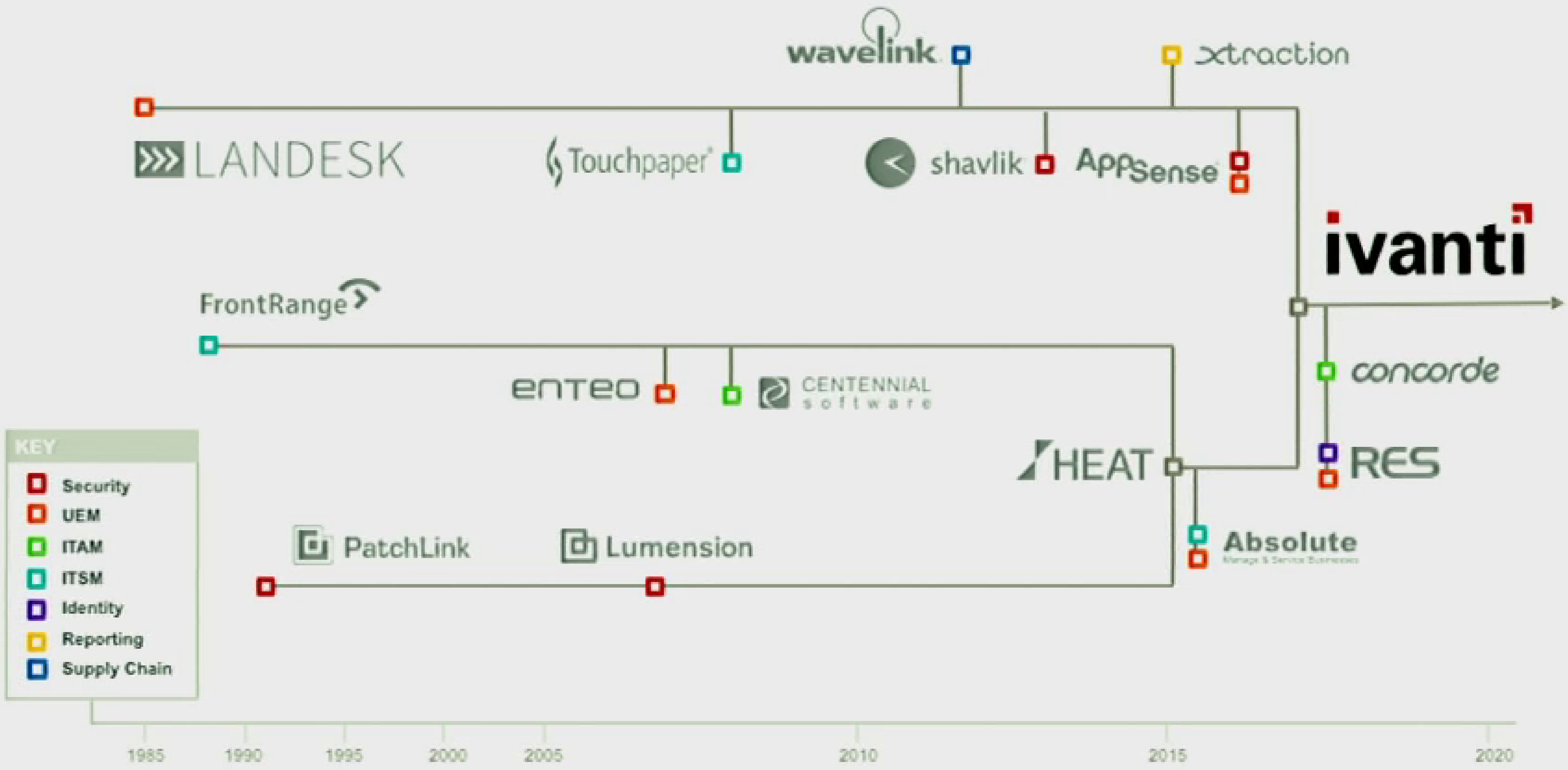
How Ivanti can help minimize the headaches around GDPR

Tamas Szalai, pre-sales engineer

RelNet Technológia Kft.

Ivanti DNA



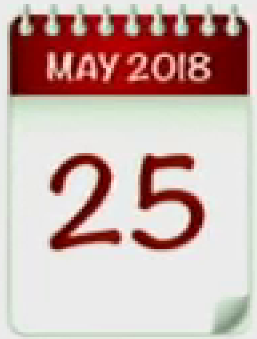
wavelink
xtraction
LANDESK
Touchpaper
shavlik
AppSense
ivanti
FrontRange
enteo
CENTENNIAL software
concorde
HEAT
RES
Absolute
Manage & Service Businesses
PatchLink
Lumension

KEY

- Security
- UEM
- ITAM
- ITSM
- Identity
- Reporting
- Supply Chain

1985
1990
1995
2000
2005
2010
2015
2020

What you should already know..



