inetum

realdolmen

Positive digital flow

DELL Technologies

Datacentermodernisatie (Davy De Bleecker) & IT Cybersecurity (Anthony De Smet)

inetum realdolmen

Positive digital flow

DELL Technologies

Datacentermodernisatie (Davy De Bleecker)

Agenda

- Datacentermodernisatie
- IT Cybersecurity

Agenda

- Datacentermodernisatie
  - Hoe begin je eraan?
  - Private / Hybride / Public cloud
    (verschillende oplossingen binnen private cloud)
  - Beheer
  - Monitoring
  - AI
  - Life cycle management
  - CAPEX vs OPEX

Hoe begin je eraan?

- Analyse van de business en requirements

- Analyse van de huidige omgeving en definiëren van potentiële verbeteringen naar de toekomst toe, maar ook huidige bottlenecks etc…

- Praten met mensen van de business en IT staff inzake gebruik, beheer en monitoring van de huidige omgeving en toekomstige omgeving

DELL Technologies

inetum realdolmen
Positive digital flow

Hoe begin je eraan?

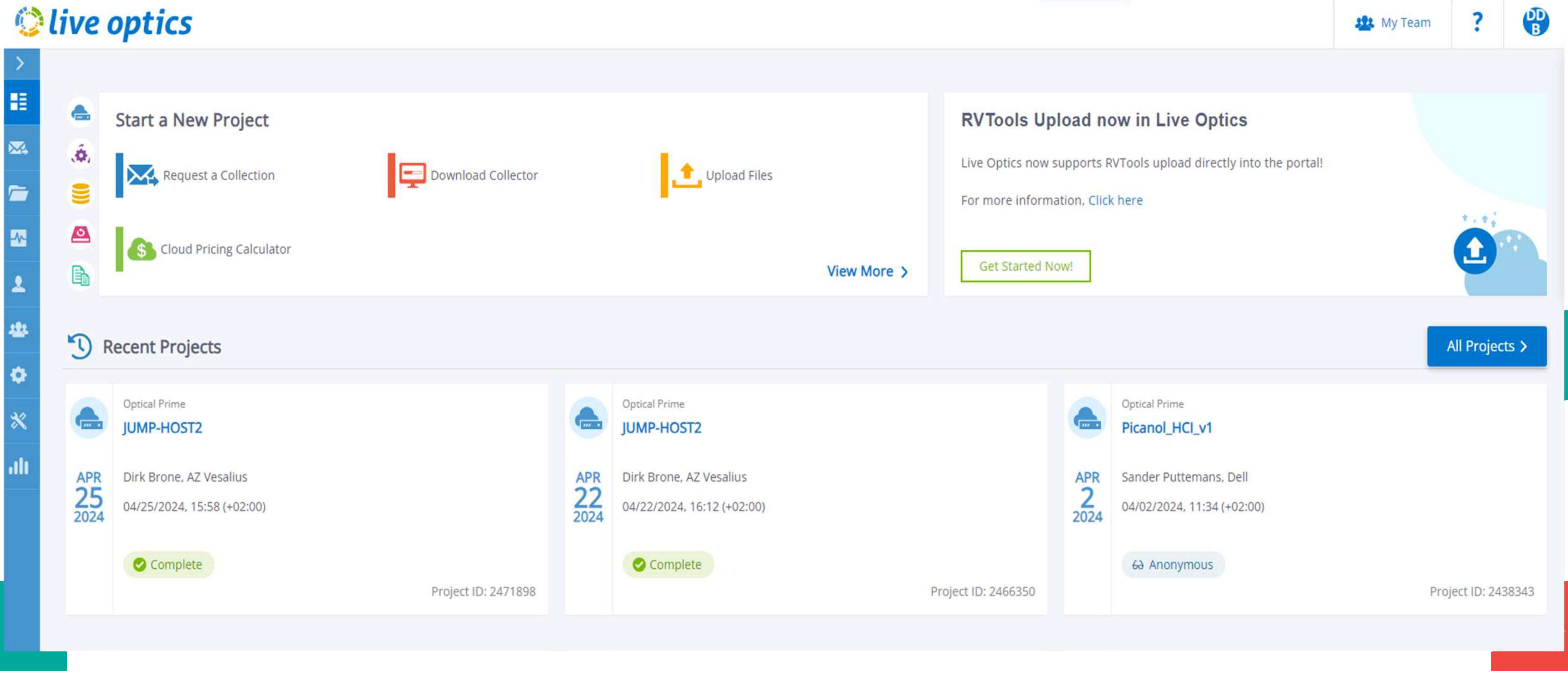
live optics

- Je contacteert ons en doet beroep op onze professionele expertise door b.v. het laten opstellen van een roadmap

- Professionele tooling voor een diepte-analyse van uw omgeving

live optics

Hoe begin je eraan?



Start a New Project

RVTools Upload now in Live Optics

Live Optics now supports RVTools upload directly into the portal!

For more information, Click here

Recent Projects

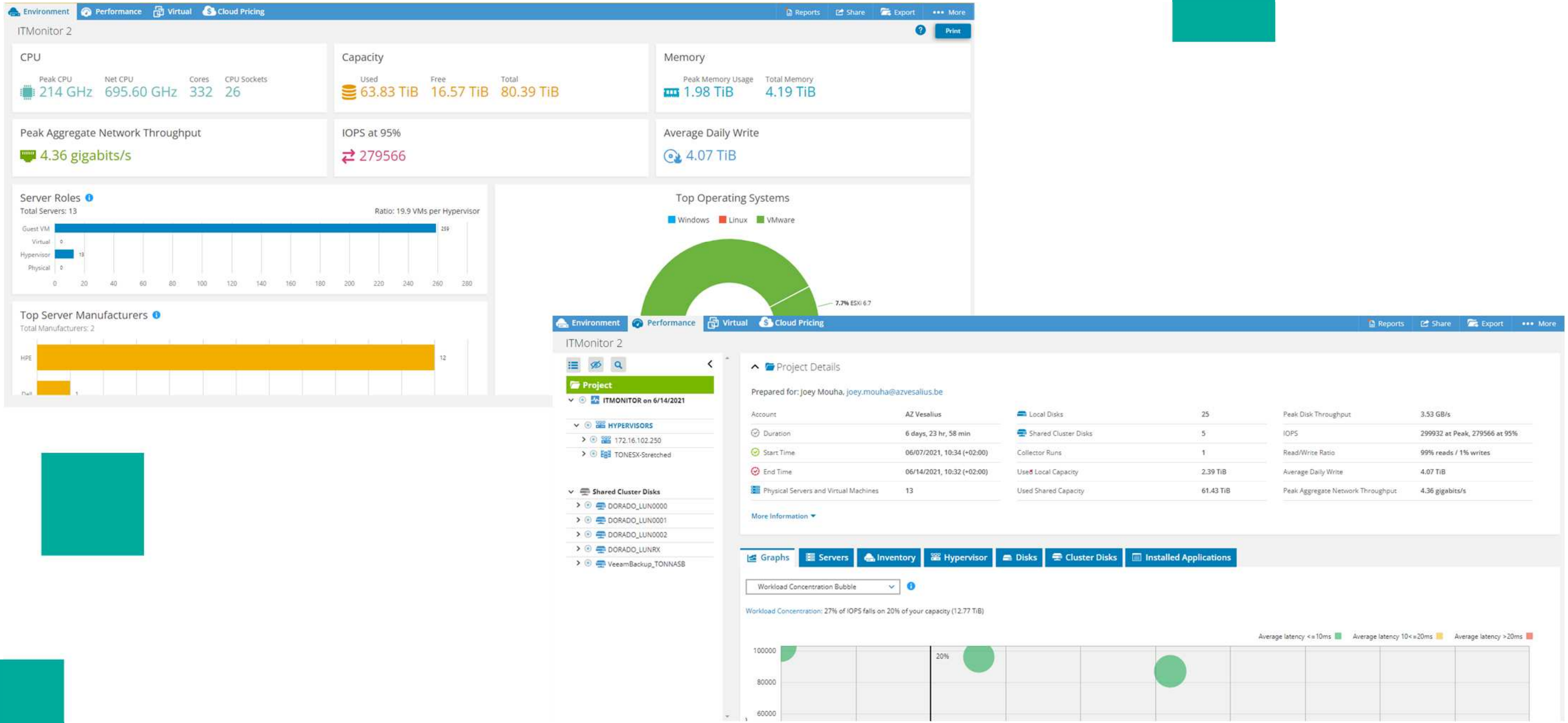
Optical Prime	JUMP-HOST2	Dirk Brone, AZ Vesalius	APR 25 2024
	04/25/2024, 15:58 (+02:00)	Complete	Project ID: 2471898
Optical Prime	JUMP-HOST2	Dirk Brone, AZ Vesalius	APR 22 2024
	04/22/2024, 16:12 (+02:00)	Complete	Project ID: 2466350
Optical Prime	Picanol_HCI_v1	Sander Puttemans, Dell	APR 2 2024
	04/02/2024, 11:34 (+02:00)	Anonymous	Project ID: 2438343

DELL Technologies

inetum realdolmen
Positive digital flow

live optics

Hoe begin je eraan?



ITMonitor 2

CPU

Peak CPU	Net CPU	Cores	CPU Sockets
214 GHz	695.60 GHz	332	26

Capacity

Used	Free	Total
63.83 TiB	16.57 TiB	80.39 TiB

Memory

Peak Memory Usage	Total Memory
1.98 TiB	4.19 TiB

Peak Aggregate Network Throughput
4.36 gigabits/s

IOPS at 95%
279566

Average Daily Write
4.07 TiB

Server Roles
Total Servers: 13
Ratio: 19.9 VMs per Hypervisor

Top Operating Systems

Top Server Manufacturers
Total Manufacturers: 2

ITMonitor 2

Project Details

Prepared for: Joey Mouha, joey.mouha@azvesalius.be

Account	AZ Vesalius	Local Disks	25	Peak Disk Throughput	3.53 GB/s
Duration	6 days, 23 hr, 58 min	Shared Cluster Disks	5	IOPS	299932 at Peak, 279566 at 95%
Start Time	06/07/2021, 10:34 (+02:00)	Collector Runs	1	Read/Write Ratio	99% reads / 1% writes
End Time	06/14/2021, 10:32 (+02:00)	Used Local Capacity	2.39 TiB	Average Daily Write	4.07 TiB
Physical Servers and Virtual Machines	13	Used Shared Capacity	61.43 TiB	Peak Aggregate Network Throughput	4.36 gigabits/s

Workload Concentration Bubble

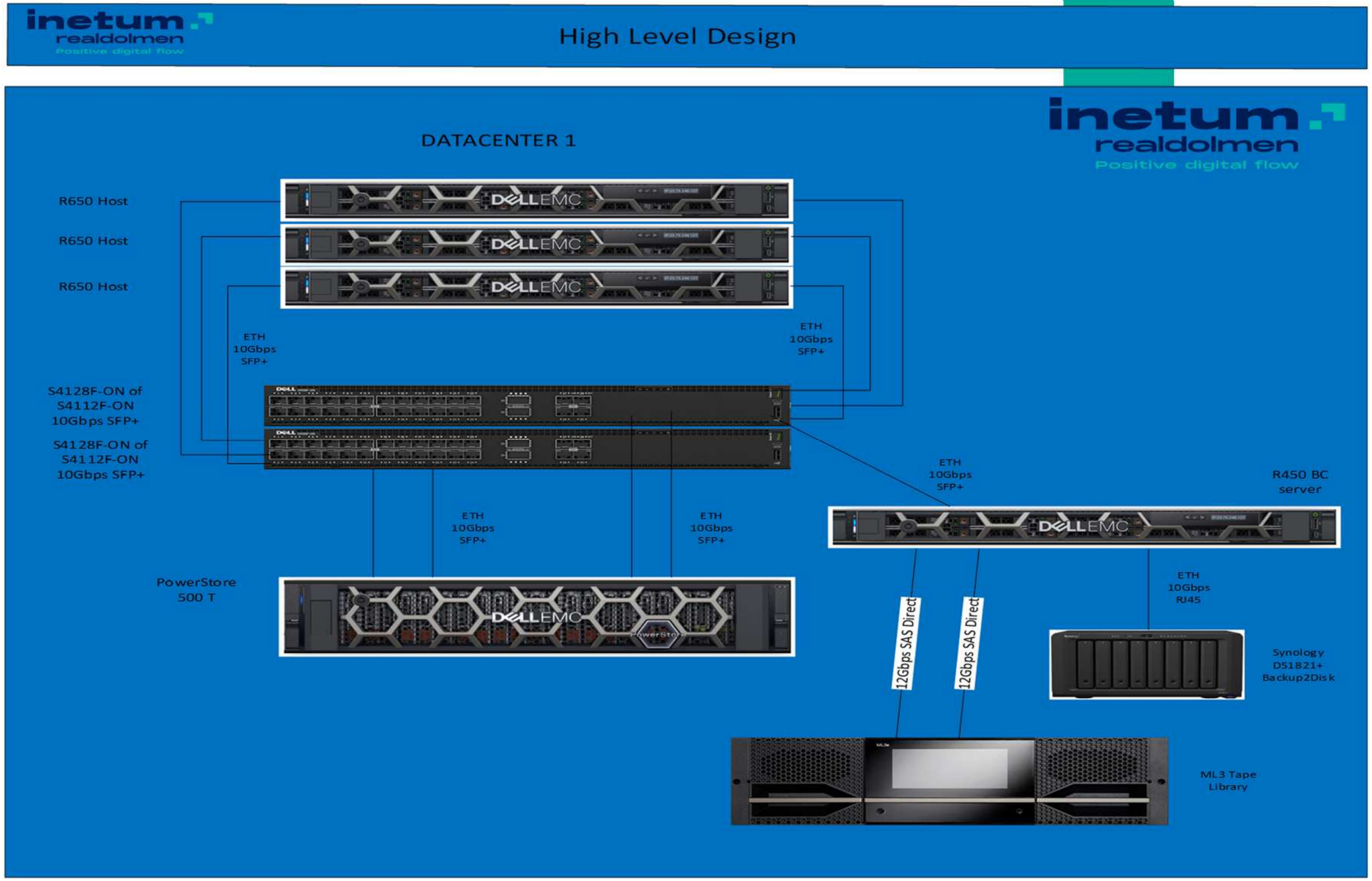
Workload Concentration: 27% of IOPS falls on 20% of your capacity (12.77 TiB)

Private / Hybride / Public cloud

Private cloud

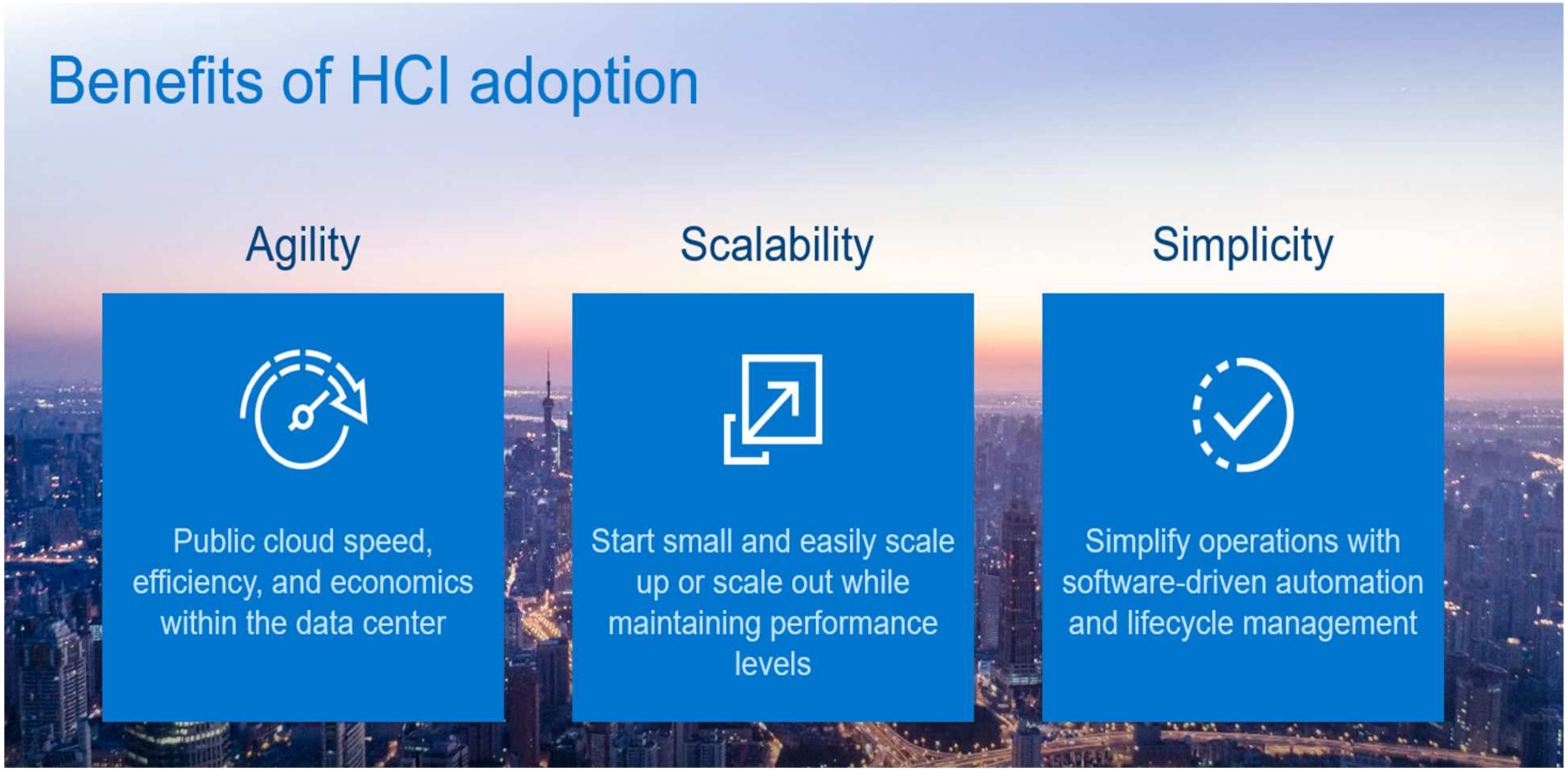
- Klassieke 3 Tier oplossing – DELLEMC Server + Switch + Storage
- Full HCI oplossing – DELLEMC VXRAIL (Vmware)
- Converged Infrastructure (CI oplossing) – DELLEMC
  >> VXRAIL Dyn Nodes + Storage (DELLEMC Powerstore)
- Hybride oplossing – DELLEMC Powerflex – Software Defined Infrastructure (Multi hypervisor)

Private cloud – 3 TIER



Private cloud – HCI VXRAIL

- Full HCI oplossing – DELLEMC VXRAIL (Vmware)



Benefits of HCI adoption

Agility

Public cloud speed, efficiency, and economics within the data center

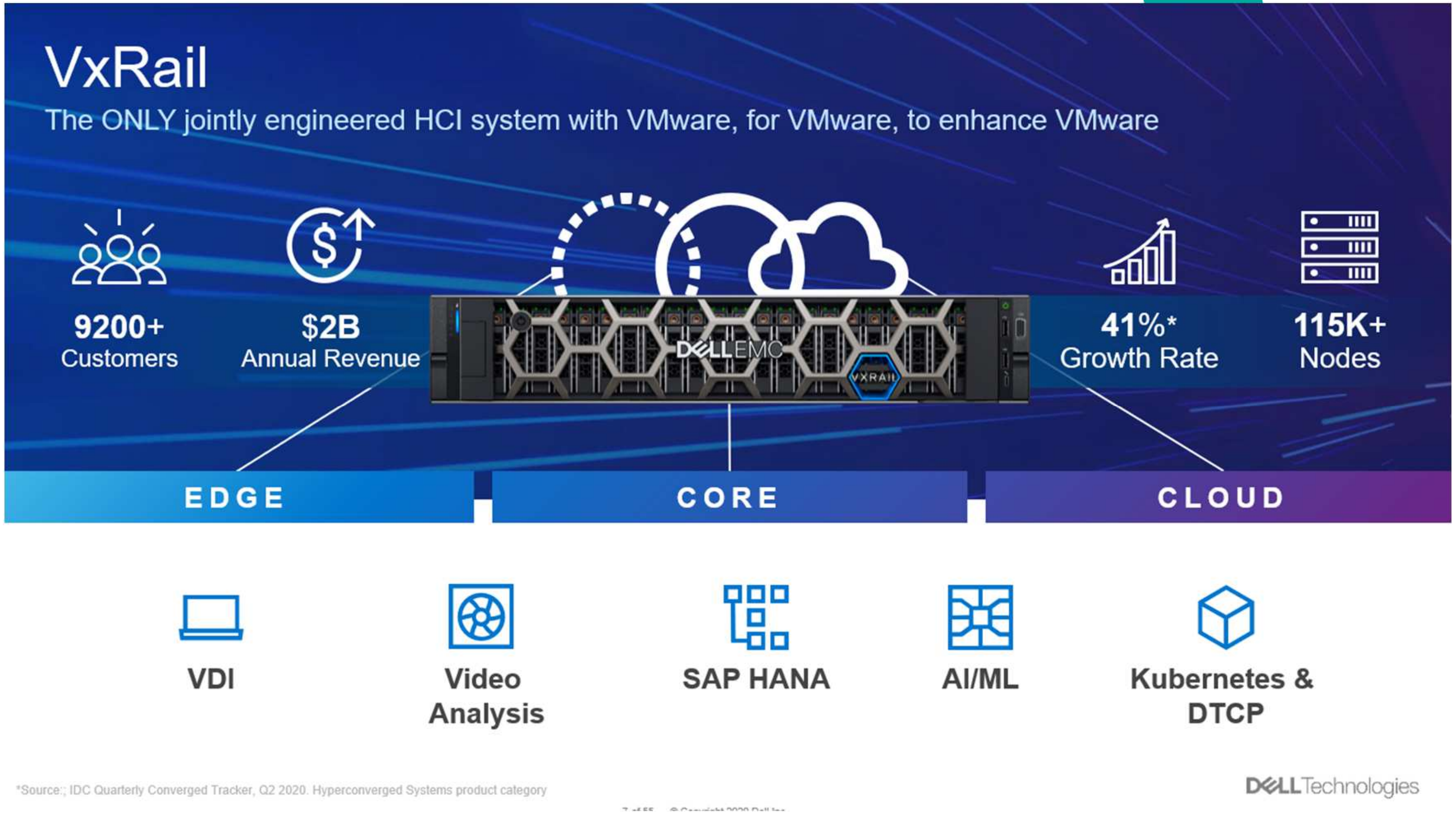
Scalability

Start small and easily scale up or scale out while maintaining performance levels

Simplicity

Simplify operations with software-driven automation and lifecycle management

Private cloud – HCI VXRAIL



VxRail

The ONLY jointly engineered HCI system with VMware, for VMware, to enhance VMware

9200+ Customers

$2B Annual Revenue

41%* Growth Rate

115K+ Nodes

DELL EMC
VXRAIL

EDGE | CORE | CLOUD

VDI

Video Analysis

SAP HANA

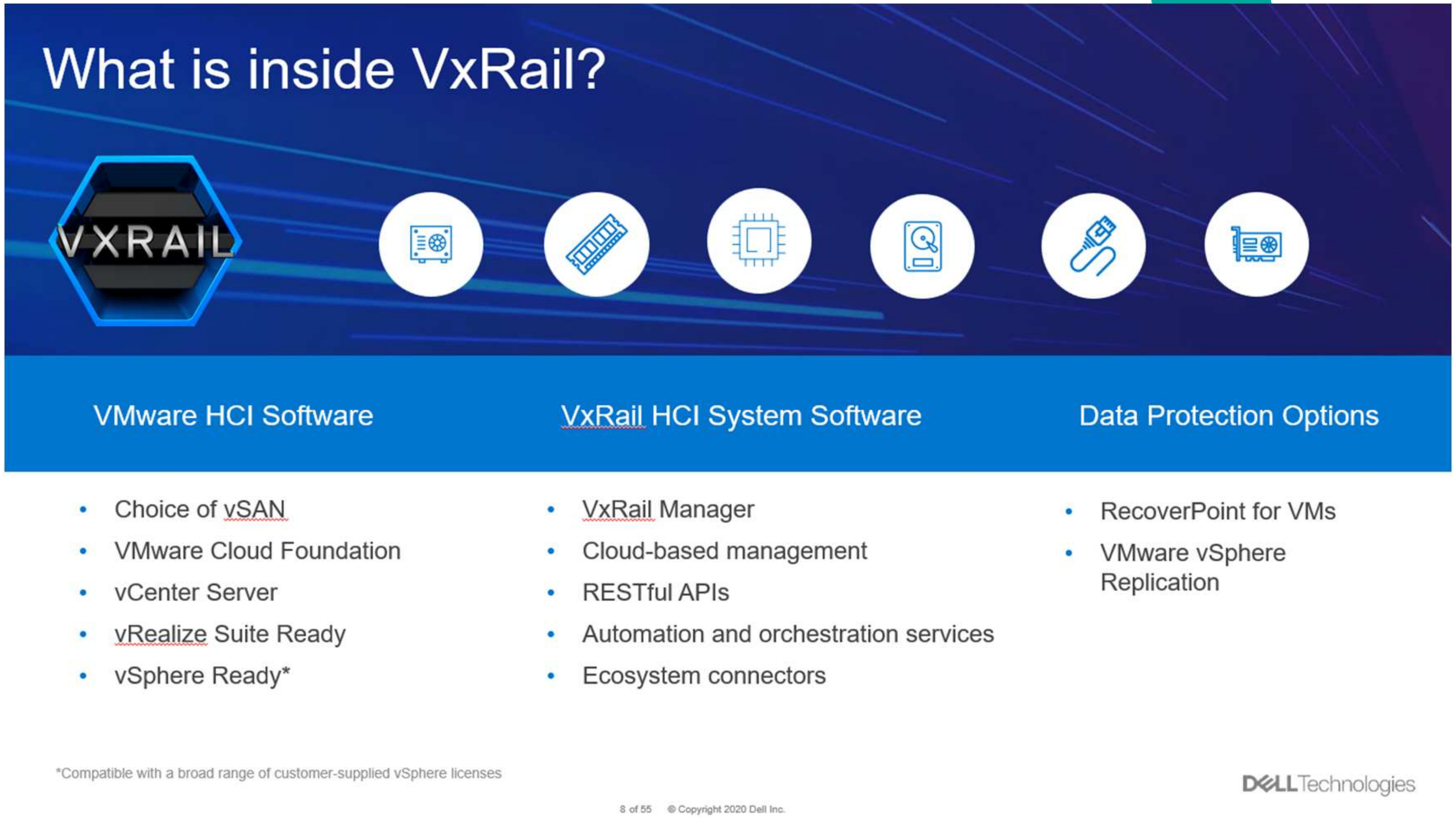
AI/ML

Kubernetes & DTCP

*Source:; IDC Quarterly Converged Tracker, Q2 2020. Hyperconverged Systems product category

DELL Technologies

Private cloud – HCI VXRAIL



What is inside VxRail?

VMware HCI Software

- Choice of vSAN
- VMware Cloud Foundation
- vCenter Server
- vRealize Suite Ready
- vSphere Ready*

VxRail HCI System Software

- VxRail Manager
- Cloud-based management
- RESTful APIs
- Automation and orchestration services
- Ecosystem connectors

Data Protection Options

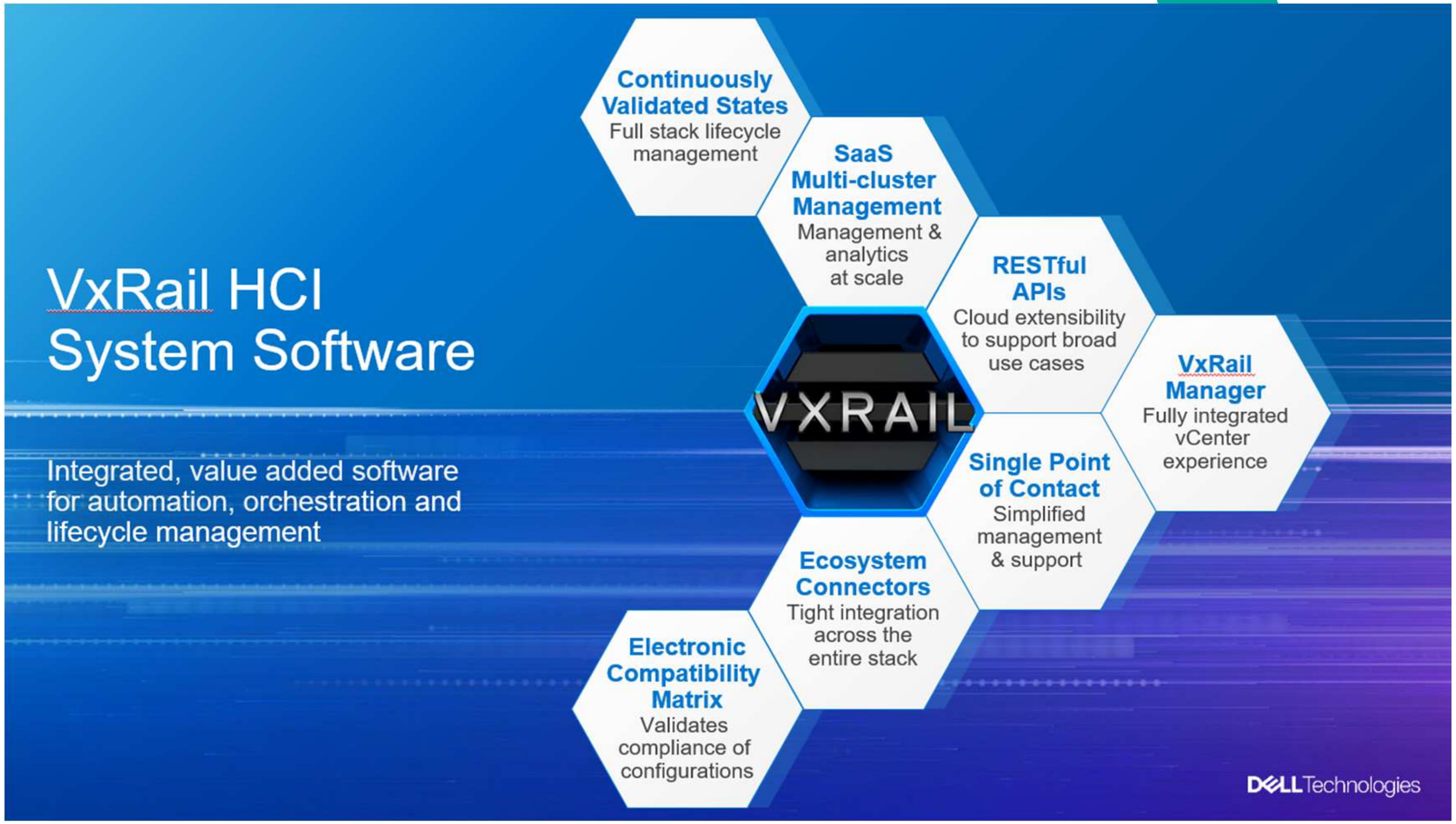
- RecoverPoint for VMs
- VMware vSphere Replication

*Compatible with a broad range of customer-supplied vSphere licenses

DELL Technologies

8 of 55 © Copyright 2020 Dell Inc.

