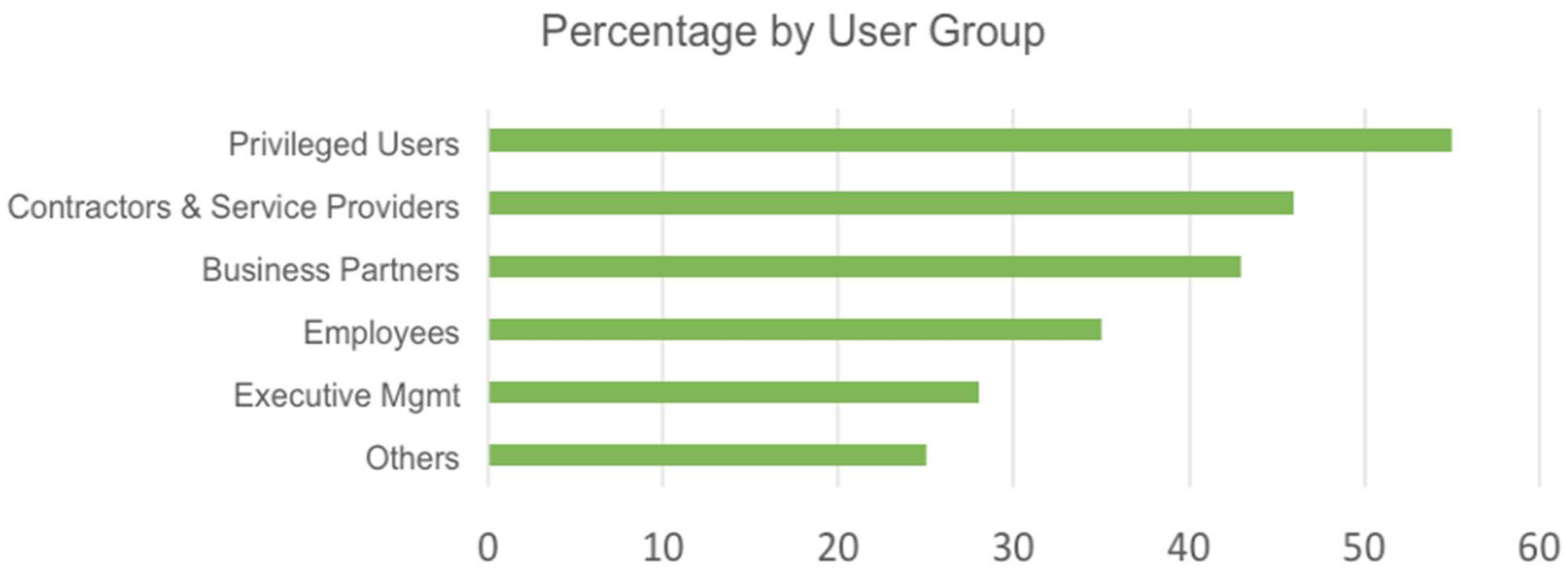
USERS

Threat #1

USERS

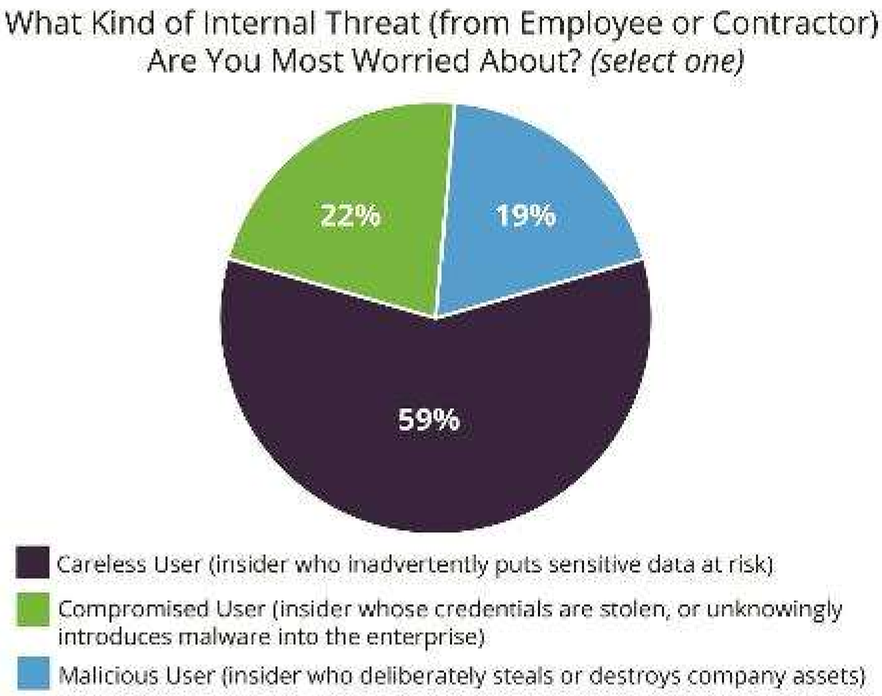
60% **Attacks are targeted to end user!**

Threat #1



https://www.skyhighnetworks.com/cloud-security-blog/protecting-against-your-biggest-vulnerability-privileged-user-threat/