When

What

Where

Who

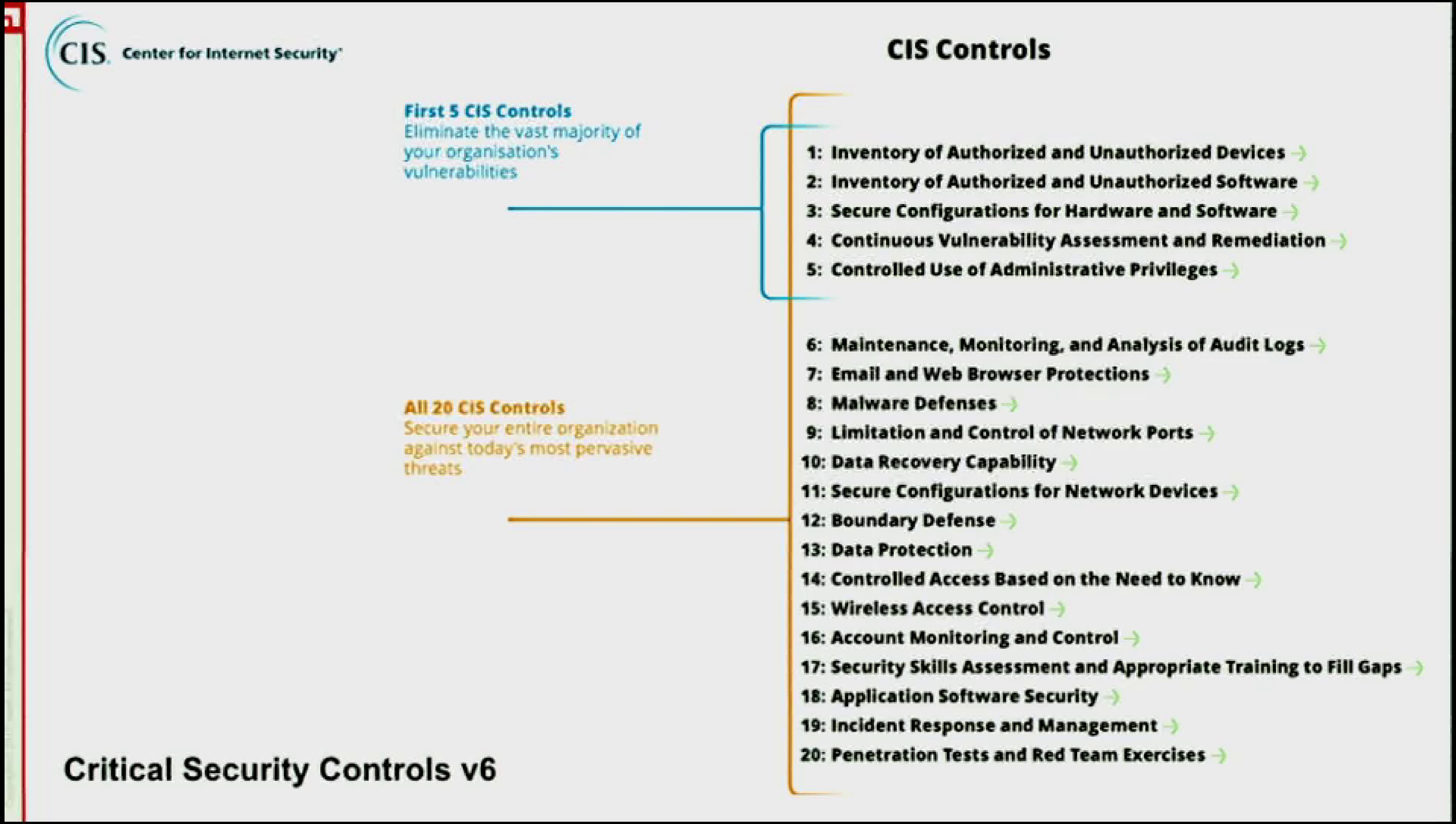
DPO

Increased fines

Time to respond

Legal Advice

How can we help?



CIS Center for Internet Security

CIS Controls

First 5 CIS Controls
Eliminate the vast majority of your organisation's vulnerabilities

1: Inventory of Authorized and Unauthorized Devices

2: Inventory of Authorized and Unauthorized Software

3: Secure Configurations for Hardware and Software

4: Continuous Vulnerability Assessment and Remediation

5: Controlled Use of Administrative Privileges

All 20 CIS Controls
Secure your entire organization against today's most pervasive threats

6: Maintenance, Monitoring, and Analysis of Audit Logs

7: Email and Web Browser Protections

8: Malware Defenses

9: Limitation and Control of Network Ports

10: Data Recovery Capability

11: Secure Configurations for Network Devices

12: Boundary Defense

13: Data Protection

14: Controlled Access Based on the Need to Know

15: Wireless Access Control

16: Account Monitoring and Control

17: Security Skills Assessment and Appropriate Training to Fill Gaps

18: Application Software Security

19: Incident Response and Management

20: Penetration Tests and Red Team Exercises

Critical Security Controls v6

The first 5 controls

CIS, US-CERT, ASD, and other authorities prioritize these five elements of cyber hygiene to significantly reduce security threats.

- Inventory of authorized and unauthorized devices
- Inventory of authorized and unauthorized software
- Secure configuration
- Controlled use of administration privileges
- Continuous vulnerability assessment and remediation