Private cloud – HCI VXRAIL

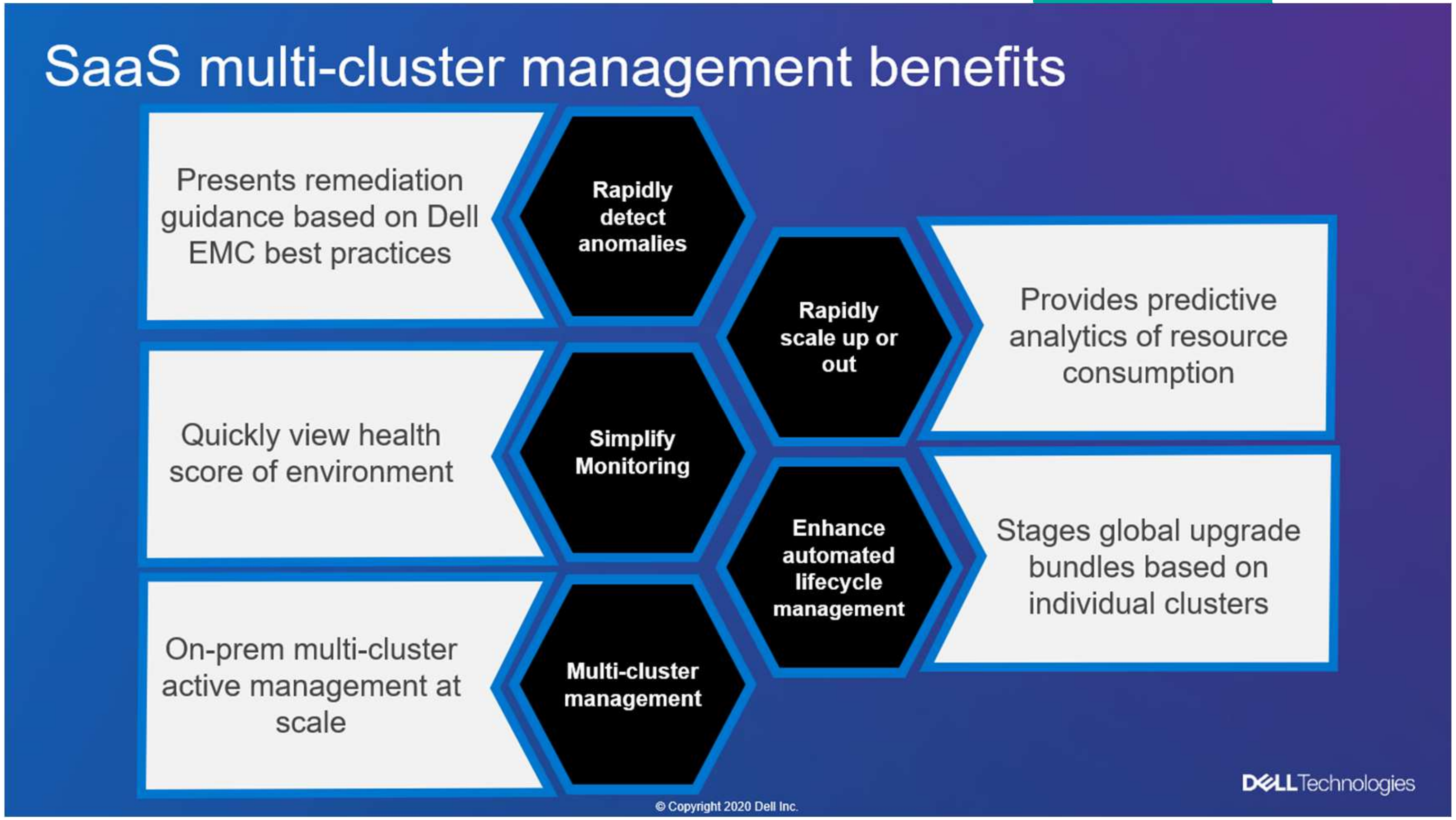


VxRail HCI
System Software

Integrated, value added software for automation, orchestration and lifecycle management

VXRAIL
Continuously Validated States
Full stack lifecycle management
SaaS Multi-cluster Management
Management & analytics at scale
RESTful APIs
Cloud extensibility to support broad use cases
VxRail Manager
Fully integrated vCenter experience
Single Point of Contact
Simplified management & support
Ecosystem Connectors
Tight integration across the entire stack
Electronic Compatibility Matrix
Validates compliance of configurations
DELL Technologies

Private cloud – HCI VXRAIL



SaaS multi-cluster management benefits

Presents remediation guidance based on Dell EMC best practices

Rapidly detect anomalies

Quickly view health score of environment

Simplify Monitoring

On-prem multi-cluster active management at scale

Multi-cluster management

Rapidly scale up or out

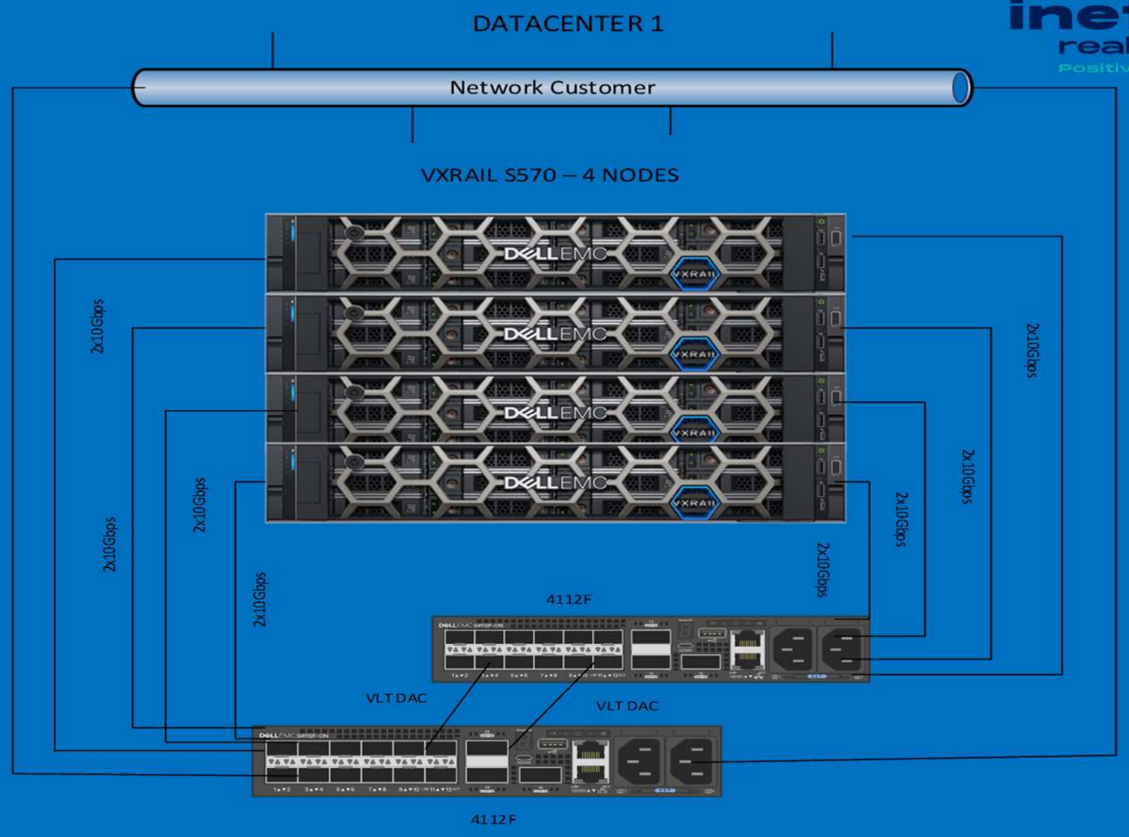
Provides predictive analytics of resource consumption

Enhance automated lifecycle management

Stages global upgrade bundles based on individual clusters

© Copyright 2020 Dell Inc.

High Level Design



DATACENTER 1

Network Customer

VXRAIL S570 – 4 NODES

2x10Gbps

2x10Gbps

2x10Gbps

2x10Gbps

2x10Gbps

2x10Gbps

2x10Gbps

2x10Gbps

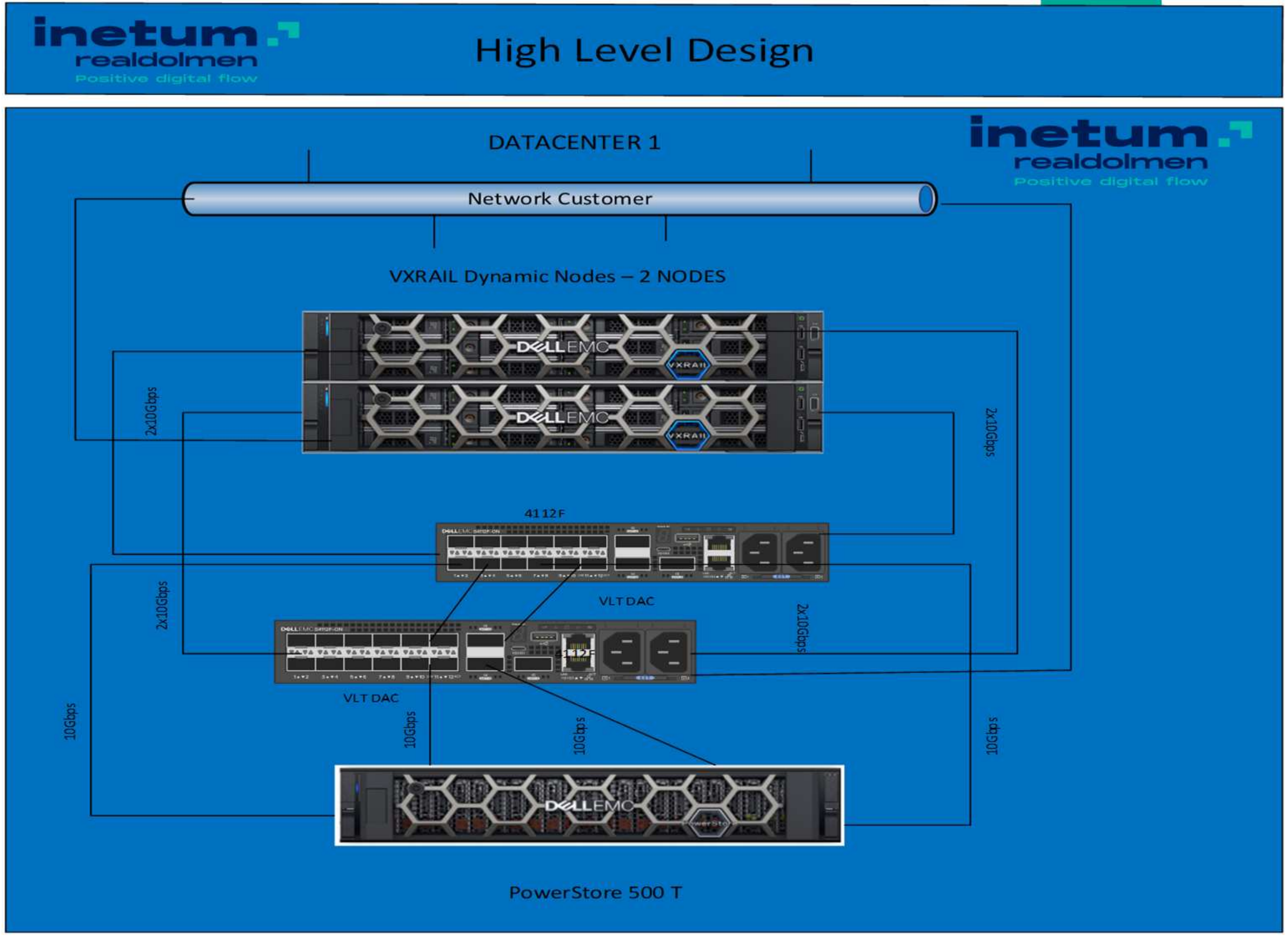
4112F

VLT DAC

VLT DAC

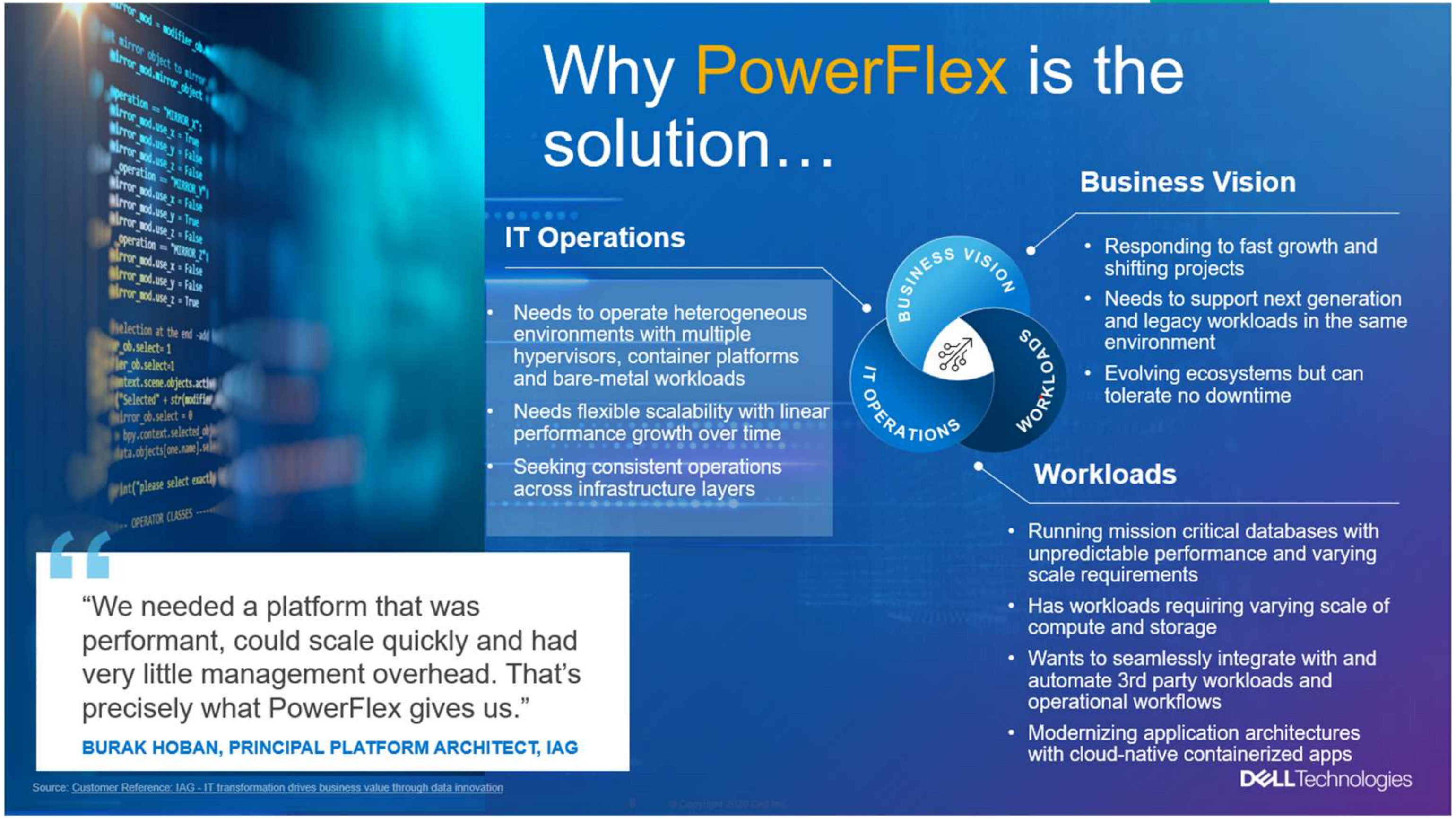
4112F

Private cloud – DYN NODES



Private cloud - POWERFLEX

- Hybride oplossing – DELLEMC Powerflex (Software Defined Infrastructure)



Why PowerFlex is the solution…

IT Operations

- Needs to operate heterogeneous environments with multiple hypervisors, container platforms and bare-metal workloads
- Needs flexible scalability with linear performance growth over time
- Seeking consistent operations across infrastructure layers

Business Vision

- Responding to fast growth and shifting projects
- Needs to support next generation and legacy workloads in the same environment
- Evolving ecosystems but can tolerate no downtime

Workloads

- Running mission critical databases with unpredictable performance and varying scale requirements
- Has workloads requiring varying scale of compute and storage
- Wants to seamlessly integrate with and automate 3rd party workloads and operational workflows
- Modernizing application architectures with cloud-native containerized apps

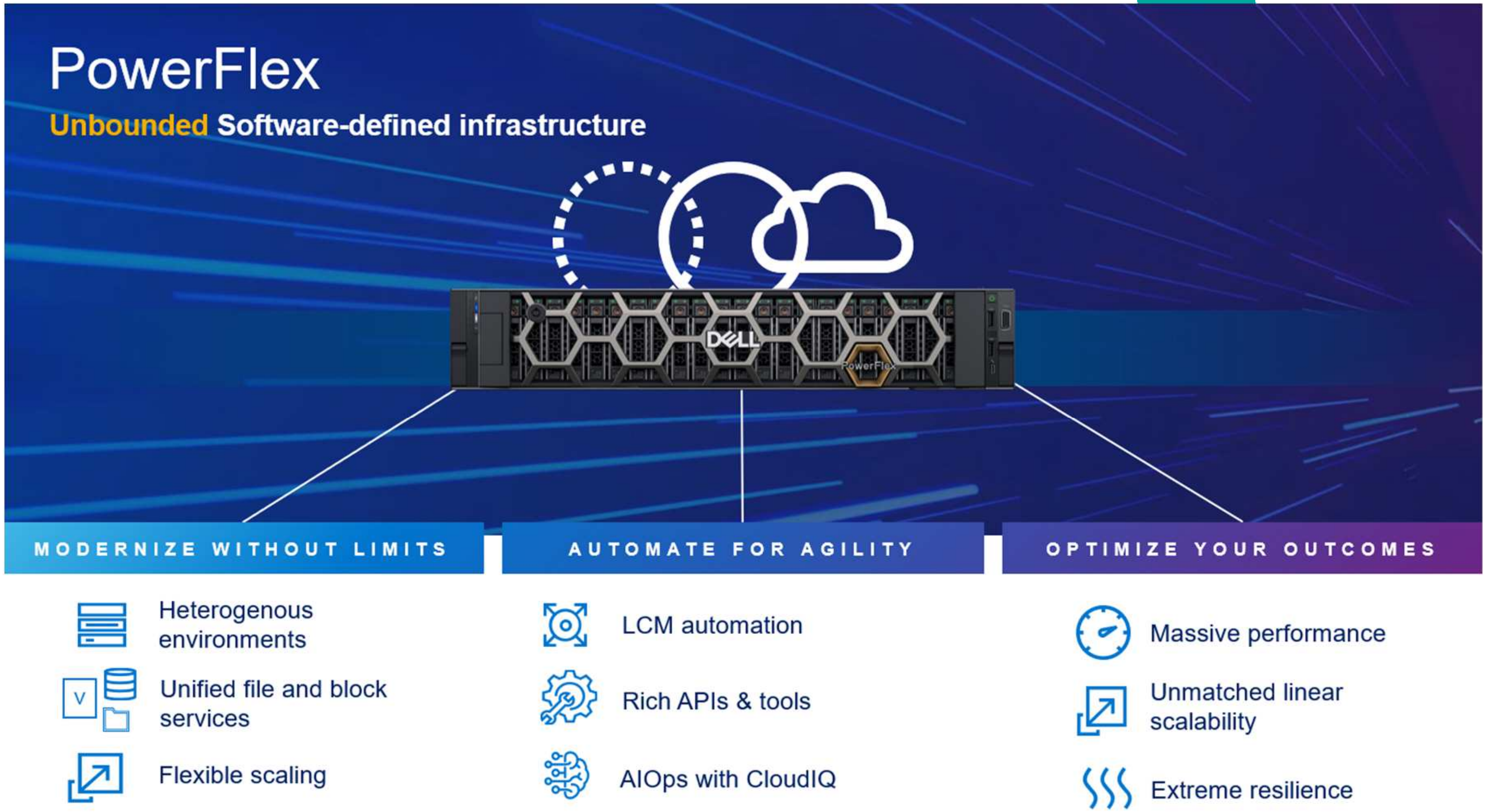
> "We needed a platform that was performant, could scale quickly and had very little management overhead. That's precisely what PowerFlex gives us."
>
> **BURAK HOBAN, PRINCIPAL PLATFORM ARCHITECT, IAG**

Source: Customer Reference: IAG - IT transformation drives business value through data innovation

8 © Copyright 2020 Dell Inc.

Private cloud - POWERFLEX

- Hybride oplossing – DELLEMC Powerflex



PowerFlex

Unbounded Software-defined infrastructure

MODERNIZE WITHOUT LIMITS

- Heterogenous environments
- Unified file and block services
- Flexible scaling

AUTOMATE FOR AGILITY

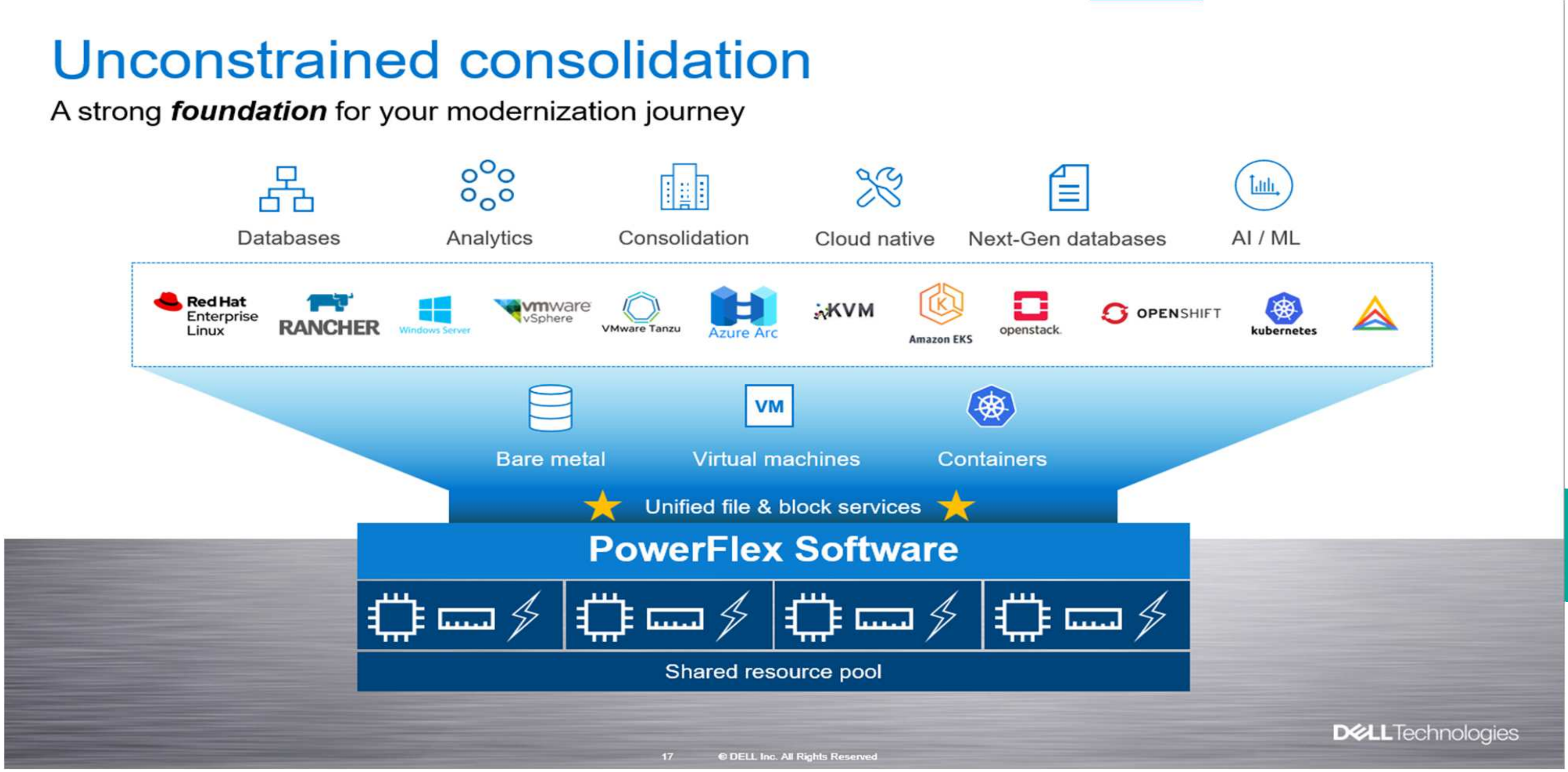
- LCM automation
- Rich APIs & tools
- AIOps with CloudIQ

OPTIMIZE YOUR OUTCOMES

- Massive performance
- Unmatched linear scalability
- Extreme resilience

Private cloud - POWERFLEX

- Hybride oplossing – DELLEMC Powerflex (Software Defined Infrastructure)



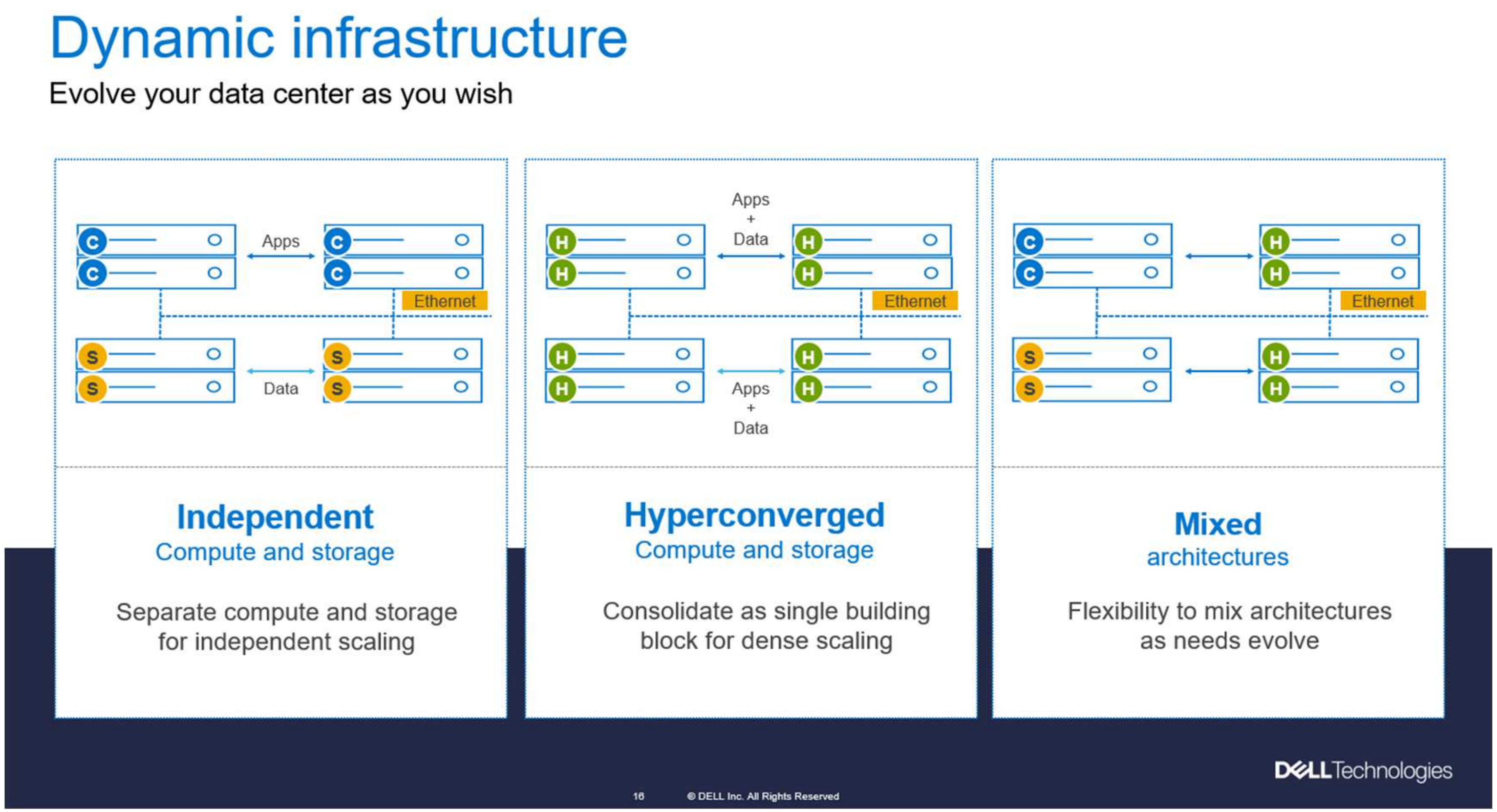
Unconstrained consolidation

A strong ***foundation*** for your modernization journey

17 © DELL Inc. All Rights Reserved

Private cloud - POWERFLEX

- Hybride oplossing – DELLEMC Powerflex



Dynamic infrastructure

Evolve your data center as you wish

Independent

Compute and storage

Separate compute and storage for independent scaling

Hyperconverged

Compute and storage

Consolidate as single building block for dense scaling

Mixed

architectures

Flexibility to mix architectures as needs evolve

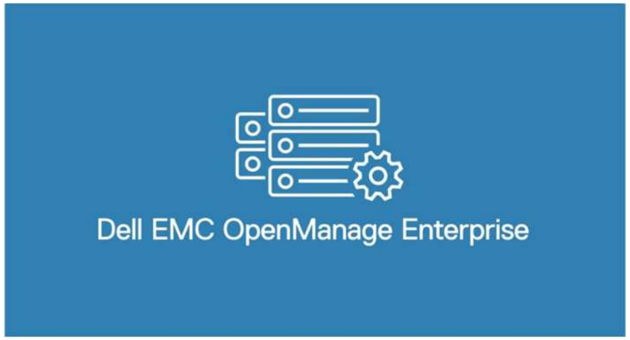
DELLTechnologies

16 © DELL Inc. All Rights Reserved

Beheer

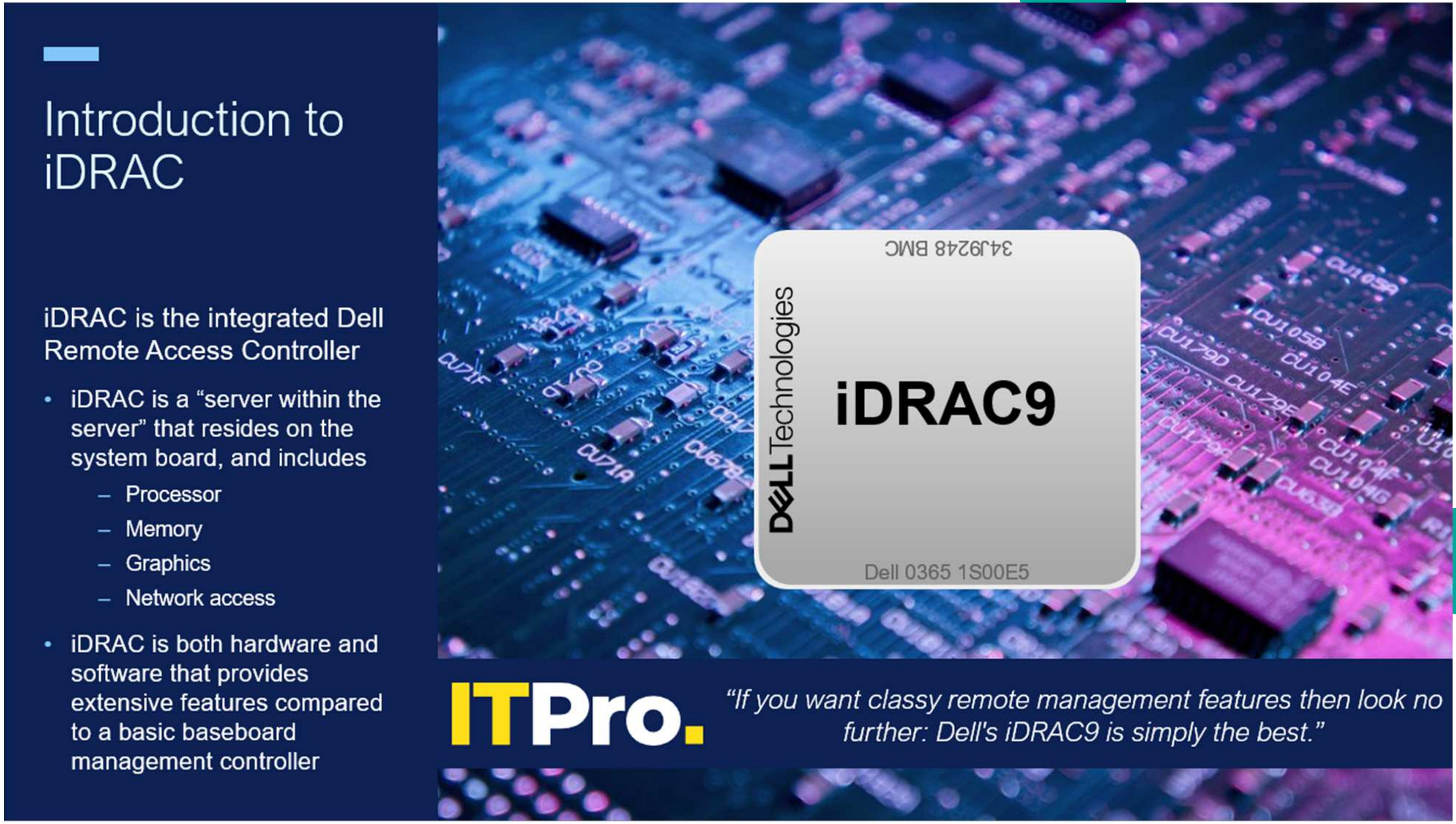
CloudIQ

34J9248 BMC
DELL Technologies
iDRAC9
Dell 0365 1S00E5


Dell EMC OpenManage Enterprise

Beheer

Beheer



Introduction to iDRAC

iDRAC is the integrated Dell Remote Access Controller

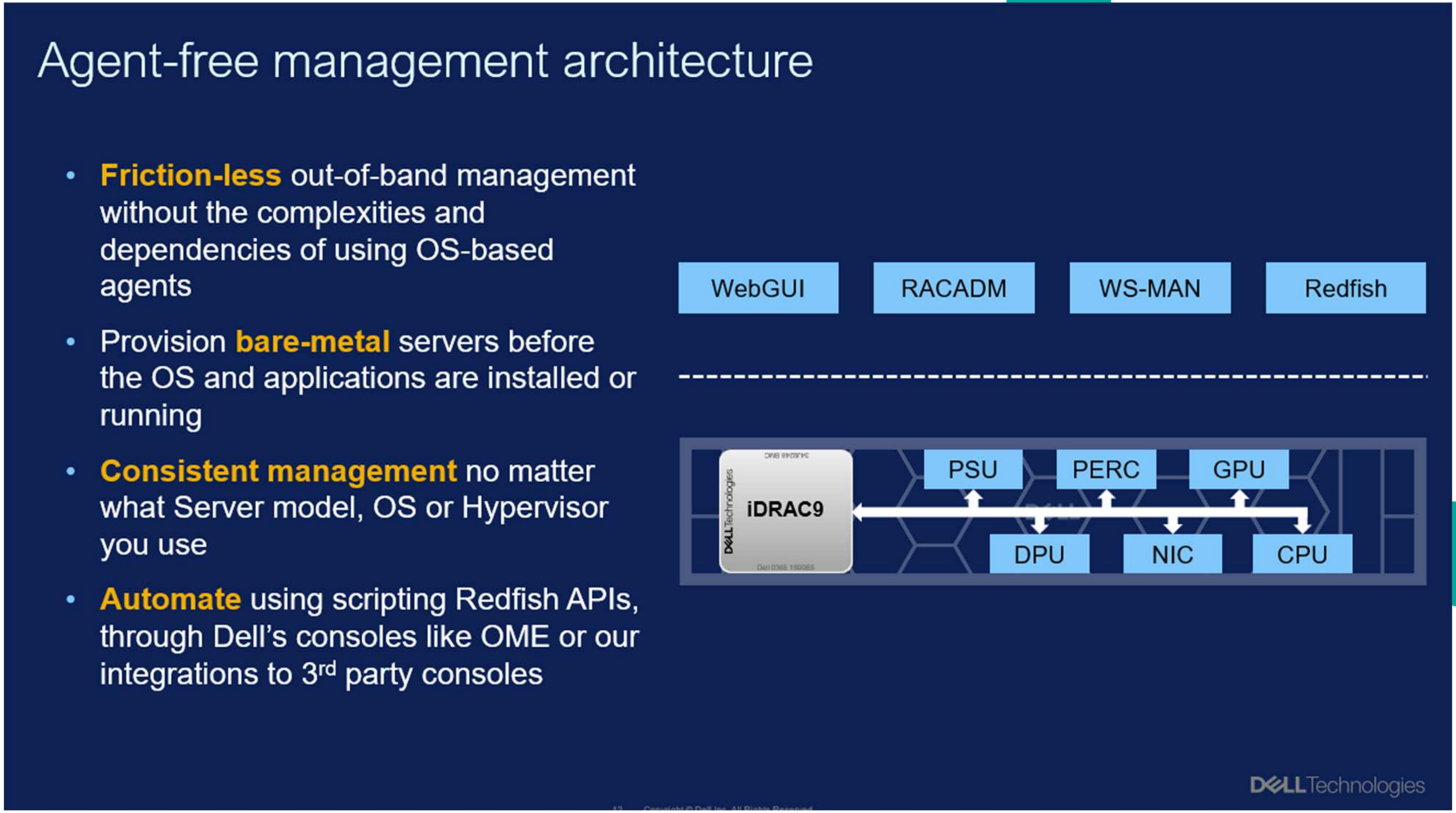
- iDRAC is a "server within the server" that resides on the system board, and includes
  - Processor
  - Memory
  - Graphics
  - Network access
- iDRAC is both hardware and software that provides extensive features compared to a basic baseboard management controller

34J9248 BMC
DELL Technologies
iDRAC9
Dell 0365 1S00E5

ITPro.

"If you want classy remote management features then look no further: Dell's iDRAC9 is simply the best."

