Viaggio al centro di un asset

da visibilità a consapevolezza

Marco Rottigni
Chief Technical Security Officer EMEA
Qualys

Ilaria Comelli
Responsabile UO Sicurezza e Processi IT
Università di Parma

UNIVERSITÀ DI PARMA

Viaggio al centro di un asset

il percorso verso una soluzione

Parma, 14 novembre 2019

Ilaria Comelli

2016 Anno Zero


Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri
Area Sistemi, tecnologie e sicurezza informatica

MISURE MINIME DI SICUREZZA ICT

PER LE PUBBLICHE AMMINISTRAZIONI

(Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015)

26 APRILE 2016

GDPR art. 32 Sicurezza del trattamento

1. Tenendo conto dello **stato dell'arte** e dei **costi di attuazione**, nonché della **natura**, **dell'oggetto**, del **contesto** e delle **finalità del trattamento**, come anche del **rischio** di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire **un livello di sicurezza adeguato al rischio**, che comprendono, tra le altre, se del caso:

a) la **pseudonimizzazione** e la **cifratura** dei dati personali;
b) la capacità di assicurare su base permanente la **riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;**
c) la capacità di **ripristinare tempestivamente la disponibilità e l'accesso** dei dati personali in caso di incidente fisico o tecnico;
d) una **procedura per testare, verificare e valutare** regolarmente **l'efficacia** delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento

2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla **distruzione**, dalla **perdita**, dalla **modifica**, dalla **divulgazione non autorizzata** o **dall'accesso, in modo accidentale o illegale, a dati personali** trasmessi, conservati o comunque trattati.

Misure Minime AGID

1. GENERALITÀ.

1.1. SCOPO.

Il presente documento contiene le misure minime di sicurezza ICT per le pubbliche amministrazioni le quali costituiscono parte integrante delle linee guida per la sicurezza ICT delle pubbliche amministrazioni.

.....

La scelta di prendere le mosse dall'insieme di controlli noto come SANS 20, oggi pubblicato dal Center for Internet Security come CCSC «CIS Critical Security Controls for Effective Cyber Defense» nella versione 6.0 di ottobre 2015, trova giustificazione, oltre che nella larga diffusione ed utilizzo pratico, dal fatto che esso nasce con una particolare sensibilità per i costi di vario genere che l'implementazione di una misura di sicurezza richiede, ed i benefici che per contro è in grado di offrire. L'elenco dei venti controlli in cui esso si articola, normalmente riferiti come Critical Security Control (CSC), è ordinato sulla base dell'impatto sulla sicurezza dei sistemi; per cui ciascun controllo precede tutti quelli la cui implementazione innalza il livello di sicurezza in misura inferiore alla sua. È comune convinzione che i primi cinque controlli siano quelli indispensabili per assicurare il minimo livello di protezione nella maggior parte delle situazioni e da questi si è partiti per stabilire le misure minime di sicurezza per la pubblica amministrazione italiana, avendo ben presente le enormi differenze di dimensioni, mandato, tipologie di informazioni gestite, esposizione al rischio, e quant'altro caratterizza le oltre ventimila amministrazioni pubbliche.

