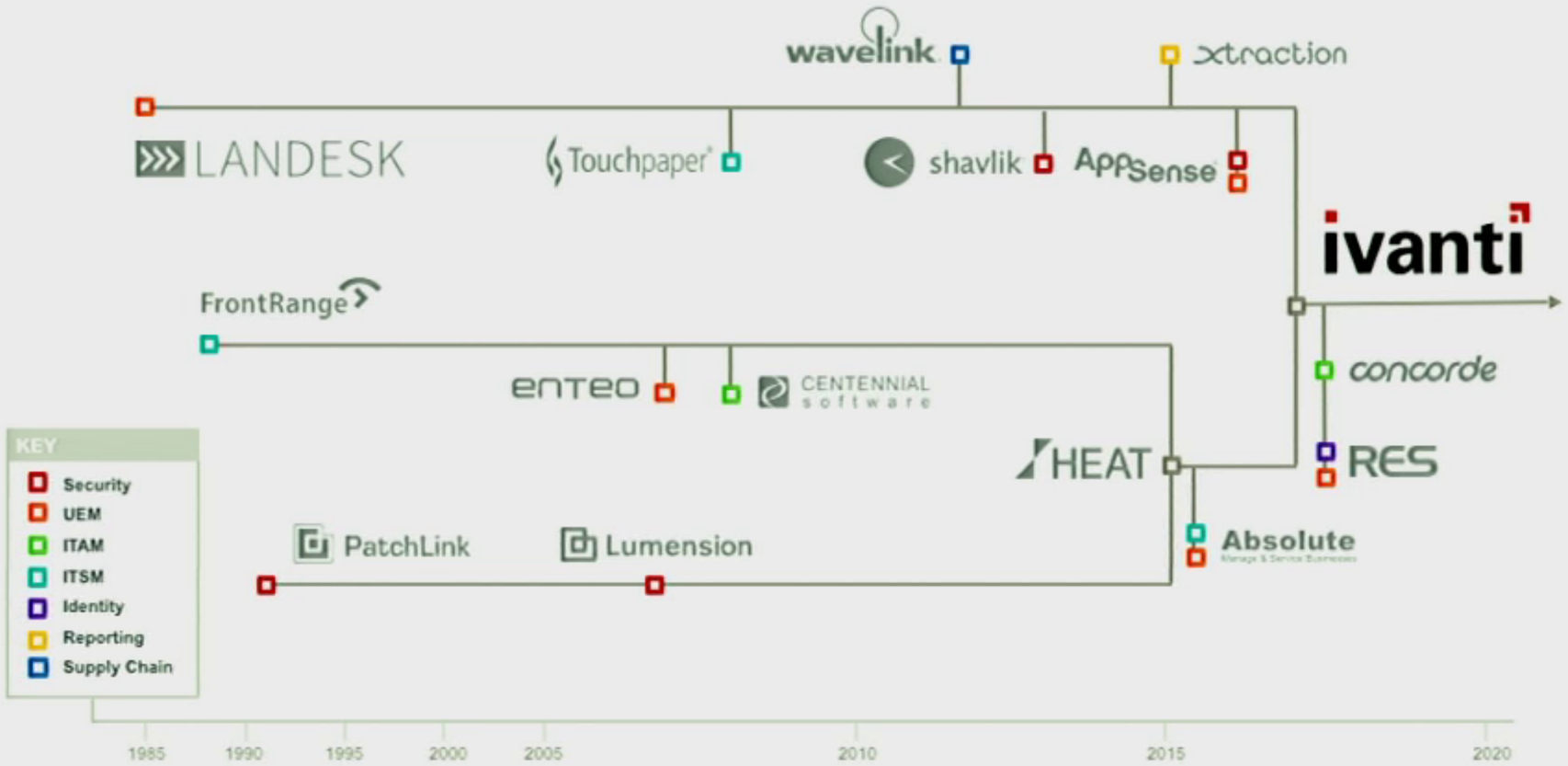
ivanti

How Ivanti can help minimize the headaches around GDPR

Tamas Szalai, pre-sales engineer

RelNet Technológia Kft.