Beheer



Agent-free management architecture

- **Friction-less** out-of-band management without the complexities and dependencies of using OS-based agents
- Provision **bare-metal** servers before the OS and applications are installed or running
- **Consistent management** no matter what Server model, OS or Hypervisor you use
- **Automate** using scripting Redfish APIs, through Dell's consoles like OME or our integrations to 3rd party consoles

Copyright © Dell Inc. All Rights Reserved.

Beheer

One To One Remote Management

Agent Free architecture
HTML5e interface

Full Remote Control

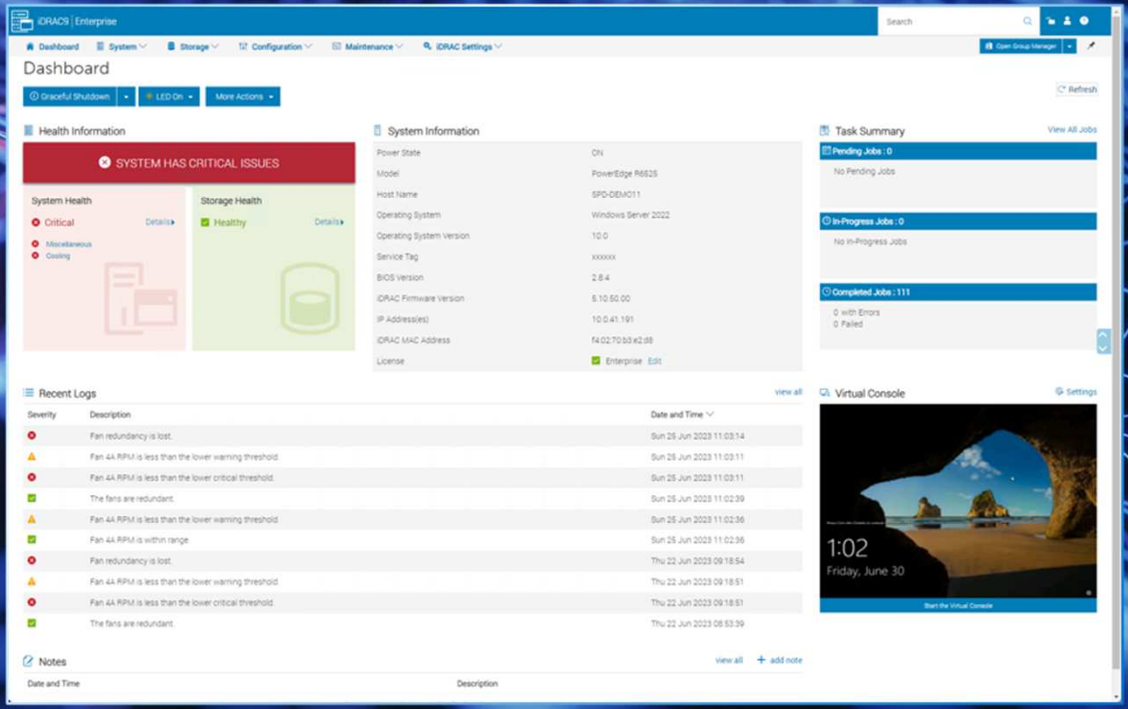
- Server | OS Console access
- Power Off | On

Monitor Health

- SNMPv3 | Syslog | SSE | Email

Deployment

- System Configuration Profile
- Zero touch provisioning



Dashboard

Health Information

SYSTEM HAS CRITICAL ISSUES

System Health
- Critical
- Miscellaneous
- Cooling

Storage Health
- Healthy

System Information

Power State	ON
Model	PowerEdge R6625
Host Name	SPD-DEMO11
Operating System	Windows Server 2022
Operating System Version	10.0
Service Tag	xxxxxx
BIOS Version	2.8.4
iDRAC Firmware Version	5.10.50.00
IP Address(es)	10.0.41.191
iDRAC MAC Address	f4:02:70:b3:e2:d8
License	✓ Enterprise Edit

Task Summary

Pending Jobs : 0
No Pending Jobs

In-Progress Jobs : 0
No In-Progress Jobs

Completed Jobs : 111
0 with Errors
0 Failed

Recent Logs

Severity	Description	Date and Time
⊗	Fan redundancy is lost.	Sun 25 Jun 2023 11:03:14
⚠	Fan 4A RPM is less than the lower warning threshold.	Sun 25 Jun 2023 11:03:11
⊗	Fan 4A RPM is less than the lower critical threshold.	Sun 25 Jun 2023 11:03:11
✓	The fans are redundant.	Sun 25 Jun 2023 11:02:39
⚠	Fan 4A RPM is less than the lower warning threshold.	Sun 25 Jun 2023 11:02:36
✓	Fan 4A RPM is within range.	Sun 25 Jun 2023 11:02:36
⊗	Fan redundancy is lost.	Thu 22 Jun 2023 09:18:54
⚠	Fan 4A RPM is less than the lower warning threshold.	Thu 22 Jun 2023 09:18:51
⊗	Fan 4A RPM is less than the lower critical threshold.	Thu 22 Jun 2023 09:18:51
✓	The fans are redundant.	Thu 22 Jun 2023 08:53:39

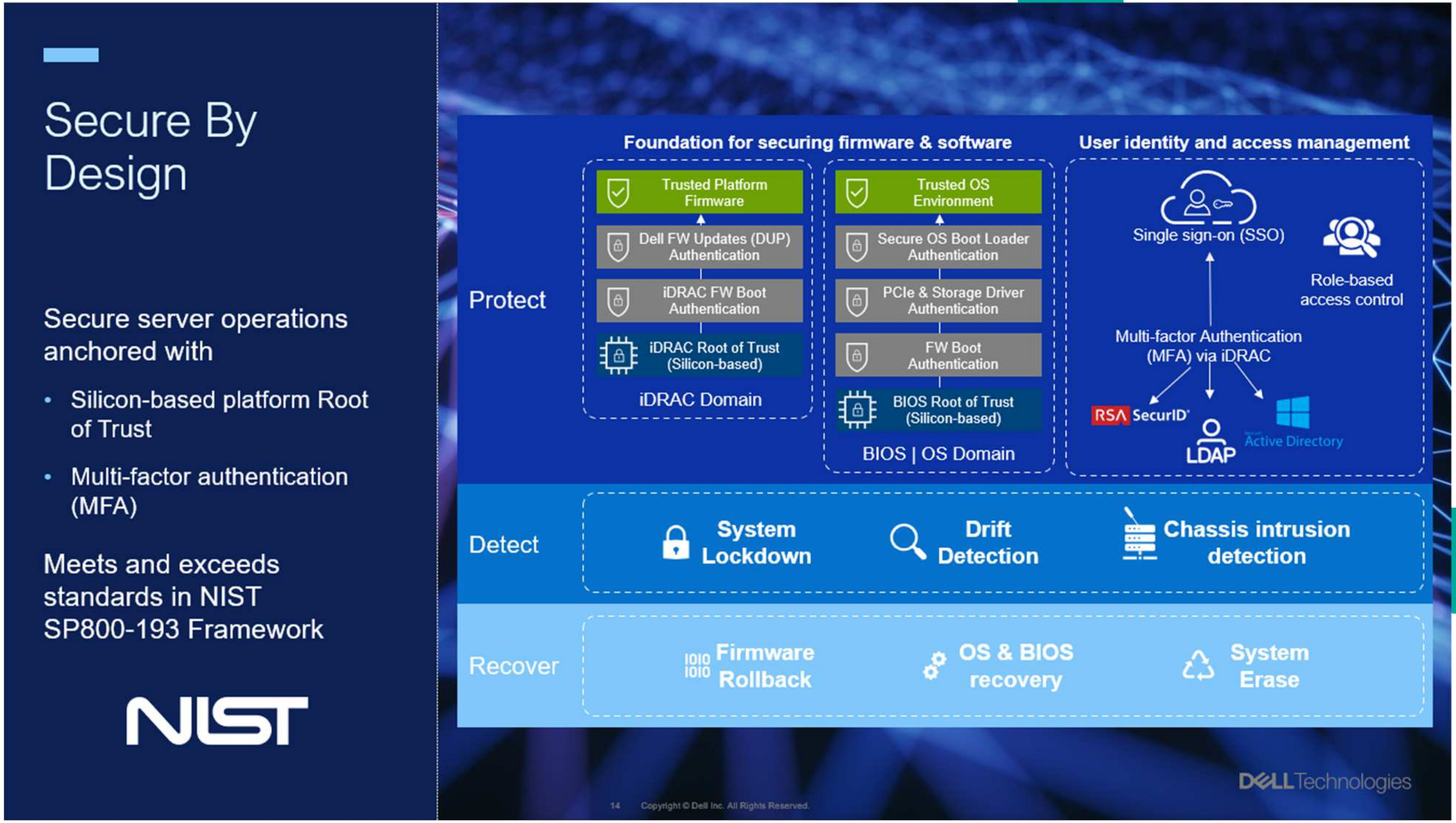
Virtual Console

Notes

Date and Time	Description

Copyright © Dell Inc. All Rights Reserved.

Beheer



Secure By Design

Secure server operations anchored with

- Silicon-based platform Root of Trust
- Multi-factor authentication (MFA)

Meets and exceeds standards in NIST SP800-193 Framework

NIST

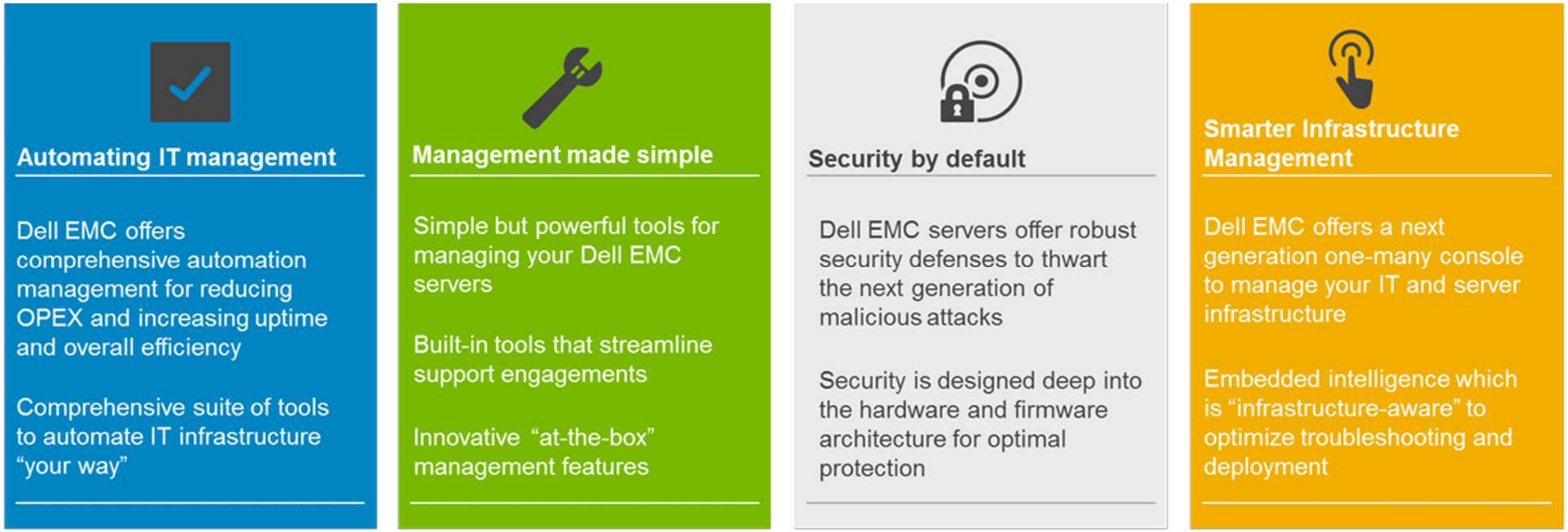
Foundation for securing firmware & software
User identity and access management
Protect
Trusted Platform Firmware
Dell FW Updates (DUP) Authentication
iDRAC FW Boot Authentication
iDRAC Root of Trust (Silicon-based)
iDRAC Domain
Trusted OS Environment
Secure OS Boot Loader Authentication
PCIe & Storage Driver Authentication
FW Boot Authentication
BIOS Root of Trust (Silicon-based)
BIOS | OS Domain
Single sign-on (SSO)
Role-based access control
Multi-factor Authentication (MFA) via iDRAC
RSA SecurID
LDAP
Active Directory
Detect
System Lockdown
Drift Detection
Chassis intrusion detection
Recover
Firmware Rollback
OS & BIOS recovery
System Erase
DELL Technologies
14
Copyright © Dell Inc. All Rights Reserved.

DELL Technologies

inetum
realdolmen
Positive digital flow

Beheer

- IDRAC



Automating IT management

Dell EMC offers comprehensive automation management for reducing OPEX and increasing uptime and overall efficiency

Comprehensive suite of tools to automate IT infrastructure "your way"

Management made simple

Simple but powerful tools for managing your Dell EMC servers

Built-in tools that streamline support engagements

Innovative "at-the-box" management features

Security by default

Dell EMC servers offer robust security defenses to thwart the next generation of malicious attacks

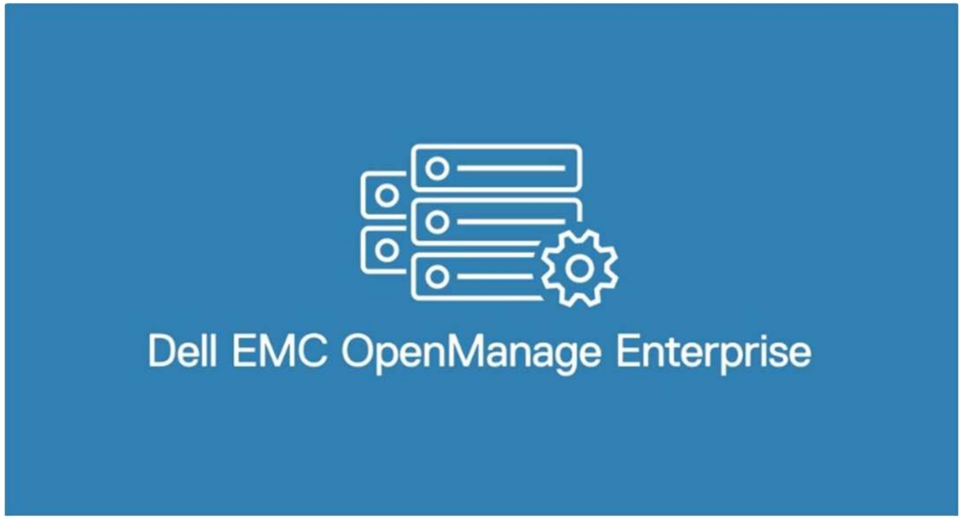
Security is designed deep into the hardware and firmware architecture for optimal protection

Smarter Infrastructure Management

Dell EMC offers a next generation one-many console to manage your IT and server infrastructure

Embedded intelligence which is "infrastructure-aware" to optimize troubleshooting and deployment

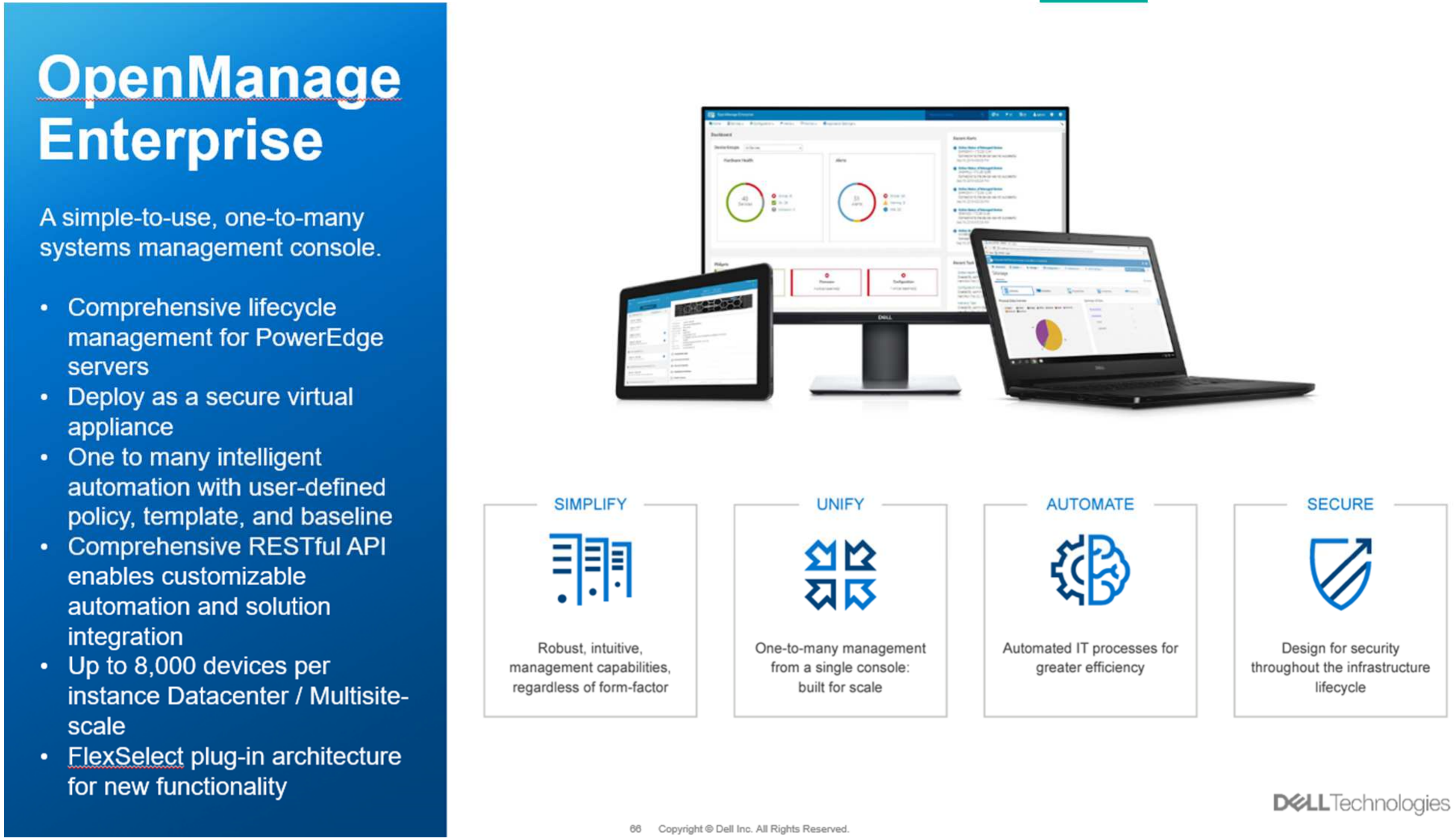
Beheer



DELL Technologies

inetum. realdolmen Positive digital flow

Beheer



OpenManage Enterprise

A simple-to-use, one-to-many systems management console.

- Comprehensive lifecycle management for PowerEdge servers
- Deploy as a secure virtual appliance
- One to many intelligent automation with user-defined policy, template, and baseline
- Comprehensive RESTful API enables customizable automation and solution integration
- Up to 8,000 devices per instance Datacenter / Multisite-scale
- FlexSelect plug-in architecture for new functionality

SIMPLIFY

Robust, intuitive, management capabilities, regardless of form-factor

UNIFY

One-to-many management from a single console: built for scale

AUTOMATE

Automated IT processes for greater efficiency

SECURE

Design for security throughout the infrastructure lifecycle

DELL Technologies

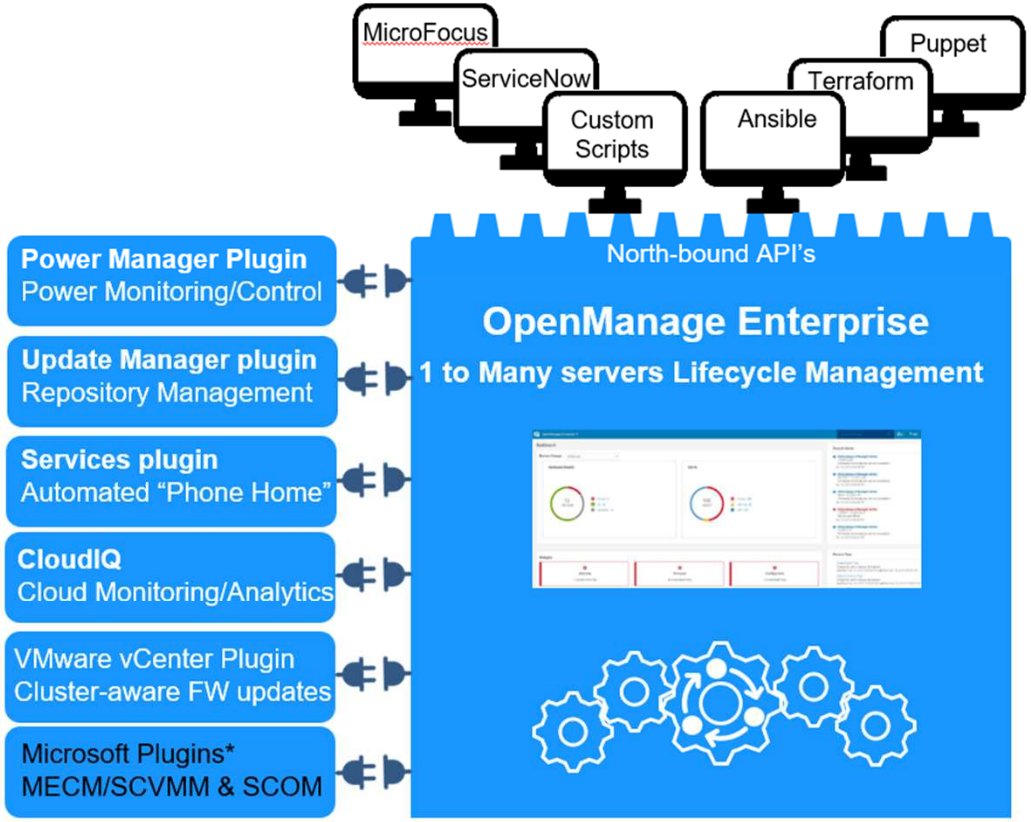
66 Copyright © Dell Inc. All Rights Reserved.

Beheer

OpenManage Enterprise

FlexSelect Plugin Architecture

- Modular software design allows for easy development cycles to add functionality with new plugin modules.
- Single console for all management functions.
- Fully integrated plugin module upgrade process within OME console.



MicroFocus

ServiceNow

Custom Scripts

Ansible

Terraform

Puppet

North-bound API's

OpenManage Enterprise

1 to Many servers Lifecycle Management

Power Manager Plugin
Power Monitoring/Control

Update Manager plugin
Repository Management

Services plugin
Automated "Phone Home"

CloudIQ
Cloud Monitoring/Analytics

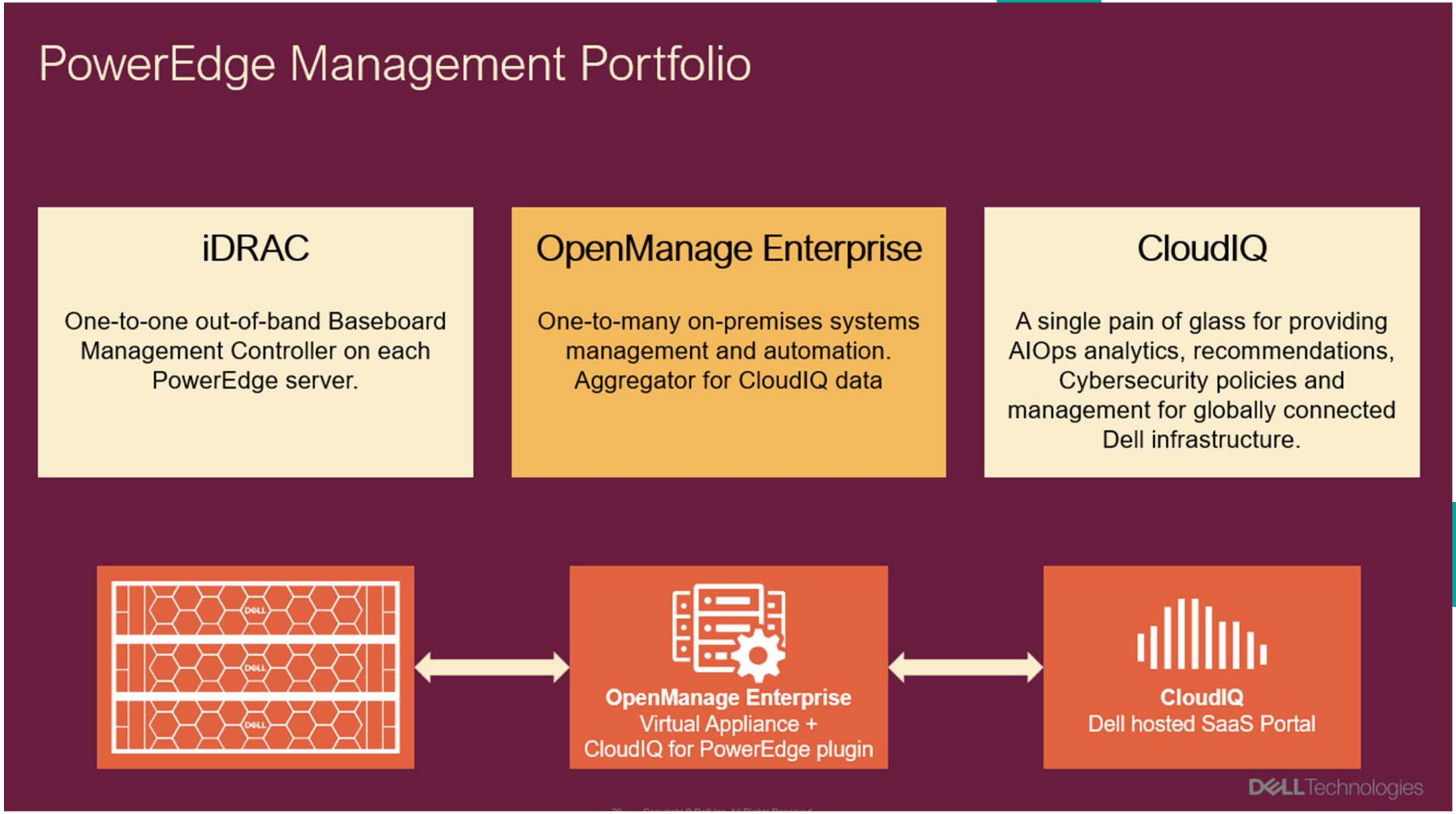
VMware vCenter Plugin
Cluster-aware FW updates

Microsoft Plugins*
MECM/SCVMM & SCOM

* System Center Available Q422

Copyright © Dell Inc. All Rights Reserved.

Beheer



PowerEdge Management Portfolio

iDRAC

One-to-one out-of-band Baseboard Management Controller on each PowerEdge server.

OpenManage Enterprise

One-to-many on-premises systems management and automation. Aggregator for CloudIQ data

CloudIQ

A single pain of glass for providing AIOps analytics, recommendations, Cybersecurity policies and management for globally connected Dell infrastructure.