Recommendations across the world…

1. Discover Assets
2. Patch OS + Applications
3. Application Whitelisting
4. Minimize Admin Privileges

As recommended by…

Center for Internet Security

National Cyber Security Centre
a part of GCHQ

Australian Government
Department of Defence
Intelligence and Security

Bundesamt
für Sicherheit in der
Informationstechnik

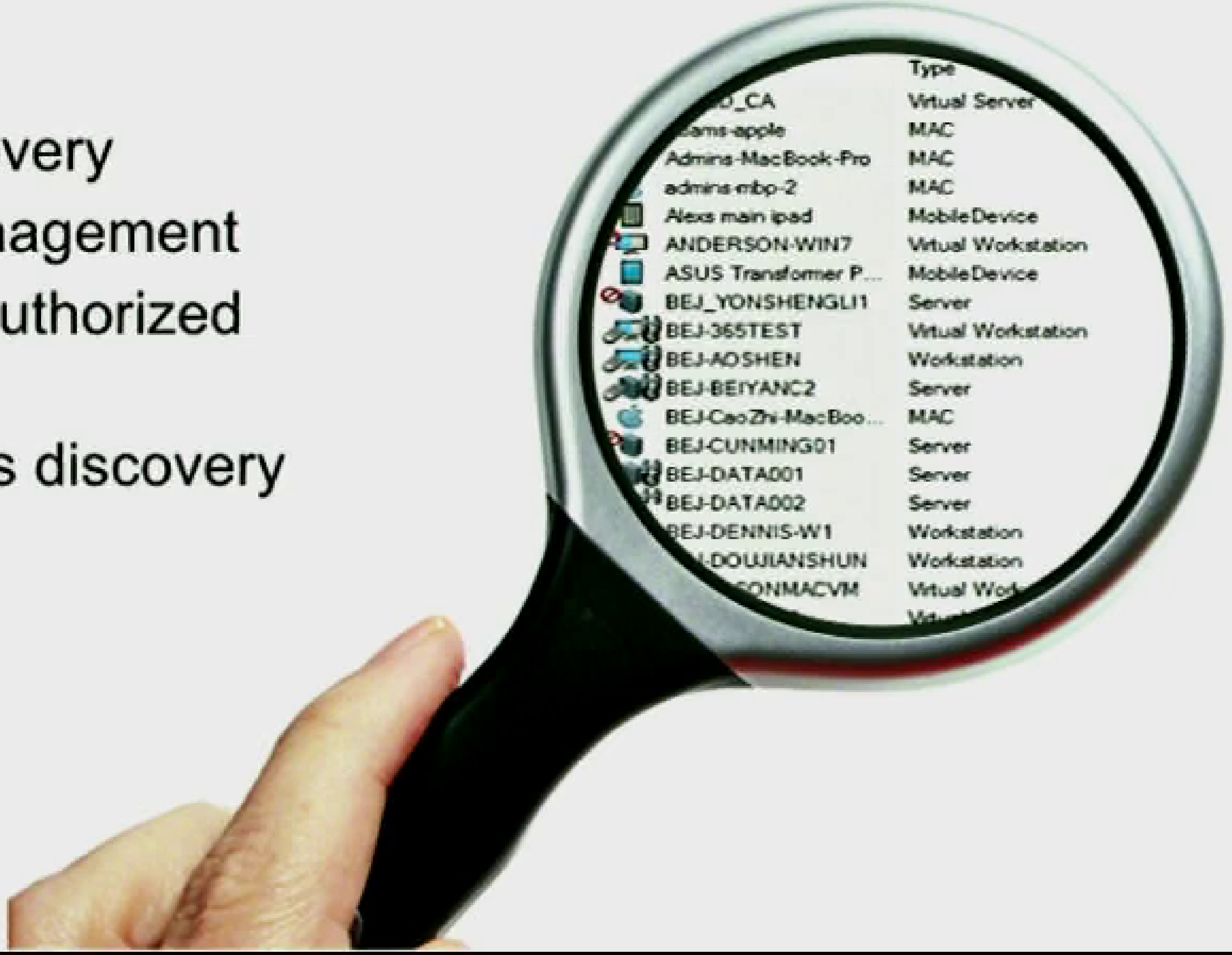
Department of Justice
Federal Bureau of Investigation

Discovery

Discovery

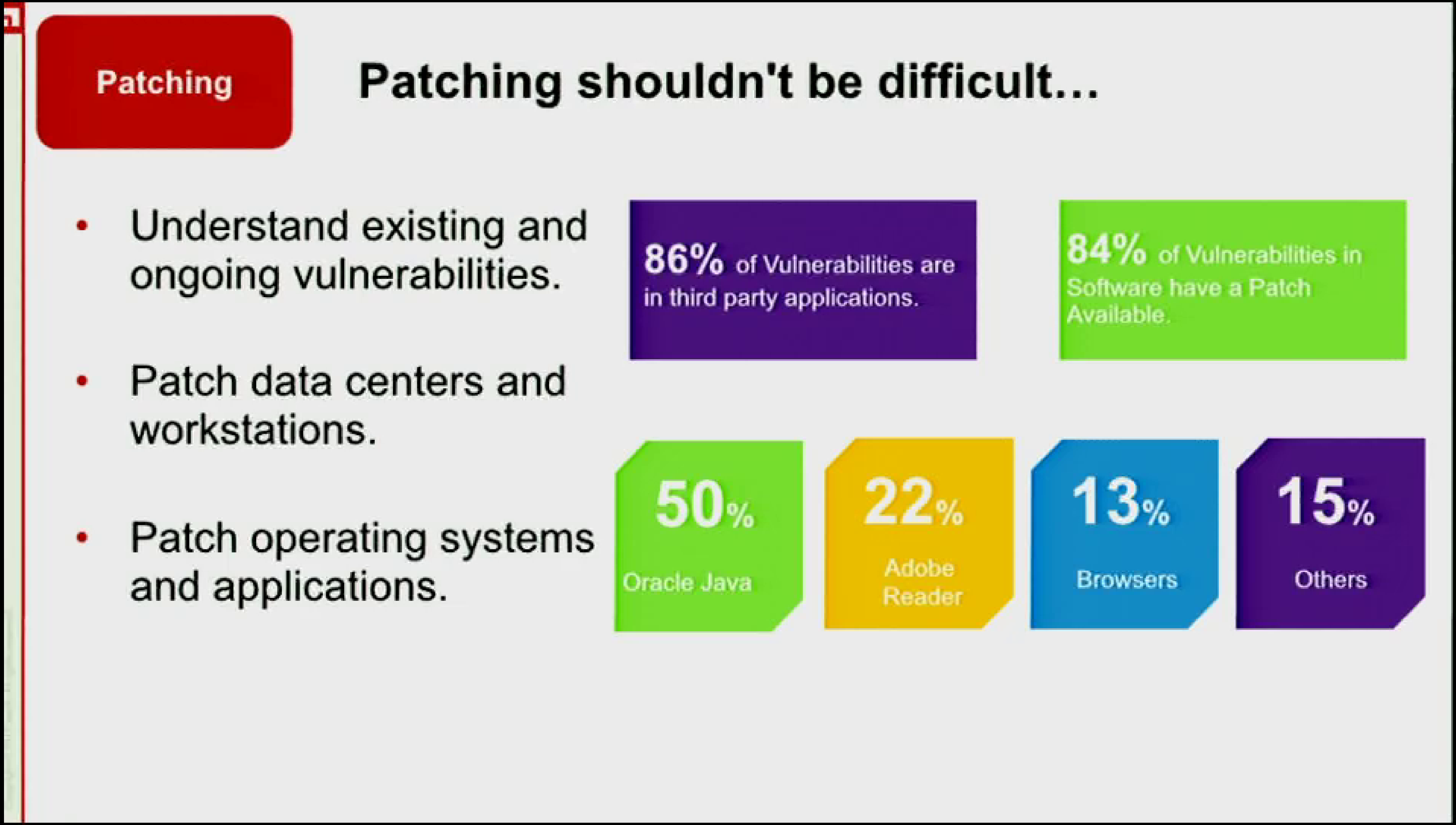
“You don’t know what you don’t know”