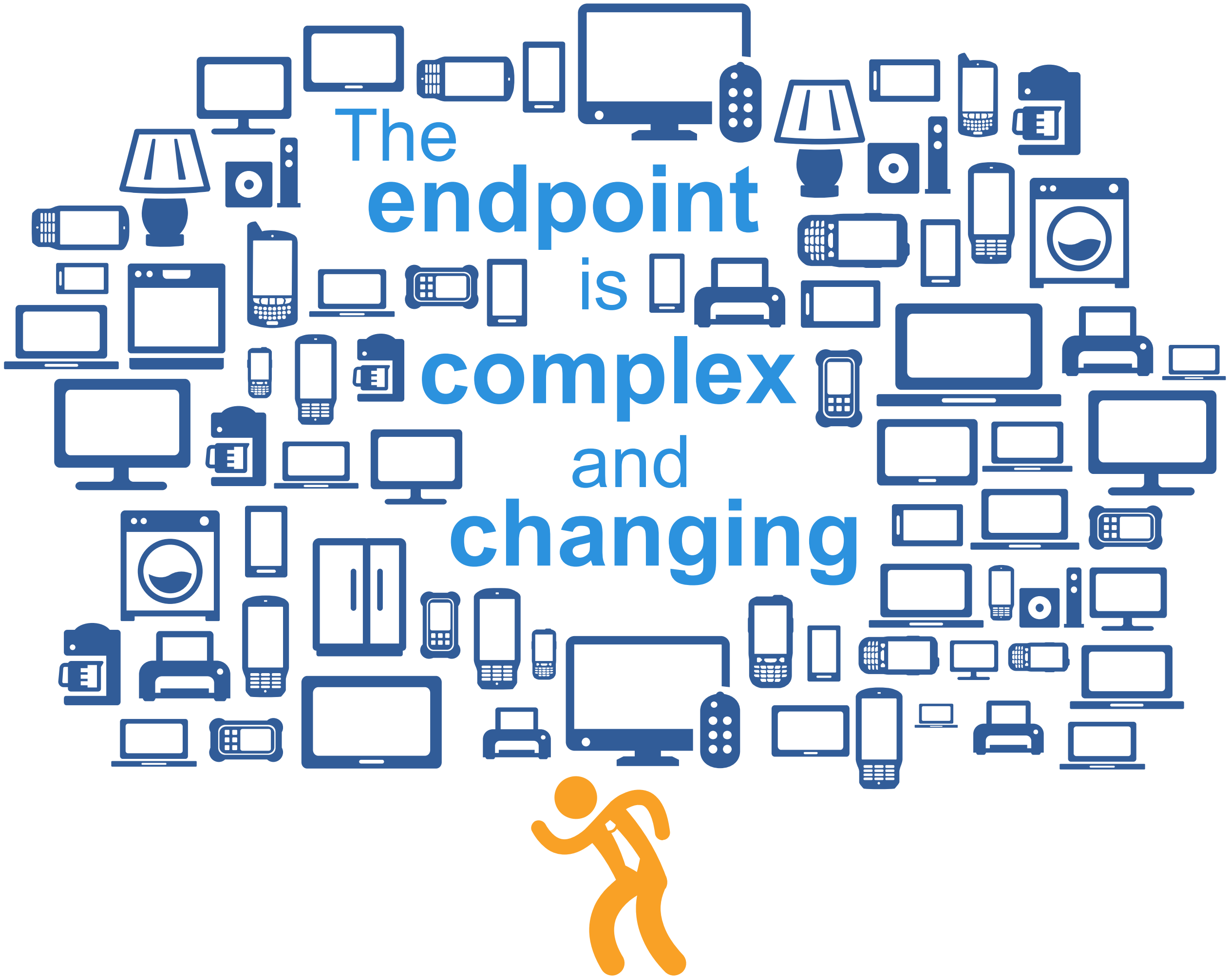
Threat #1



https://www.imperva.com/blog/top-insider-threat-concern-careless-users-survey/

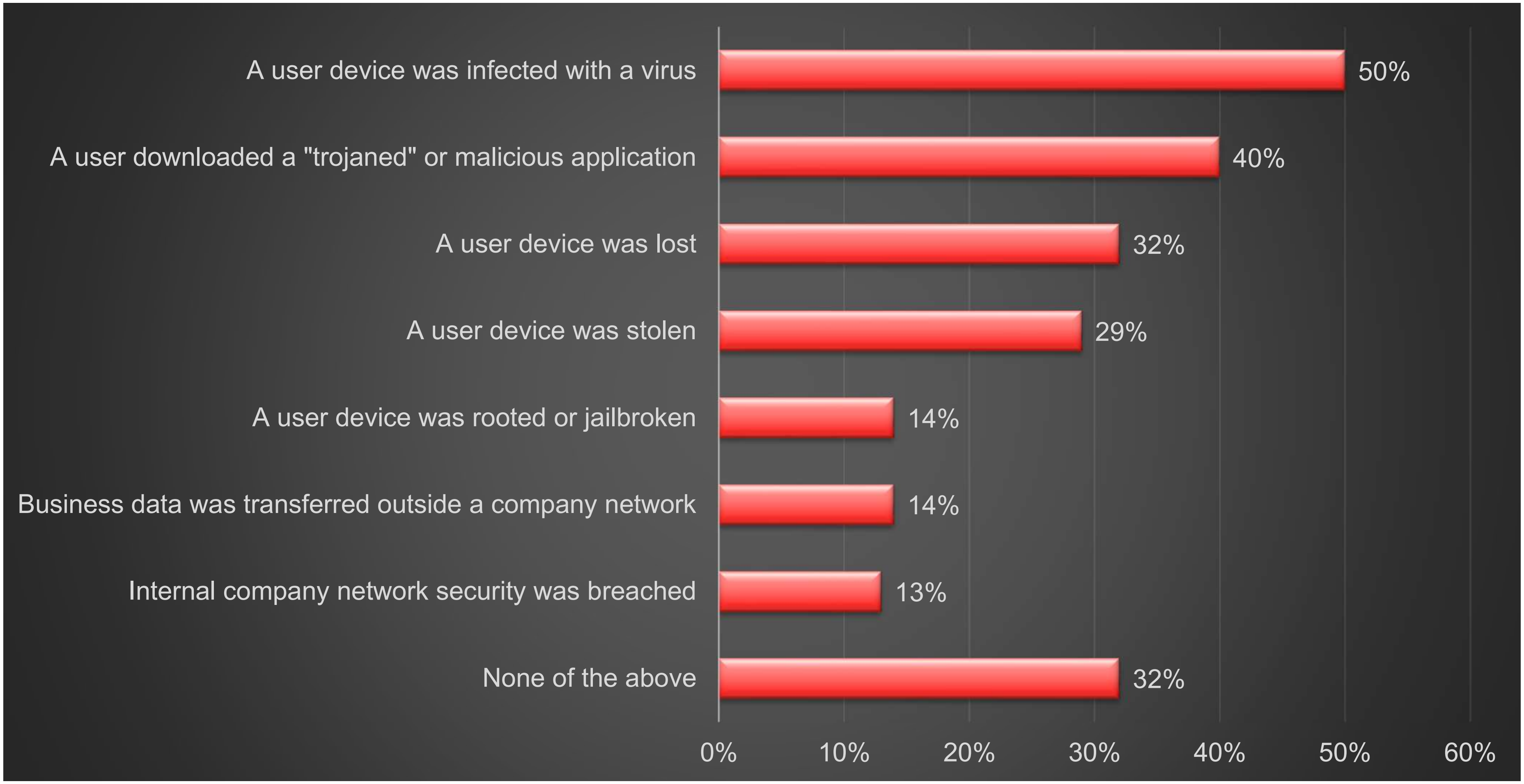
Threat #2

DEVICES



The **endpoint** is **complex** and **changing**

Which of the following security breaches occurred in the last 12 months in your organization?



© 2017 Enterprise Management Associates, Inc.