OpenManage Enterprise
Virtual Appliance +
CloudIQ for PowerEdge plugin

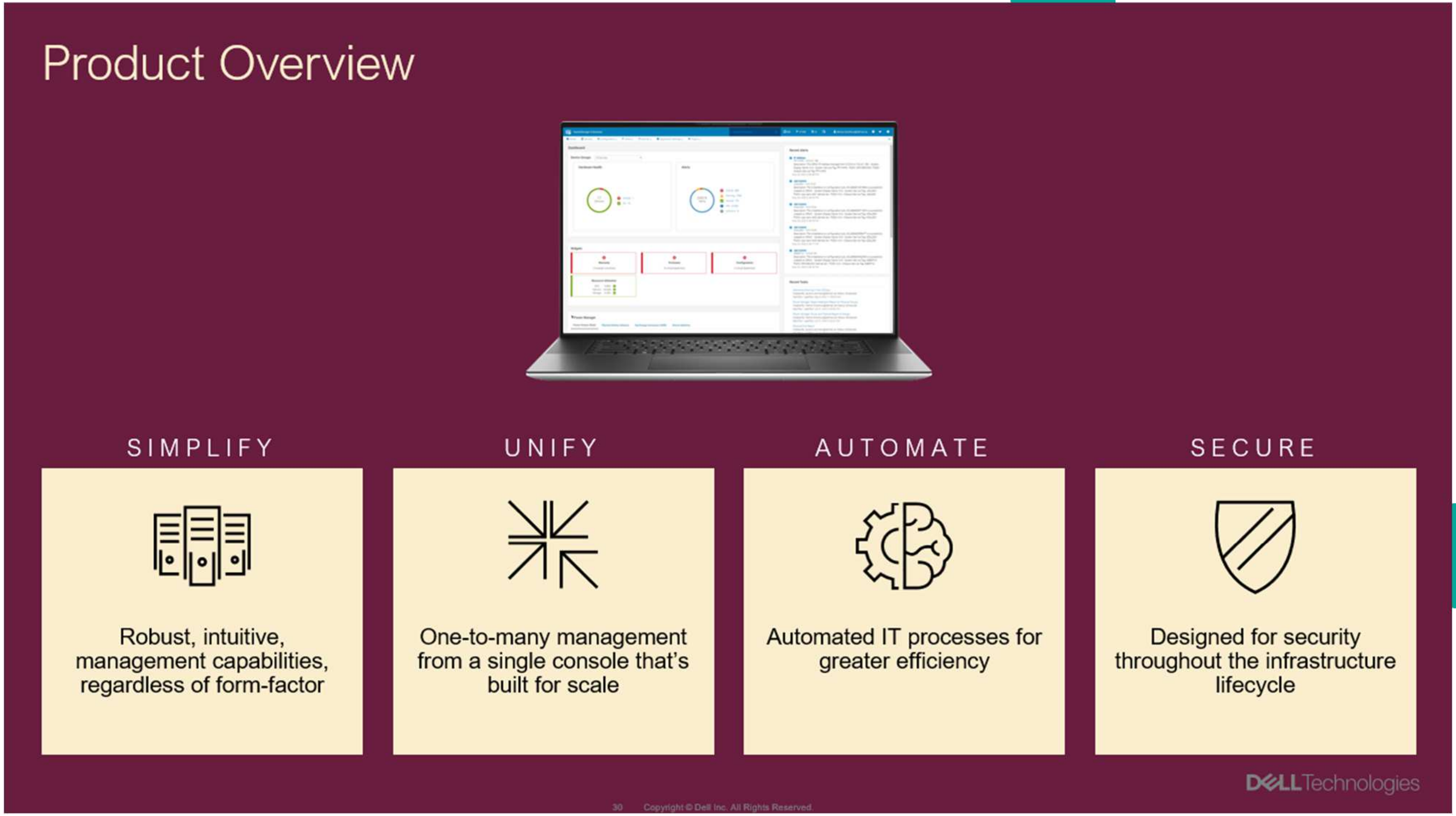
CloudIQ
Dell hosted SaaS Portal

DELL Technologies

DELL Technologies

inetum realdolmen
Positive digital flow

Beheer



Product Overview

SIMPLIFY

Robust, intuitive, management capabilities, regardless of form-factor

UNIFY

One-to-many management from a single console that's built for scale

AUTOMATE

Automated IT processes for greater efficiency

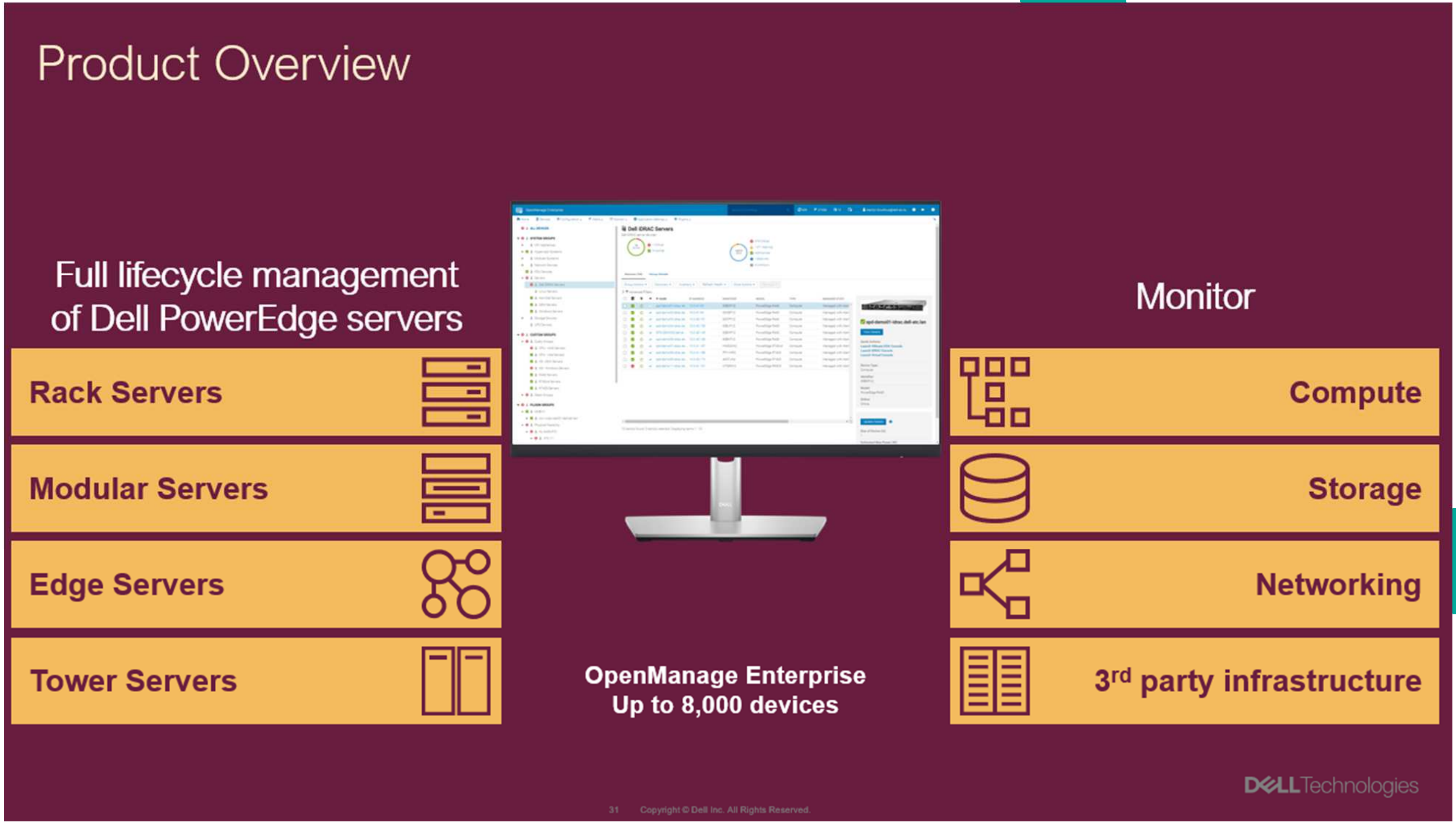
SECURE

Designed for security throughout the infrastructure lifecycle

DELL Technologies

30 Copyright © Dell Inc. All Rights Reserved.

Beheer



Product Overview

Full lifecycle management of Dell PowerEdge servers

- Rack Servers
- Modular Servers
- Edge Servers
- Tower Servers

OpenManage Enterprise
Up to 8,000 devices

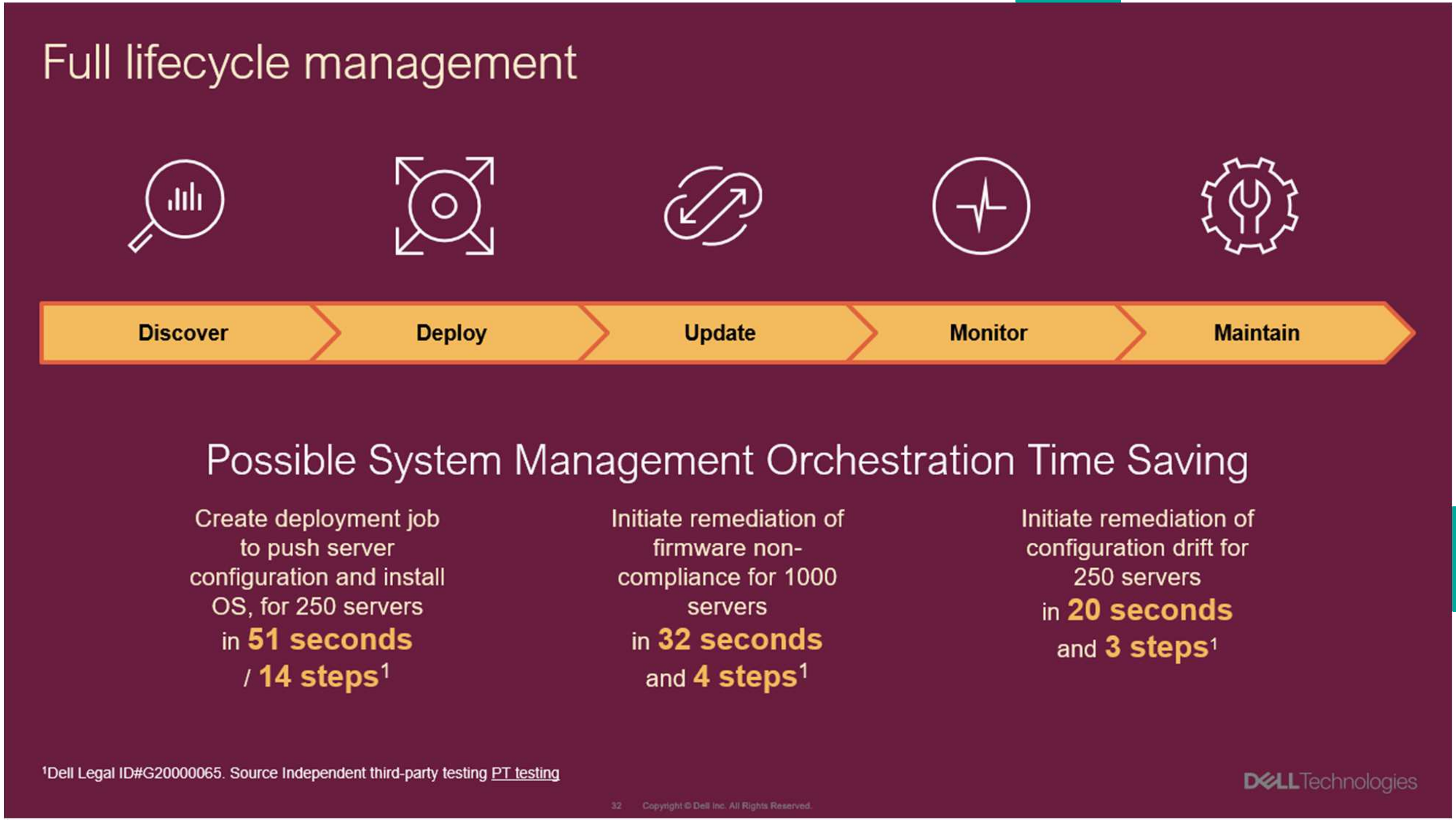
Monitor

- Compute
- Storage
- Networking
- 3rd party infrastructure

DELL Technologies

31 Copyright © Dell Inc. All Rights Reserved.

Beheer



Full lifecycle management

Possible System Management Orchestration Time Saving

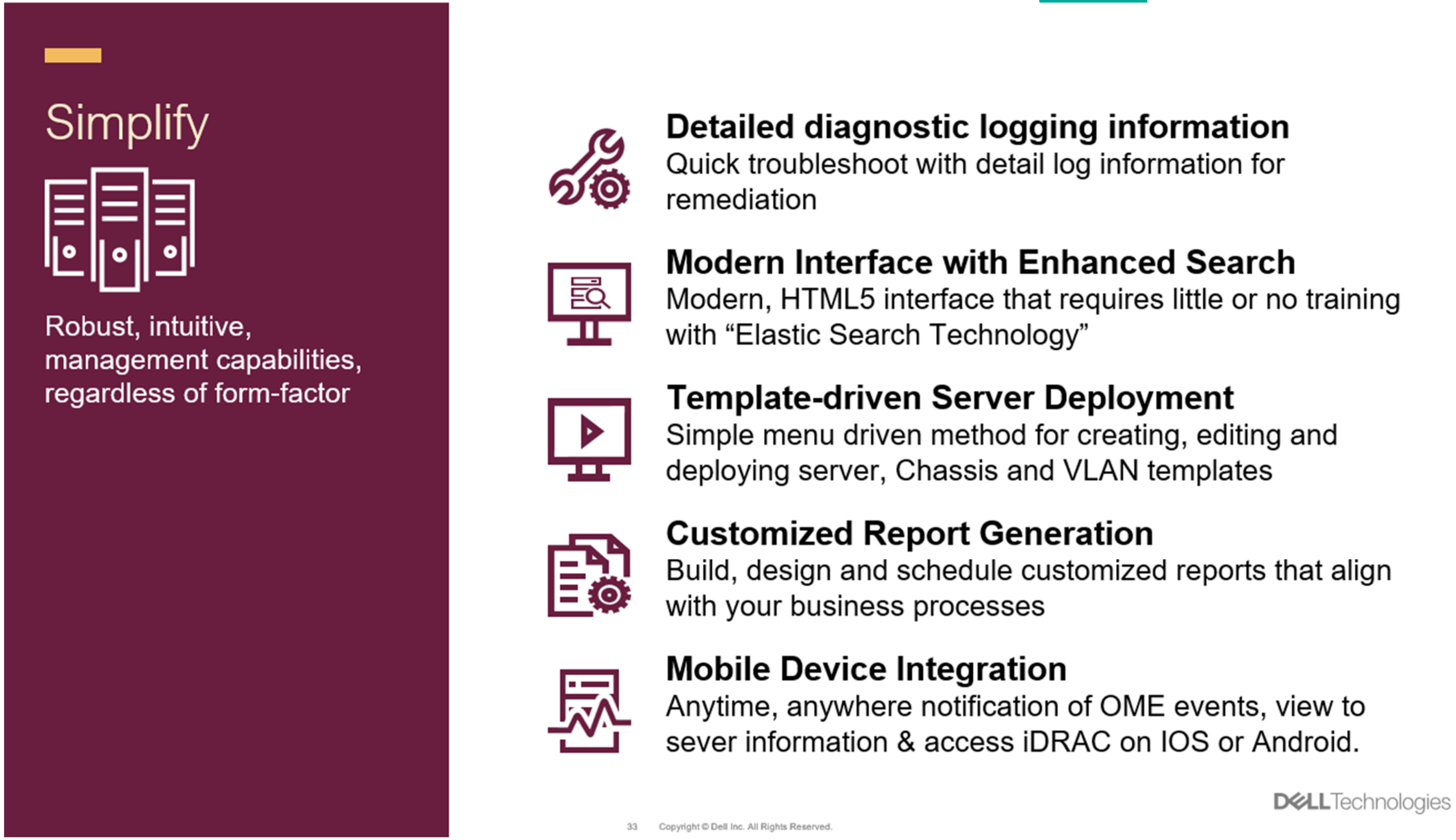
Create deployment job to push server configuration and install OS, for 250 servers in **51 seconds** / **14 steps**[1]

Initiate remediation of firmware non-compliance for 1000 servers in **32 seconds** and **4 steps**[1]

Initiate remediation of configuration drift for 250 servers in **20 seconds** and **3 steps**[1]

[1] Dell Legal ID#G20000065. Source Independent third-party testing PT testing

Beheer



Simplify

Robust, intuitive, management capabilities, regardless of form-factor

Detailed diagnostic logging information
Quick troubleshoot with detail log information for remediation

Modern Interface with Enhanced Search
Modern, HTML5 interface that requires little or no training with “Elastic Search Technology”

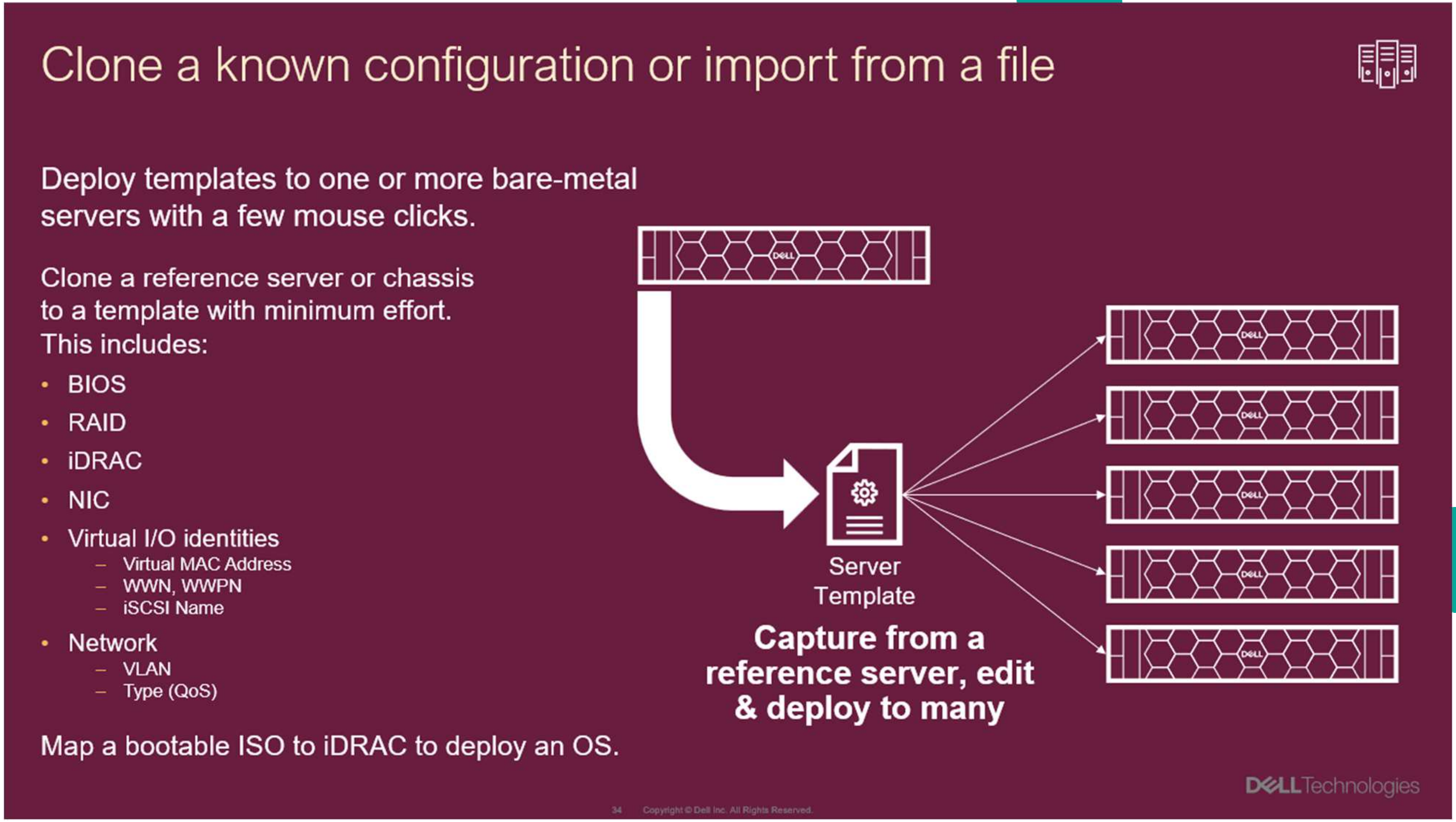
Template-driven Server Deployment
Simple menu driven method for creating, editing and deploying server, Chassis and VLAN templates

Customized Report Generation
Build, design and schedule customized reports that align with your business processes

Mobile Device Integration
Anytime, anywhere notification of OME events, view to sever information & access iDRAC on IOS or Android.

Copyright © Dell Inc. All Rights Reserved.

Beheer



Clone a known configuration or import from a file

Deploy templates to one or more bare-metal servers with a few mouse clicks.

Clone a reference server or chassis to a template with minimum effort. This includes:

- BIOS
- RAID
- iDRAC
- NIC
- Virtual I/O identities
  - Virtual MAC Address
  - WWN, WWPN
  - iSCSI Name
- Network
  - VLAN
  - Type (QoS)

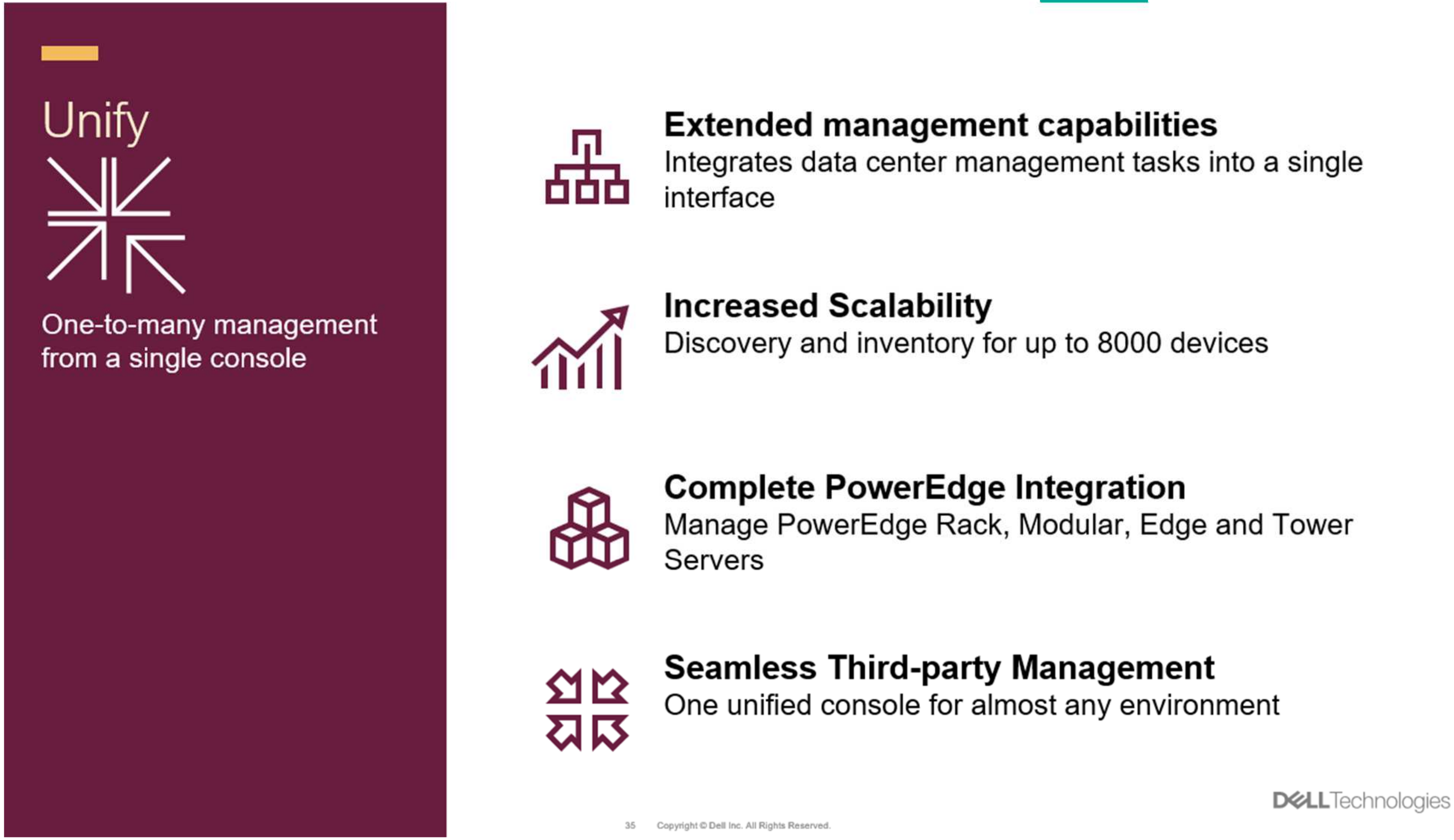
Map a bootable ISO to iDRAC to deploy an OS.

Server Template

Capture from a reference server, edit & deploy to many

Copyright © Dell Inc. All Rights Reserved.

Beheer



Unify

One-to-many management from a single console

Extended management capabilities
Integrates data center management tasks into a single interface

Increased Scalability
Discovery and inventory for up to 8000 devices

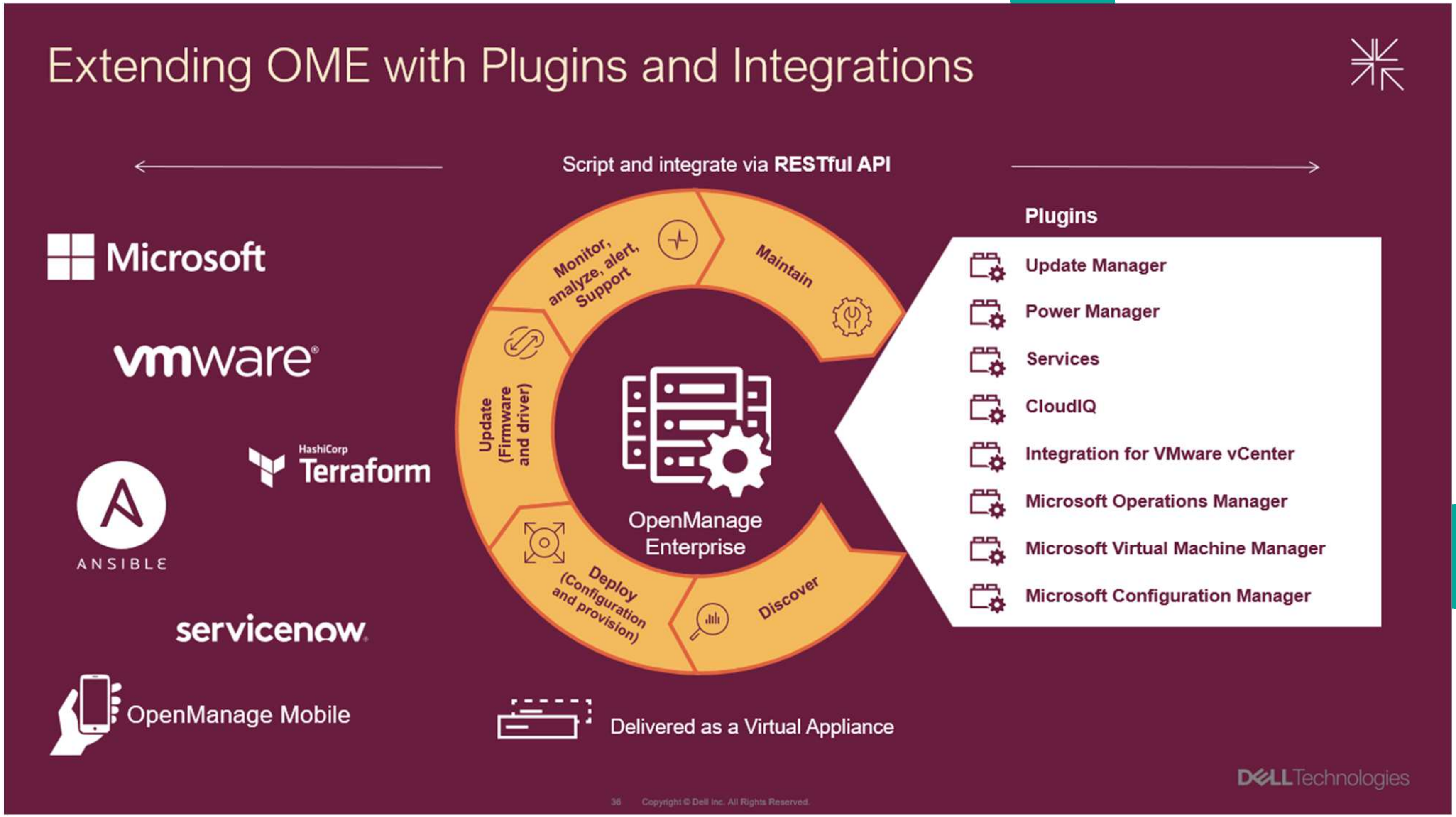
Complete PowerEdge Integration
Manage PowerEdge Rack, Modular, Edge and Tower Servers

Seamless Third-party Management
One unified console for almost any environment

DELL Technologies

35 Copyright © Dell Inc. All Rights Reserved.

Beheer



Extending OME with Plugins and Integrations

Script and integrate via **RESTful API**

Microsoft
vmware
HashiCorp Terraform
ANSIBLE
servicenow
Monitor, analyze, alert, Support
Maintain
Update (Firmware and driver)
Deploy (Configuration and provision)
Discover
OpenManage Enterprise

Plugins

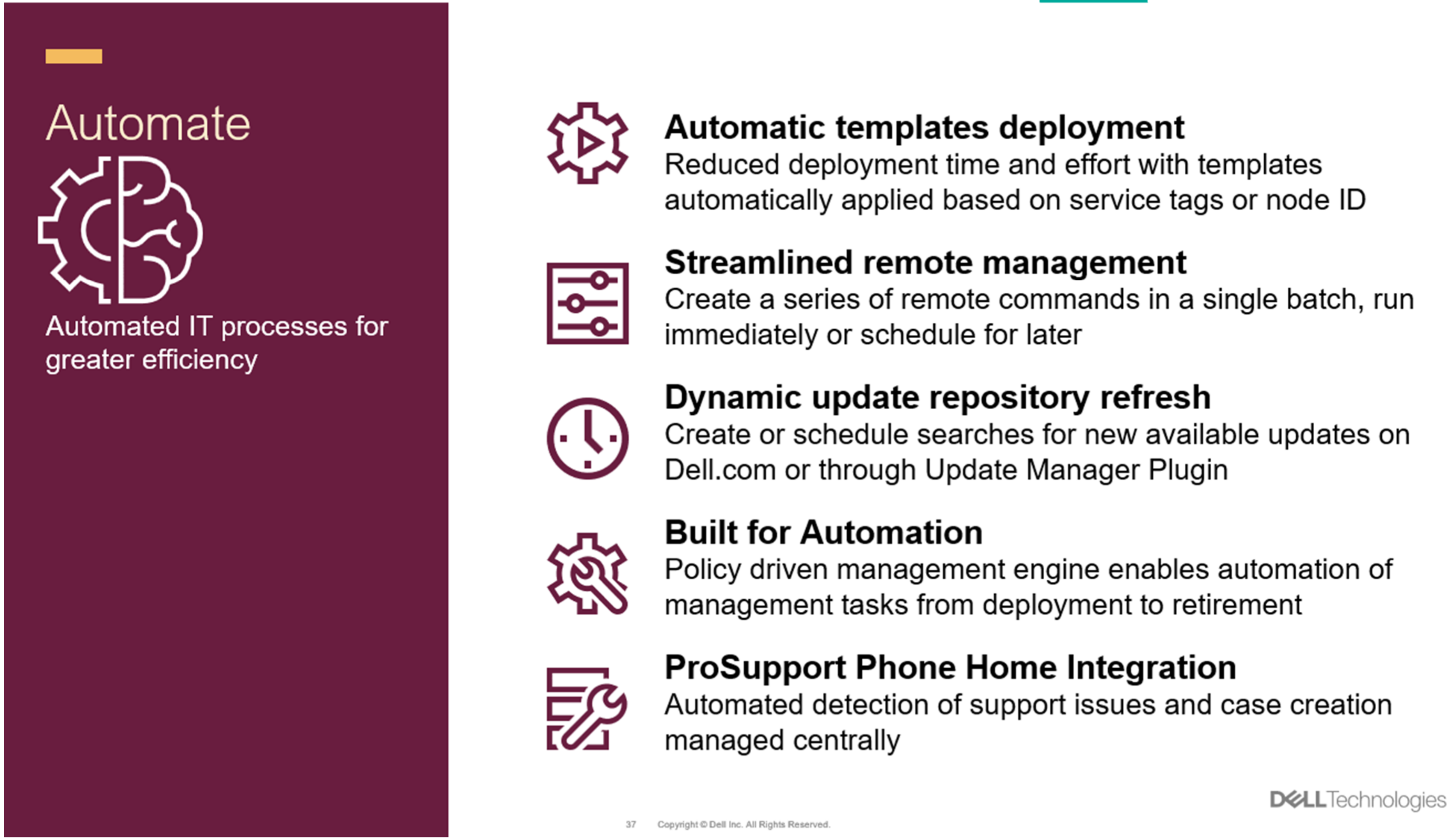
- Update Manager
- Power Manager
- Services
- CloudIQ
- Integration for VMware vCenter
- Microsoft Operations Manager
- Microsoft Virtual Machine Manager
- Microsoft Configuration Manager

OpenManage Mobile

Delivered as a Virtual Appliance

36 Copyright © Dell Inc. All Rights Reserved.

Beheer



Automate

Automated IT processes for greater efficiency

Automatic templates deployment
Reduced deployment time and effort with templates automatically applied based on service tags or node ID

Streamlined remote management
Create a series of remote commands in a single batch, run immediately or schedule for later

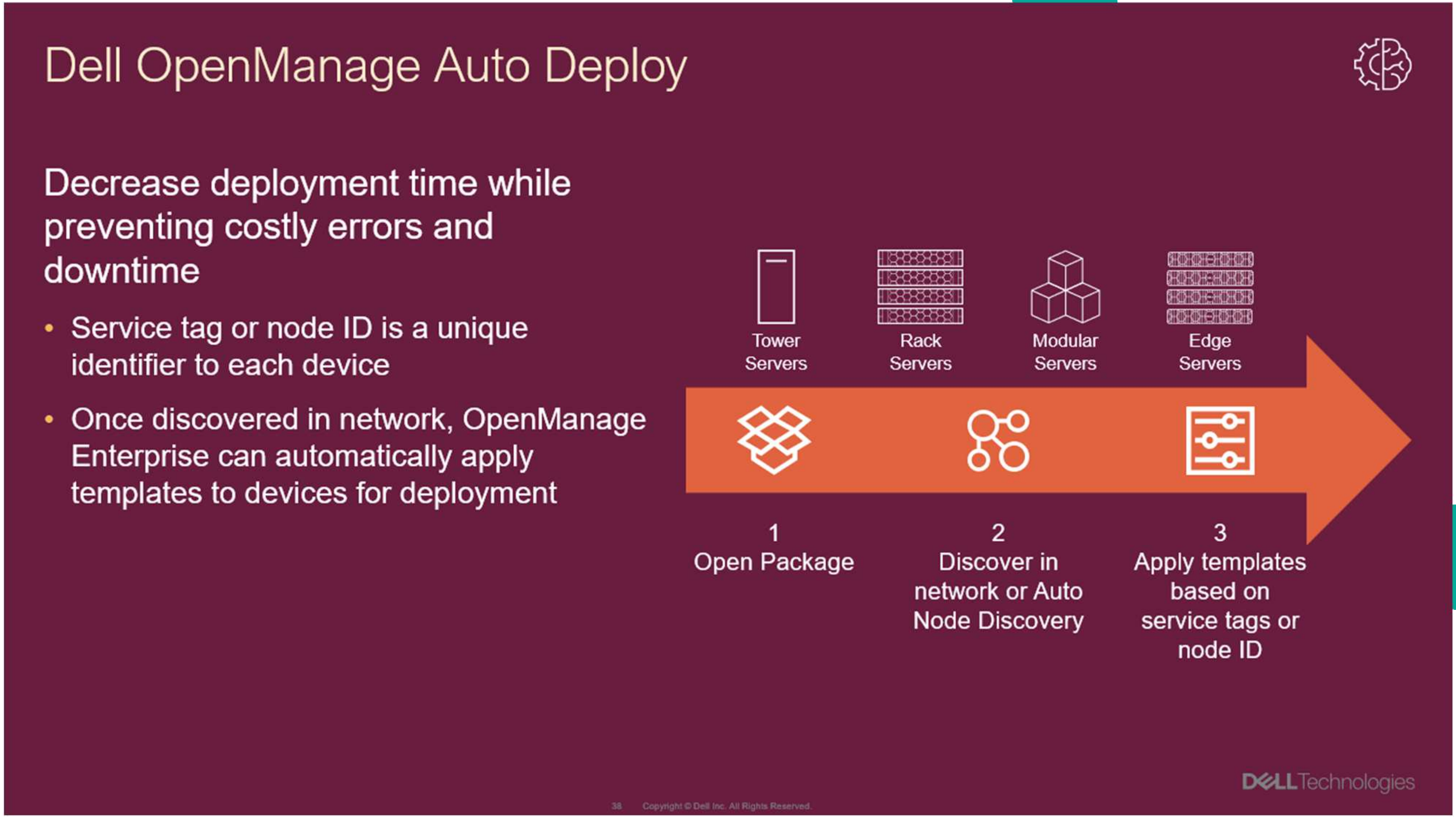
Dynamic update repository refresh
Create or schedule searches for new available updates on Dell.com or through Update Manager Plugin

Built for Automation
Policy driven management engine enables automation of management tasks from deployment to retirement

ProSupport Phone Home Integration
Automated detection of support issues and case creation managed centrally

37 Copyright © Dell Inc. All Rights Reserved.

Beheer



Dell OpenManage Auto Deploy

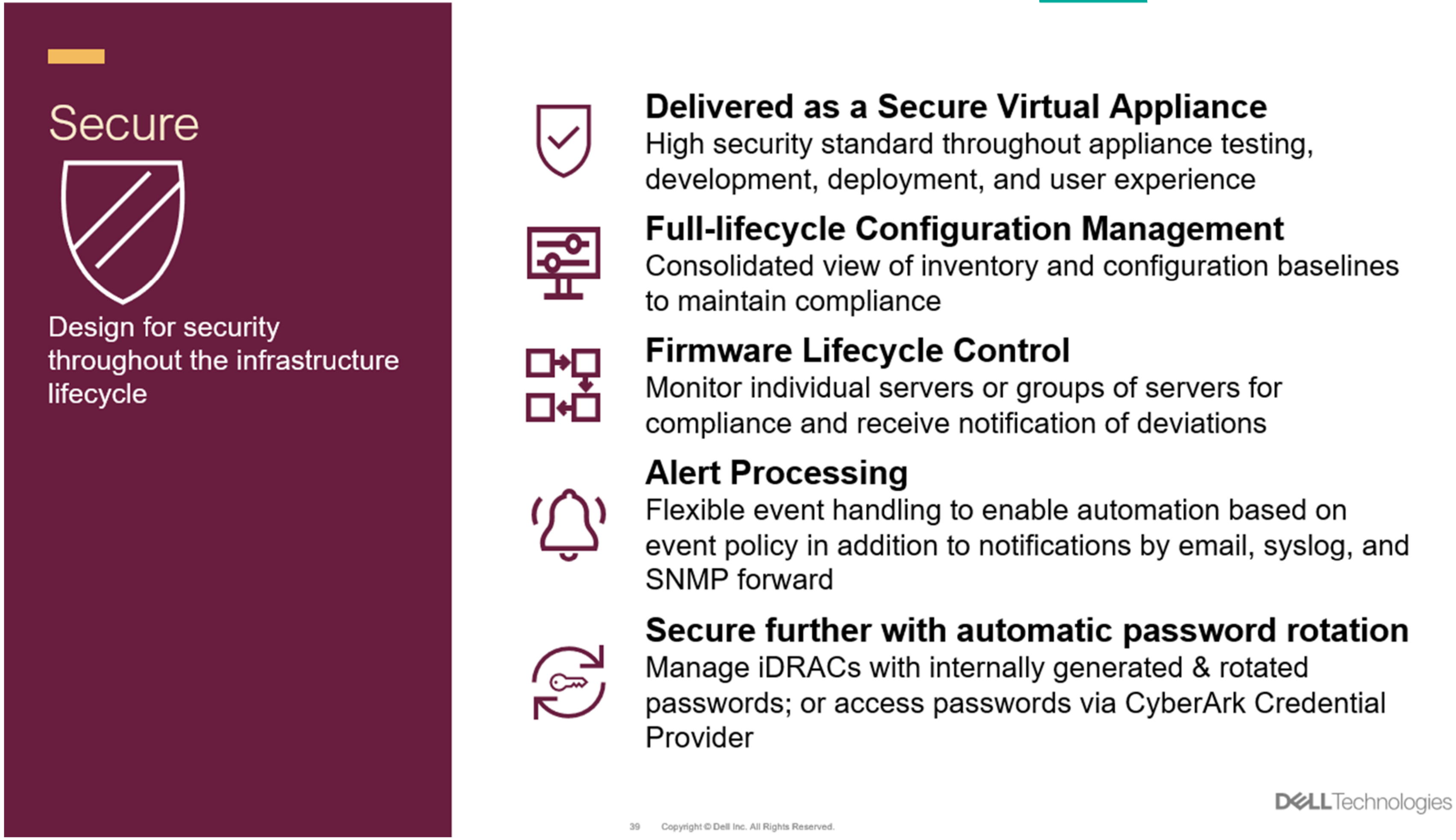
Decrease deployment time while preventing costly errors and downtime

- Service tag or node ID is a unique identifier to each device
- Once discovered in network, OpenManage Enterprise can automatically apply templates to devices for deployment

Tower Servers
Rack Servers
Modular Servers
Edge Servers
1
Open Package
2
Discover in network or Auto Node Discovery
3
Apply templates based on service tags or node ID
DELL Technologies

38 Copyright © Dell Inc. All Rights Reserved.

Beheer



Secure

Design for security throughout the infrastructure lifecycle

Delivered as a Secure Virtual Appliance
High security standard throughout appliance testing, development, deployment, and user experience

Full-lifecycle Configuration Management
Consolidated view of inventory and configuration baselines to maintain compliance

Firmware Lifecycle Control
Monitor individual servers or groups of servers for compliance and receive notification of deviations

Alert Processing
Flexible event handling to enable automation based on event policy in addition to notifications by email, syslog, and SNMP forward

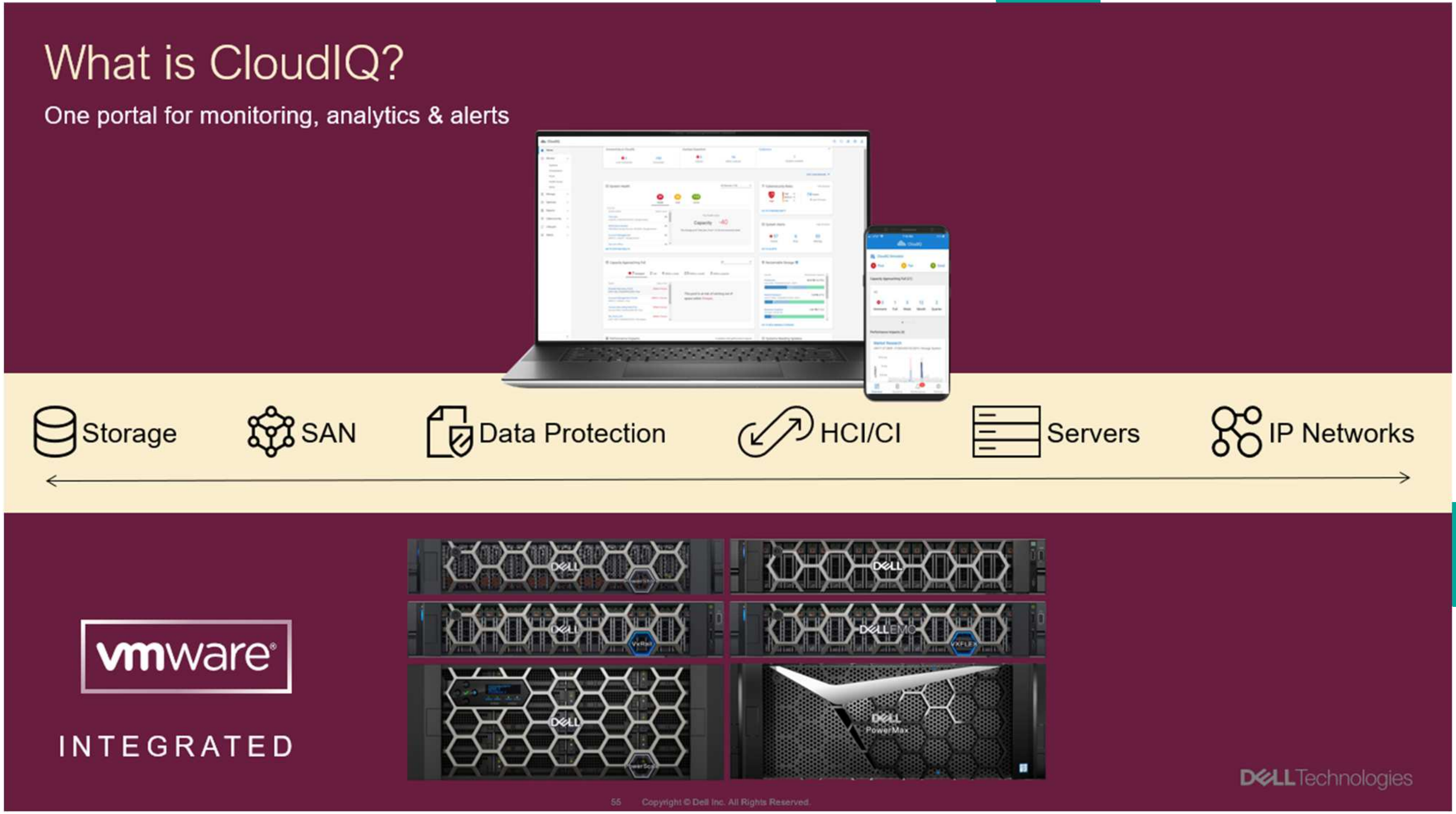
Secure further with automatic password rotation
Manage iDRACs with internally generated & rotated passwords; or access passwords via CyberArk Credential Provider

39

Copyright © Dell Inc. All Rights Reserved.