Misure Minime: da dove vengono

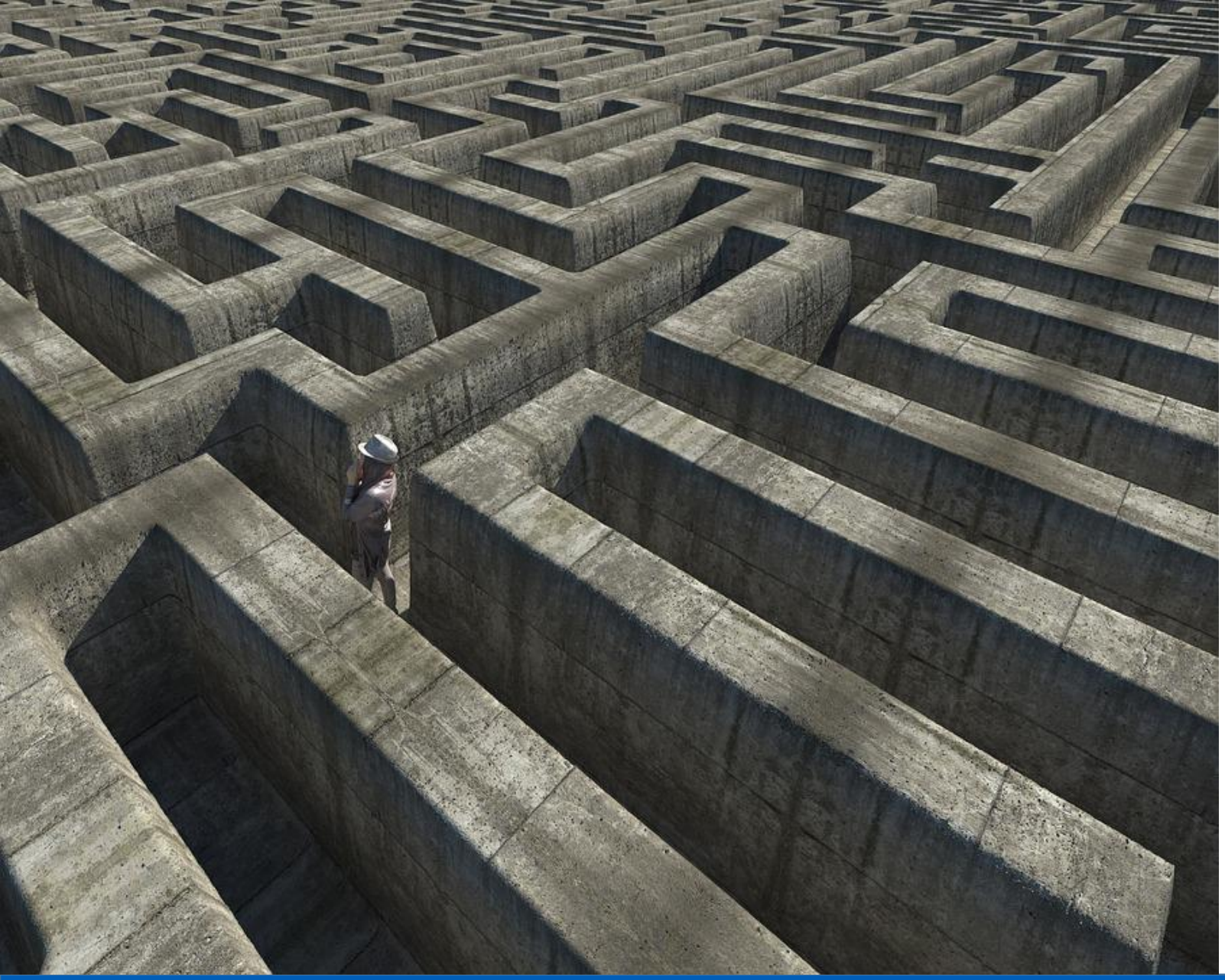
CIS: i primi 5 controlli

- **Inventory** of Authorized and Unauthorized **Devices**
- **Inventory** of Authorized and Unauthorized **Software**
- **Secure Configurations** for Hardware and Software
- **Continuous Vulnerability Assessment** and Remediation
- **Controlled** Use of Administrative **Privileges**

Fonte: https://www.cisecurity.org/controls/

Misure Minime AGID

- inventario dei dispositivi autorizzati e non autorizzati
- inventario del software autorizzato e non autorizzati
- configurazione sicura di hardware e software
- adozione di un processo di gestione continua delle vulnerabilità
- utilizzo controllato dei privilegi amministrativi
- adozione di difese contro i programmi malware
- capacità di recuperare l'operatività in caso di incidente, ovvero Business Continuity
- protezione dei dati attraverso l’adozione di idonee misure di sicurezza



Come definire le priorità?

Da dove cominciare?

Chi siamo? Qualche numero

27.709
Studenti

848
Docenti

854
Personale T.A.

13
Sedi

35
Plessi

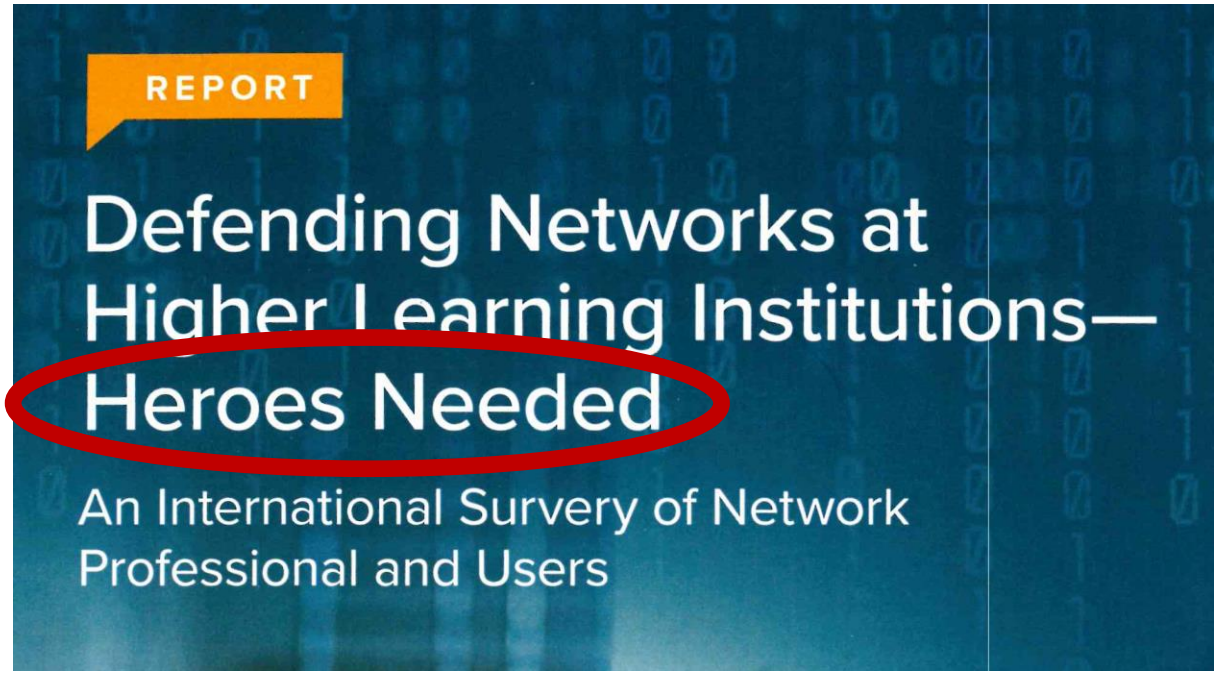
1,6 Gbps
Banda utilizzata

135
Subnet attive

7k circa
Dispositivi connessi

Chi siamo? Categorie di utenti

- Docenti
  - Professori Ordinari
  - Professori Associati
  - Ricercatori
  - Docenti a contratto
  - Professori emeriti
  - Professori onorari
- Personale Tecnico Amministrativo
- Dottorandi
- Borsisti di ricerca
- Assegnisti di ricerca
- Specializzandi
- Studenti
  - Iscritti UniPR
  - Erasmus
  - interateneo
- Collaboratori
- Fornitori