70% MOBILE DEVICE **35%** LAPTOP PC

personally own the devices they use to perform their jobs

40%

regularly use insecure methods for sharing company data

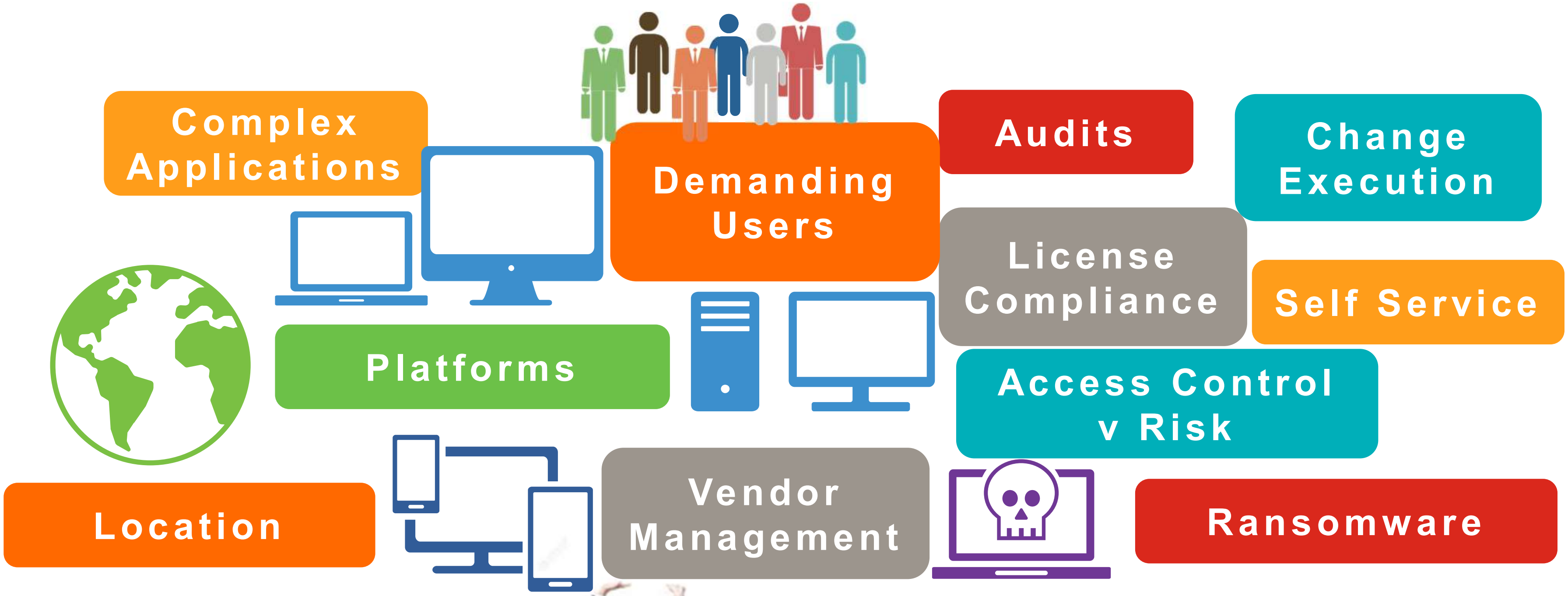
50%

all business tasks are performed outside the physical workplace

5% surveyed organizations indicate they are fully prepared to support all modern endpoint management requirements

Customer expectations

I want to work in any place, in any time using any device.



Complex Applications

Demanding Users

Audits

Change Execution

License Compliance

Self Service

Platforms

Access Control v Risk

Location

Vendor Management

Ransomware

Lead Digital Transformation…

not like this!

Process Chaos

67%

of service desks time is spent firefighting

SDI Benchmarking Report

“I am stuck in firefighting long call queues, call abandonment, rates, resolution times are up - rather than service improvement”

I have to balance current needs with new but we don’t get additional resources”

“We are inconsistent in the way we handle issues”

“We are our own worst enemy in some cases our service level breaches have been caused by our own changes”

Dissatisfied End User Customers

96%

of desks state that they will use more self-help and self service facilities in the future

SDI Benchmarking Report

“My end users are complaining they can’t get access to new applications quickly”

“We have long call queues and 30% are just password reset requests”

“IT does nothing to help me in my job, I’ll find my own IT software”

What is going on

70%

of respondents do not measure cost per call, and 74% do not measure cost per email

SDI Benchmarking Report

"I can't see into our operation to justify our performance or budget requirements for more resources"

"I can't pull the reports I need quickly"

"We don't always get information from other IT teams"

IT Complexity

52%

Do not have enough resource available

93%

Said that their service desk needs to be more efficient

“ We can’t leverage existing IT investments so we are using several siloed systems to manage the service desk.”

“ We are creating errors and unnecessary delays through our own inefficiencies.”

SDI Report – Anatomy of a Service Desk

Service Desk Staff are Unhappy.

- “Staff morale is at an all time low and its having knock on effect in how they deal with end user customers”
- “They have too much to do and no resources”
- “They are constrained by outdated processes and systems which don’t match our employee expectations of what they should get from IT support”
- Staff skills are not improving and they are leaving to get better jobs

SDI Benchmarking Report

FBI: 9 steps to protect against RANSOMWARE attacks

1. Patch the critical operating systems and applications
2. Ensure that antivirus software is up-to-date and that regular scans are scheduled
3. Manage the use of privileged accounts
4. Implement access control that focuses on the data
5. Define, implement, and enforce software rules
6. Disable macros from Microsoft Office files
7. Implement applications whitelisting
8. Restrict users to virtualized or containerized environments
9. Back up critical files frequently