CloudIQ

Monitoring - AI



What is CloudIQ?

One portal for monitoring, analytics & alerts

Storage | SAN | Data Protection | HCI/CI | Servers | IP Networks

vmware

INTEGRATED

55 Copyright © Dell Inc. All Rights Reserved.

CAPEX vs OPEX

- DELLEMC APEX

APEX
Multicloud
As-a-Service
End-to-End global support services
Supply chain leadership

inetum

realdolmen

Positive digital flow

inetum.world

FRANCE | SPAIN | PORTUGAL | BELGIUM | SWITZERLAND | LUXEMBOURG | ENGLAND |
POLAND | ROMANIA | MOROCCO | TUNISIA | SENEGAL | CÔTE D'IVOIRE | ANGOLA |
CAMEROON | USA | BRAZIL | COLOMBIA | MEXICO | RP OF PANAMA | PERU | CHILI |
COSTA RICA | DOMINICAN REPUBLIC | ARGENTINA | SINGAPORE | UAE

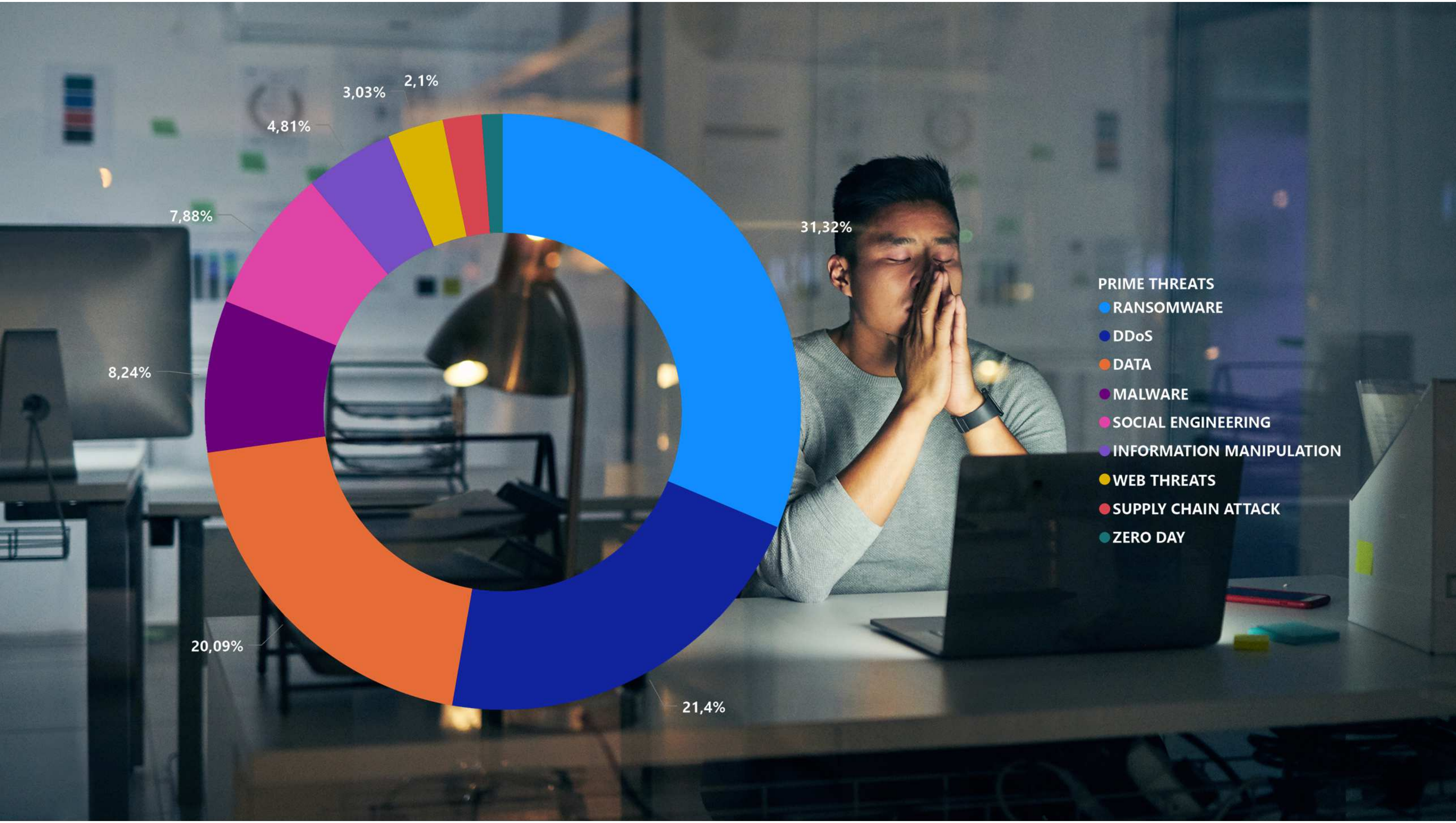
inetum realdolmen

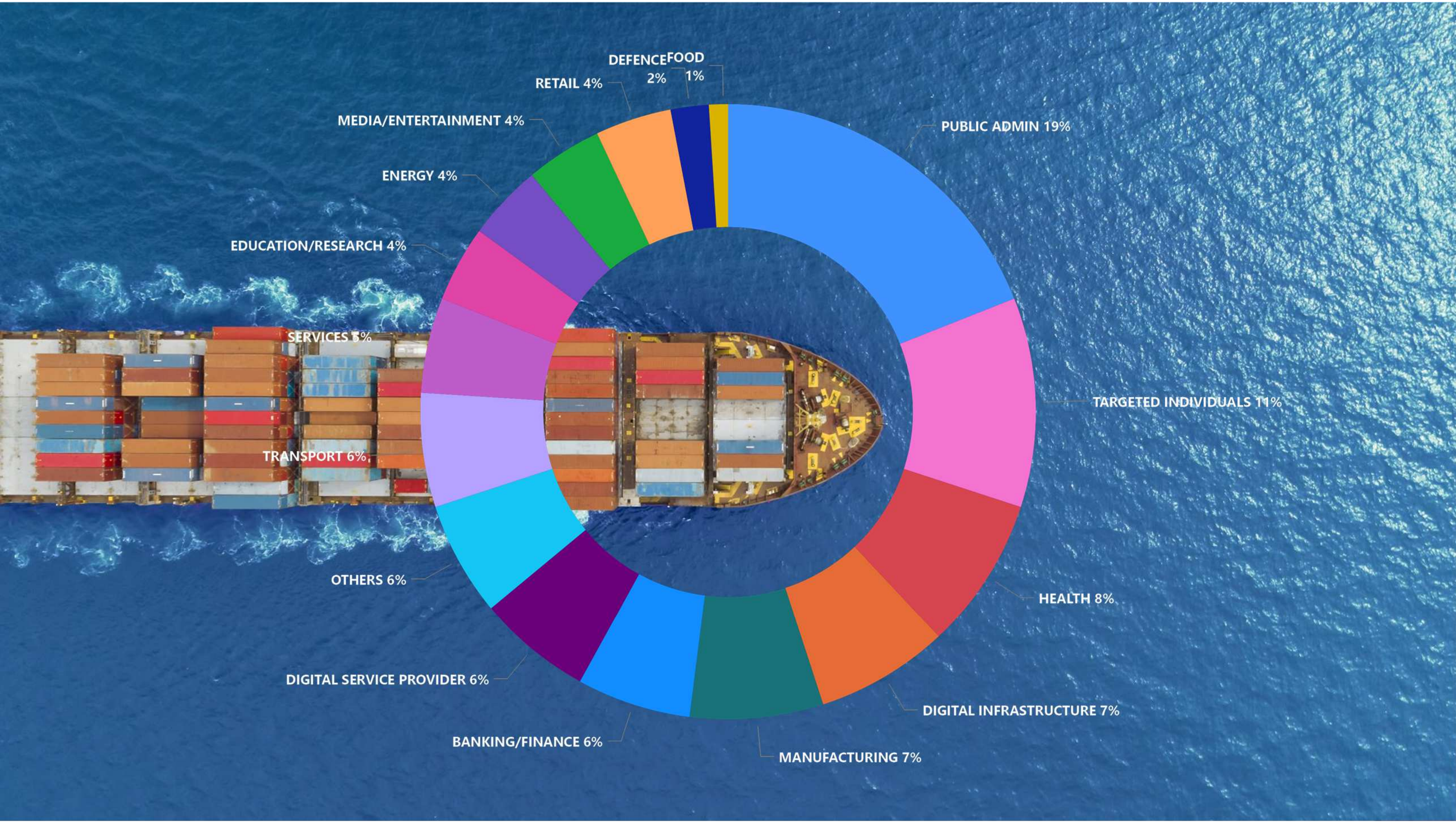
Positive digital flow

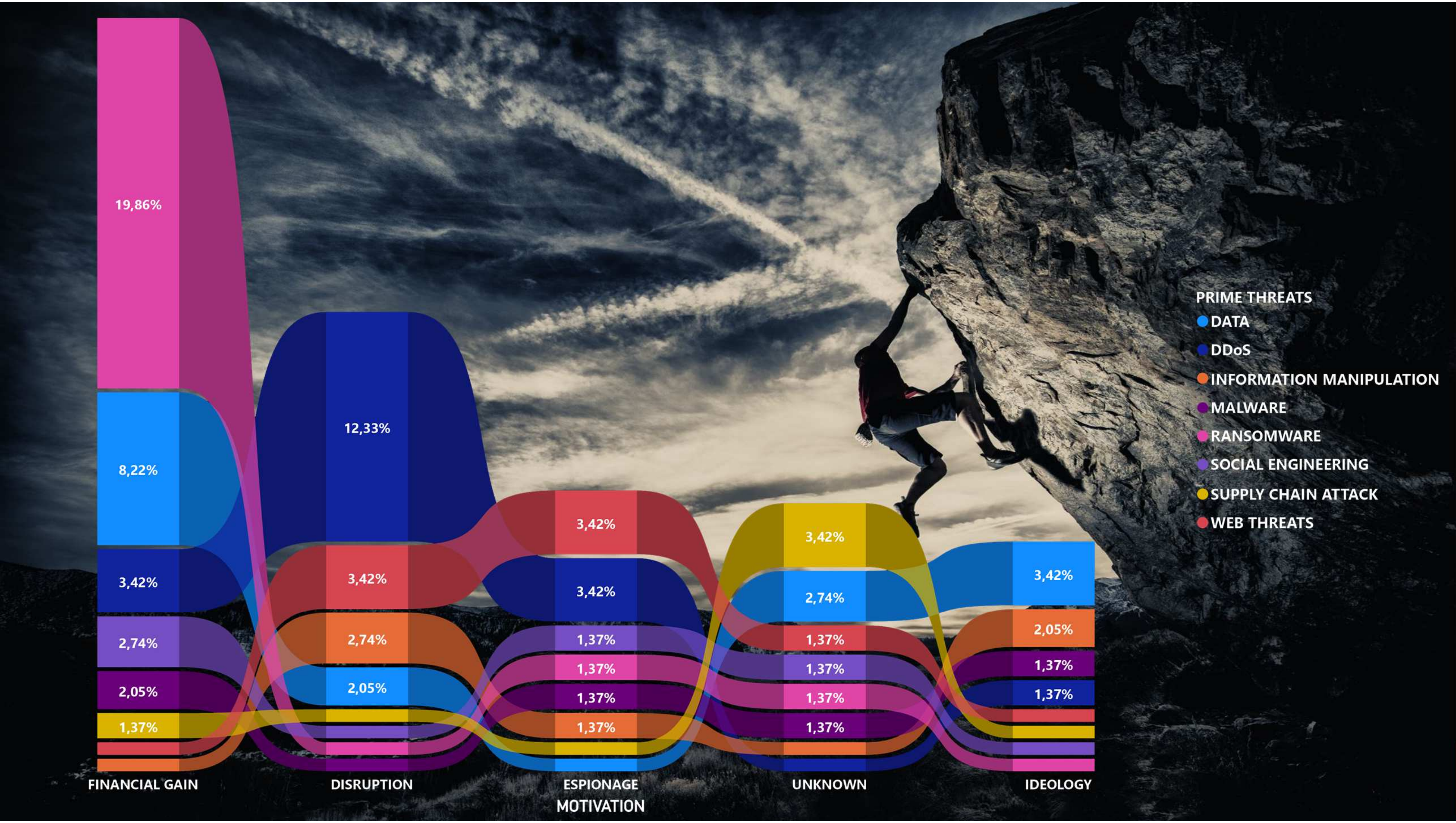
IT Cybersecurity (Anthony De Smet)

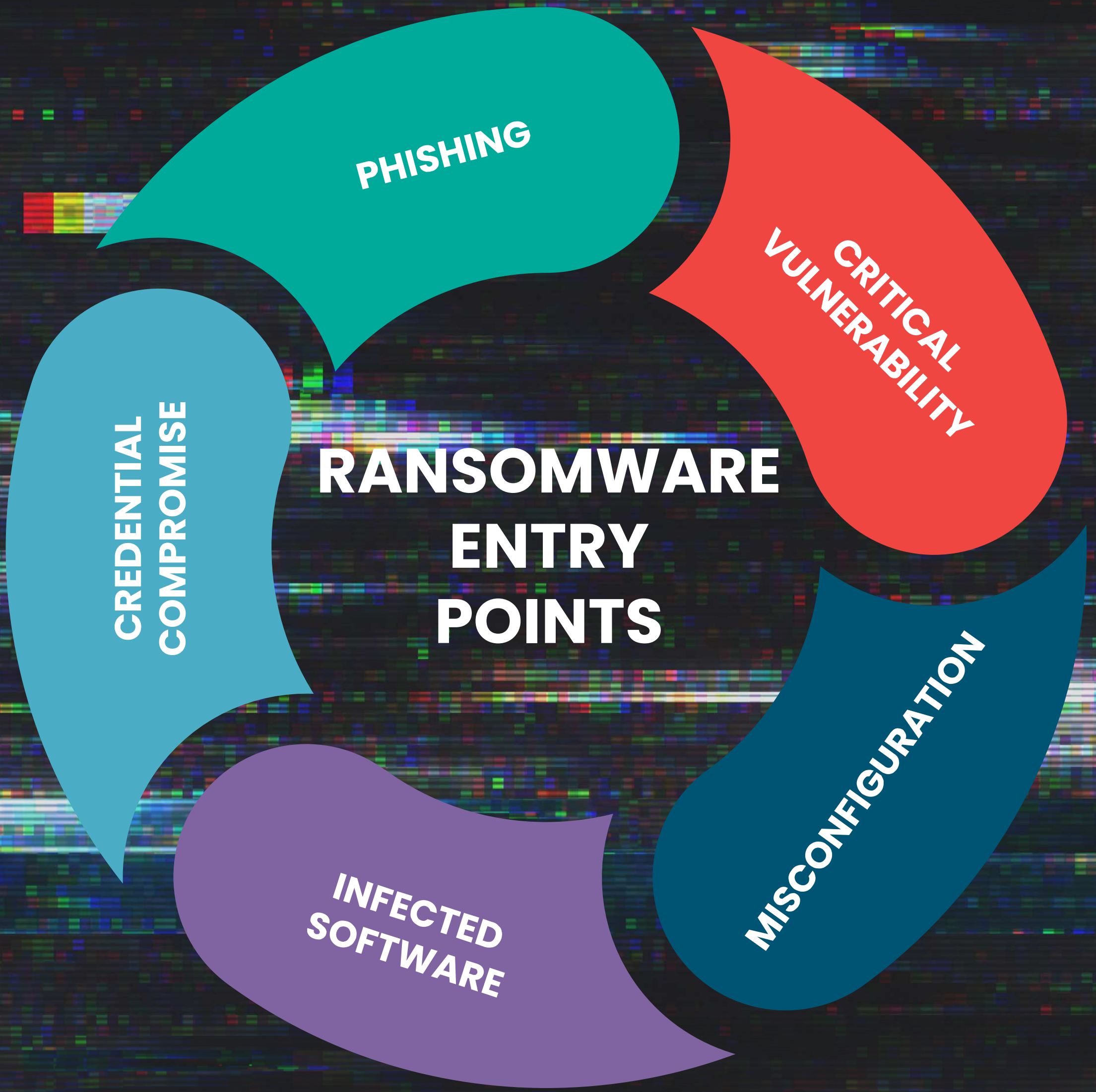
inetum realdolmen
Positive digital flow

State of Cybersecurity 2024


2,1%
3,03%
4,81%
7,88%
31,32%
8,24%
20,09%
21,4%
PRIME THREATS
● RANSOMWARE
● DDoS
● DATA
● MALWARE
● SOCIAL ENGINEERING
● INFORMATION MANIPULATION
● WEB THREATS
● SUPPLY CHAIN ATTACK
● ZERO DAY


DEFENCE 2%
FOOD 1%
RETAIL 4%
MEDIA/ENTERTAINMENT 4%
PUBLIC ADMIN 19%
ENERGY 4%
EDUCATION/RESEARCH 4%
SERVICES 5%
TARGETED INDIVIDUALS 11%
TRANSPORT 6%
OTHERS 6%
HEALTH 8%
DIGITAL SERVICE PROVIDER 6%
DIGITAL INFRASTRUCTURE 7%
BANKING/FINANCE 6%
MANUFACTURING 7%


19,86%
8,22%
3,42%
2,74%
2,05%
1,37%
12,33%
3,42%
2,74%
2,05%
3,42%
3,42%
1,37%
1,37%
1,37%
1,37%
3,42%
2,74%
1,37%
1,37%
1,37%
1,37%
3,42%
2,05%
1,37%
1,37%
FINANCIAL GAIN
DISRUPTION
ESPIONAGE
MOTIVATION
UNKNOWN
IDEOLOGY
PRIME THREATS
● DATA
● DDoS
● INFORMATION MANIPULATION
● MALWARE
● RANSOMWARE
● SOCIAL ENGINEERING
● SUPPLY CHAIN ATTACK
● WEB THREATS



RANSOMWARE ENTRY POINTS

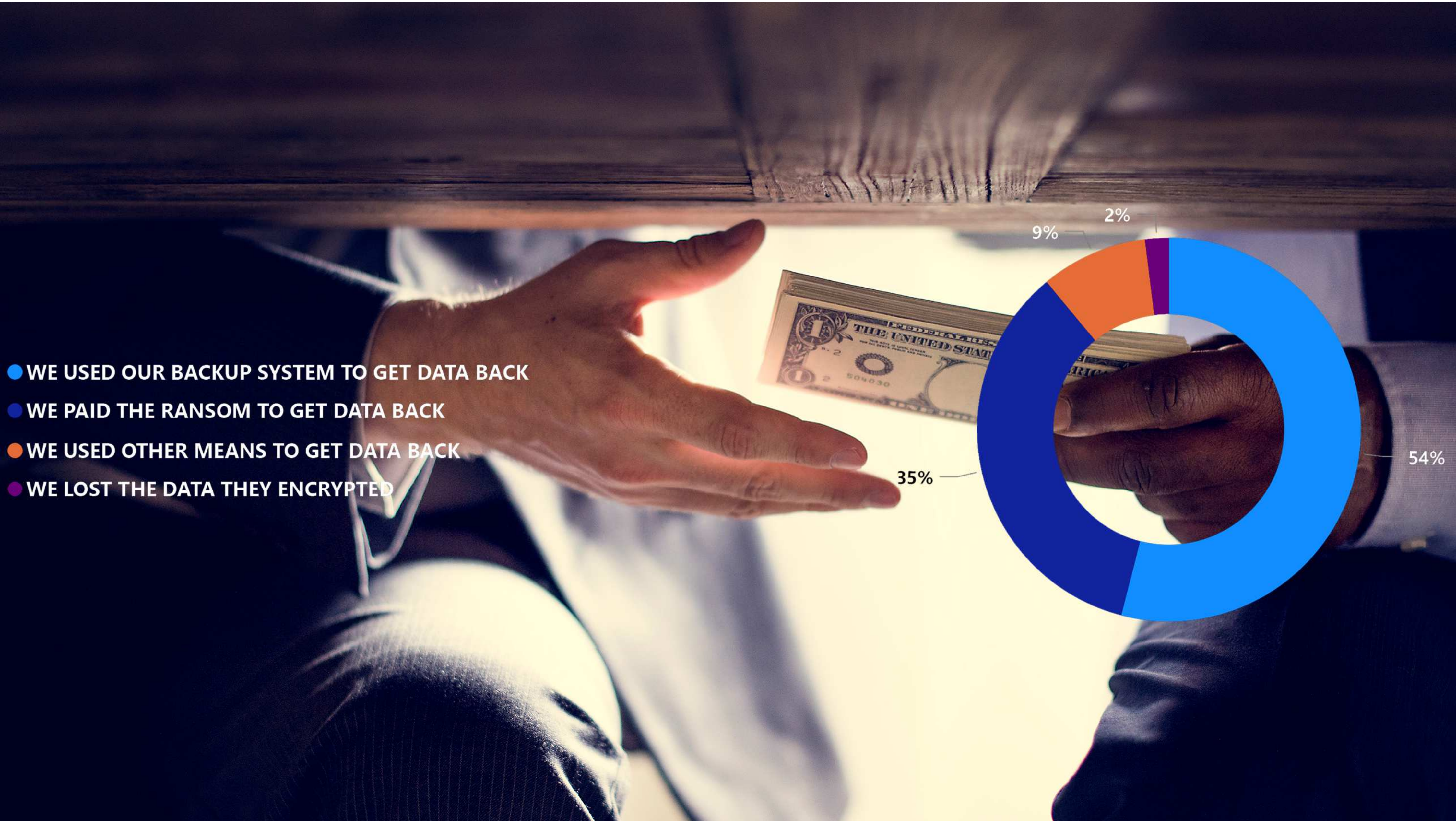
PHISHING

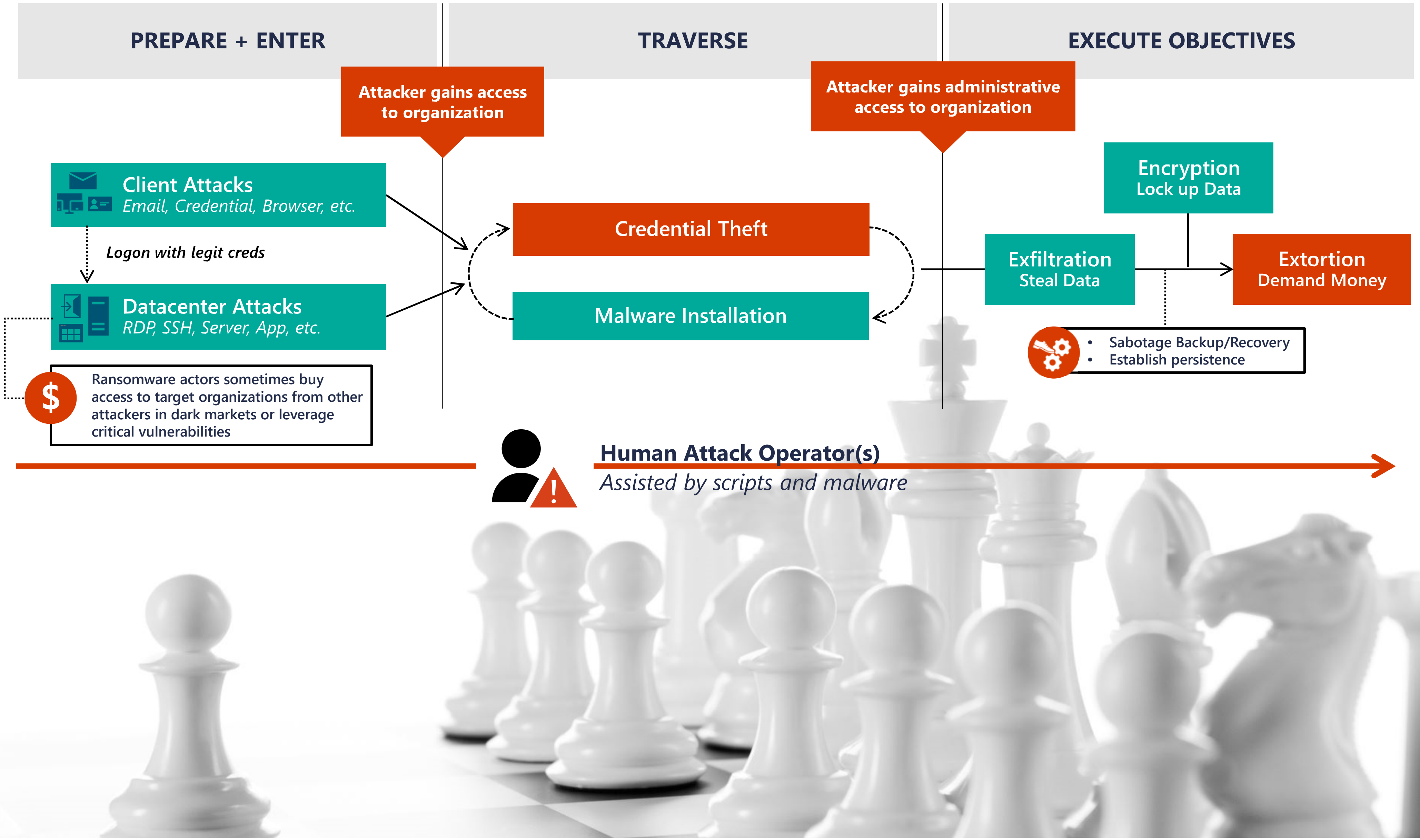
CRITICAL VULNERABILITY

MISCONFIGURATION

INFECTED SOFTWARE

CREDENTIAL COMPROMISE


● WE USED OUR BACKUP SYSTEM TO GET DATA BACK
● WE PAID THE RANSOM TO GET DATA BACK
● WE USED OTHER MEANS TO GET DATA BACK
● WE LOST THE DATA THEY ENCRYPTED
2%
9%
35%
54%



PREPARE + ENTER

TRAVERSE

EXECUTE OBJECTIVES

Attacker gains access to organization

Attacker gains administrative access to organization

Client Attacks
Email, Credential, Browser, etc.

Logon with legit creds

Datacenter Attacks
RDP, SSH, Server, App, etc.