Criticità

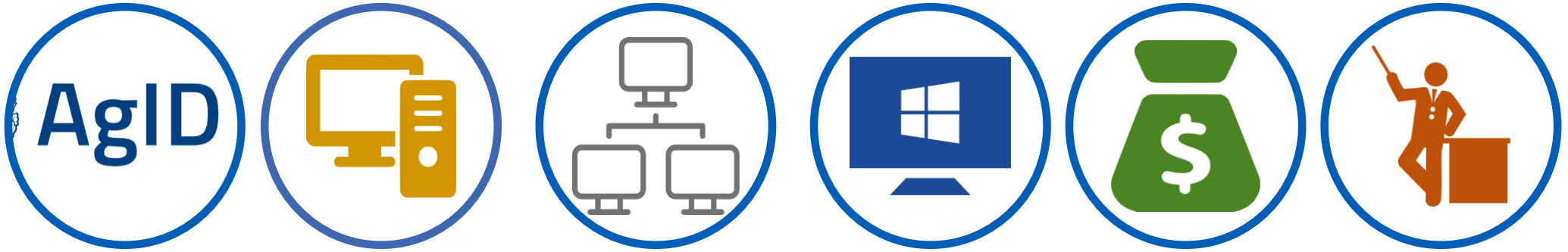

Utenti diversi
Prassi stratificate nel tempo
Numerosità ed eterogeneità dei punti di accesso
Scarsa consapevolezza dei rischi