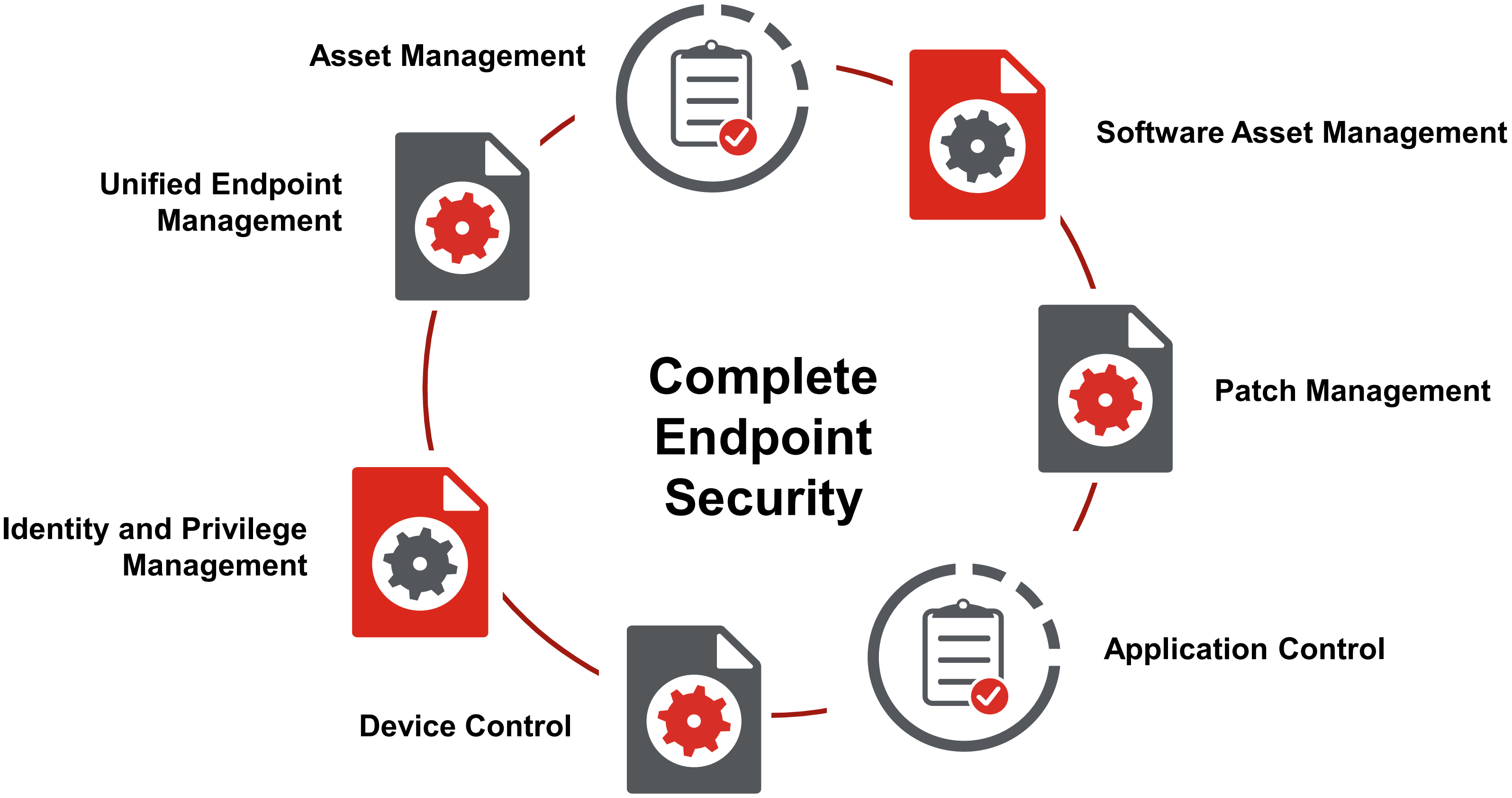
Top 5 things you can do to stay secure

1. Remove/control admin rights
2. Remediate OS vulnerabilities
3. Remediate app vulnerabilities
4. Implement application whitelisting
5. Control peripheral connections

Security and automation – stay secure inside your organization

PREVENTION
IS BETTER
THAN
CURE

Endpoint Security according IVANTI



Asset Management

Software Asset Management

Unified Endpoint Management

Complete Endpoint Security

Patch Management

Identity and Privilege Management

Application Control

Device Control

Why Patch Management

83%

of breaches are made through *3rdparty* applications

11%

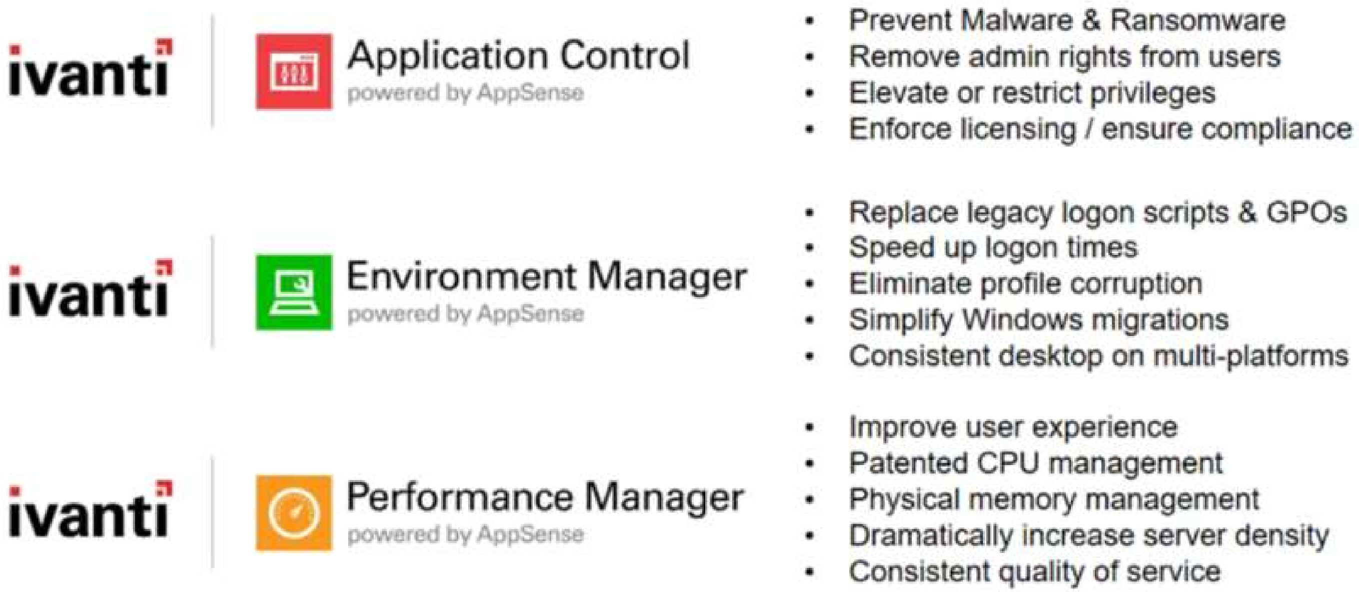
of breaches are made through Operating Systems

Patch Management

Ivanti has about 60% of the global patching market

1. **Ivanti Patch for Endpoints Manager (Clients, Servers)**
2. **Ivanti Security Controls (Clients, Servers)**
3. **Ivanti Patch for Linux, UNIX, Mac**
4. **Ivanti Patch for SCCM**

Application Control



ivanti | Application Control
powered by AppSense

- Prevent Malware & Ransomware
- Remove admin rights from users
- Elevate or restrict privileges
- Enforce licensing / ensure compliance

ivanti | Environment Manager
powered by AppSense

- Replace legacy logon scripts & GPOs
- Speed up logon times
- Eliminate profile corruption
- Simplify Windows migrations
- Consistent desktop on multi-platforms

ivanti | Performance Manager
powered by AppSense

- Improve user experience
- Patented CPU management
- Physical memory management
- Dramatically increase server density
- Consistent quality of service

Device Control

1. Discover all removable devices that are currently connected or have ever been connected to your endpoints.

2. Assess all “plug and play” devices by class, group, model, and/or specific ID and define policy through a whitelist approach.