$ Ransomware actors sometimes buy access to target organizations from other attackers in dark markets or leverage critical vulnerabilities

Credential Theft

Malware Installation

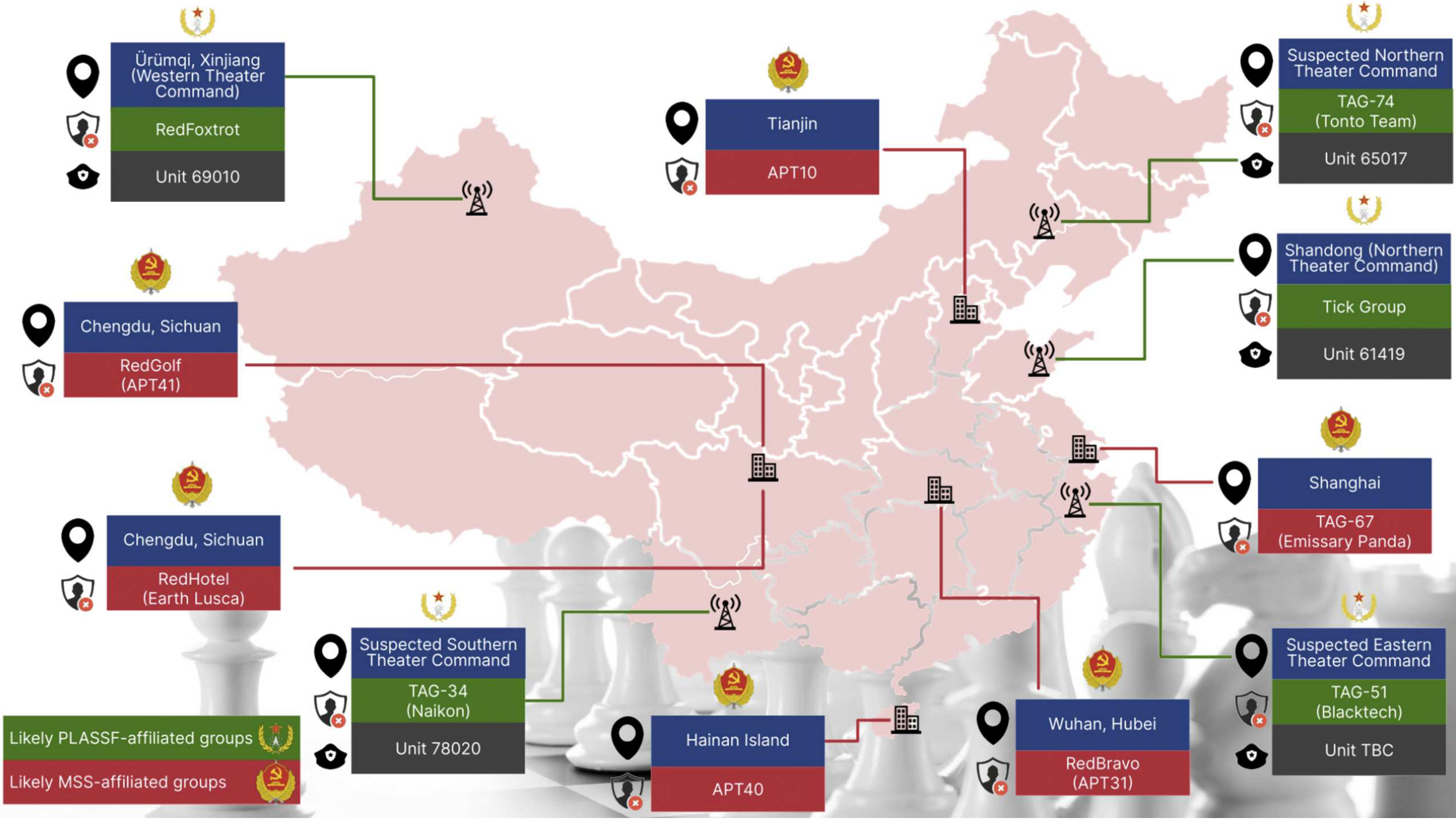
Encryption
Lock up Data

Exfiltration
Steal Data

Extortion
Demand Money

- Sabotage Backup/Recovery
- Establish persistence

Human Attack Operator(s)
Assisted by scripts and malware



Ürümqi, Xinjiang (Western Theater Command)
RedFoxtrot
Unit 69010

Tianjin
APT10

Suspected Northern Theater Command
TAG-74 (Tonto Team)
Unit 65017

Chengdu, Sichuan
RedGolf (APT41)

Shandong (Northern Theater Command)
Tick Group
Unit 61419

Chengdu, Sichuan
RedHotel (Earth Lusca)

Shanghai
TAG-67 (Emissary Panda)

Suspected Southern Theater Command
TAG-34 (Naikon)
Unit 78020

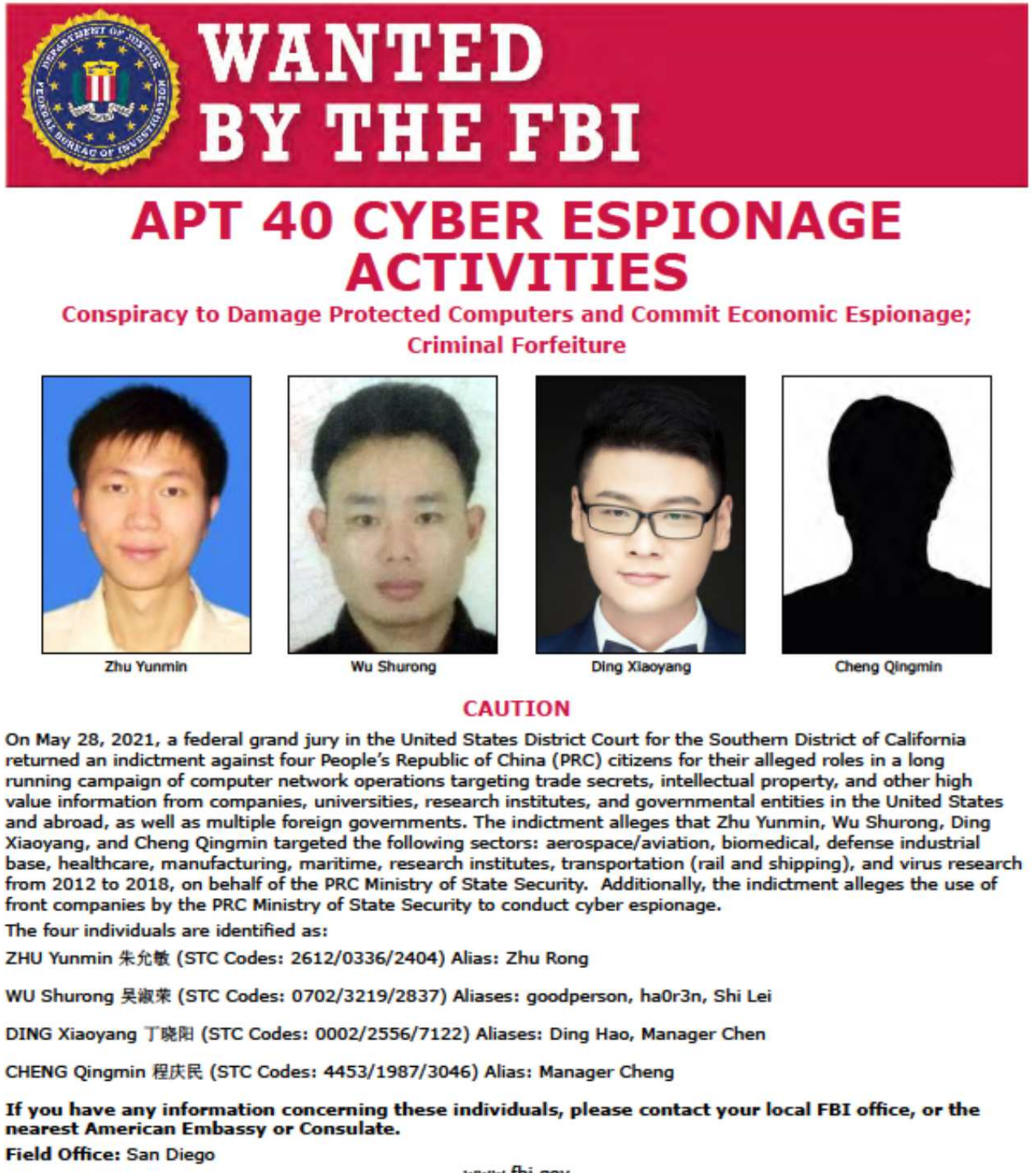
Suspected Eastern Theater Command
TAG-51 (Blacktech)
Unit TBC

Hainan Island
APT40

Wuhan, Hubei
RedBravo (APT31)

Likely PLASSF-affiliated groups

Likely MSS-affiliated groups



WANTED BY THE FBI

APT 40 CYBER ESPIONAGE ACTIVITIES

Conspiracy to Damage Protected Computers and Commit Economic Espionage; Criminal Forfeiture

Zhu Yunmin

Wu Shurong

Ding Xiaoyang

Cheng Qingmin

CAUTION

On May 28, 2021, a federal grand jury in the United States District Court for the Southern District of California returned an indictment against four People's Republic of China (PRC) citizens for their alleged roles in a long running campaign of computer network operations targeting trade secrets, intellectual property, and other high value information from companies, universities, research institutes, and governmental entities in the United States and abroad, as well as multiple foreign governments. The indictment alleges that Zhu Yunmin, Wu Shurong, Ding Xiaoyang, and Cheng Qingmin targeted the following sectors: aerospace/aviation, biomedical, defense industrial base, healthcare, manufacturing, maritime, research institutes, transportation (rail and shipping), and virus research from 2012 to 2018, on behalf of the PRC Ministry of State Security. Additionally, the indictment alleges the use of front companies by the PRC Ministry of State Security to conduct cyber espionage.

The four individuals are identified as:

ZHU Yunmin 朱允敏 (STC Codes: 2612/0336/2404) Alias: Zhu Rong

WU Shurong 吴淑荣 (STC Codes: 0702/3219/2837) Aliases: goodperson, ha0r3n, Shi Lei

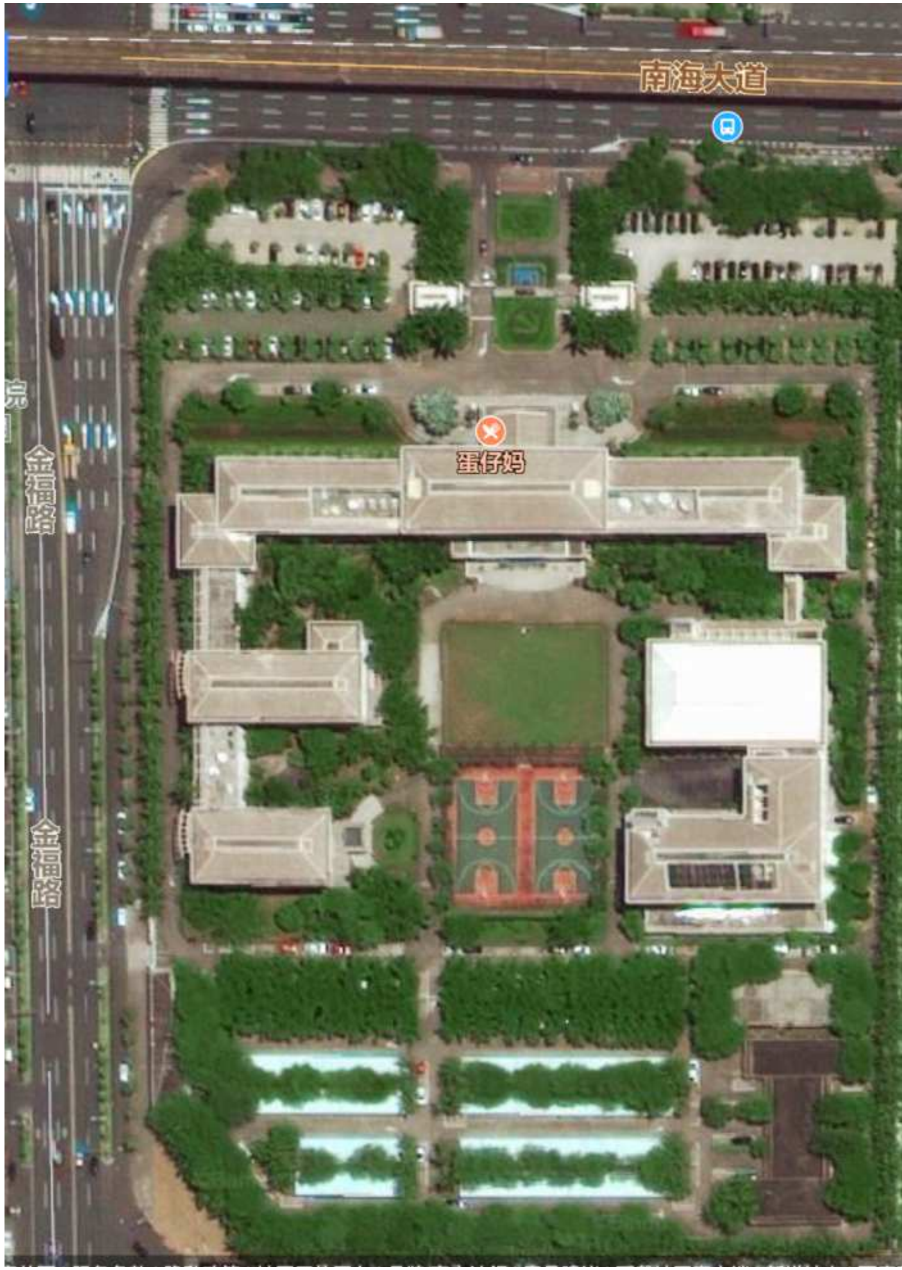
DING Xiaoyang 丁晓阳 (STC Codes: 0002/2556/7122) Aliases: Ding Hao, Manager Chen

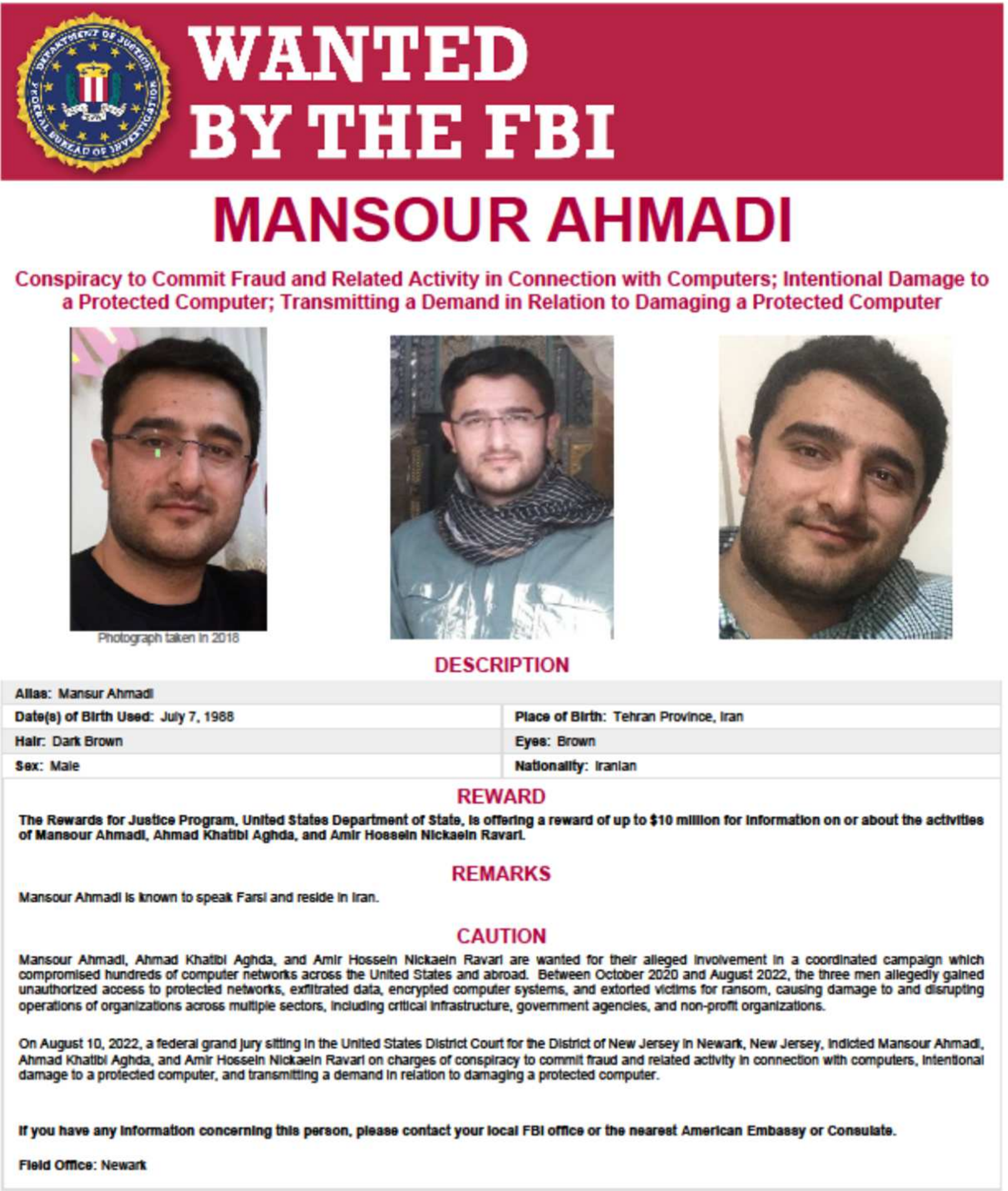
CHENG Qingmin 程庆民 (STC Codes: 4453/1987/3046) Alias: Manager Cheng

If you have any information concerning these individuals, please contact your local FBI office, or the nearest American Embassy or Consulate.

Field Office: San Diego

www.fbi.gov





WANTED BY THE FBI

MANSOUR AHMADI

Conspiracy to Commit Fraud and Related Activity in Connection with Computers; Intentional Damage to a Protected Computer; Transmitting a Demand in Relation to Damaging a Protected Computer

Photograph taken in 2018

DESCRIPTION

Alias: Mansur Ahmadi	
Date(s) of Birth Used: July 7, 1988	**Place of Birth:** Tehran Province, Iran
Hair: Dark Brown	**Eyes:** Brown
Sex: Male	**Nationality:** Iranian

REWARD

The Rewards for Justice Program, United States Department of State, is offering a reward of up to $10 million for information on or about the activities of Mansour Ahmadi, Ahmad Khatibi Aghda, and Amir Hossein Nickaein Ravari.

REMARKS

Mansour Ahmadi is known to speak Farsi and reside in Iran.

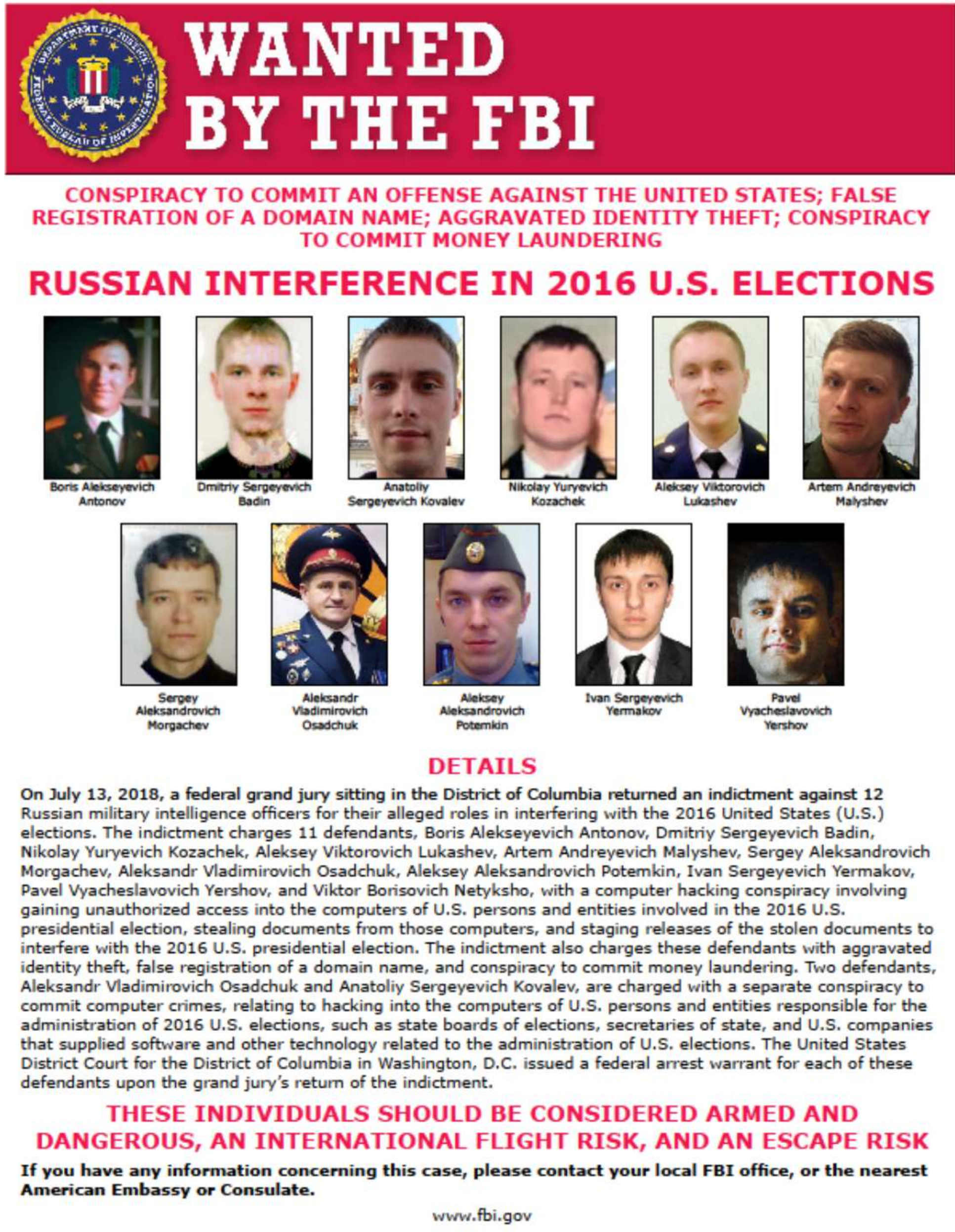
CAUTION

Mansour Ahmadi, Ahmad Khatibi Aghda, and Amir Hossein Nickaein Ravari are wanted for their alleged involvement in a coordinated campaign which compromised hundreds of computer networks across the United States and abroad. Between October 2020 and August 2022, the three men allegedly gained unauthorized access to protected networks, exfiltrated data, encrypted computer systems, and extorted victims for ransom, causing damage to and disrupting operations of organizations across multiple sectors, including critical infrastructure, government agencies, and non-profit organizations.

On August 10, 2022, a federal grand jury sitting in the United States District Court for the District of New Jersey in Newark, New Jersey, indicted Mansour Ahmadi, Ahmad Khatibi Aghda, and Amir Hossein Nickaein Ravari on charges of conspiracy to commit fraud and related activity in connection with computers, intentional damage to a protected computer, and transmitting a demand in relation to damaging a protected computer.

If you have any information concerning this person, please contact your local FBI office or the nearest American Embassy or Consulate.

Field Office: Newark



WANTED BY THE FBI

CONSPIRACY TO COMMIT AN OFFENSE AGAINST THE UNITED STATES; FALSE REGISTRATION OF A DOMAIN NAME; AGGRAVATED IDENTITY THEFT; CONSPIRACY TO COMMIT MONEY LAUNDERING

RUSSIAN INTERFERENCE IN 2016 U.S. ELECTIONS

Boris Alekseyevich Antonov

Dmitriy Sergeyevich Badin

Anatoliy Sergeyevich Kovalev

Nikolay Yuryevich Kozachek

Aleksey Viktorovich Lukashev

Artem Andreyevich Malyshev

Sergey Aleksandrovich Morgachev

Aleksandr Vladimirovich Osadchuk

Aleksey Aleksandrovich Potemkin

Ivan Sergeyevich Yermakov

Pavel Vyacheslavovich Yershov

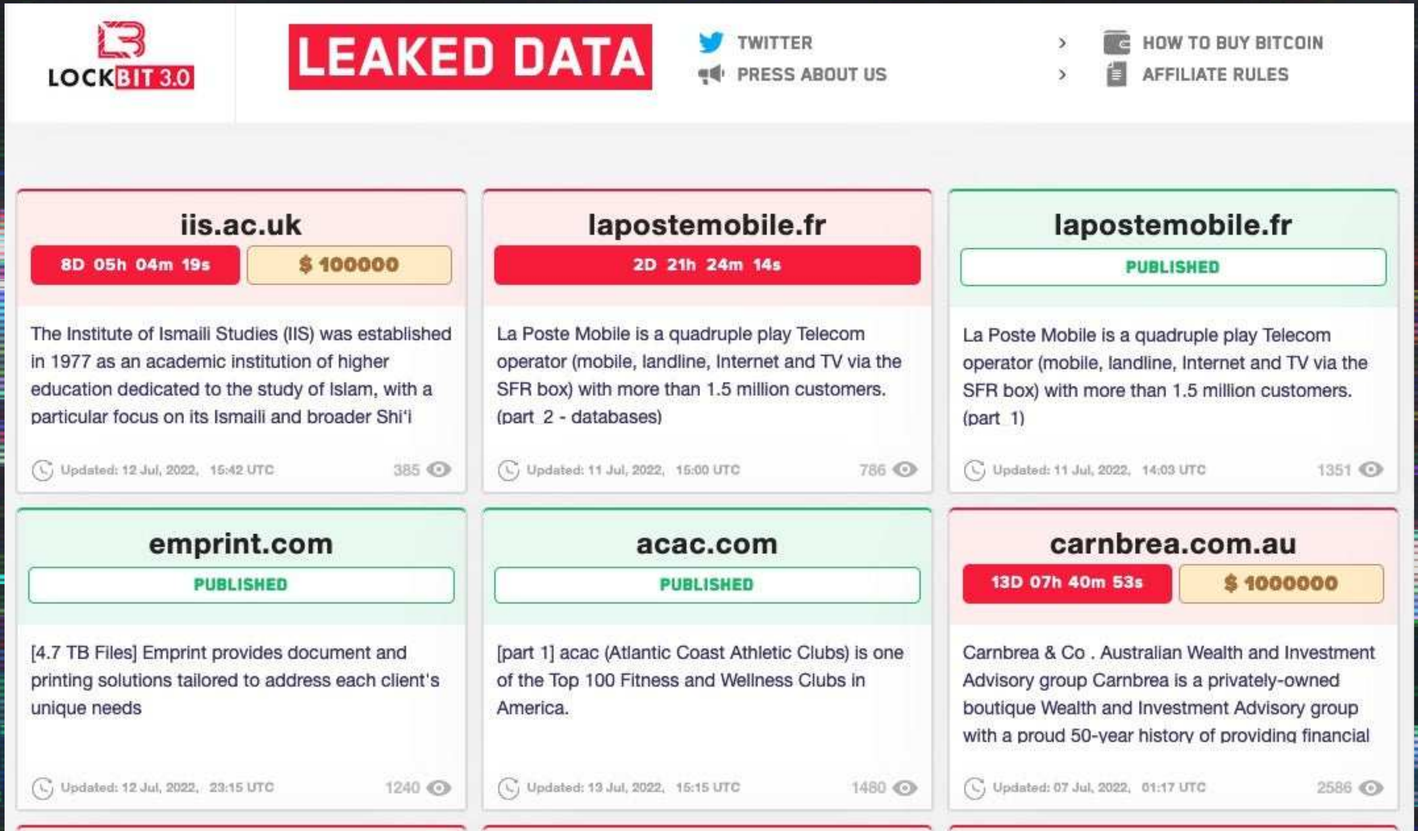
DETAILS

On July 13, 2018, a federal grand jury sitting in the District of Columbia returned an indictment against 12 Russian military intelligence officers for their alleged roles in interfering with the 2016 United States (U.S.) elections. The indictment charges 11 defendants, Boris Alekseyevich Antonov, Dmitriy Sergeyevich Badin, Nikolay Yuryevich Kozachek, Aleksey Viktorovich Lukashev, Artem Andreyevich Malyshev, Sergey Aleksandrovich Morgachev, Aleksandr Vladimirovich Osadchuk, Aleksey Aleksandrovich Potemkin, Ivan Sergeyevich Yermakov, Pavel Vyacheslavovich Yershov, and Viktor Borisovich Netyksho, with a computer hacking conspiracy involving gaining unauthorized access into the computers of U.S. persons and entities involved in the 2016 U.S. presidential election, stealing documents from those computers, and staging releases of the stolen documents to interfere with the 2016 U.S. presidential election. The indictment also charges these defendants with aggravated identity theft, false registration of a domain name, and conspiracy to commit money laundering. Two defendants, Aleksandr Vladimirovich Osadchuk and Anatoliy Sergeyevich Kovalev, are charged with a separate conspiracy to commit computer crimes, relating to hacking into the computers of U.S. persons and entities responsible for the administration of 2016 U.S. elections, such as state boards of elections, secretaries of state, and U.S. companies that supplied software and other technology related to the administration of U.S. elections. The United States District Court for the District of Columbia in Washington, D.C. issued a federal arrest warrant for each of these defendants upon the grand jury's return of the indictment.

THESE INDIVIDUALS SHOULD BE CONSIDERED ARMED AND DANGEROUS, AN INTERNATIONAL FLIGHT RISK, AND AN ESCAPE RISK

If you have any information concerning this case, please contact your local FBI office, or the nearest American Embassy or Consulate.

www.fbi.gov



iis.ac.uk

8D 05h 04m 19s | $ 100000

The Institute of Ismaili Studies (IIS) was established in 1977 as an academic institution of higher education dedicated to the study of Islam, with a particular focus on its Ismaili and broader Shi'i

Updated: 12 Jul, 2022, 15:42 UTC 385

lapostemobile.fr

2D 21h 24m 14s

La Poste Mobile is a quadruple play Telecom operator (mobile, landline, Internet and TV via the SFR box) with more than 1.5 million customers. (part 2 - databases)

Updated: 11 Jul, 2022, 15:00 UTC 786

lapostemobile.fr

PUBLISHED

La Poste Mobile is a quadruple play Telecom operator (mobile, landline, Internet and TV via the SFR box) with more than 1.5 million customers. (part 1)

Updated: 11 Jul, 2022, 14:03 UTC 1351

emprint.com

PUBLISHED

[4.7 TB Files] Emprint provides document and printing solutions tailored to address each client's unique needs

Updated: 12 Jul, 2022, 23:15 UTC 1240

acac.com

PUBLISHED

[part 1] acac (Atlantic Coast Athletic Clubs) is one of the Top 100 Fitness and Wellness Clubs in America.

Updated: 13 Jul, 2022, 15:15 UTC 1480

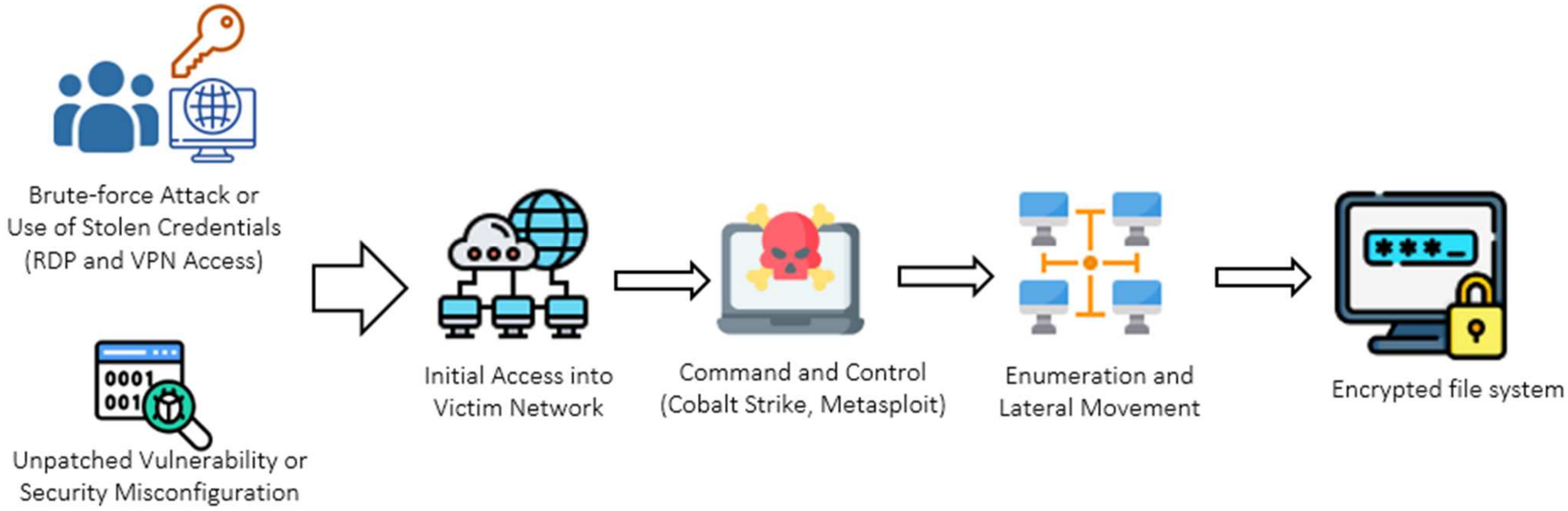
carnbrea.com.au

13D 07h 40m 53s | $ 1000000

Carnbrea & Co . Australian Wealth and Investment Advisory group Carnbrea is a privately-owned boutique Wealth and Investment Advisory group with a proud 50-year history of providing financial

Updated: 07 Jul, 2022, 01:17 UTC 2586

LOCKBIT 3.0



Brute-force Attack or Use of Stolen Credentials (RDP and VPN Access)

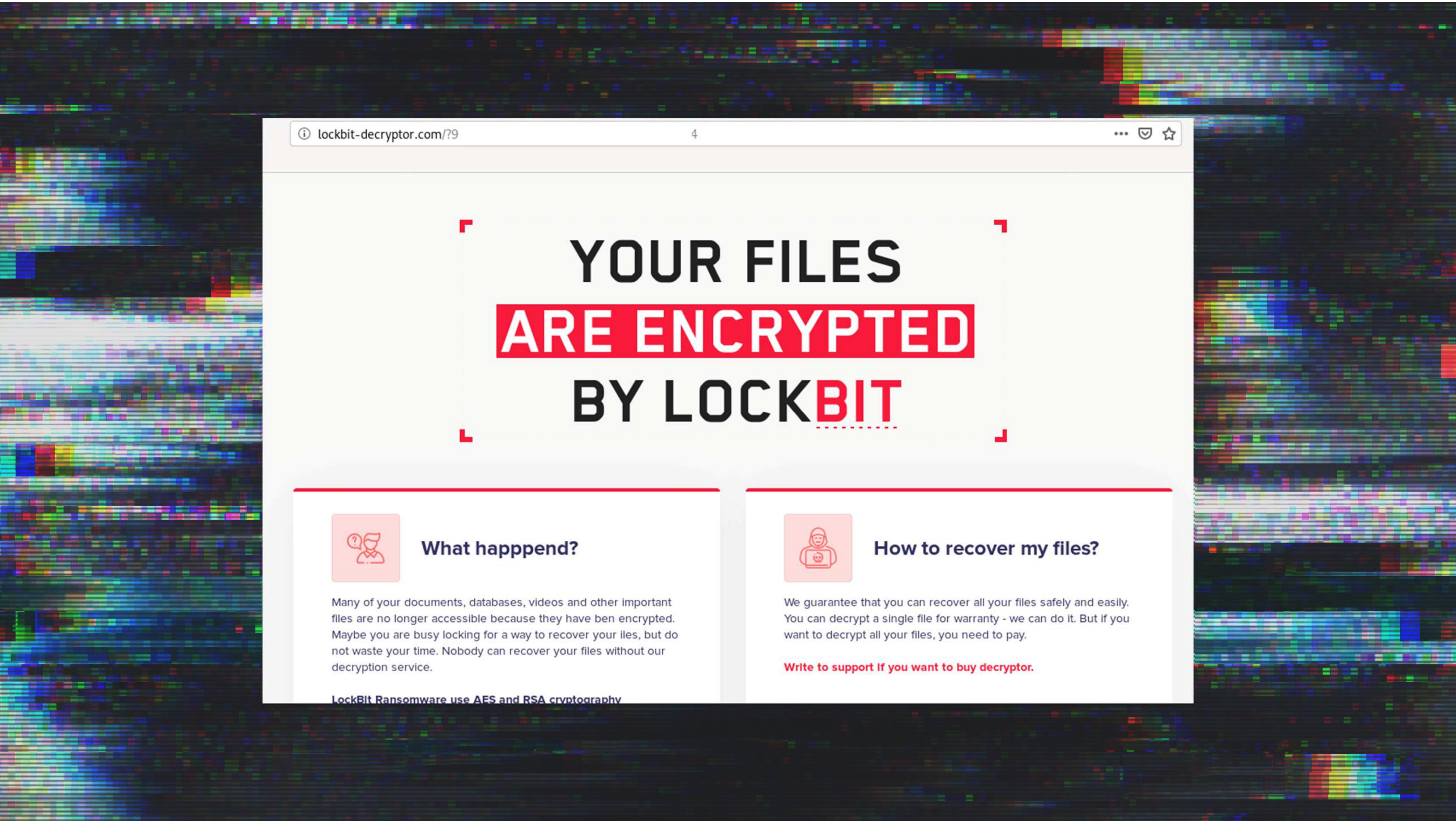
Unpatched Vulnerability or Security Misconfiguration

Initial Access into Victim Network

Command and Control (Cobalt Strike, Metasploit)

Enumeration and Lateral Movement

Encrypted file system



YOUR FILES ARE ENCRYPTED BY LOCKBIT

What happpend?

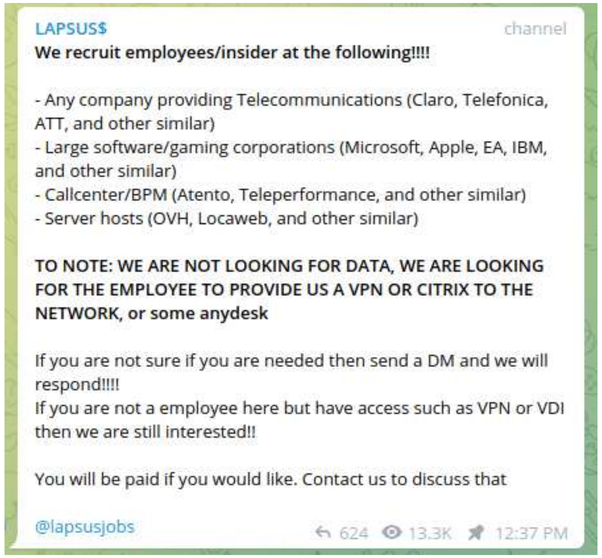
Many of your documents, databases, videos and other important files are no longer accessible because they have ben encrypted. Maybe you are busy locking for a way to recover your iles, but do not waste your time. Nobody can recover your files without our decryption service.

LockBit Ransomware use AES and RSA cryptography

How to recover my files?

We guarantee that you can recover all your files safely and easily. You can decrypt a single file for warranty - we can do it. But if you want to decrypt all your files, you need to pay.

Write to support if you want to buy decryptor.



LAPSUS$ channel

We recruit employees/insider at the following!!!!