Equilibrio da trovare

Sicurezza
dei dati

Libertà
della ricerca

Come scegliere le soluzioni



ambiti misure minime coperti

azioni su endpoint

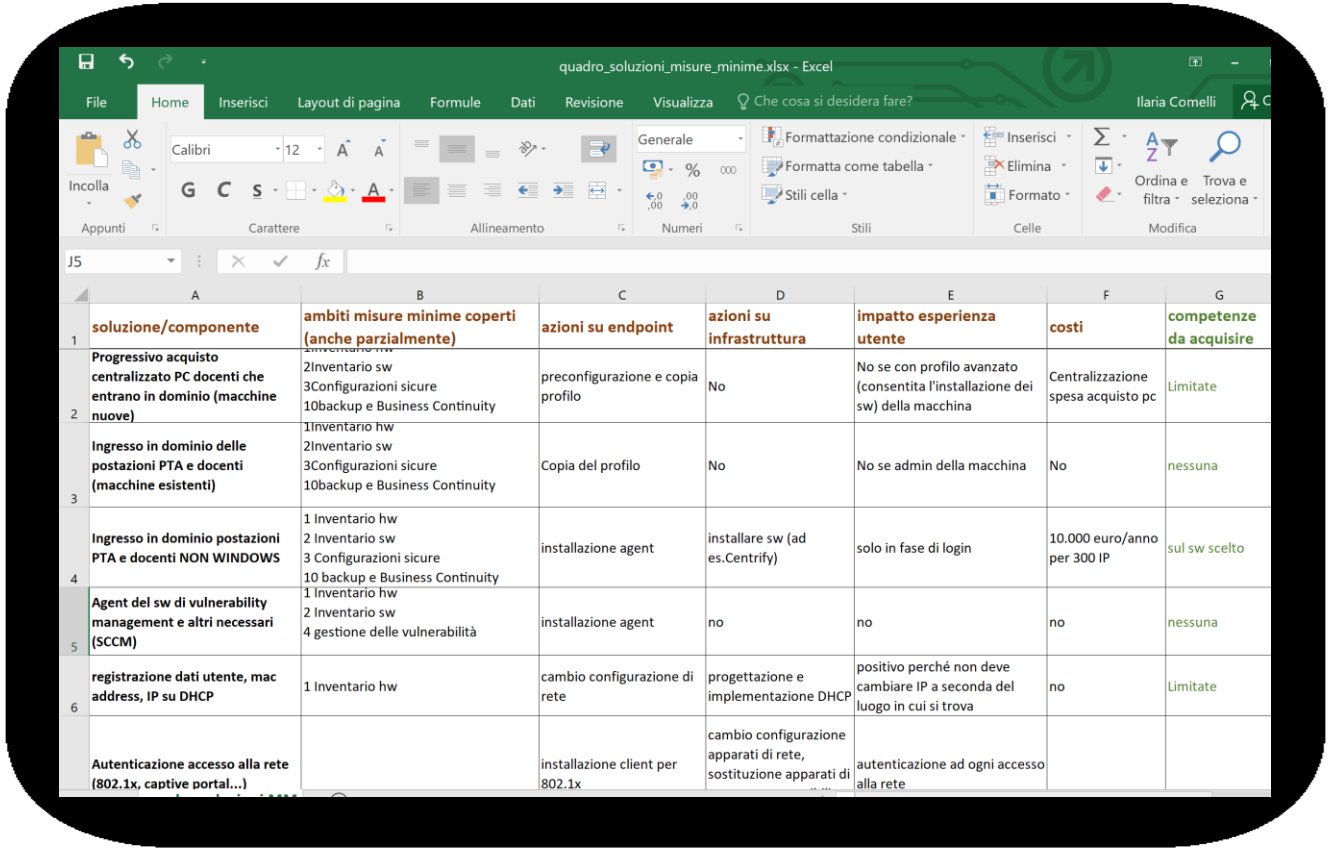
azioni su infrastruttura

impatto esperienza utente

costi

competenze da acquisire

Come scegliere le soluzioni



	A	B	C	D	E	F	G
1	soluzione/componente	ambiti misure minime coperti (anche parzialmente)	azioni su endpoint	azioni su infrastruttura	impatto esperienza utente	costi	competenze da acquisire
2	Progressivo acquisto centralizzato PC docenti che entrano in dominio (macchine nuove)	2Inventario sw 3Configurazioni sicure 10backup e Business Continuity	preconfigurazione e copia profilo	No	No se con profilo avanzato (consentita l'installazione dei sw) della macchina	Centralizzazione spesa acquisto pc	Limitate
3	Ingresso in dominio delle postazioni PTA e docenti (macchine esistenti)	1Inventario hw 2Inventario sw 3Configurazioni sicure 10backup e Business Continuity	Copia del profilo	No	No se admin della macchina	No	nessuna
4	Ingresso in dominio postazioni PTA e docenti NON WINDOWS	1 Inventario hw 2 Inventario sw 3 Configurazioni sicure 10 backup e Business Continuity	installazione agent	installare sw (ad es.Centrify)	solo in fase di login	10.000 euro/anno per 300 IP	sul sw scelto
5	Agent del sw di vulnerability management e altri necessari (SCCM)	1 Inventario hw 2 Inventario sw 4 gestione delle vulnerabilità	installazione agent	no	no	no	nessuna
6	registrazione dati utente, mac address, IP su DHCP	1 Inventario hw	cambio configurazione di rete	progettazione e implementazione DHCP	positivo perché non deve cambiare IP a seconda del luogo in cui si trova	no	Limitate
	Autenticazione accesso alla rete (802.1x, captive portal...)		installazione client per 802.1x	cambio configurazione apparati di rete, sostituzione apparati di	autenticazione ad ogni accesso alla rete		

Inventario vs Gestione degli asset

- Indirizzo IP
- Localizzazione
- Tipologia hardware
- Elenco software
- Vulnerabilità
- Stato di salute

UNIVERSITÀ DI PARMA

Viaggio al centro di un asset

Dalla Visibilità alla Consapevolezza

Marco Rottigni
Chief Technical Security Officer EMEA
Qualys

Ilaria Comelli
Responsabile UO Sicurezza, Processi IT
Università di Parma

Cosa è stato realizzato?

CLOUD-BASED ARCHITECTURE

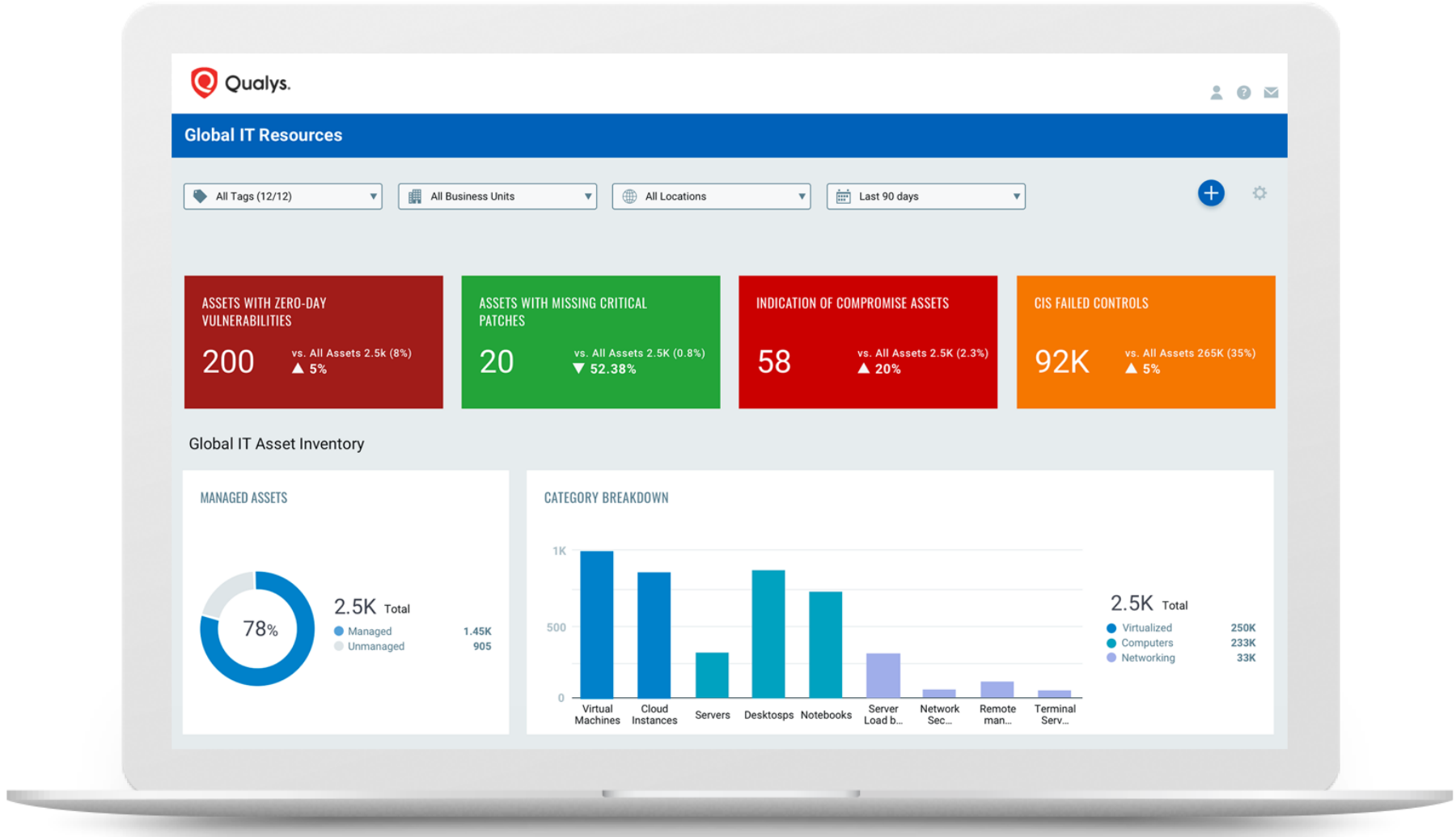
UNIVERSITÀ DI PARMA

Qualys.

Occhi e Cervello

UNIVERSITÀ DI PARMA

Qualys.