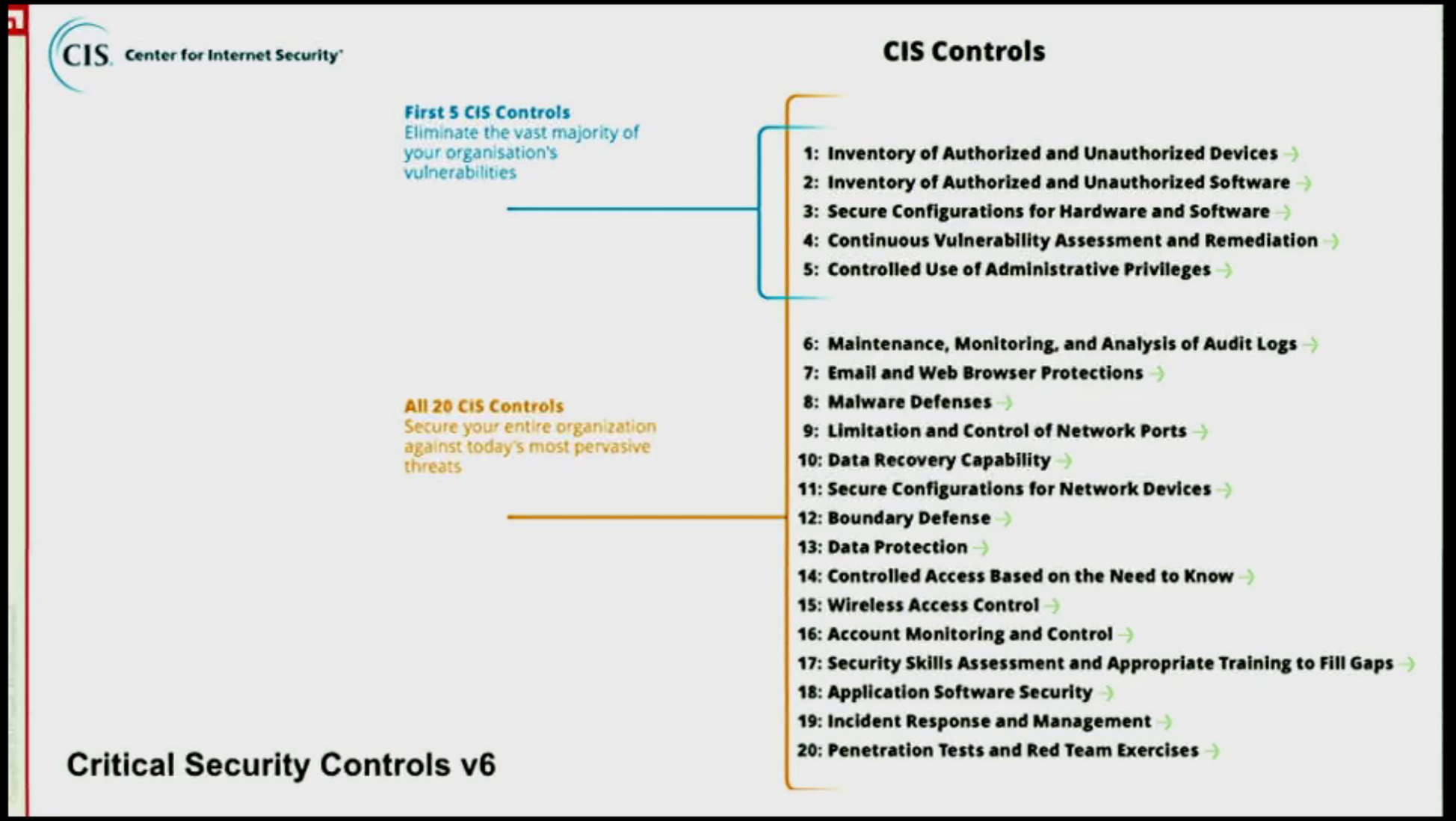
Ivanti DNA


wavelink
xtraction
LANDESK
Touchpaper
shavlik
AppSense
ivanti
FrontRange
concorde
enteo
CENTENNIAL software
HEAT
RES
KEY
Security
UEM
ITAM
ITSM
Identity
Reporting
Supply Chain
PatchLink
Lumension
Absolute
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
All 20 CIS Controls
Secure your entire organization against today's most pervasive threats
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
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