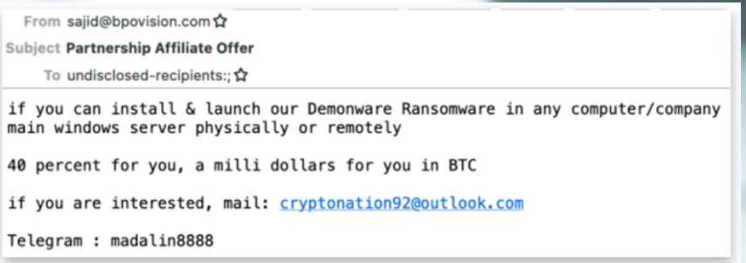
- Any company providing Telecommunications (Claro, Telefonica, ATT, and other similar)
- Large software/gaming corporations (Microsoft, Apple, EA, IBM, and other similar)
- Callcenter/BPM (Atento, Teleperformance, and other similar)
- Server hosts (OVH, Locaweb, and other similar)

TO NOTE: WE ARE NOT LOOKING FOR DATA, WE ARE LOOKING FOR THE EMPLOYEE TO PROVIDE US A VPN OR CITRIX TO THE NETWORK, or some anydesk

If you are not sure if you are needed then send a DM and we will respond!!!!
If you are not a employee here but have access such as VPN or VDI then we are still interested!!

You will be paid if you would like. Contact us to discuss that

@lapsusjobs



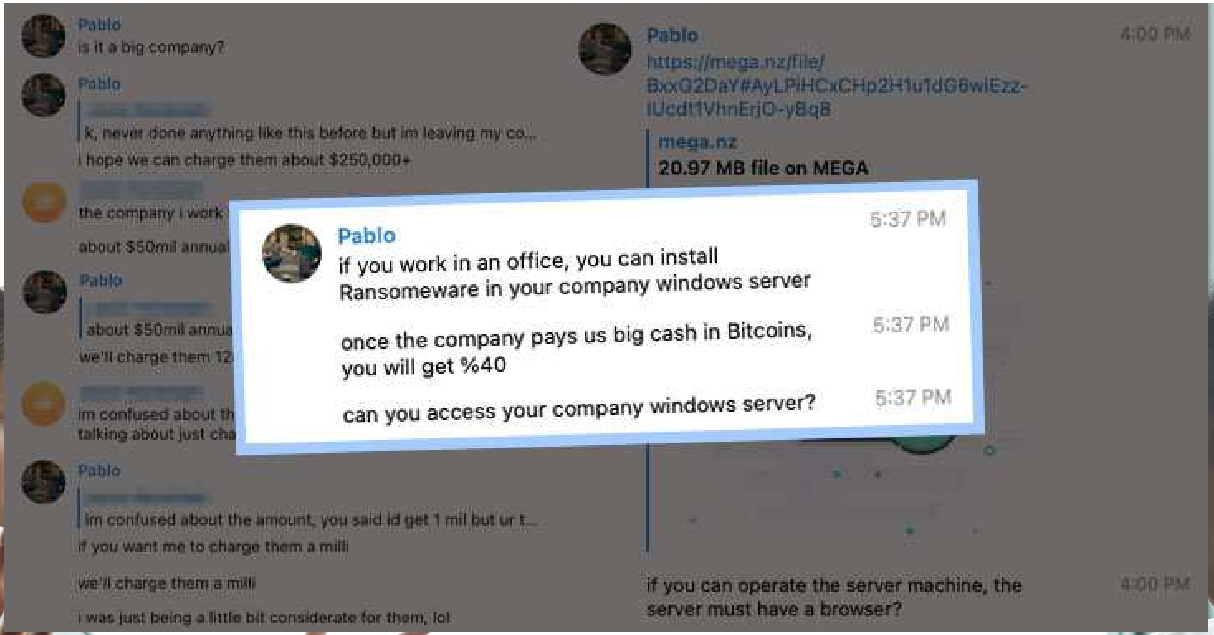
From sajid@bpovision.com
Subject **Partnership Affiliate Offer**
To undisclosed-recipients:;

```
if you can install & launch our Demonware Ransomware in any computer/company
main windows server physically or remotely

40 percent for you, a milli dollars for you in BTC

if you are interested, mail: cryptonation92@outlook.com

Telegram : madalin8888
```



Pablo
is it a big company?

Pablo
[redacted]
k, never done anything like this before but im leaving my co...
i hope we can charge them about $250,000+

[redacted]
the company i work

about $50mil annual

Pablo
[redacted]
about $50mil annua
we'll charge them 12

[redacted]
im confused about th
talking about just cha

Pablo
[redacted]
im confused about the amount, you said id get 1 mil but ur t...
if you want me to charge them a milli

we'll charge them a milli

i was just being a little bit considerate for them, lol

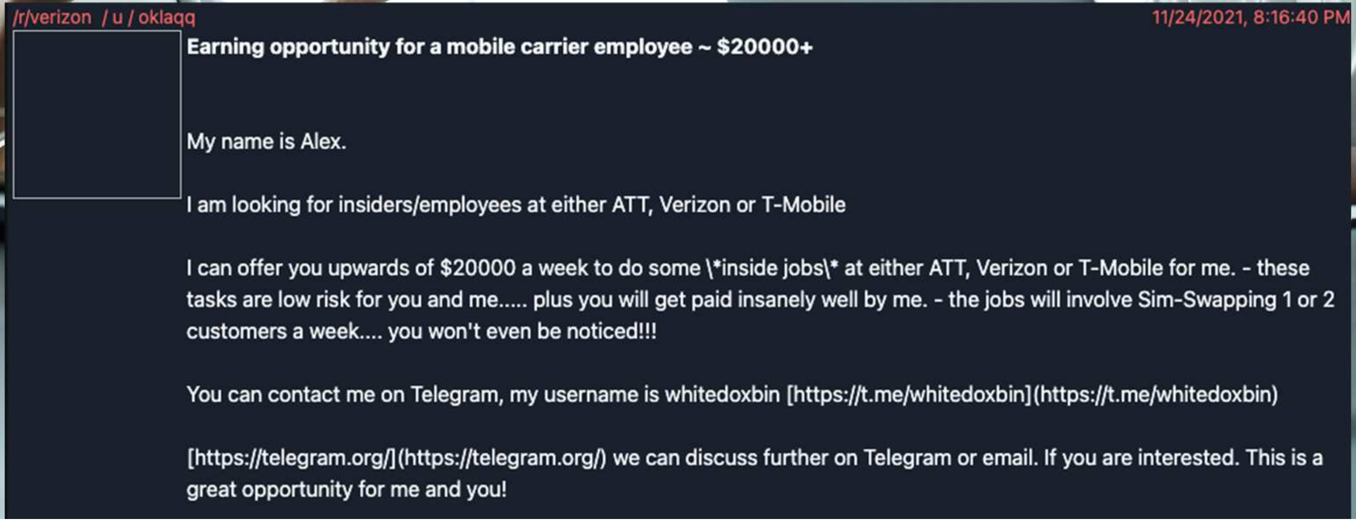
Pablo 4:00 PM
https://mega.nz/file/BxxG2DaY#AyLPiHCxCHp2H1u1dG6wlEzz-iUcdt1VhnErjO-yBq8
mega.nz
20.97 MB file on MEGA

if you can operate the server machine, the server must have a browser? 4:00 PM

Pablo 5:37 PM
if you work in an office, you can install Ransomeware in your company windows server

once the company pays us big cash in Bitcoins, you will get %40 5:37 PM

can you access your company windows server? 5:37 PM



/r/verizon / u / oklaqq 11/24/2021, 8:16:40 PM

Earning opportunity for a mobile carrier employee ~ $20000+

My name is Alex.

I am looking for insiders/employees at either ATT, Verizon or T-Mobile

I can offer you upwards of $20000 a week to do some *inside jobs* at either ATT, Verizon or T-Mobile for me. - these tasks are low risk for you and me..... plus you will get paid insanely well by me. - the jobs will involve Sim-Swapping 1 or 2 customers a week.... you won't even be noticed!!!

You can contact me on Telegram, my username is whitedoxbin https://t.me/whitedoxbin

https://telegram.org/ we can discuss further on Telegram or email. If you are interested. This is a great opportunity for me and you!

ZERO-DAY EXPLOITED IN THE WILD
CVE-2023-35078
Ivanti Endpoint Manager Mobile (EPMM)

CVSSv3	Severity
10.0	Critical

Authentication bypass vulnerability

↓

Access to specific API paths

↓

Obtain PII data from the server (about the managed mobiles devices)

↓

Modify the server’s configuration file (create admin, deploy web shells, push malicious package to mobiles devices)

```
irror_mod = modifier_ob
t mirror object to mirror
irror_mod.mirror_object
peration == "MIRROR_X":
irror_mod.use_x = True
irror_mod.use_y = False
irror_mod.use_z = False
_operation == "MIRROR_Y":
irror_mod.use_x = False
irror_mod.use_y = True
irror_mod.use_z = False
_operation == "MIRROR_Z":
irror_mod.use_x = False
irror_mod.use_y = False
irror_mod.use_z = True

election at the end -add
_ob.select= 1
er_ob.select=1
ntext.scene.objects.activ
("Selected" + str(modifier
irror_ob.select = 0
bpy.context.selected_obj
ata.objects[one.name].sel

int("please select exactl

OPERATOR CLASSES ----

types.Operator):
X mirror to the selected
ject.mirror_mirror_x"
```

ZERO-DAY EXPLOITED IN THE WILD

CVE-2023-35081

Ivanti Endpoint Manager Mobile (EPMM)

CVSSv3	Severity
7.2	High

Path traversal vulnerability

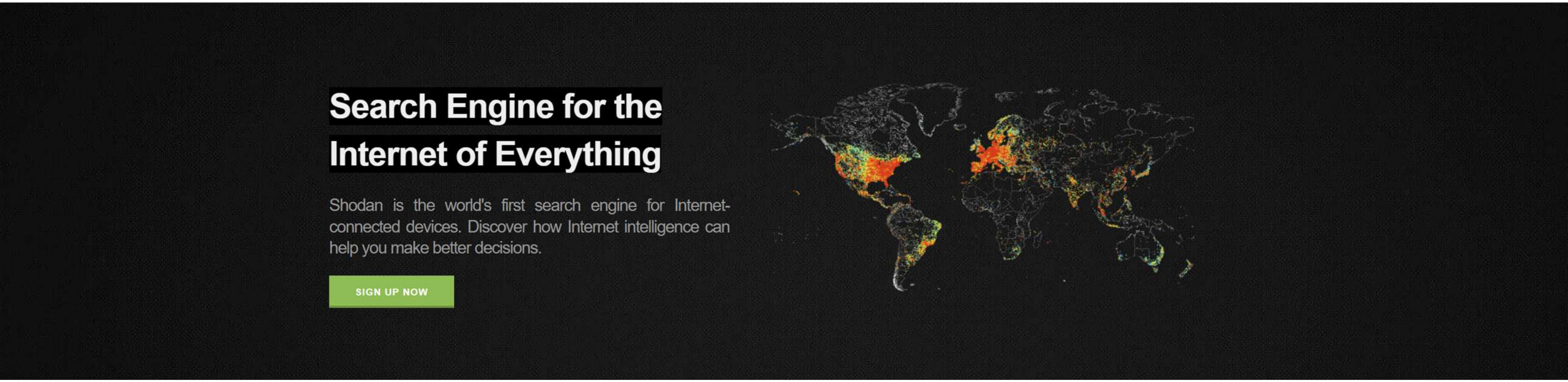
⇩

Authenticated administrator can write new files to the EPMM server

⇩

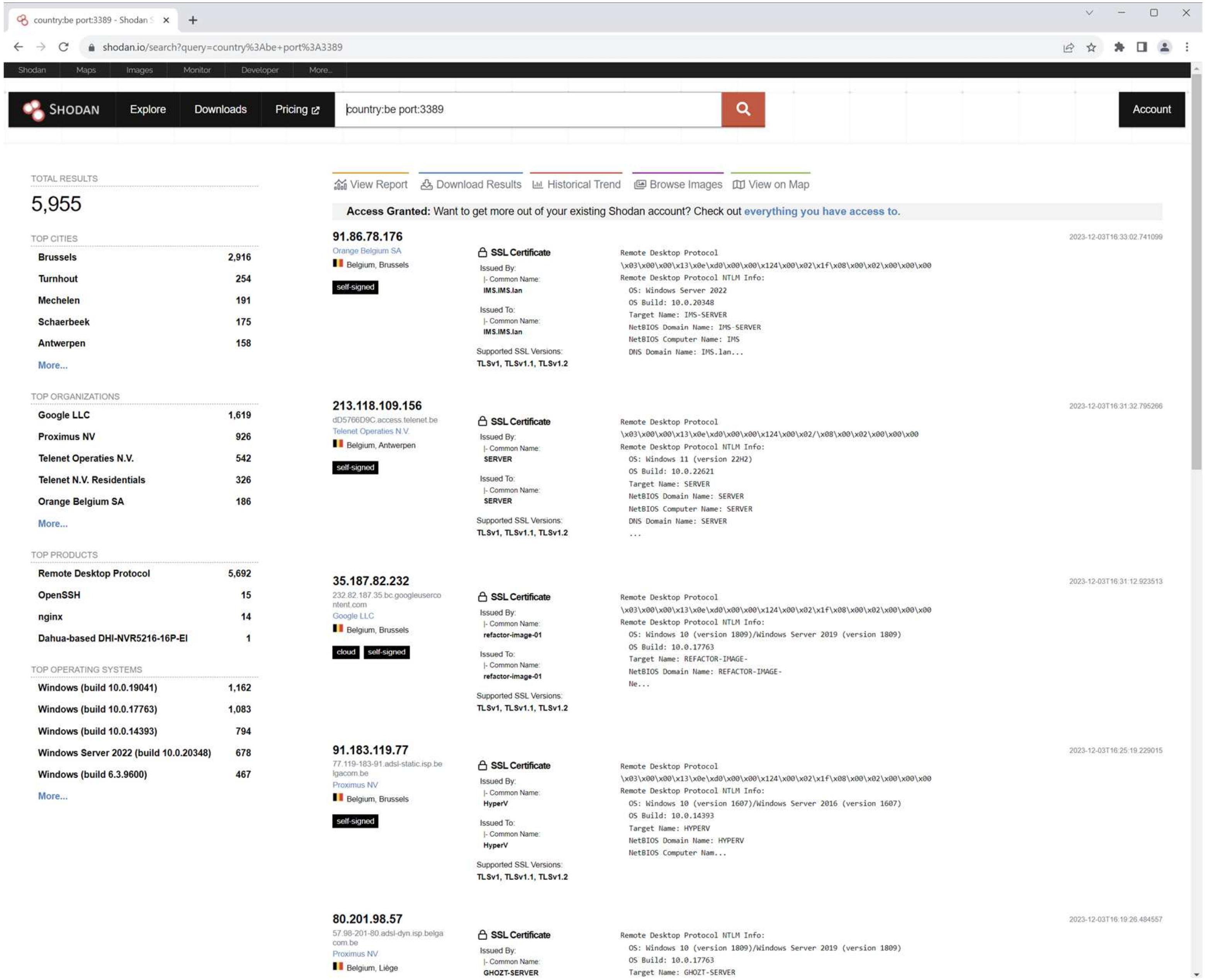
Perform malicious activities with admin privileges

SHODAN



Search Engine for the Internet of Everything

Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.



TOTAL RESULTS

5,955

TOP CITIES	
Brussels	2,916
Turnhout	254
Mechelen	191
Schaerbeek	175
Antwerpen	158
More...	

TOP ORGANIZATIONS	
Google LLC	1,619
Proximus NV	926
Telenet Operaties N.V.	542
Telenet N.V. Residentials	326
Orange Belgium SA	186
More...	

TOP PRODUCTS	
Remote Desktop Protocol	5,692
OpenSSH	15
nginx	14
Dahua-based DHI-NVR5216-16P-EI	1

TOP OPERATING SYSTEMS	
Windows (build 10.0.19041)	1,162
Windows (build 10.0.17763)	1,083
Windows (build 10.0.14393)	794
Windows Server 2022 (build 10.0.20348)	678
Windows (build 6.3.9600)	467
More...	

Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to.

91.86.78.176 2023-12-03T16:33:02.741099

Orange Belgium SA
Belgium, Brussels
self-signed

SSL Certificate
Issued By:
|- Common Name:
IMS.IMS.lan
Issued To:
|- Common Name:
IMS.IMS.lan
Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

```
Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00
Remote Desktop Protocol NTLM Info:
  OS: Windows Server 2022
  OS Build: 10.0.20348
  Target Name: IMS-SERVER
  NetBIOS Domain Name: IMS-SERVER
  NetBIOS Computer Name: IMS
  DNS Domain Name: IMS.lan...
```

213.118.109.156 2023-12-03T16:31:32.795266

dD5766D9C.access.telenet.be
Telenet Operaties N.V.
Belgium, Antwerpen
self-signed

SSL Certificate
Issued By:
|- Common Name:
SERVER
Issued To:
|- Common Name:
SERVER
Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

```
Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02/\x08\x00\x02\x00\x00\x00
Remote Desktop Protocol NTLM Info:
  OS: Windows 11 (version 22H2)
  OS Build: 10.0.22621
  Target Name: SERVER
  NetBIOS Domain Name: SERVER
  NetBIOS Computer Name: SERVER
  DNS Domain Name: SERVER
  ...
```

35.187.82.232 2023-12-03T16:31:12.923513

232.82.187.35.bc.googleusercontent.com
Google LLC
Belgium, Brussels
cloud self-signed

SSL Certificate
Issued By:
|- Common Name:
refactor-image-01
Issued To:
|- Common Name:
refactor-image-01
Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

```
Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00
Remote Desktop Protocol NTLM Info:
  OS: Windows 10 (version 1809)/Windows Server 2019 (version 1809)
  OS Build: 10.0.17763
  Target Name: REFACTOR-IMAGE-
  NetBIOS Domain Name: REFACTOR-IMAGE-
  Ne...
```

91.183.119.77 2023-12-03T16:25:19.229015

77.119-183-91.adsl-static.isp.belgacom.be
Proximus NV
Belgium, Brussels
self-signed

SSL Certificate
Issued By:
|- Common Name:
HyperV
Issued To:
|- Common Name:
HyperV
Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

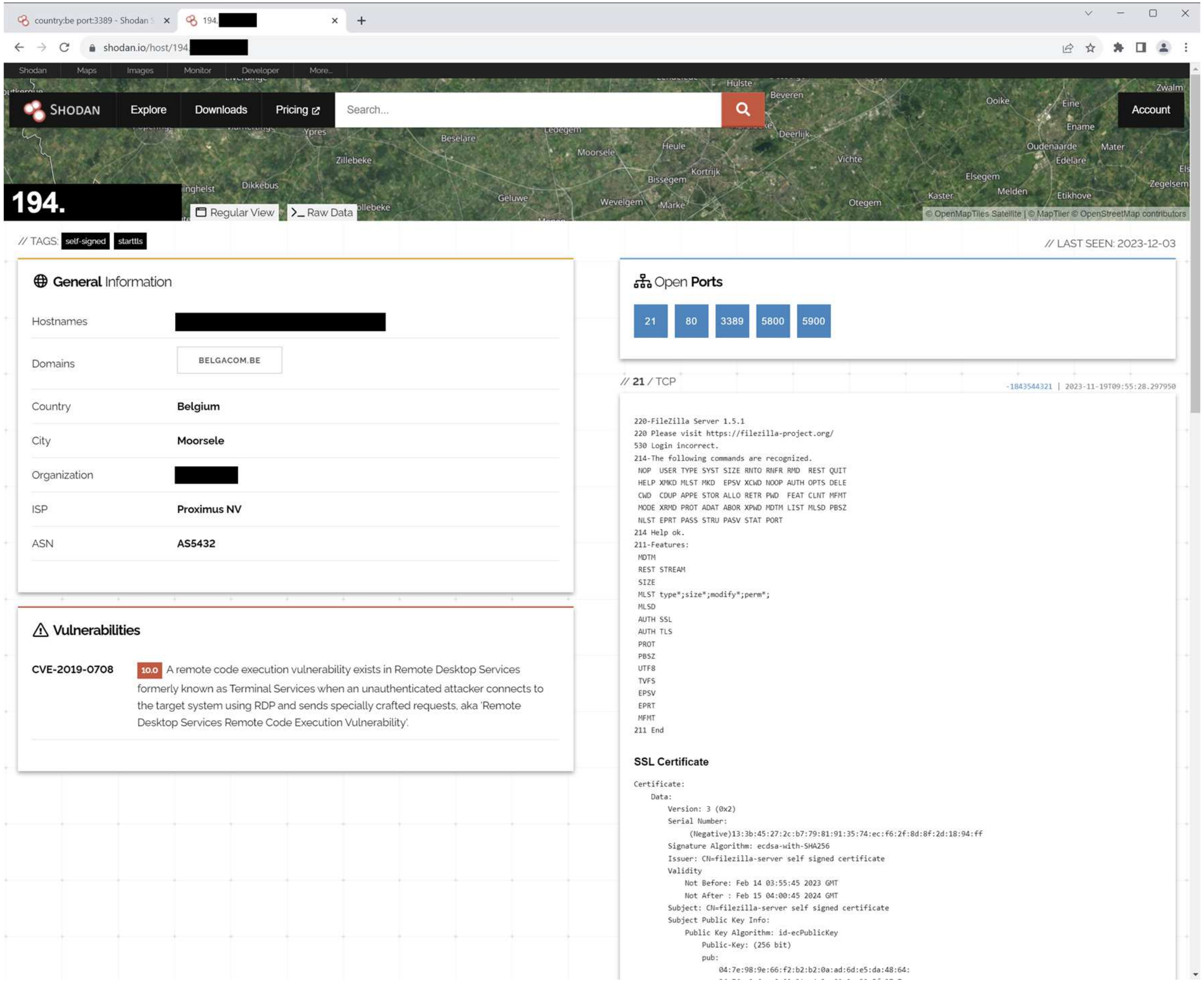
```
Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00
Remote Desktop Protocol NTLM Info:
  OS: Windows 10 (version 1607)/Windows Server 2016 (version 1607)
  OS Build: 10.0.14393
  Target Name: HYPERV
  NetBIOS Domain Name: HYPERV
  NetBIOS Computer Nam...
```

80.201.98.57 2023-12-03T16:19:26.484557

57.98-201-80.adsl-dyn.isp.belgacom.be
Proximus NV
Belgium, Liège

SSL Certificate
Issued By:
|- Common Name:
GHOZT-SERVER

```
Remote Desktop Protocol NTLM Info:
  OS: Windows 10 (version 1809)/Windows Server 2019 (version 1809)
  OS Build: 10.0.17763
  Target Name: GHOZT-SERVER
```


country:be port:3389 - Shodan S
194.[redacted]
shodan.io/host/194.[redacted]
Shodan
Maps
Images
Monitor
Developer
More...
SHODAN
Explore
Downloads
Pricing
Search...
Account
Regular View
Raw Data
© OpenMapTiles Satellite | © MapTiler © OpenStreetMap contributors

194.[redacted]

// TAGS: self-signed starttls

// LAST SEEN: 2023-12-03

General Information

Hostnames	[redacted]
Domains	BELGACOM.BE
Country	**Belgium**
City	**Moorsele**
Organization	[redacted]
ISP	**Proximus NV**
ASN	**AS5432**

Vulnerabilities

CVE-2019-0708 10.0 A remote code execution vulnerability exists in Remote Desktop Services formerly known as Terminal Services when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka 'Remote Desktop Services Remote Code Execution Vulnerability'.

Open **Ports**

21 80 3389 5800 5900

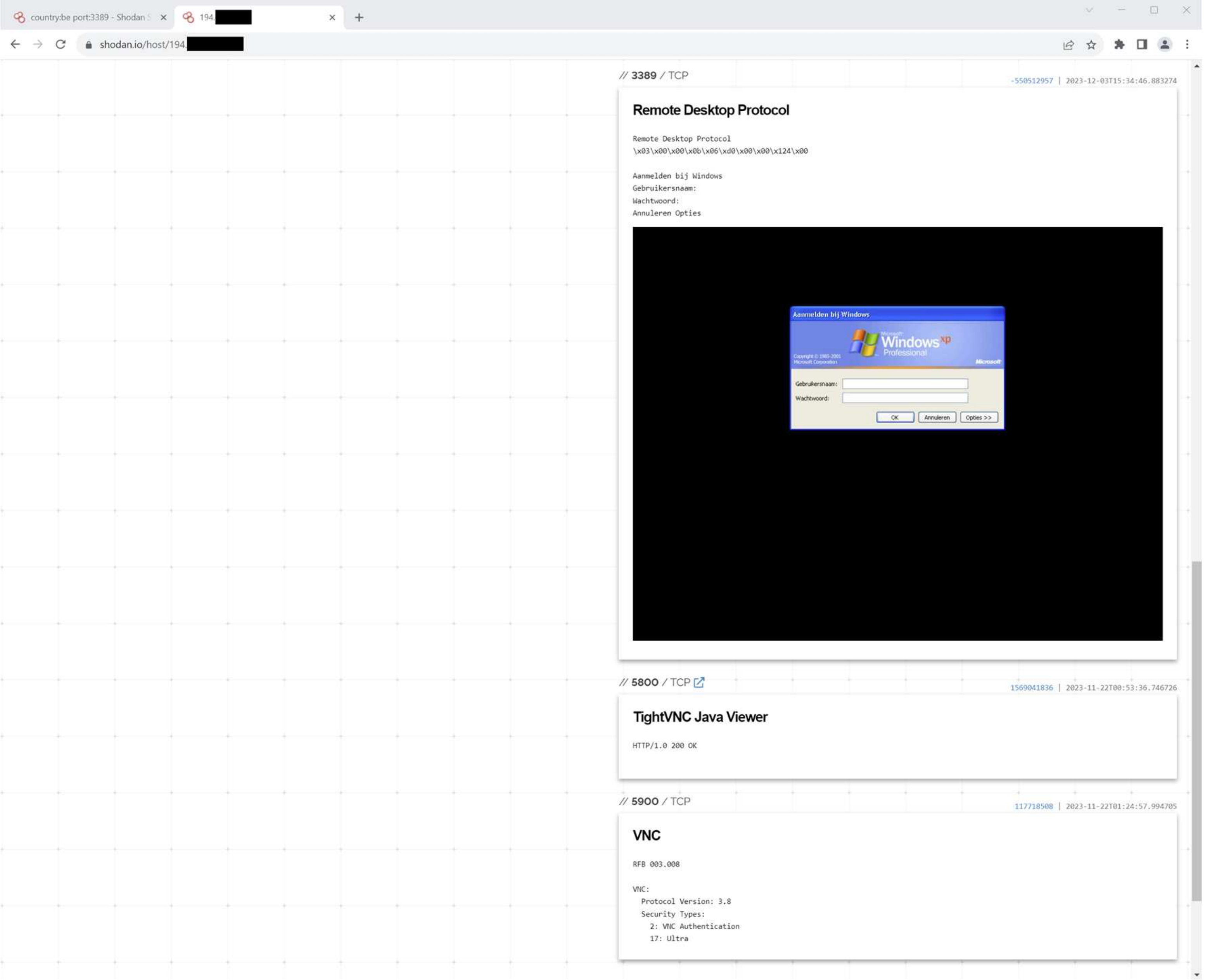
// **21** / TCP

-1843544321 | 2023-11-19T09:55:28.297950

```
220-FileZilla Server 1.5.1
220 Please visit https://filezilla-project.org/
530 Login incorrect.
214-The following commands are recognized.
 NOP  USER TYPE SYST SIZE RNTO RNFR RMD  REST QUIT
 HELP XMKD MLST MKD  EPSV XCWD NOOP AUTH OPTS DELE
 CWD  CDUP APPE STOR ALLO RETR PWD  FEAT CLNT MFMT
 MODE XRMD PROT ADAT ABOR XPWD MDTM LIST MLSD PBSZ
 NLST EPRT PASS STRU PASV STAT PORT
214 Help ok.
211-Features:
 MDTM
 REST STREAM
 SIZE
 MLST type*;size*;modify*;perm*;
 MLSD
 AUTH SSL
 AUTH TLS
 PROT
 PBSZ
 UTF8
 TVFS
 EPSV
 EPRT
 MFMT
211 End
```

SSL Certificate

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            (Negative)13:3b:45:27:2c:b7:79:81:91:35:74:ec:f6:2f:8d:8f:2d:18:94:ff
        Signature Algorithm: ecdsa-with-SHA256
        Issuer: CN=filezilla-server self signed certificate
        Validity
            Not Before: Feb 14 03:55:45 2023 GMT
            Not After : Feb 15 04:00:45 2024 GMT
        Subject: CN=filezilla-server self signed certificate
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:7e:98:9e:66:f2:b2:b2:0a:ad:6d:e5:da:48:64:
```



// **3389** / TCP

-550512957 | 2023-12-03T15:34:46.883274

Remote Desktop Protocol

```
Remote Desktop Protocol
\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00

Aanmelden bij Windows
Gebruikersnaam:
Wachtwoord:
Annuleren Opties
```

// **5800** / TCP

1569041836 | 2023-11-22T00:53:36.746726

TightVNC Java Viewer

```
HTTP/1.0 200 OK
```

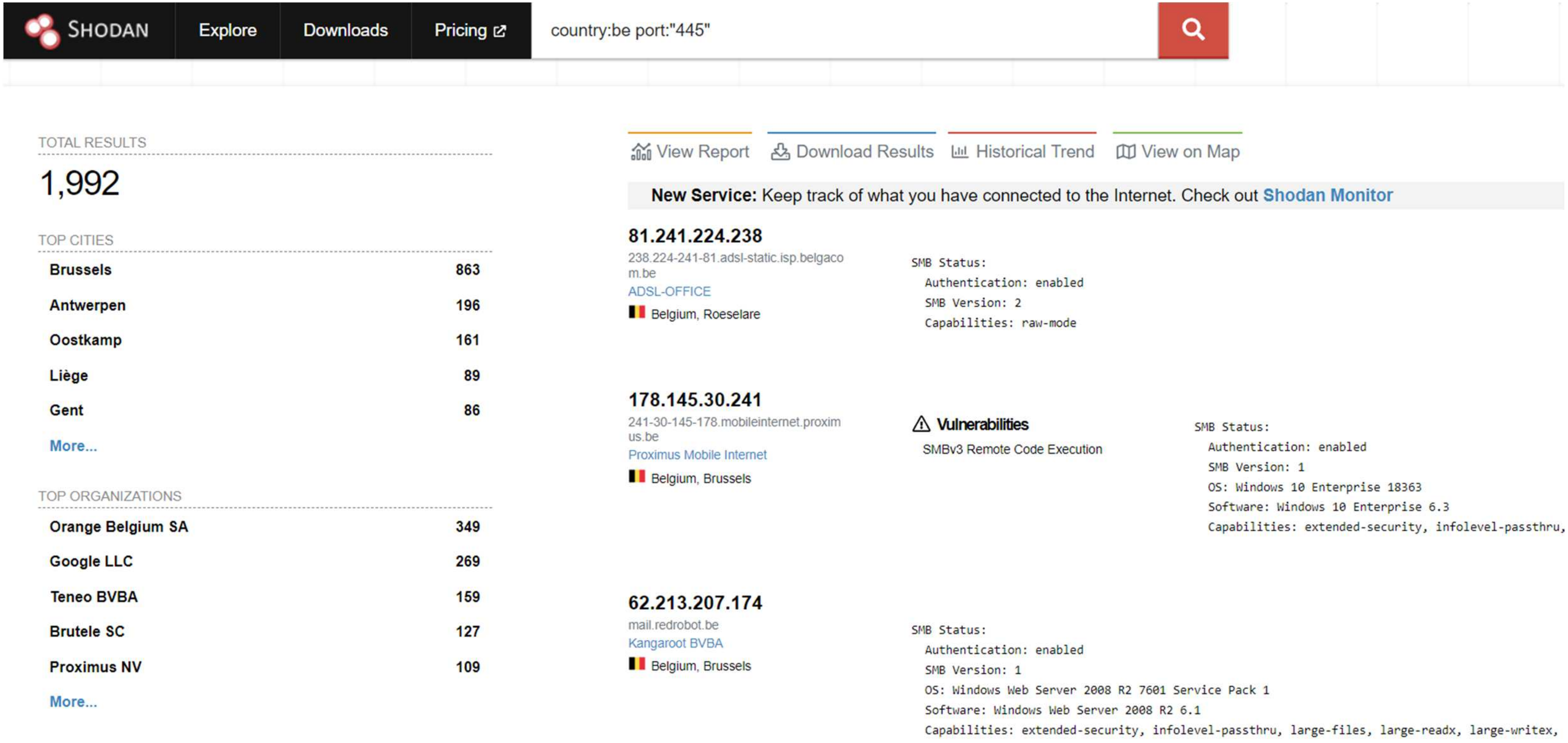
// **5900** / TCP

117718508 | 2023-11-22T01:24:57.994705

VNC

```
RFB 003.008

VNC:
  Protocol Version: 3.8
  Security Types:
    2: VNC Authentication
    17: Ultra
```



country:be port:"445"

TOTAL RESULTS

1,992

TOP CITIES

Brussels	863
Antwerpen	196
Oostkamp	161
Liège	89
Gent	86

More...

TOP ORGANIZATIONS

Orange Belgium SA	349
Google LLC	269
Teneo BVBA	159
Brutele SC	127
Proximus NV	109

More...

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

81.241.224.238

238.224-241-81.adsl-static.isp.belgacom.be

ADSL-OFFICE

Belgium, Roeselare

```
SMB Status:
  Authentication: enabled
  SMB Version: 2
  Capabilities: raw-mode
```

178.145.30.241

241-30-145-178.mobileinternet.proximus.be

Proximus Mobile Internet

Belgium, Brussels

⚠ **Vulnerabilities**

SMBv3 Remote Code Execution