UNIVERSITÀ DI PARMA

Qualys.

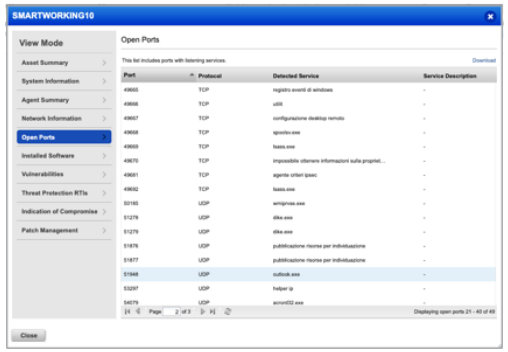
Il valore aggiunto di un Partner

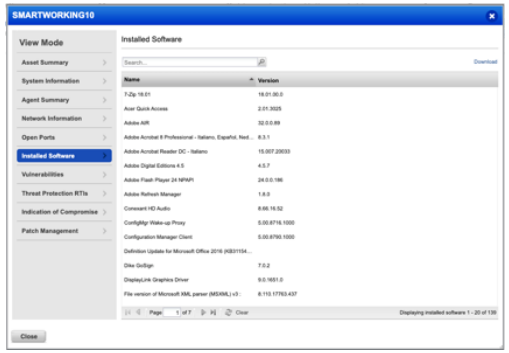
- Competenza
- Agilità nella messa in opera
- Supporto operativo

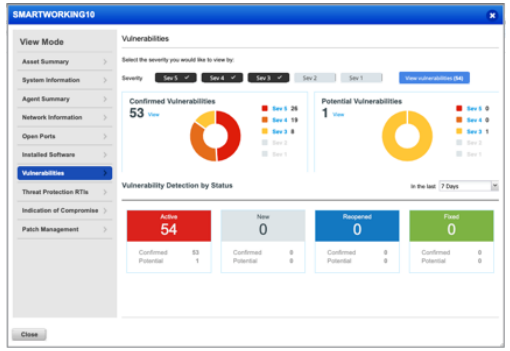
UNIVERSITÀ DI PARMA

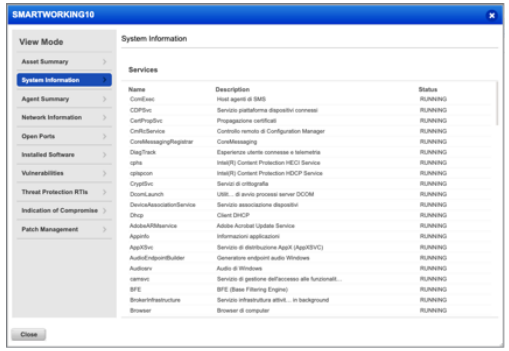
Qualys.

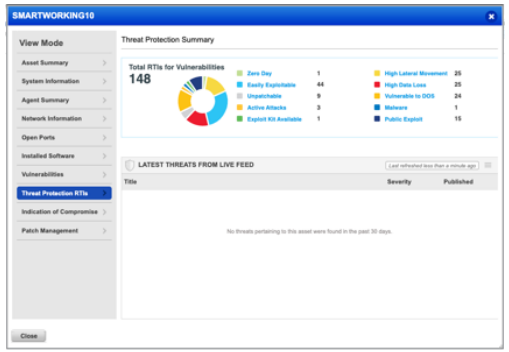
L’Inventario «Multi-Prospettiva»…

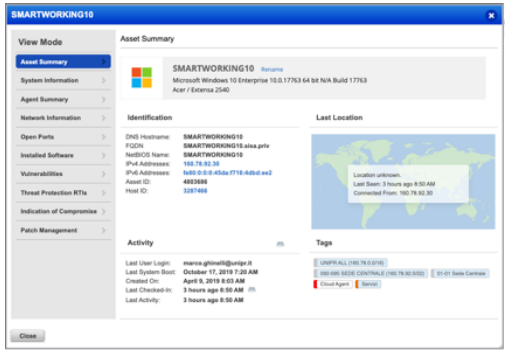


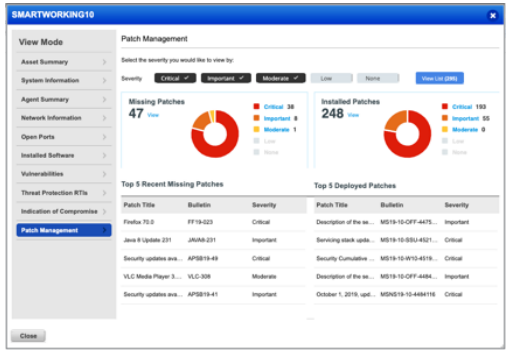


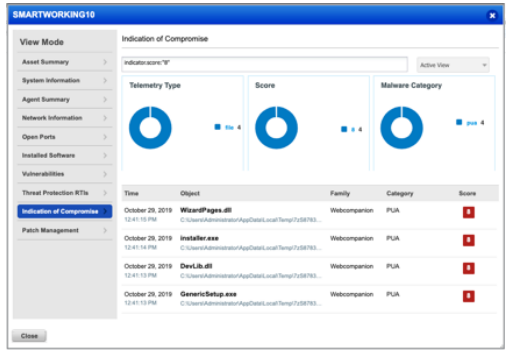












UNIVERSITÀ DI PARMA

Qualys.