- Device-based discovery
- Software asset management
- Authorized and unauthorized application usage
- Administrative rights discovery
- Data discovery



	Type
D_CA	Virtual Server
dams-apple	MAC
Admins-MacBook-Pro	MAC
admins-mbp-2	MAC
Alexs main ipad	MobileDevice
ANDERSON-WIN7	Virtual Workstation
ASUS Transformer P...	MobileDevice
BEJ_YONSHENGLI1	Server
BEJ-365TEST	Virtual Workstation
BEJ-AOSHEN	Workstation
BEJ-BEIYANC2	Server
BEJ-CaoZhi-MacBoo...	MAC
BEJ-CUNMING01	Server
BEJ-DATA001	Server
BEJ-DATA002	Server
BEJ-DENNIS-W1	Workstation
-DOUJIANSHUN	Workstation
ONMACVM	Virtual Wor

Secure



Patching

Patching shouldn't be difficult…

- Understand existing and ongoing vulnerabilities.
- Patch data centers and workstations.
- Patch operating systems and applications.

86% of Vulnerabilities are in third party applications.

84% of Vulnerabilities in Software have a Patch Available.

50% Oracle Java

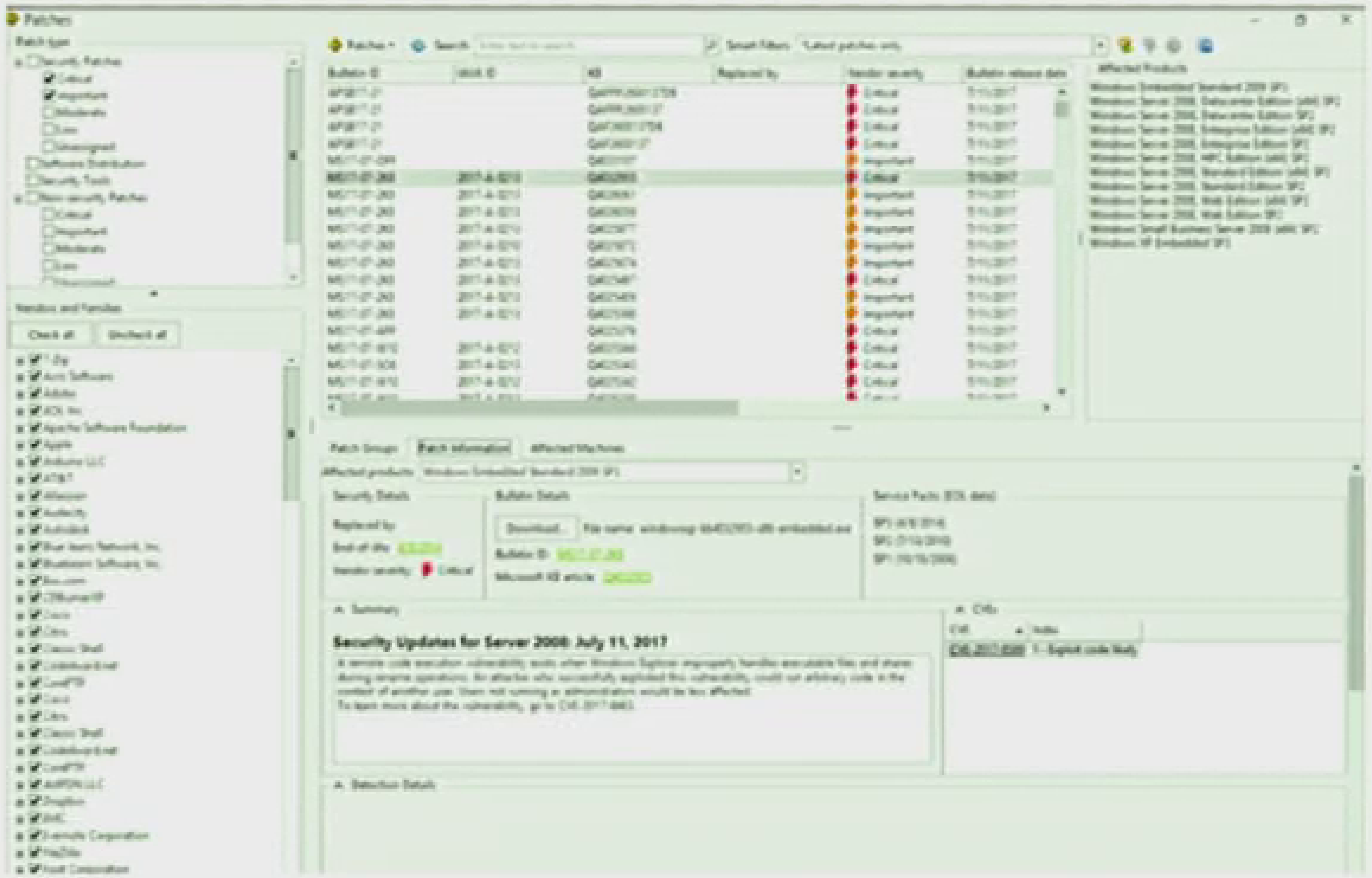
22% Adobe Reader

13% Browsers

15% Others

Patching

- Simple
- Automated
- Multiple OS support
- Large 3rd-party app support
- SCCM integration