3. Implement file copy limitations, file type filtering, and forced encryption policies for data moved onto removable devices.

4. Monitor all policy changes, administrator activities, and file transfers to ensure continuous policy enforcement.

5. Report on device and data usage to document compliance with corporate and/or regulatory policies.

Why IT Asset Management?

Software Audit

Compliance

Hardware Lifecycle/Refresh

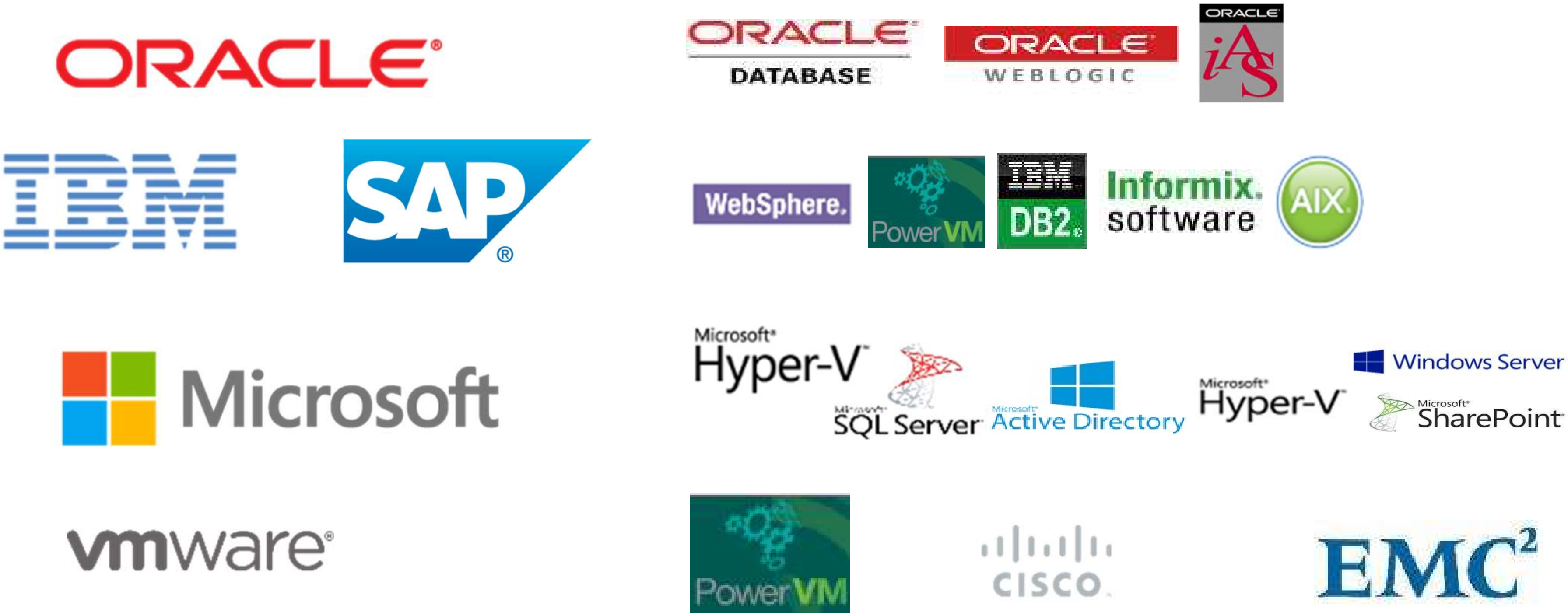
Software Lifecycle/Refresh

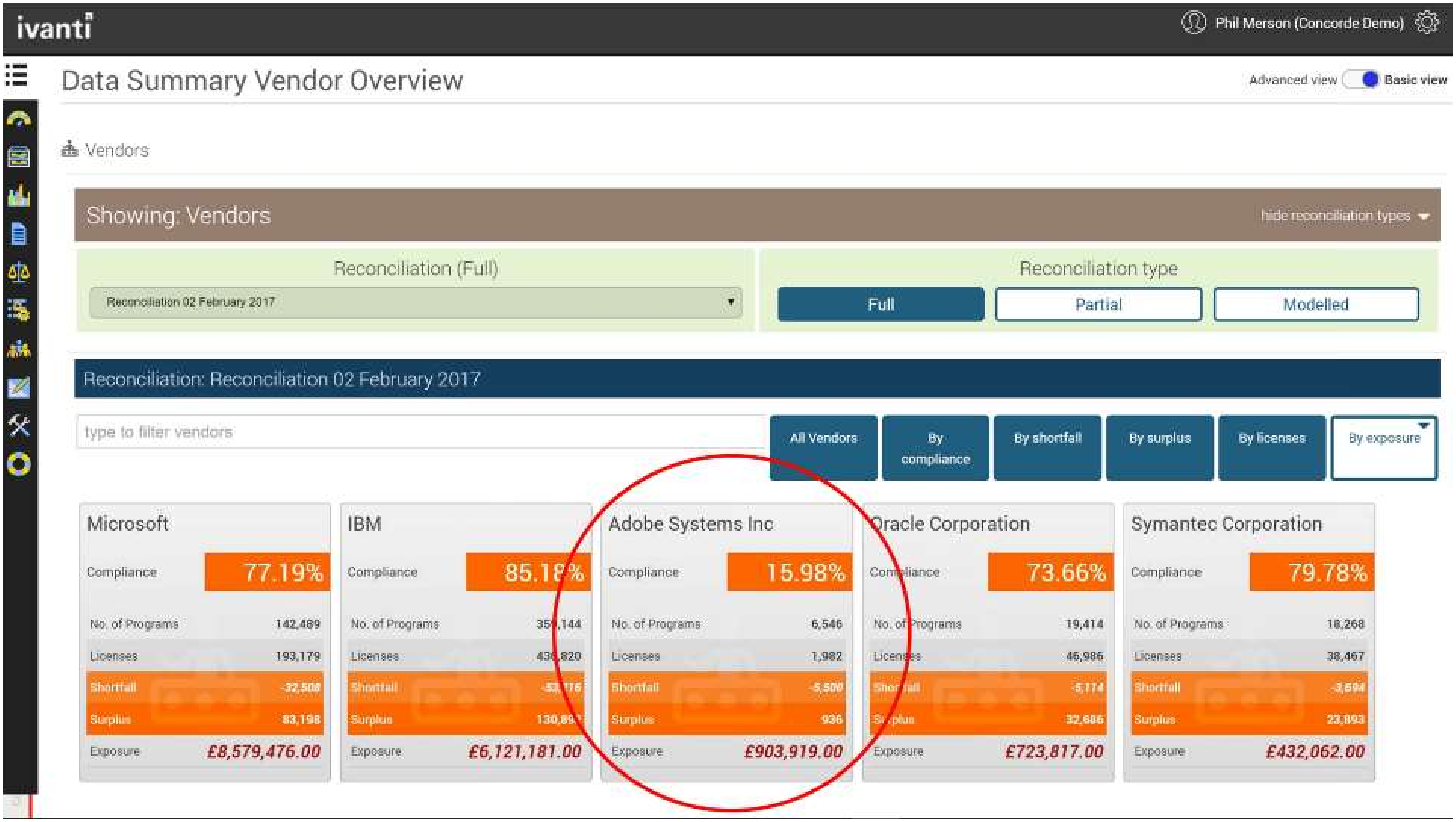
Asset Loss

Security Threat

License Optimizer (SAM)

Supported Vendors





Data Summary Vendor Overview