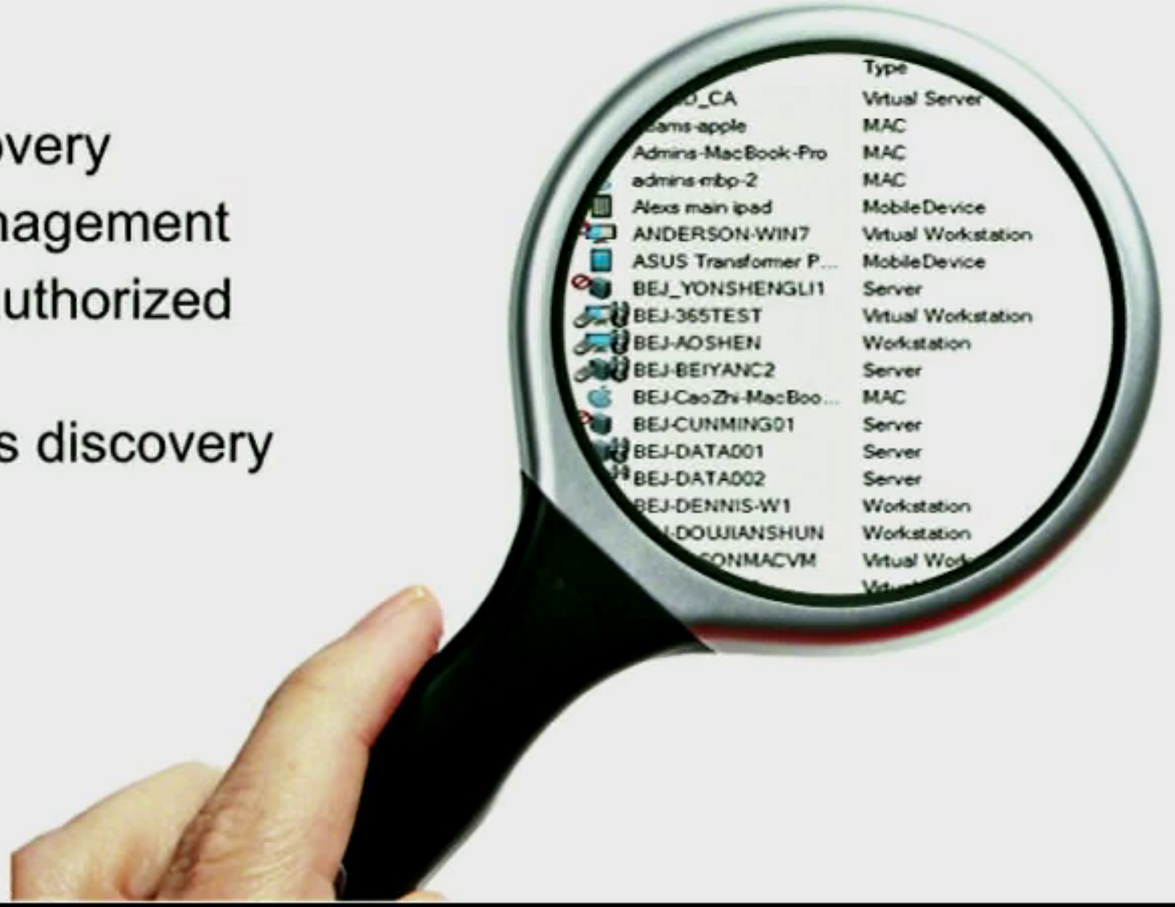
FEDERAL BUREAU OF INVESTIGATION · DEPARTMENT OF JUSTICE