L’Inventario «Multi-Prospettiva»…

SMARTWORKING10

View Mode

- Asset Summary
- System Information
- Agent Summary
- Network Information
- Open Ports
- Installed Software
- Vulnerabilities
- Threat Protection RTIs
- Indication of Compromise
- Patch Management

Asset Summary

SMARTWORKING10 Rename

Microsoft Windows 10 Enterprise 10.0.17763 64 bit N/A Build 17763

Acer [redacted]

Identification

DNS Hostname:	SMARTWORKING10
FQDN	SMARTWORKING10.[redacted]
NetBIOS Name:	SMARTWORKING10
IPv4 Addresses:	160.78[redacted]
IPv6 Addresses:	fe80:0:0:0.[redacted]
Asset ID:	4803686
Host ID:	3287466

Last Location

Location unknown.
Last Seen: 3 hours ago 8:50 AM
Connected From: 160.78[redacted]

Activity

Last User Login:	[redacted]@unipr.it
Last System Boot:	October 17, 2019 7:20 AM
Created On:	April 9, 2019 8:03 AM
Last Checked-In:	3 hours ago 8:50 AM
Last Activity:	3 hours ago 8:50 AM

Tags

UNIPR ALL (160.78.0.0/16)
[redacted]SEDE CENTRALE (160.78.[redacted]
01-01 Sede Centrale
Cloud Agent
Servizi

Close

UNIVERSITÀ DI PARMA

Qualys.

L’Inventario «Multi-Prospettiva»…

SMARTWORKING10

View Mode

- Asset Summary
- System Information
- Agent Summary
- Network Information
- Open Ports
- Installed Software
- Vulnerabilities
- Threat Protection RTIs
- Indication of Compromise
- Patch Management

System Information

Services

Name	Description	Status
CcmExec	Host agenti di SMS	RUNNING
CDPSvc	Servizio piattaforma dispositivi connessi	RUNNING
CertPropSvc	Propagazione certificati	RUNNING
CmRcService	Controllo remoto di Configuration Manager	RUNNING
CoreMessagingRegistrar	CoreMessaging	RUNNING
DiagTrack	Esperienze utente connesse e telemetria	RUNNING
cphs	Intel(R) Content Protection HECI Service	RUNNING
cplspcon	Intel(R) Content Protection HDCP Service	RUNNING
CryptSvc	Servizi di crittografia	RUNNING
DcomLaunch	Utilit… di avvio processi server DCOM	RUNNING
DeviceAssociationService	Servizio associazione dispositivi	RUNNING
Dhcp	Client DHCP	RUNNING
AdobeARMservice	Adobe Acrobat Update Service	RUNNING
Appinfo	Informazioni applicazioni	RUNNING
AppXSvc	Servizio di distribuzione AppX (AppXSVC)	RUNNING
AudioEndpointBuilder	Generatore endpoint audio Windows	RUNNING
Audiosrv	Audio di Windows	RUNNING
camsvc	Servizio di gestione dell'accesso alle funzionalit…	RUNNING
BFE	BFE (Base Filtering Engine)	RUNNING
BrokerInfrastructure	Servizio infrastruttura attivit… in background	RUNNING
Browser	Browser di computer	RUNNING

Close

UNIVERSITÀ DI PARMA

Qualys.

L’Inventario «Multi-Prospettiva»…

SMARTWORKING10

View Mode

- Asset Summary
- System Information
- Agent Summary
- Network Information
- **Open Ports**
- Installed Software
- Vulnerabilities
- Threat Protection RTIs
- Indication of Compromise
- Patch Management

Open Ports

This list includes ports with listening services. Download

Port	Protocol	Detected Service	Service Description
49665	TCP	registro eventi di windows	-
49666	TCP	utilit	-
49667	TCP	configurazione desktop remoto	-
49668	TCP	spoolsv.exe	-
49669	TCP	lsass.exe	-
49670	TCP	impossibile ottenere informazioni sulla propriet…	-
49681	TCP	agente criteri ipsec	-
49692	TCP	lsass.exe	-
50185	UDP	wmiprvse.exe	-
51278	UDP	dike.exe	-
51279	UDP	dike.exe	-
51876	UDP	pubblicazione risorse per individuazione	-
51877	UDP	pubblicazione risorse per individuazione	-
51948	UDP	outlook.exe	-
53297	UDP	helper ip	-
54079	UDP	acrord32.exe	-

Page 2 of 3 Displaying open ports 21 - 40 of 49

Close

UNIVERSITÀ DI PARMA

Qualys.

L’Inventario «Multi-Prospettiva»…

SMARTWORKING10

View Mode

- Asset Summary
- System Information
- Agent Summary
- Network Information
- Open Ports
- Installed Software
- Vulnerabilities
- Threat Protection RTIs
- Indication of Compromise
- Patch Management

Installed Software

Search...

Download

Name	Version
7-Zip 18.01	18.01.00.0
Acer Quick Access	2.01.3025
Adobe AIR	32.0.0.89
Adobe Acrobat 8 Professional - Italiano, Español, Ned…	8.3.1
Adobe Acrobat Reader DC - Italiano	15.007.20033
Adobe Digital Editions 4.5	4.5.7
Adobe Flash Player 24 NPAPI	24.0.0.186
Adobe Refresh Manager	1.8.0
Conexant HD Audio	8.66.16.52
ConfigMgr Wake-up Proxy	5.00.8716.1000
Configuration Manager Client	5.00.8790.1000
Definition Update for Microsoft Office 2016 (KB31154…	
Dike GoSign	7.0.2
DisplayLink Graphics Driver	9.0.1651.0
File version of Microsoft XML parser (MSXML) v3 :	8.110.17763.437

Page 1 of 7 Clear Displaying installed software 1 - 20 of 139

Close

UNIVERSITÀ DI PARMA

Qualys.