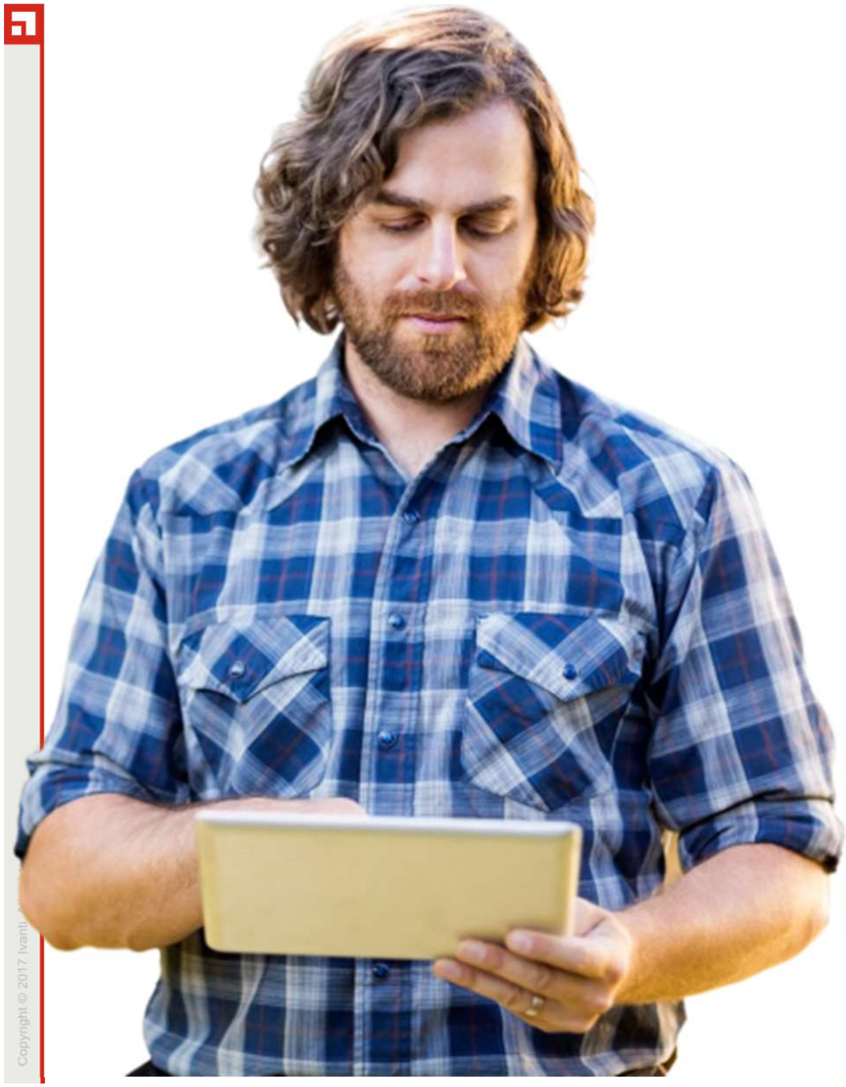
Showing: Vendors

Reconciliation (Full): Reconciliation 02 February 2017

Reconciliation type: Full | Partial | Modelled

Reconciliation: Reconciliation 02 February 2017

	Microsoft	IBM	Adobe Systems Inc	Oracle Corporation	Symantec Corporation
Compliance	77.19%	85.18%	15.98%	73.66%	79.78%
No. of Programs	142,489	35[illegible],144	6,546	19,414	18,268
Licenses	193,179	43[illegible],820	1,982	46,986	38,467
Shortfall	-32,508	-5[illegible],[illegible]76	-5,500	-5,114	-3,694
Surplus	83,198	130,89[illegible]	936	32,686	23,893
Exposure	£8,579,476.00	£6,121,181.00	£903,919.00	£723,817.00	£432,062.00