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



Secure

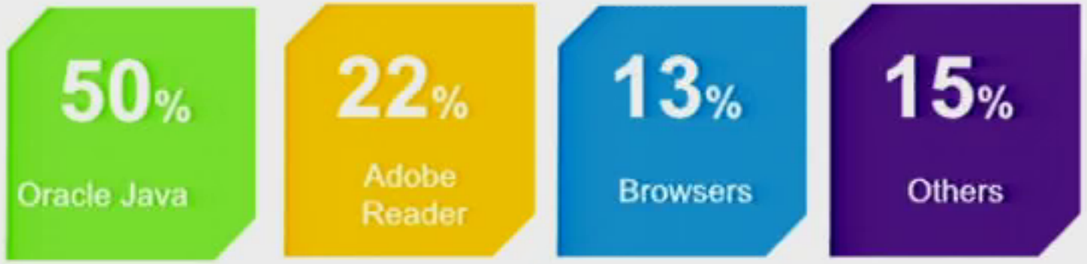
Patching

Patching shouldn't be difficult…

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

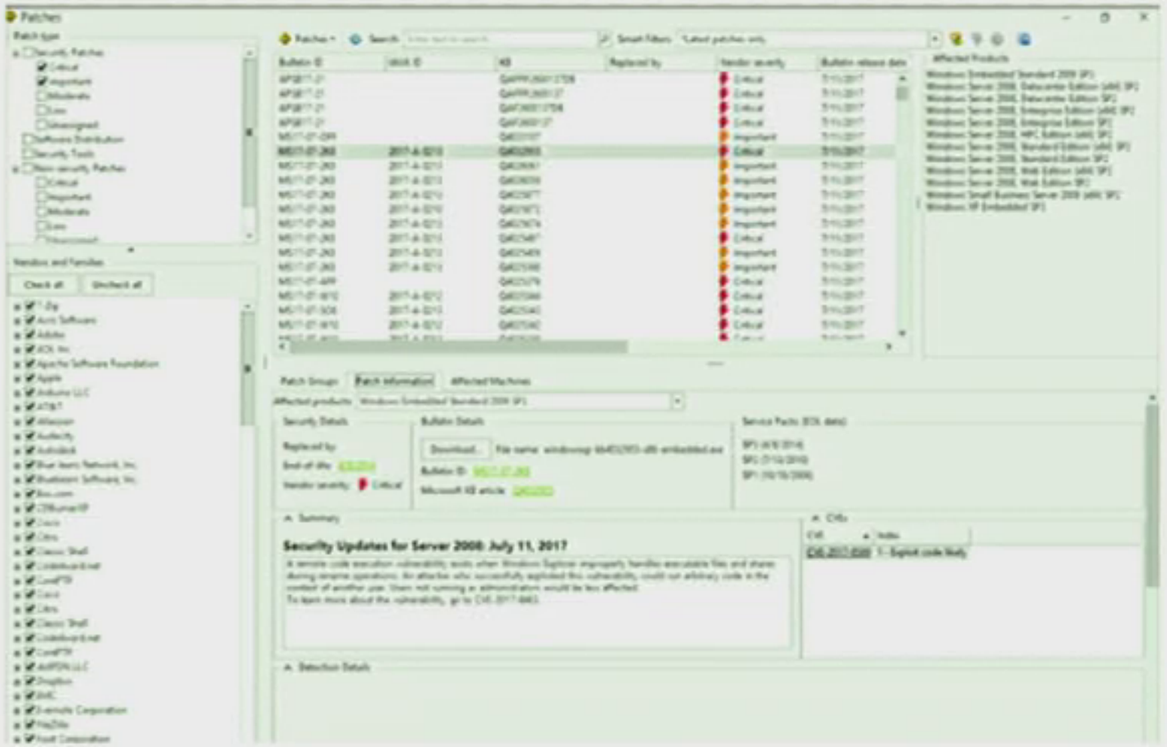
86% of Vulnerabilities are in third party applications.

84% of Vulnerabilities in Software have a Patch Available.