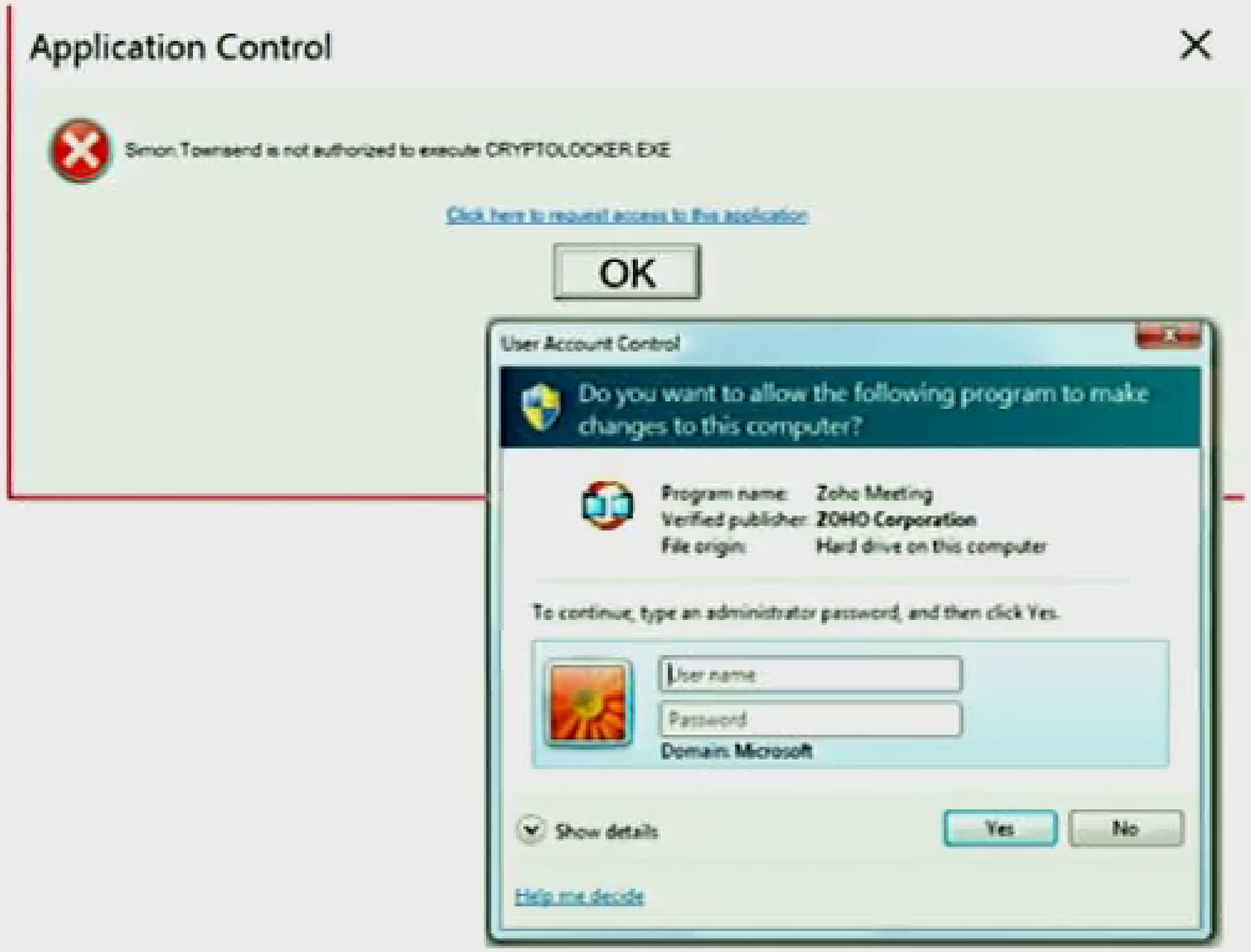


Security Updates for Server 2008: July 11, 2017

App Control

Application Control is Essential

- Prevent unknown ransomware
- Only allow apps to run that were installed by a trusted user
- Control both authorized and unauthorized software
- Raise, lower, or eliminate privileges on a per-user, application at a granular policy level



Application Control

Simon Townsend is not authorized to execute CRYPTOLOCKER.EXE

Click here to request access to this application

User Account Control

Do you want to allow the following program to make changes to this computer?

Program name: Zoho Meeting
Verified publisher: ZOHO Corporation
File origin: Hard drive on this computer

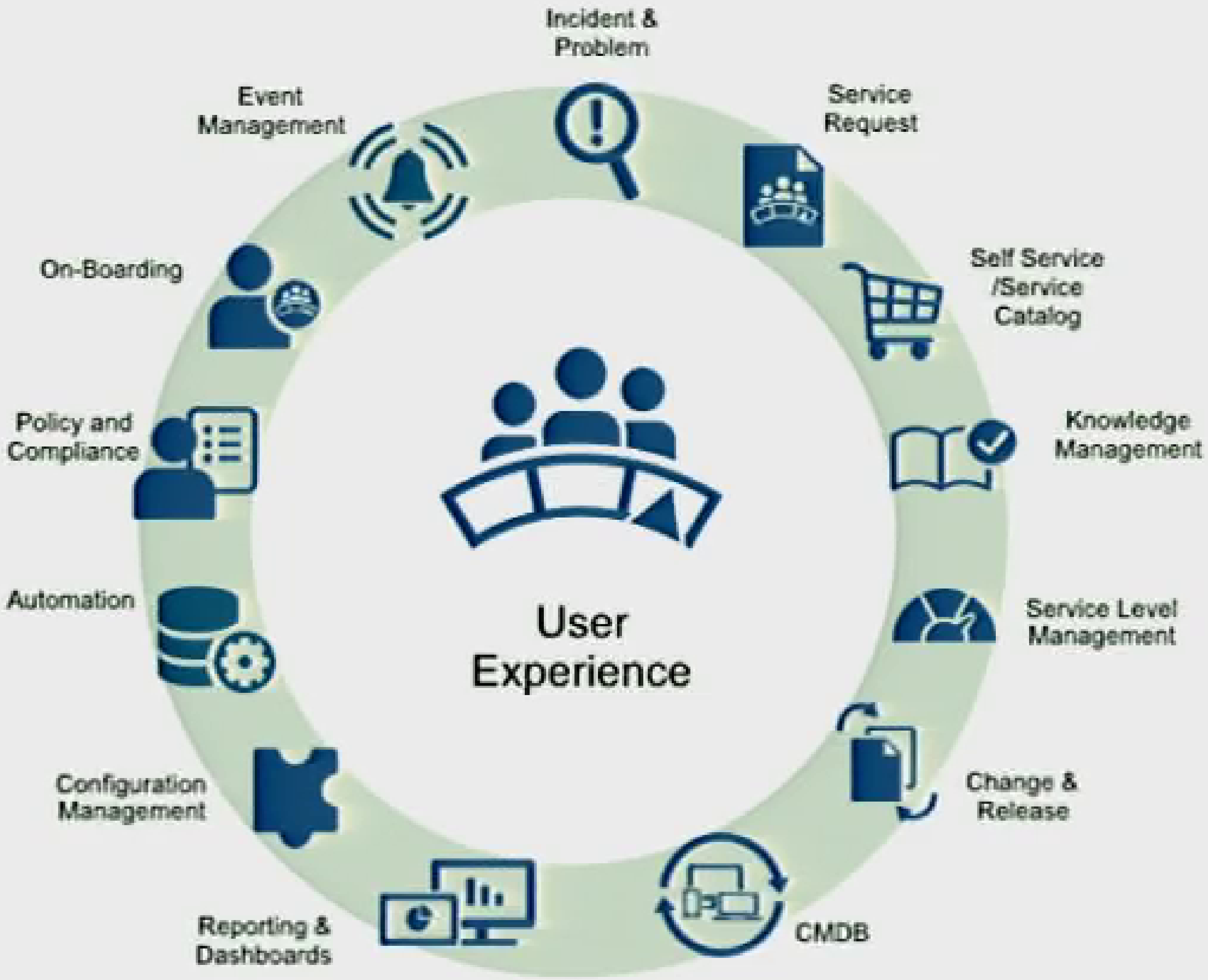
To continue, type an administrator password, and then click Yes.