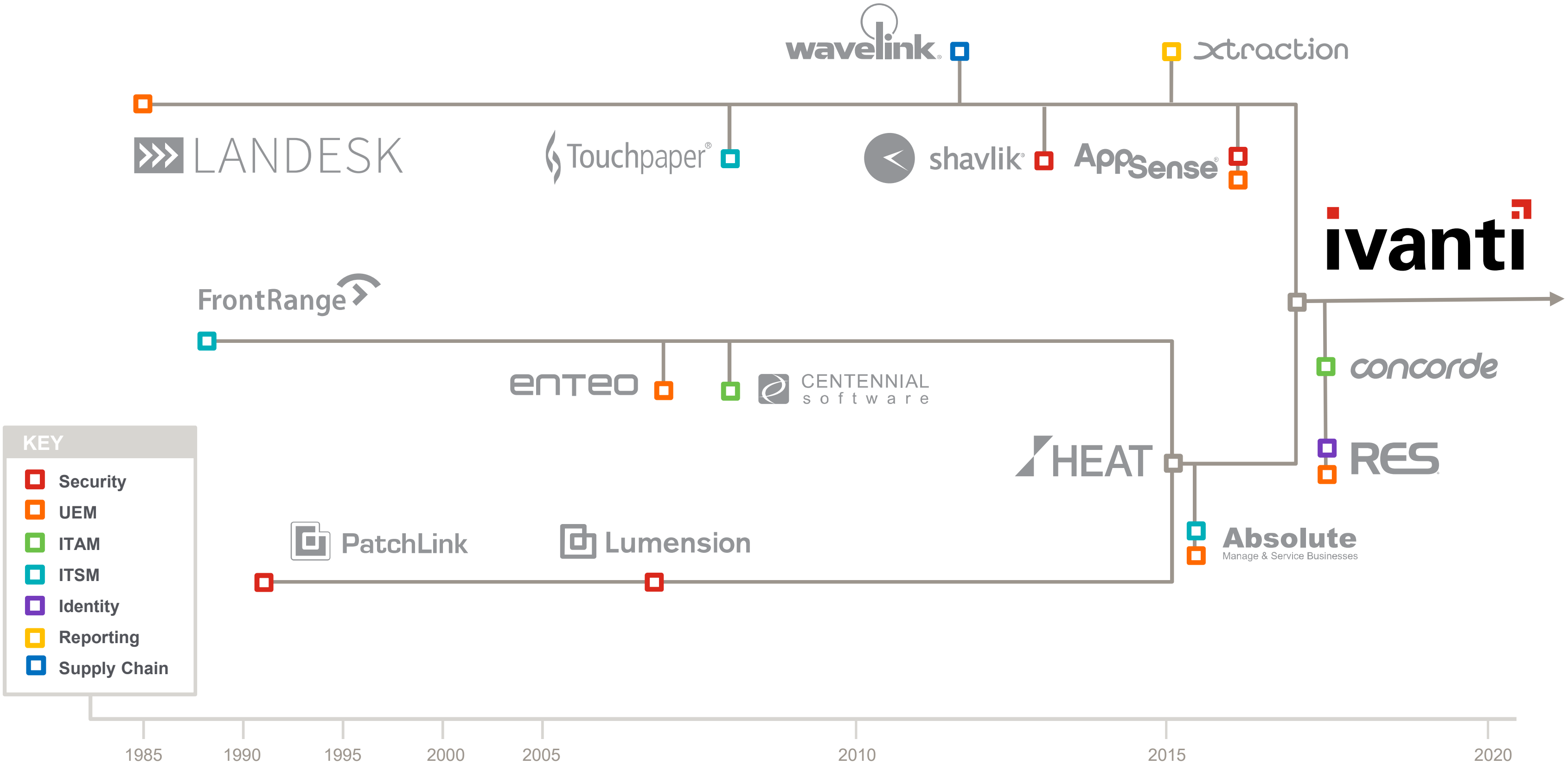
Our goal

Enable users to be their most productive, and in the same time helping IT depts keeping full control.

ivanti

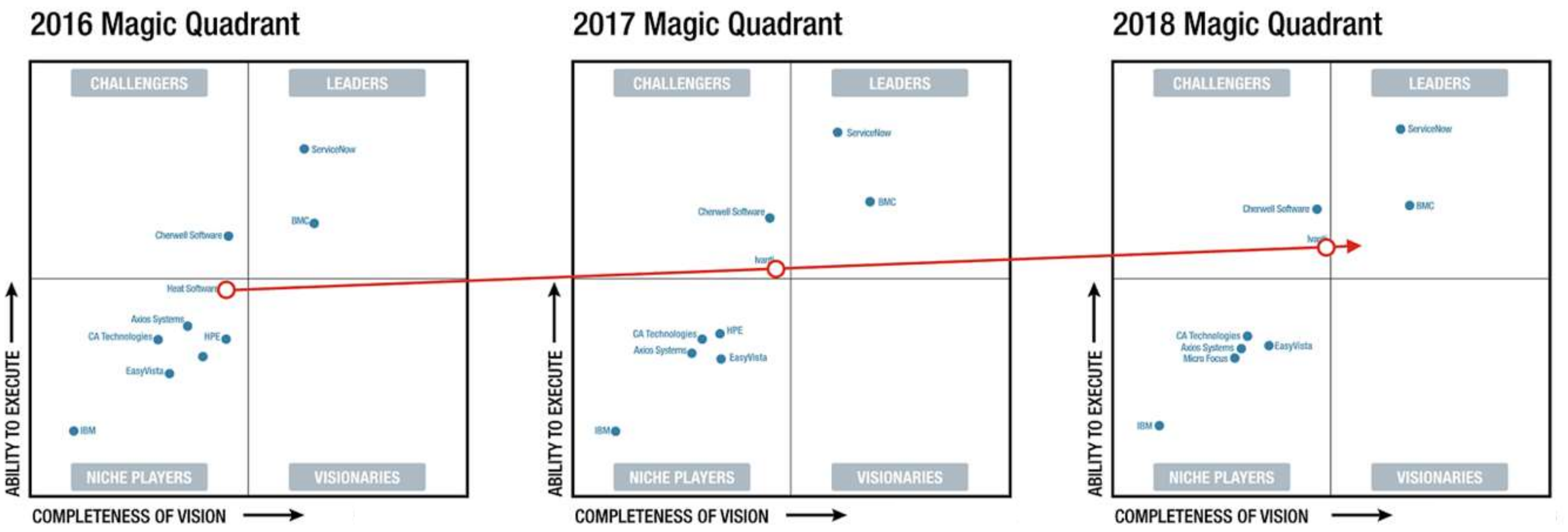
- Established in 1985, owned by ***Intel*** by 12 years
- Actual owner is Clearlake Capital Group
- HQ in Salt Lake City, UT. USA
- 1900+ employees in 36 countries
- 27 500+ customers, 47 M+ endpoints
- 1500+ partners
- 10 acquisitions from 2012 (the last is RES)
- EMEA Support Center in Warszawa
  150 employees

Ivanti DNA


wavelink
xtraction
LANDESK
Touchpaper
shavlik
AppSense
ivanti
FrontRange
enteo
CENTENNIAL software
concorde
HEAT
RES
Absolute
Manage & Service Businesses
PatchLink
Lumension
KEY
🟥 Security
🟧 UEM
🟩 ITAM
ITSM
🟪 Identity
🟨 Reporting
🟦 Supply Chain
1985
1990
1995
2000
2005
2010
2015
2020