Patching

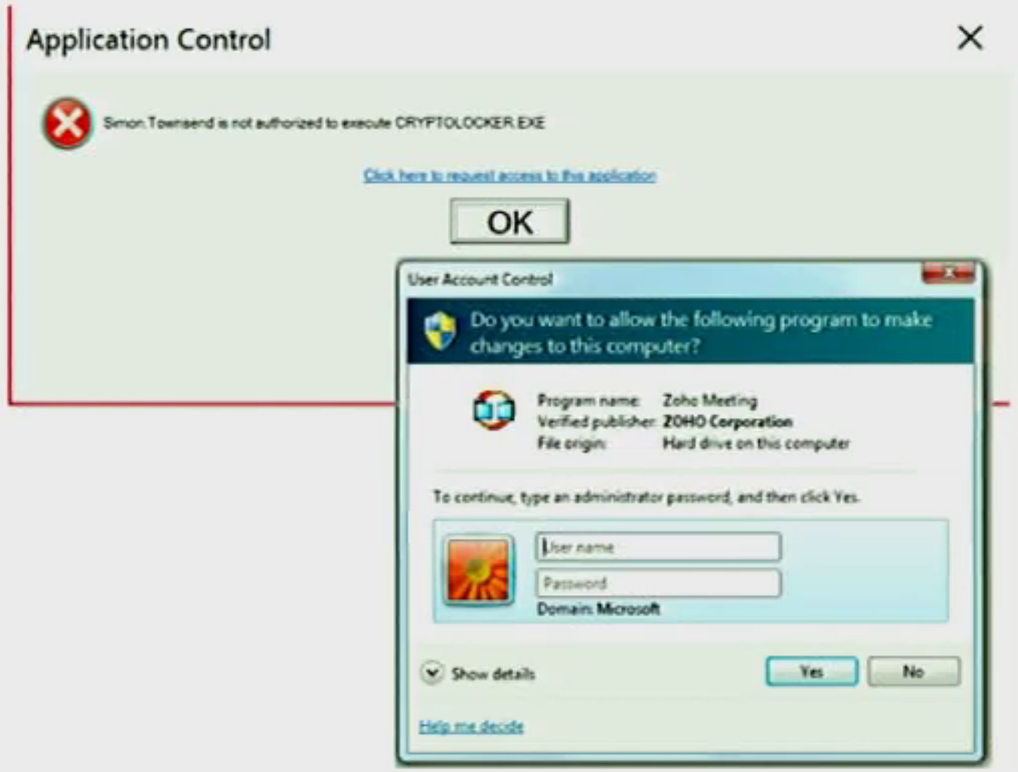
- Simple
- Automated
- Multiple OS support
- Large 3rd-party app support
- SCCM integration