L’Inventario «Multi-Prospettiva»…

SMARTWORKING10

View Mode

- Asset Summary
- System Information
- Agent Summary
- Network Information
- Open Ports
- Installed Software
- Vulnerabilities
- Threat Protection RTIs
- Indication of Compromise
- Patch Management

Vulnerabilities

Select the severity you would like to view by:

Severity: Sev 5 ✓ | Sev 4 ✓ | Sev 3 ✓ | Sev 2 | Sev 1 | View vulnerabilities (54)

Confirmed Vulnerabilities
53 View

Sev 5 26
Sev 4 19
Sev 3 8
Sev 2
Sev 1

Potential Vulnerabilities
1 View

Sev 5 0
Sev 4 0
Sev 3 1
Sev 2
Sev 1

Vulnerability Detection by Status

In the last 7 Days

Active	New	Reopened	Fixed
54	0	0	0
Confirmed 53	Confirmed 0	Confirmed 0	Confirmed 0
Potential 1	Potential 0	Potential 0	Potential 0

Close

UNIVERSITÀ DI PARMA

Qualys.

L’Inventario «Multi-Prospettiva»…

SMARTWORKING10

View Mode

- Asset Summary
- System Information
- Agent Summary
- Network Information
- Open Ports
- Installed Software
- Vulnerabilities
- **Threat Protection RTIs**
- Indication of Compromise
- Patch Management

Threat Protection Summary

Total RTIs for Vulnerabilities
148

Zero Day	1	High Lateral Movement	25
Easily Exploitable	44	High Data Loss	25
Unpatchable	9	Vulnerable to DOS	24
Active Attacks	3	Malware	1
Exploit Kit Available	1	Public Exploit	15

LATEST THREATS FROM LIVE FEED — *Last refreshed less than a minute ago*

Title	Severity	Published

No threats pertaining to this asset were found in the past 30 days.

Close

UNIVERSITÀ DI PARMA

Qualys.

L’Inventario «Multi-Prospettiva»…

SMARTWORKING10

View Mode

- Asset Summary
- System Information
- Agent Summary
- Network Information
- Open Ports
- Installed Software
- Vulnerabilities
- Threat Protection RTIs
- Indication of Compromise
- Patch Management

Indication of Compromise

indicator.score:"8"

Active View

Telemetry Type

Score

Malware Category

Time	Object	Family	Category	Score
October 29, 2019 12:41:15 PM	**WizardPages.dll** C:\Users\Administrator\AppData\Local\Temp\7zS8783…	Webcompanion	PUA	8
October 29, 2019 12:41:14 PM	**installer.exe** C:\Users\Administrator\AppData\Local\Temp\7zS8783…	Webcompanion	PUA	8
October 29, 2019 12:41:13 PM	**DevLib.dll** C:\Users\Administrator\AppData\Local\Temp\7zS8783…	Webcompanion	PUA	8
October 29, 2019 12:41:13 PM	**GenericSetup.exe** C:\Users\Administrator\AppData\Local\Temp\7zS8783…	Webcompanion	PUA	8

Close

UNIVERSITÀ DI PARMA

Qualys.

L’Inventario «Multi-Prospettiva»…

SMARTWORKING10

View Mode

- Asset Summary
- System Information
- Agent Summary
- Network Information
- Open Ports
- Installed Software
- Vulnerabilities
- Threat Protection RTIs
- Indication of Compromise
- Patch Management

Patch Management

Select the severity you would like to view by:

Severity: Critical ✓ | Important ✓ | Moderate ✓ | Low | None | View List (295)

Missing Patches
47 View

Critical 38
Important 8
Moderate 1
Low
None

Installed Patches
248 View

Critical 193
Important 55
Moderate 0
Low
None

Top 5 Recent Missing Patches

Patch Title	Bulletin	Severity
Firefox 70.0	FF19-023	Critical
Java 8 Update 231	JAVA8-231	Important
Security updates ava…	APSB19-49	Critical
VLC Media Player 3.…	VLC-308	Moderate
Security updates ava…	APSB19-41	Important

Top 5 Deployed Patches

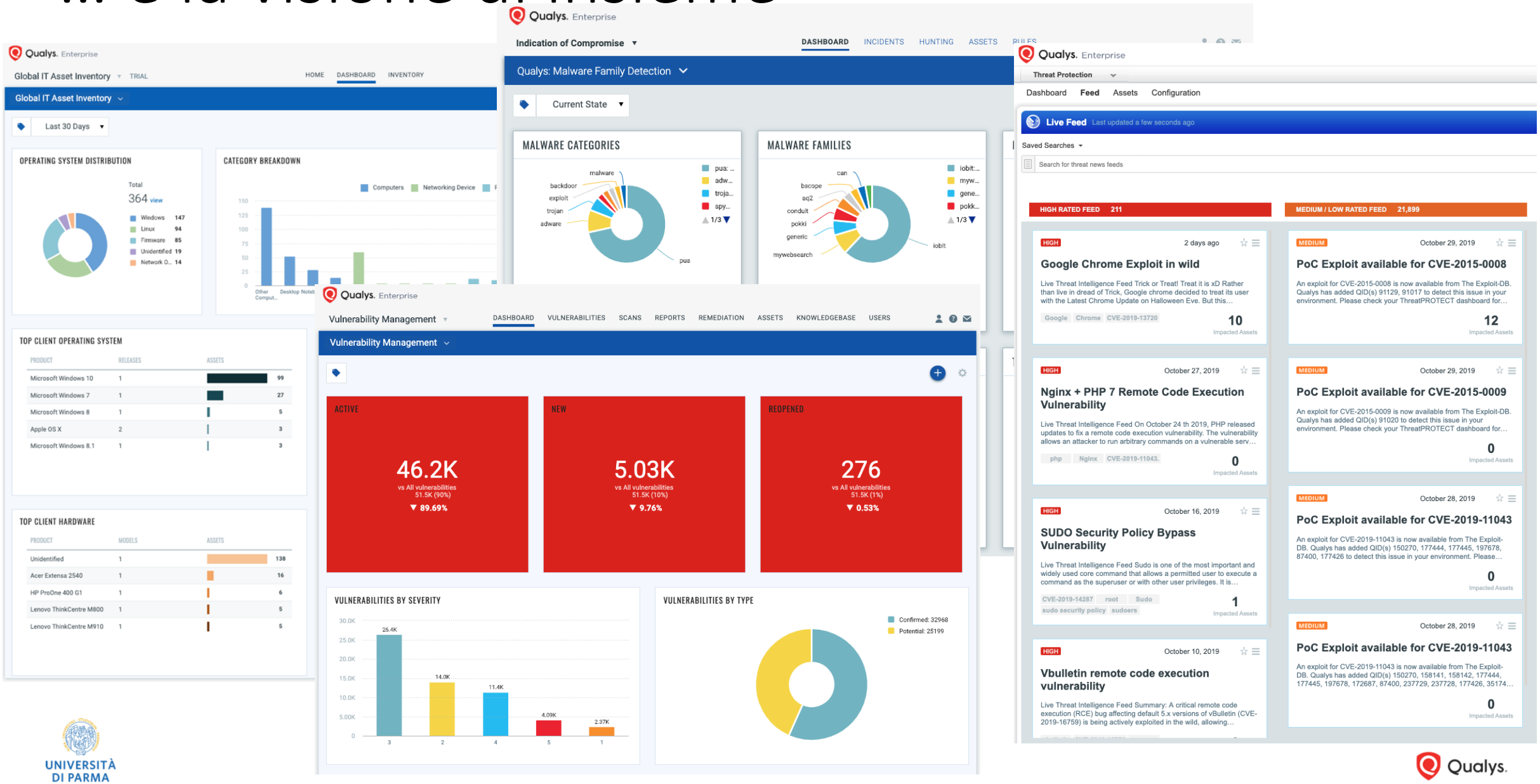
Patch Title	Bulletin	Severity
Description of the se…	MS19-10-OFF-4475…	Important
Servicing stack upda…	MS19-10-SSU-4521…	Critical
Security Cumulative …	MS19-10-W10-4519…	Critical
Description of the se…	MS19-10-OFF-4484…	Important
October 1, 2019, upd…	MSNS19-10-4484116	Critical