Gartner - Magic Quadrant - IT Service Support Management Tools

ITSM: Moving in the Right Direction

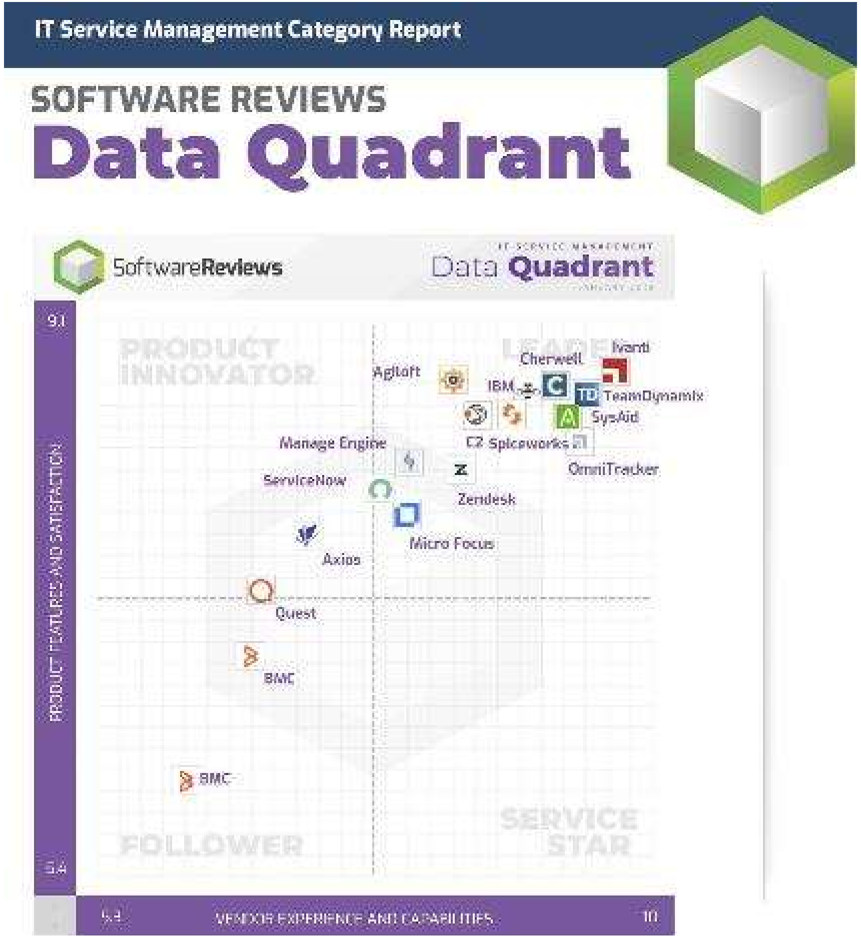


2016 Magic Quadrant

2017 Magic Quadrant

2018 Magic Quadrant

Info-Tech Research Group – ITSM Report



IT Service Management Category Report

SOFTWARE REVIEWS

Data Quadrant

PinkVERIFY ITIL Certification

No need to reinvent the ITSM wheel

ITIL Incident Management (IM)

ITIL Service Catalog (SCM)

ITIL Problem Management (PM)

ITIL Service Portfolio Management (SPM)

ITIL Change Management (CHG)

ITIL Knowledge Management (KM)

ITIL Request Fulfillment (RF)

ITIL Availability Management (AVM)

ITIL Release and Deployment Management (REL)

ITIL Event Management (EV)

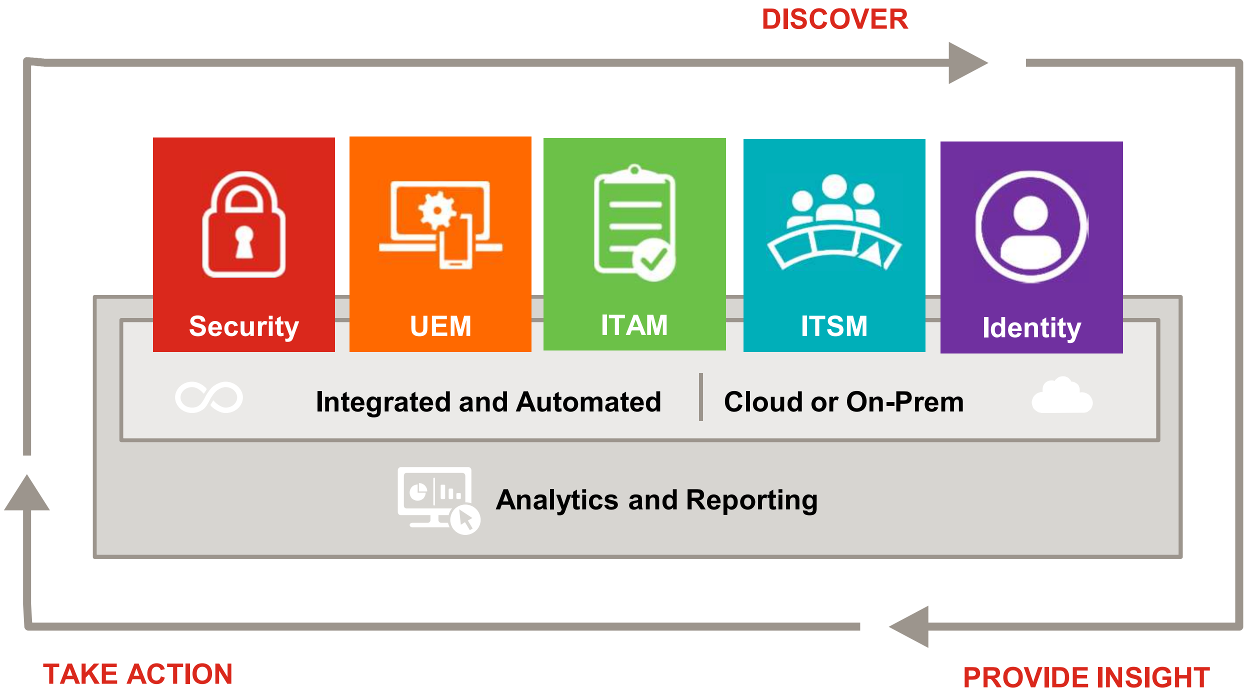
ITIL Service Asset and Configuration Management (SACM)

ITIL Financial Management (FM)

ITIL Service Level Management (SLM)

BACK

Unified IT



DISCOVER

Security

UEM

ITAM

ITSM

Identity

Integrated and Automated

Cloud or On-Prem

Analytics and Reporting

TAKE ACTION

PROVIDE INSIGHT

Unified IT - Ivanti Portfolio

Operational Security

- AV / Anti-Malware
- Patch Management
- Device and App Control
- Privilege Management
- Configuration Management

Unified Endpoint Management

- Physical, Virtual & Mobile Mgmt.
- Environment Management
- File & Profile Migration
- Remote Control
- Software Distribution

IT Asset Management

- Software License Management
- Hardware Asset Management
- License Optimization
- Audit Defense
- Lifecycle Management

Service Management

- Full ITSM / ITIL Support
- Voice Automation / Telephony
- Service Catalog
- Project Portfolio Management
- On-boarding / Off-boarding

Identity Management

- Identity Lifecycle Management
- Policy and Role Management
- Entitlements Management
- Access Request
- Identity Workflow & Fulfillment

Discovery | **Integration** | **Cloud or On-Premises** | **Workflow and Process Automation** | **Business Value Dashboards, Analytics and Reporting**

Do you have any questions?

Thank you!

Find out more:
WWW: www.ivanti.com
Forums: http://community.ivanti.com
Twitter: #goivanti

ivanti

Thank you for your attention