Domain: Microsoft

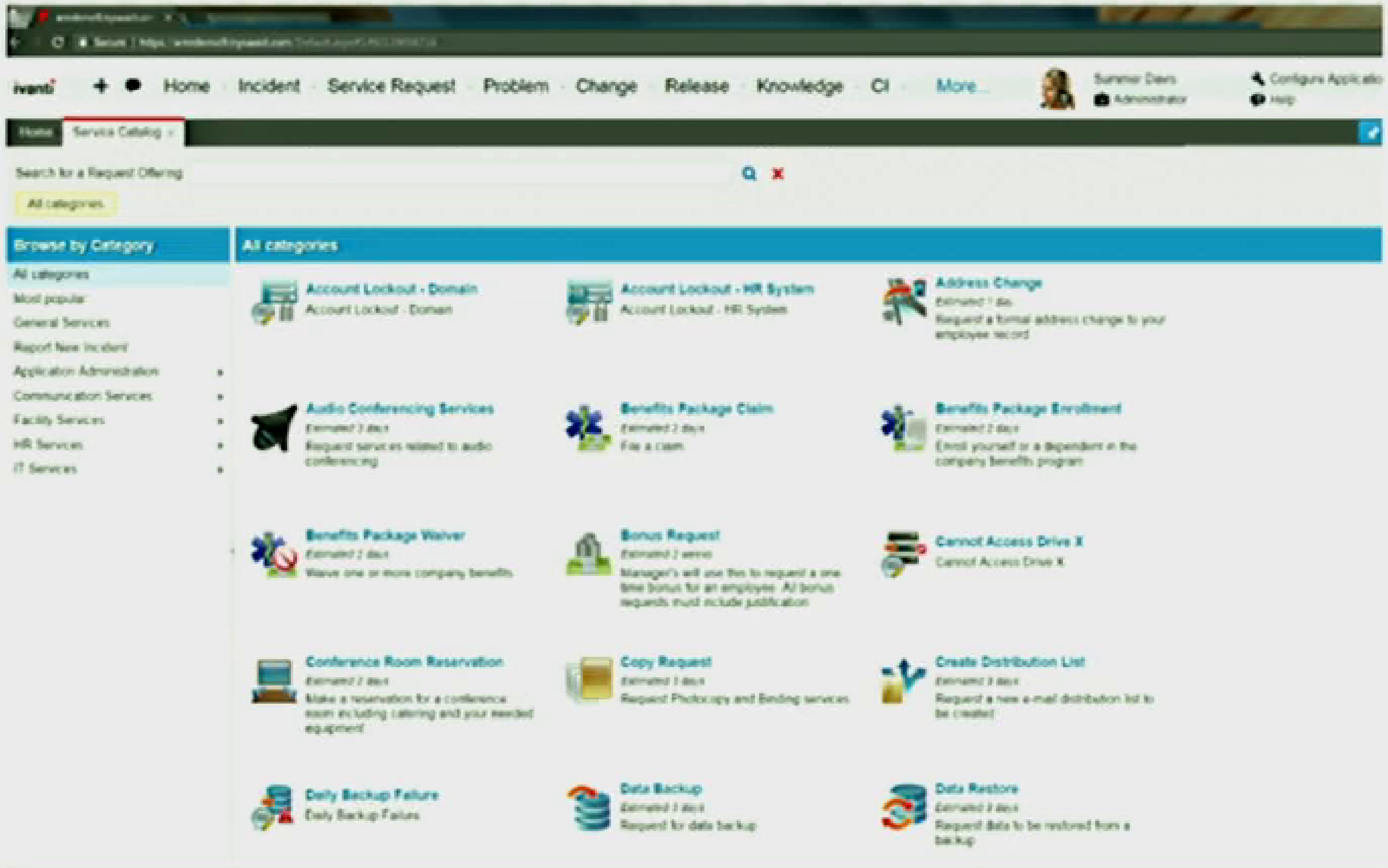
Service Management

Service Management

- Respond to PII requests
- Automate workflows
- Audit requests and changes
- Respond and automate should a breach occur



Service Management



All categories

Account Lockout - Domain
Account Lockout - Domain

Account Lockout - HR System
Account Lockout - HR System

Address Change
Estimated 1 day
Request a formal address change to your employee record

Audio Conferencing Services
Estimated 3 days
Request services related to audio conferencing

Benefits Package Claim
Estimated 2 days
File a claim

Benefits Package Enrollment
Estimated 2 days
Enroll yourself or a dependent in the company benefits program

Benefits Package Waiver
Estimated 2 days
Waive one or more company benefits

Bonus Request
Estimated 2 weeks
Manager's will use this to request a one time bonus for an employee. All bonus requests must include justification

Cannot Access Drive X
Cannot Access Drive X

Conference Room Reservation
Estimated 2 days
Make a reservation for a conference room including catering and your needed equipment