App Control

Application Control is Essential

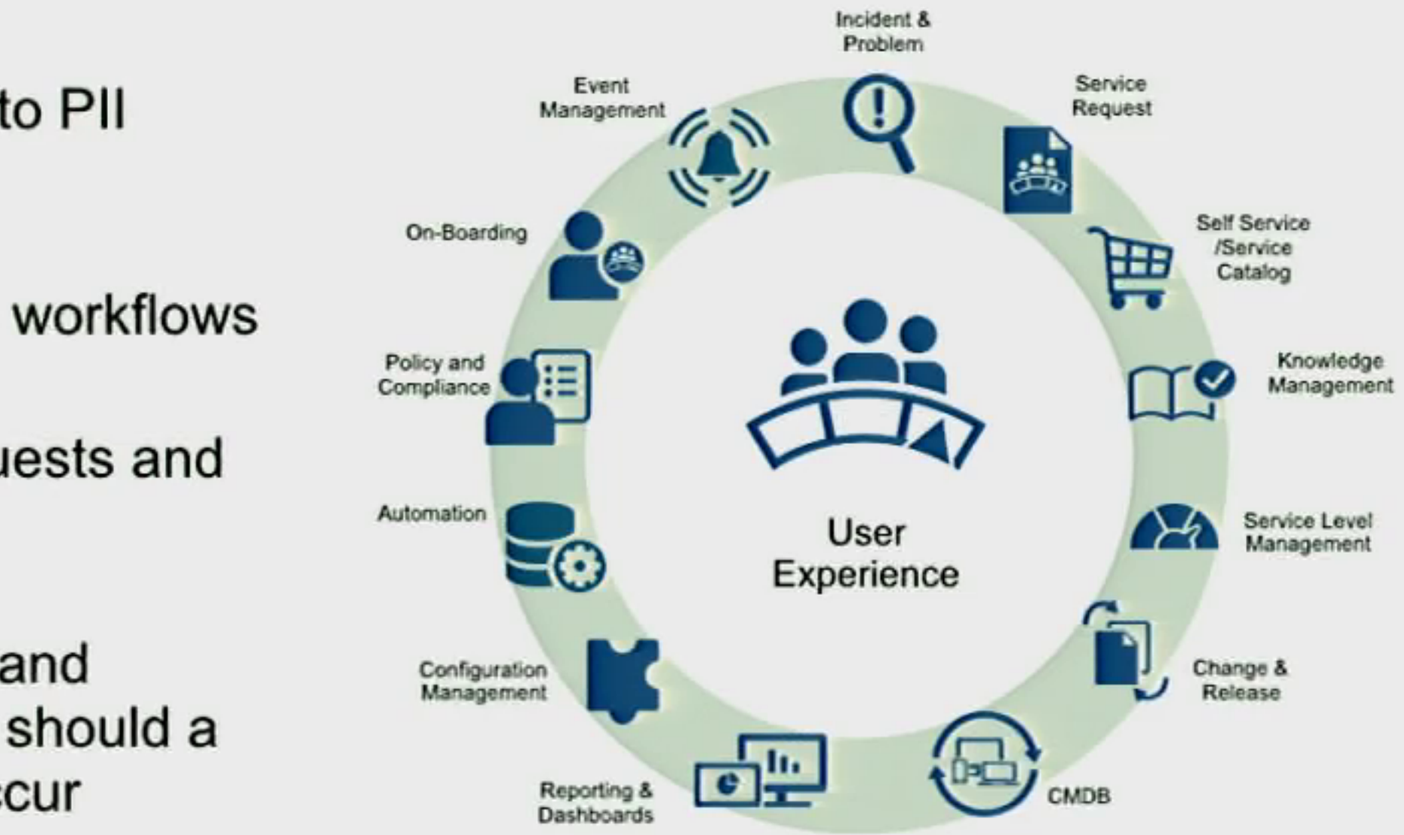
- Prevent unknown ransomware
- Only allow apps to run that were installed by a trusted user
- Control both authorized and unauthorized software
- Raise, lower, or eliminate privileges on a per-user, application at a granular policy level