Close

UNIVERSITÀ DI PARMA

Qualys.

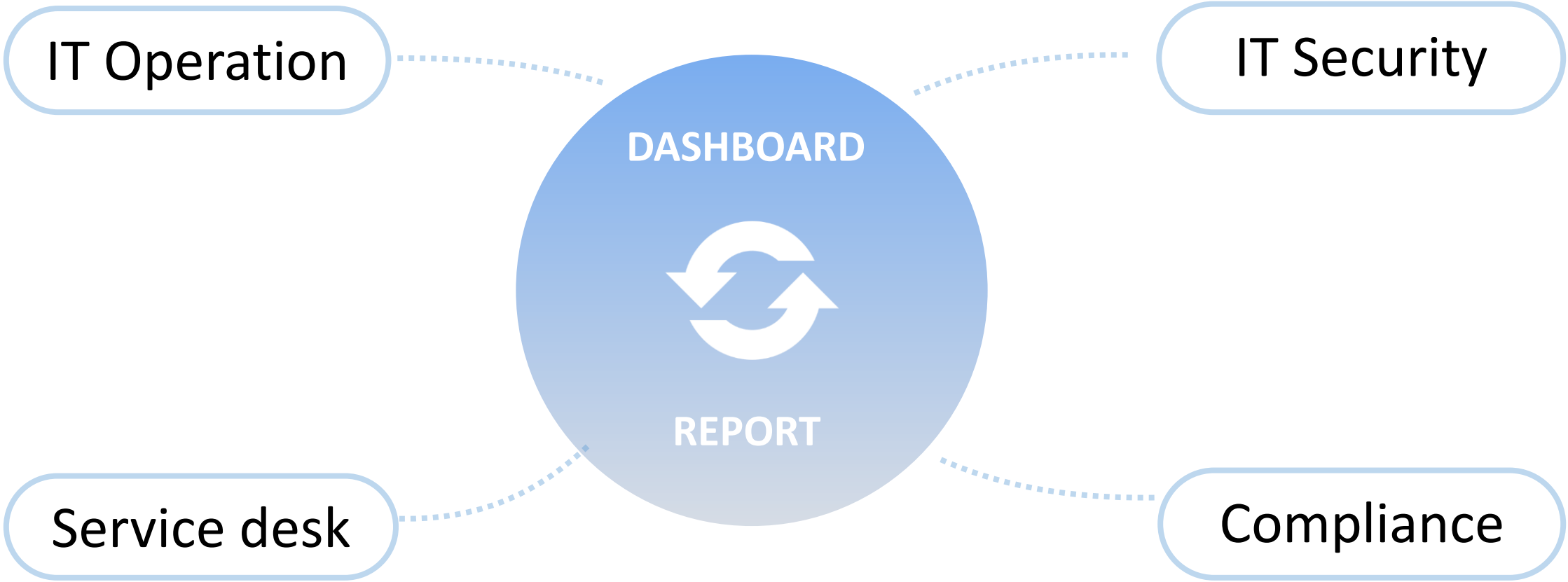
… e la visione di insieme



UNIVERSITÀ DI PARMA

Qualys.

Dati consumabili da più utenti



Take home messages

- Single Pane of Glass, Single Source of Truth
- Futura integrazione con altre piattaforme (es. CMDB)
- Creare utenti differenziati che abbiano visibilità su ambienti di competenza ➔ condivisione strutturata delle informazioni

Certo, avremmo potuto noleggiare un servizio…
ma non senza rinunciare ad una crescita delle competenze interne che riteniamo fondamentale!

Ilaria Comelli

Grazie!

ilaria.comelli@unipr.it

marco@qualys.com

UNIVERSITÀ DI PARMA

Qualys.