Copy Request
Estimated 1 days
Request Photocopy and Binding services

Create Distribution List
Estimated 3 days
Request a new e-mail distribution list to be created

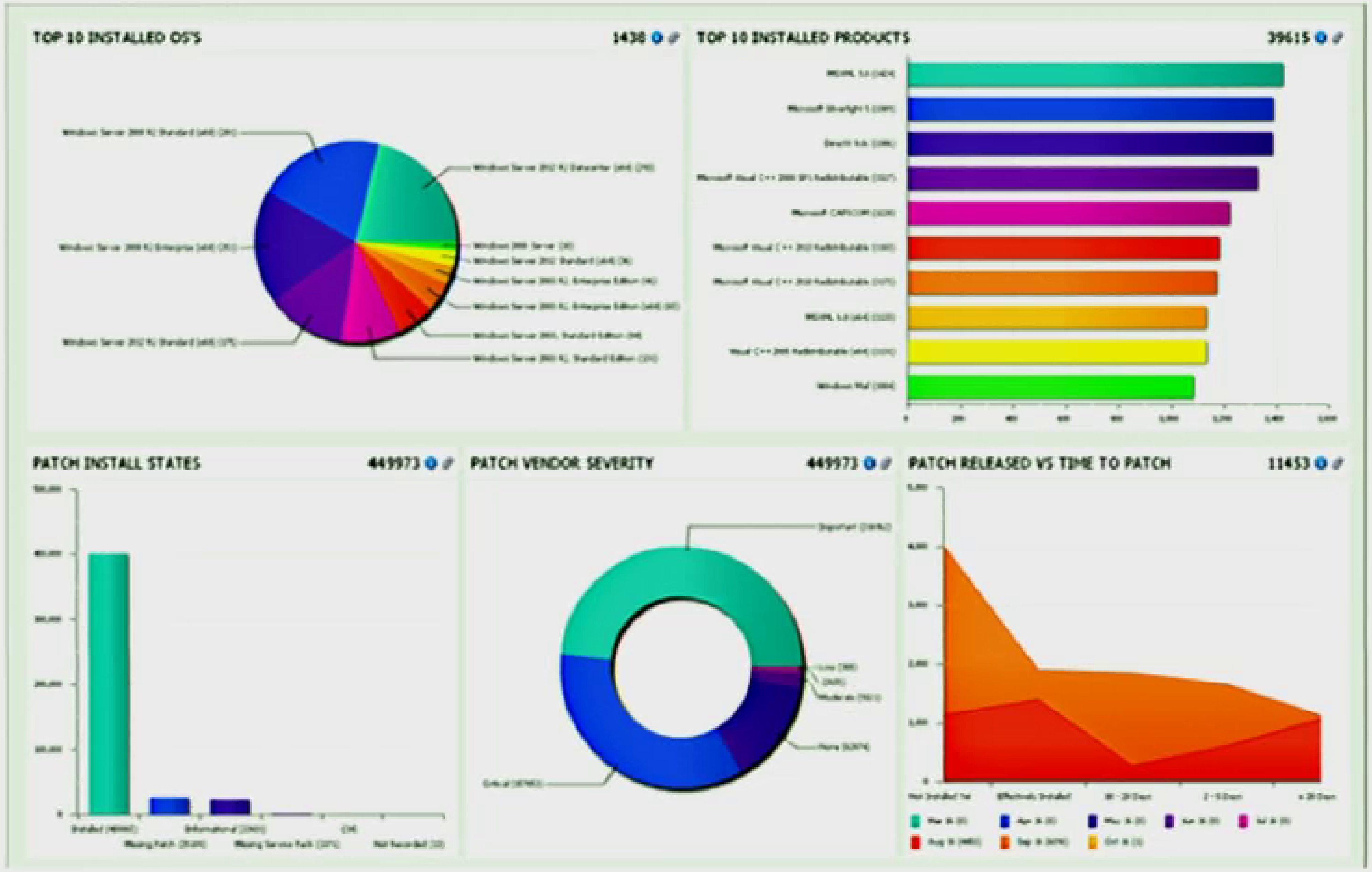
Daily Backup Failure
Daily Backup Failure

Data Backup
Estimated 1 days
Request for data backup

Data Restore
Estimated 3 days
Request data to be restored from a backup

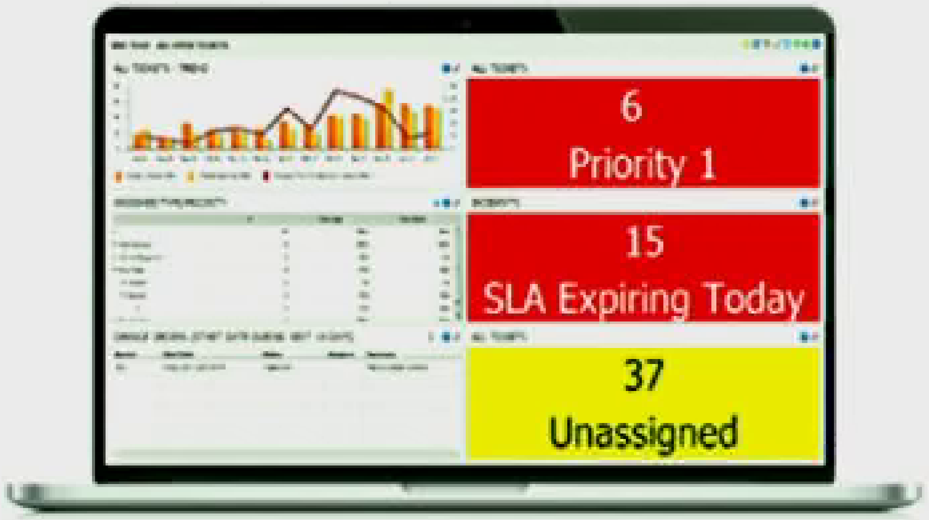
A powerful automation engine, on premises or SaaS…