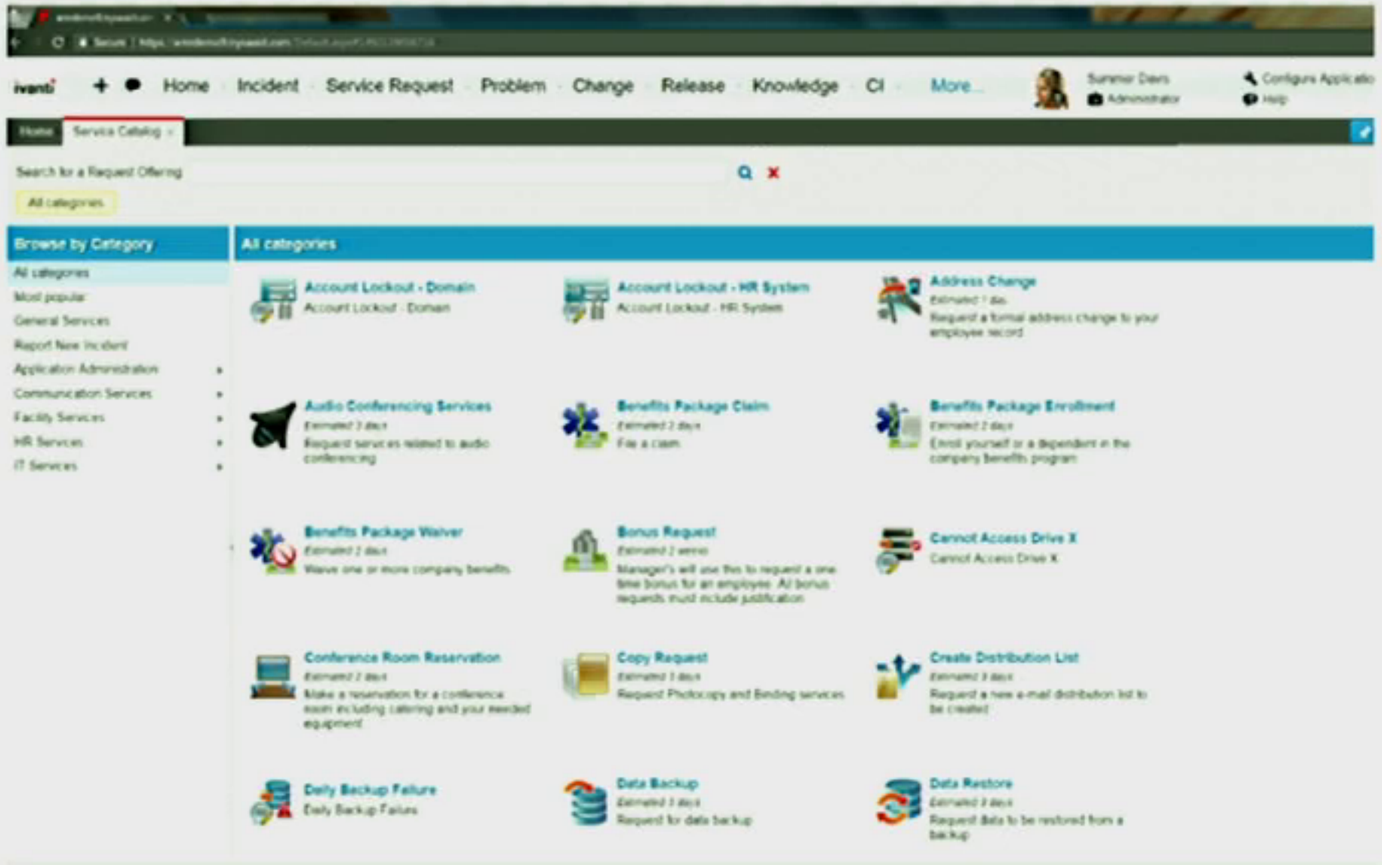
Service Management

Service Management

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



Service Management



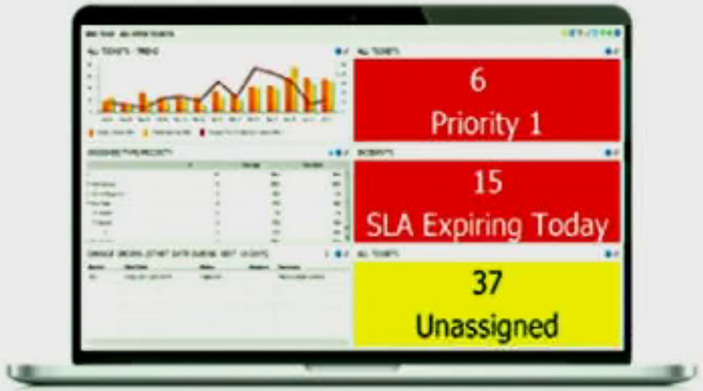
A powerful automation engine, on premises or SaaS…

Visibility

TOP 10 INSTALLED OS'S
1438
TOP 10 INSTALLED PRODUCTS
39615
PATCH INSTALL STATES
449973
PATCH VENDOR SEVERITY
449973
PATCH RELEASED VS TIME TO PATCH
11453

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

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
ivanti
Simplify GDPR
(General Data Protection Regulation) Compliance

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