Visibility

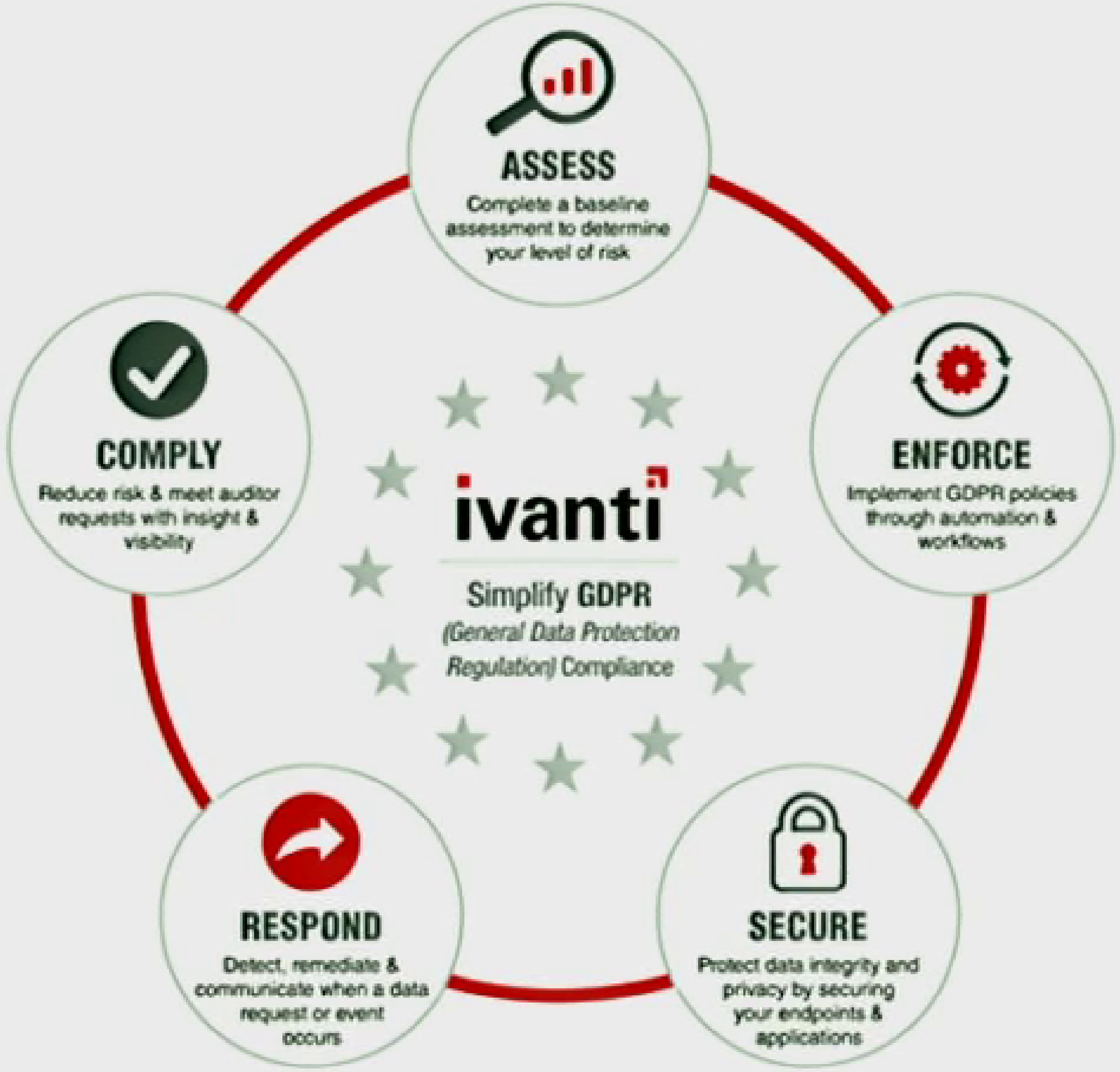

TOP 10 INSTALLED OS'S
1438
Windows Server 2008 R2 Standard (x64)
Windows Server 2012 R2 Datacenter (x64)
Windows Server 2008 R2 Enterprise (x64)
Windows 2000 Server
Windows Server 2012 Standard (x64)
Windows Server 2003 R2, Enterprise Edition
Windows Server 2003 R2, Enterprise Edition (x64)
Windows Server 2003, Standard Edition
Windows Server 2012 R2 Standard (x64)
Windows Server 2003 R2, Standard Edition
TOP 10 INSTALLED PRODUCTS
39615
MSXML 3.0
Microsoft Silverlight 5
DirectX 9.0c
Microsoft Visual C++ 2005 SP1 Redistributable
Microsoft CAPICOM
Microsoft Visual C++ 2012 Redistributable
Microsoft Visual C++ 2010 Redistributable
MSXML 6.0 (x64)
Visual C++ 2005 Redistributable (x64)
Windows Mail
0
200
400
600
800
1,000
1,200
1,400
1,600
PATCH INSTALL STATES
449973
50,000
40,000
30,000
20,000
10,000
0
Installed
Missing Patch
Informational
Missing Service Pack
CVE
Not Recorded
PATCH VENDOR SEVERITY
449973
Important
Low
Moderate
None
Critical
PATCH RELEASED VS TIME TO PATCH
11453
5,000
4,000
3,000
2,000
1,000
0
Not Installed Yet
Effectively Installed
10 - 20 Days
2 - 5 Days
> 20 Days
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct

Reporting and Analytics

- Stop depending on specialized staff for dashboards and use self-service access
- Gain comprehensive insights—view IT status, track performance, and assess risks to take action
- Find lost assets, unused services, or vulnerable devices via real-time views



Strategy



ivanti

Simplify GDPR

(General Data Protection Regulation) Compliance

ASSESS

Complete a baseline assessment to determine your level of risk

ENFORCE

Implement GDPR policies through automation & workflows

SECURE

Protect data integrity and privacy by securing your endpoints & applications

RESPOND

Detect, remediate & communicate when a data request or event occurs

COMPLY

Reduce risk & meet auditor requests with insight & visibility

Summary

- GDPR is happening, although it’s not a point in time.
- There is no one-solution fix.
- It’s more than just a technology challenge.
- Understanding and Securing PII data is key.
- Protecting users and endpoints is fundamental.

Thank You

ivanti