```
SMB Status:
  Authentication: enabled
  SMB Version: 1
  OS: Windows 10 Enterprise 18363
  Software: Windows 10 Enterprise 6.3
  Capabilities: extended-security, infolevel-passthru,
```

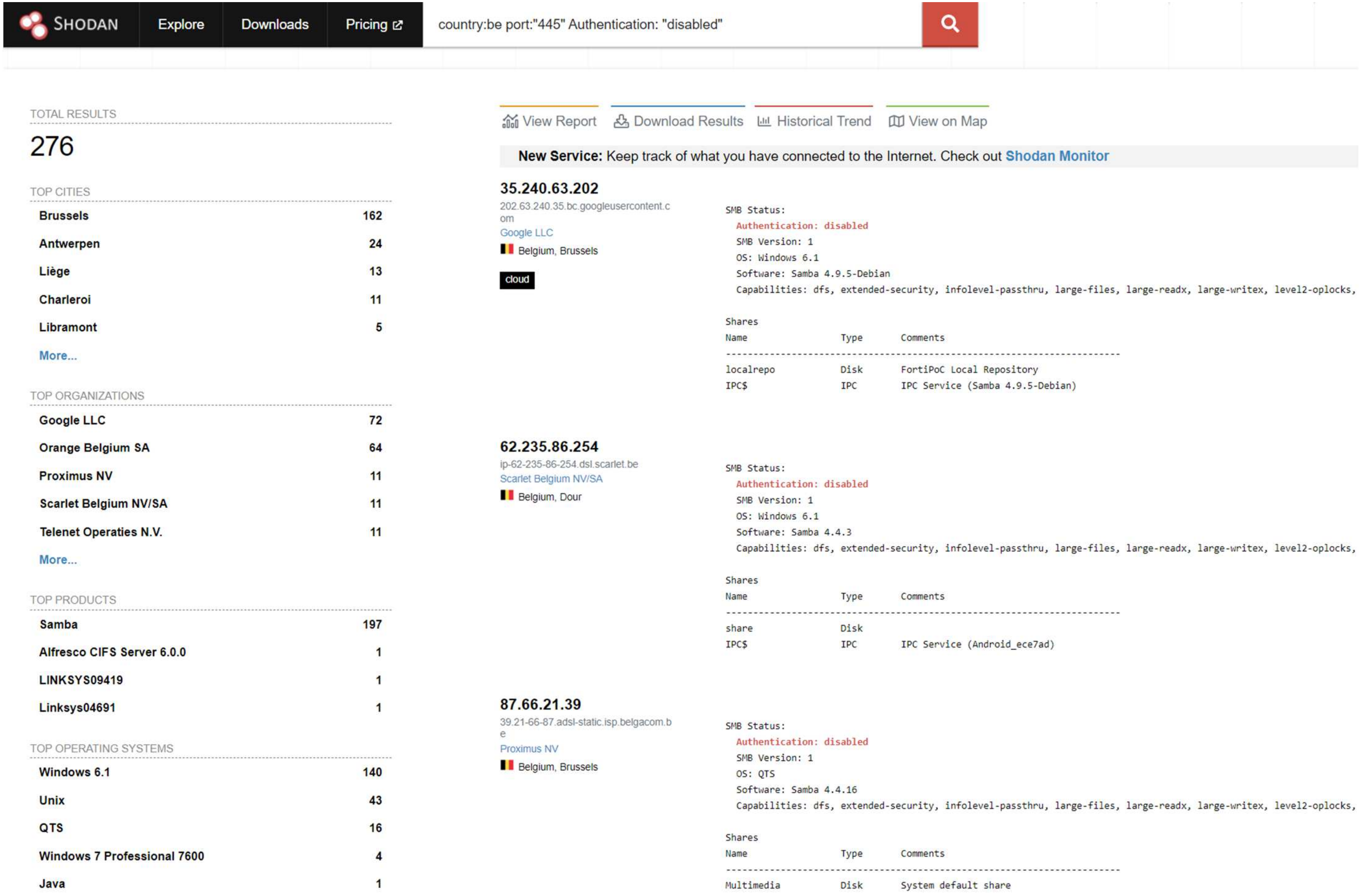
62.213.207.174

mail.redrobot.be

Kangaroot BVBA

Belgium, Brussels

```
SMB Status:
  Authentication: enabled
  SMB Version: 1
  OS: Windows Web Server 2008 R2 7601 Service Pack 1
  Software: Windows Web Server 2008 R2 6.1
  Capabilities: extended-security, infolevel-passthru, large-files, large-readx, large-writex,
```



country:be port:"445" Authentication: "disabled"

TOTAL RESULTS

276

TOP CITIES	
Brussels	162
Antwerpen	24
Liège	13
Charleroi	11
Libramont	5
More...	

TOP ORGANIZATIONS	
Google LLC	72
Orange Belgium SA	64
Proximus NV	11
Scarlet Belgium NV/SA	11
Telenet Operaties N.V.	11
More...	

TOP PRODUCTS	
Samba	197
Alfresco CIFS Server 6.0.0	1
LINKSYS09419	1
Linksys04691	1

TOP OPERATING SYSTEMS	
Windows 6.1	140
Unix	43
QTS	16
Windows 7 Professional 7600	4
Java	1

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

35.240.63.202
202.63.240.35.bc.googleusercontent.com
Google LLC
Belgium, Brussels
cloud

```
SMB Status:
  Authentication: disabled
  SMB Version: 1
  OS: Windows 6.1
  Software: Samba 4.9.5-Debian
  Capabilities: dfs, extended-security, infolevel-passthru, large-files, large-readx, large-writex, level2-oplocks,

Shares
Name                 Type       Comments
------------------------------------------------------------------------
localrepo            Disk       FortiPoC Local Repository
IPC$                 IPC        IPC Service (Samba 4.9.5-Debian)
```

62.235.86.254
ip-62-235-86-254.dsl.scarlet.be
Scarlet Belgium NV/SA
Belgium, Dour

```
SMB Status:
  Authentication: disabled
  SMB Version: 1
  OS: Windows 6.1
  Software: Samba 4.4.3
  Capabilities: dfs, extended-security, infolevel-passthru, large-files, large-readx, large-writex, level2-oplocks,

Shares
Name                 Type       Comments
------------------------------------------------------------------------
share                Disk
IPC$                 IPC        IPC Service (Android_ece7ad)
```

87.66.21.39
39.21-66-87.adsl-static.isp.belgacom.be
Proximus NV
Belgium, Brussels

```
SMB Status:
  Authentication: disabled
  SMB Version: 1
  OS: QTS
  Software: Samba 4.4.16
  Capabilities: dfs, extended-security, infolevel-passthru, large-files, large-readx, large-writex, level2-oplocks,

Shares
Name                 Type       Comments
------------------------------------------------------------------------
Multimedia           Disk       System default share
```

inetum realdolmen
Positive digital flow

Let’s secure the future, together.

Cybersecurity Challenges

Work From Anywhere

Hybrid work requires a complete revamp of how we think about and approach security

Applications & data are Everywhere

71% of organizations are pursuing a hybrid (36%) or multi-cloud strategy (35%) for integration of multiple services, scalability or business continuity reasons

Compliancy Requirements

A growing demand for law regulations and market standards like ISO27k1, NIS2, CRA, …

Operational Technology Connectivity

42% indicate that their control systems had direct connectivity to the internet up from 12% in 2019

⇦ Detection & Response ⇨

CYBERSECURITY ACCELERATOR PROGRAM

Identify & Inspire

Audit & Assessment
Ethical hacking
Roadmap
Proof of Concept

Protect & Integrate

Zero Trust implementation

- Identities
- Devices
- Data
- Applications
- Networks & Infrastructure

Detect & Operate

Managed Security Services
Vulnerability Management
MDR Services

Respond & Optimize

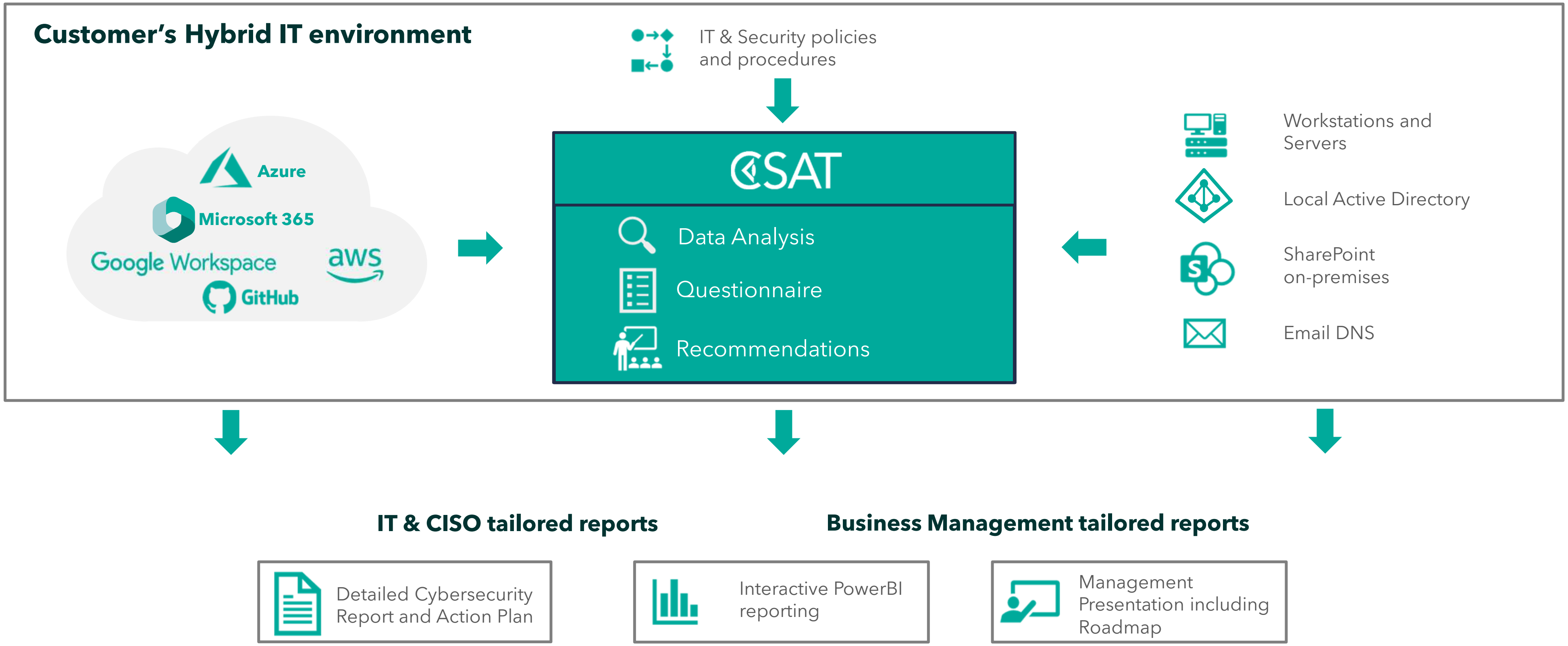
Incident Response
Governance
CISO as a Service
User Awareness

CSAT Assessment Roadmap

Why CSAT?

Organizations need to know their cyber security vulnerabilities	Organizations need an action plan to improve cyber security	Focus your limited security budgets on the highest risks	Recognized solution to conduct Cybersecurity Assessments in all segments
• Market demands to take security seriously • Law regulations and market standards (NIS2/GDPR/ISO27k) • Brand reputation damage and financial penalties	• Fact based actionable insights • Align Business Management & IT/Security Management with one common truth	• Invest in the right security initiatives by making informed decisions based on facts	• Over 2000 assessments worldwide • Global partnership with Microsoft • Customers in all segments and industries

Data collection and report generation



Customer's Hybrid IT environment

Azure

Microsoft 365

Google Workspace

aws

GitHub

IT & Security policies and procedures

CSAT

Data Analysis

Questionnaire

Recommendations

Workstations and Servers

Local Active Directory

SharePoint on-premises

Email DNS

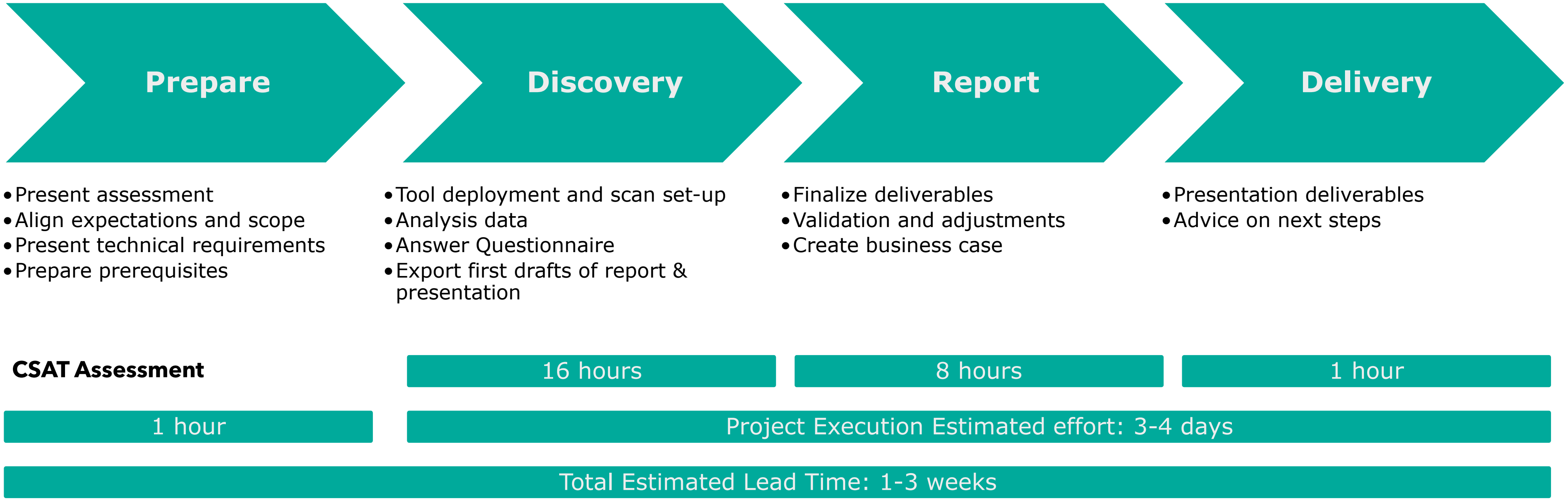
IT & CISO tailored reports

Business Management tailored reports

Detailed Cybersecurity Report and Action Plan

Interactive PowerBI reporting

Management Presentation including Roadmap



Prepare

- Present assessment
- Align expectations and scope
- Present technical requirements
- Prepare prerequisites

Discovery

- Tool deployment and scan set-up
- Analysis data
- Answer Questionnaire
- Export first drafts of report & presentation

Report

- Finalize deliverables
- Validation and adjustments
- Create business case

Delivery

- Presentation deliverables
- Advice on next steps

CSAT Assessment

16 hours

8 hours

1 hour

1 hour

Project Execution Estimated effort: 3-4 days

Total Estimated Lead Time: 1-3 weeks

Steps of the Cybersecurity Assessment

inetum realdolmen
Positive digital flow

Step 1

Let's get started!

Set-up a kick-off call with a Cybersecurity specialist to:

- Make introductions
- Discuss goals of the assessment
- Share system requirements

Prepare your environment for the assessment and plan next activities

Step 2

We **collect and analyze** your IT asset data

One of our Cybersecurity specialists runs the scans & tests to collect relevant data

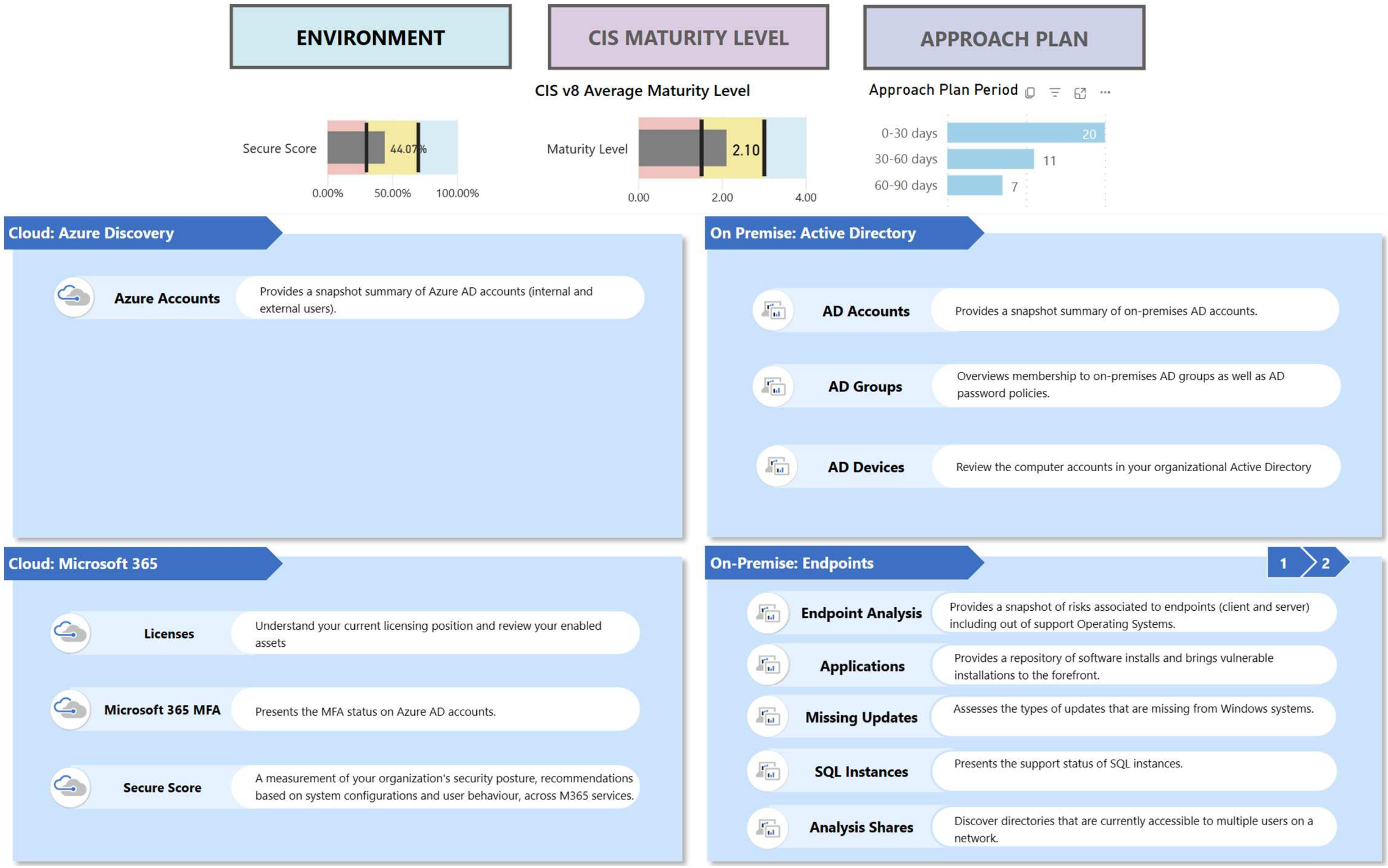
Discuss your organization's cybersecurity posture in an interview (IT manager/CIO/CISO required)

Step 3

Presentation of the report

Deliver presentation and discuss findings, conclusions and recommendations.

Share final report and presentation



Cloud: Azure Discovery

Azure Accounts Provides a snapshot summary of Azure AD accounts (internal and external users).

On Premise: Active Directory

AD Accounts Provides a snapshot summary of on-premises AD accounts.

AD Groups Overviews membership to on-premises AD groups as well as AD password policies.

AD Devices Review the computer accounts in your organizational Active Directory

Cloud: Microsoft 365

Licenses Understand your current licensing position and review your enabled assets

Microsoft 365 MFA Presents the MFA status on Azure AD accounts.

Secure Score A measurement of your organization's security posture, recommendations based on system configurations and user behaviour, across M365 services.

On-Premise: Endpoints

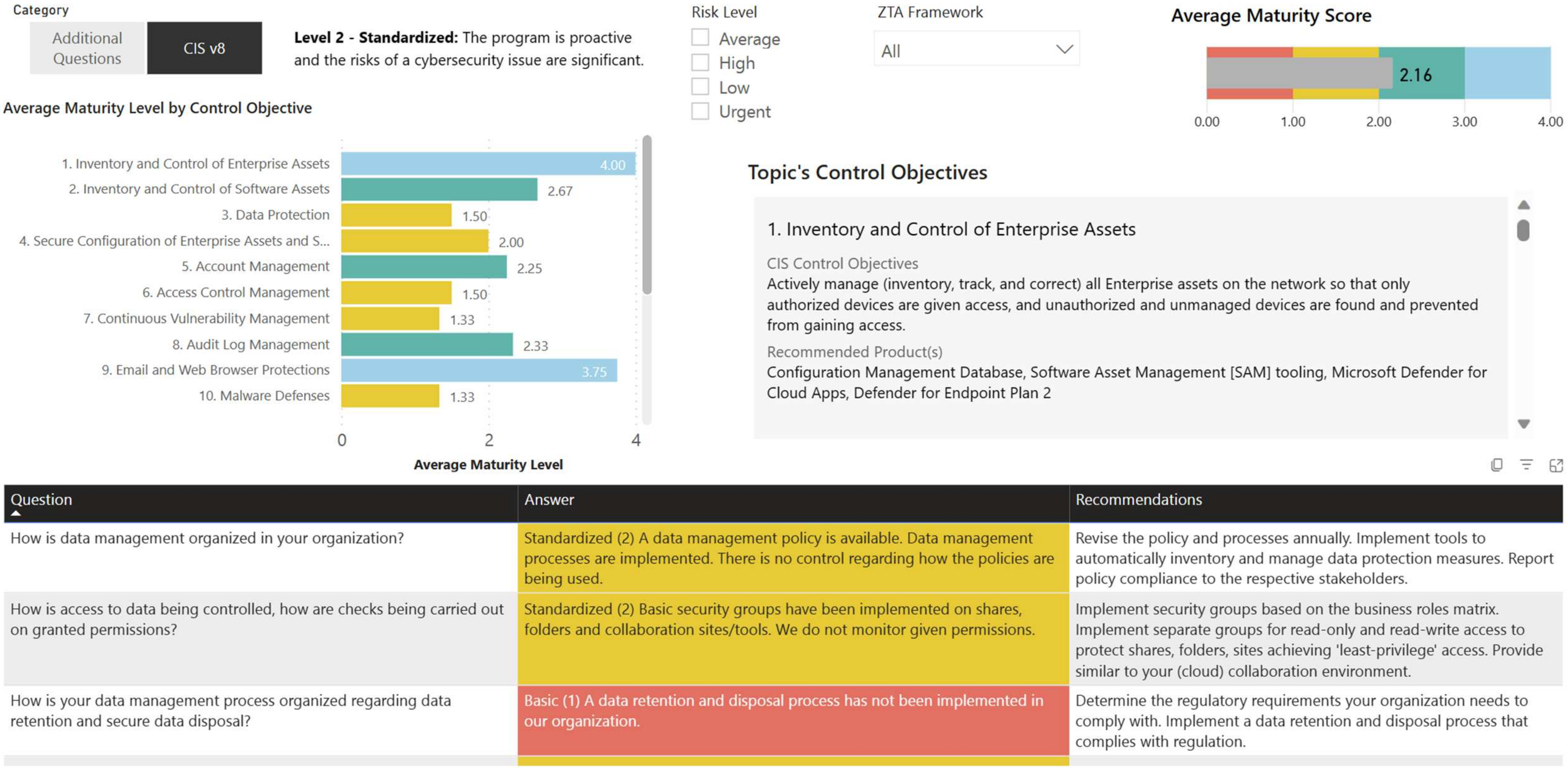
Endpoint Analysis Provides a snapshot of risks associated to endpoints (client and server) including out of support Operating Systems.

Applications Provides a repository of software installs and brings vulnerable installations to the forefront.

Missing Updates Assesses the types of updates that are missing from Windows systems.

SQL Instances Presents the support status of SQL instances.

Analysis Shares Discover directories that are currently accessible to multiple users on a network.


Category
Additional Questions
CIS v8
Average Maturity Level by Control Objective
1. Inventory and Control of Enterprise Assets 4.00
2. Inventory and Control of Software Assets 2.67
3. Data Protection 1.50
4. Secure Configuration of Enterprise Assets and S... 2.00
5. Account Management 2.25
6. Access Control Management 1.50
7. Continuous Vulnerability Management 1.33
8. Audit Log Management 2.33
9. Email and Web Browser Protections 3.75
10. Malware Defenses 1.33
0
2
4
Average Maturity Level
Risk Level
Average
High
Low
Urgent
ZTA Framework
All
Average Maturity Score
2.16
0.00
1.00
2.00
3.00
4.00

Level 2 - Standardized: The program is proactive and the risks of a cybersecurity issue are significant.

Risk Level

- □ Average
- □ High
- □ Low
- □ Urgent

ZTA Framework: All

Topic's Control Objectives

1. Inventory and Control of Enterprise Assets

CIS Control Objectives

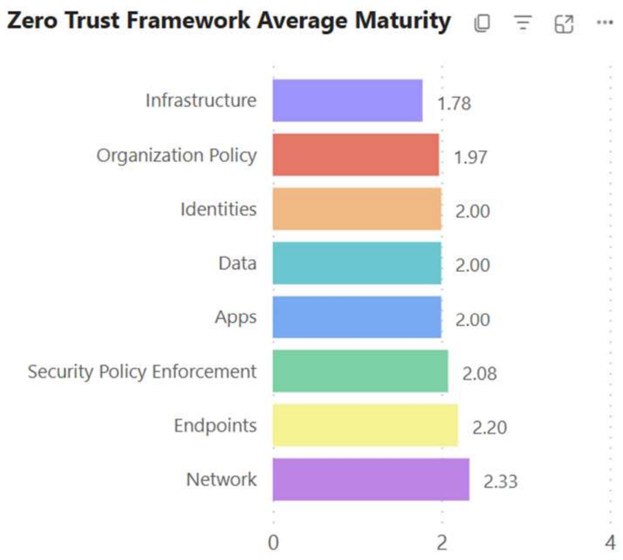
Actively manage (inventory, track, and correct) all Enterprise assets on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

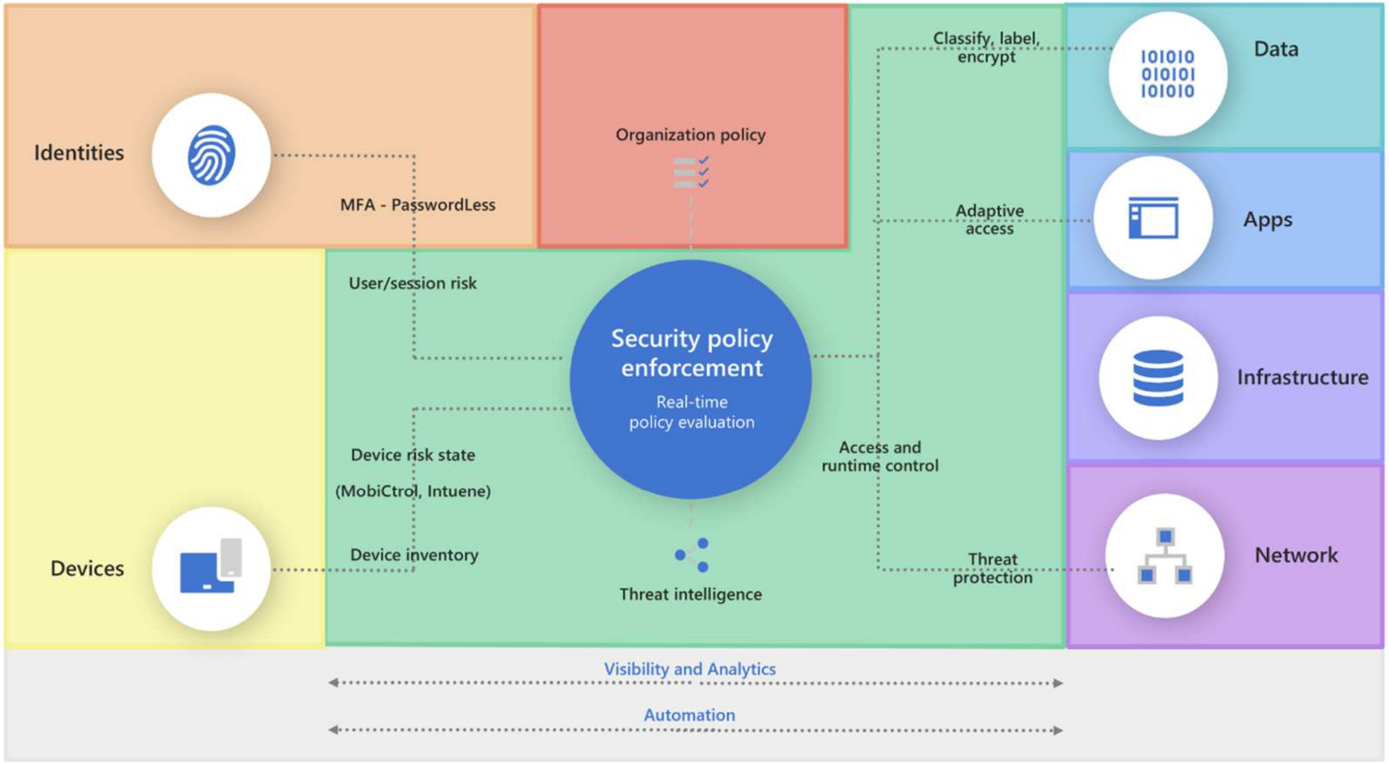
Recommended Product(s)

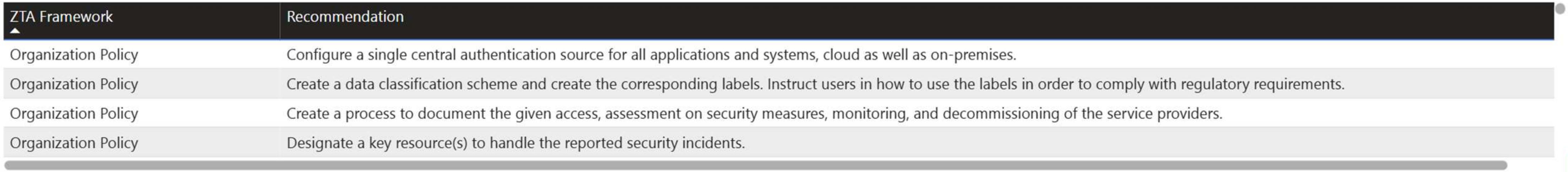
Configuration Management Database, Software Asset Management [SAM] tooling, Microsoft Defender for Cloud Apps, Defender for Endpoint Plan 2

Question	Answer	Recommendations
How is data management organized in your organization?	Standardized (2) A data management policy is available. Data management processes are implemented. There is no control regarding how the policies are being used.	Revise the policy and processes annually. Implement tools to automatically inventory and manage data protection measures. Report policy compliance to the respective stakeholders.
How is access to data being controlled, how are checks being carried out on granted permissions?	Standardized (2) Basic security groups have been implemented on shares, folders and collaboration sites/tools. We do not monitor given permissions.	Implement security groups based on the business roles matrix. Implement separate groups for read-only and read-write access to protect shares, folders, sites achieving 'least-privilege' access. Provide similar to your (cloud) collaboration environment.
How is your data management process organized regarding data retention and secure data disposal?	Basic (1) A data retention and disposal process has not been implemented in our organization.	Determine the regulatory requirements your organization needs to comply with. Implement a data retention and disposal process that complies with regulation.

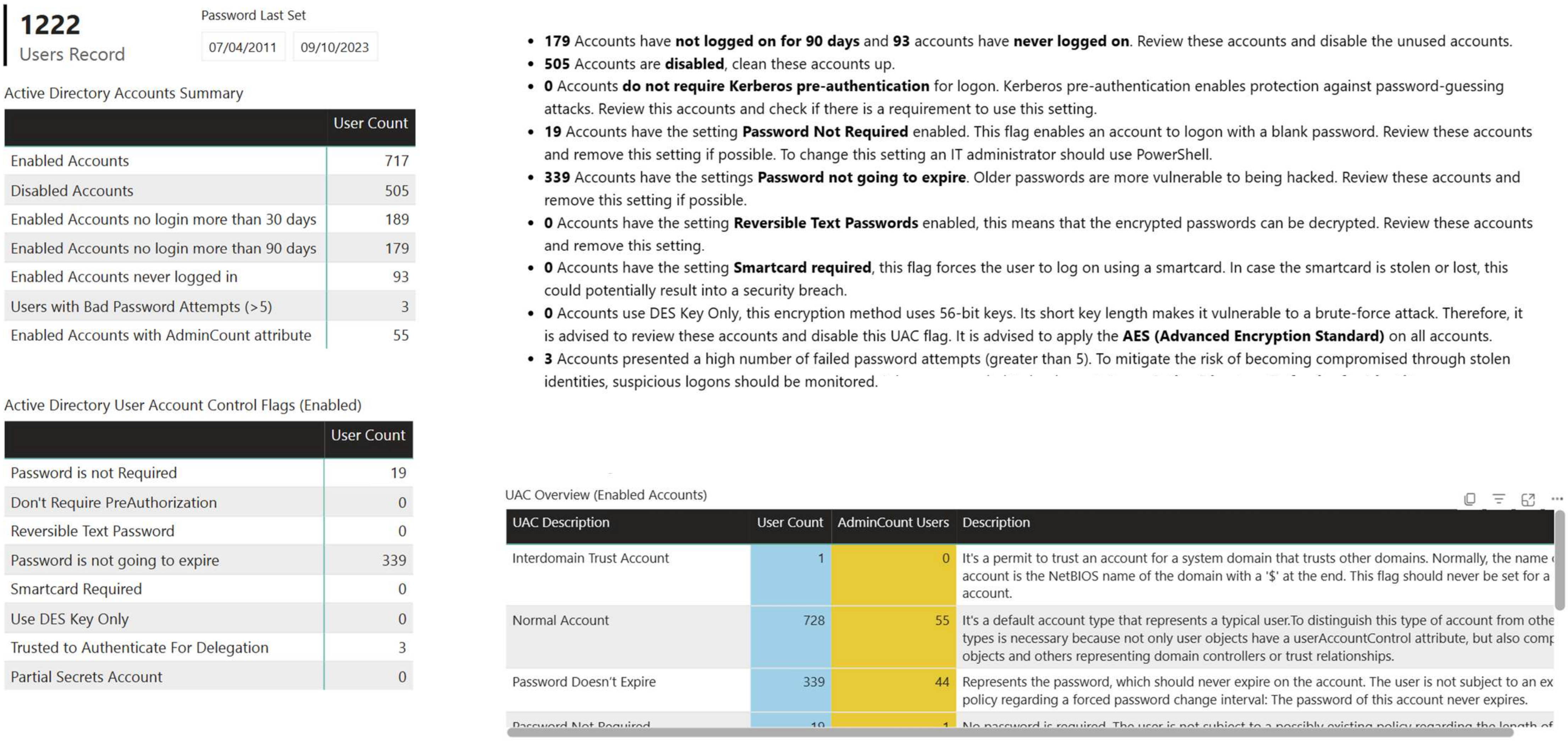
Zero-Trust Architecture *is an enterprise's cybersecurity plan that utilizes zero-trust concepts and encompasses component relationships, workflow planning, and access policies.*


Zero Trust Framework Average Maturity





ZTA Framework	Recommendation
Organization Policy	Configure a single central authentication source for all applications and systems, cloud as well as on-premises.
Organization Policy	Create a data classification scheme and create the corresponding labels. Instruct users in how to use the labels in order to comply with regulatory requirements.
Organization Policy	Create a process to document the given access, assessment on security measures, monitoring, and decommissioning of the service providers.
Organization Policy	Designate a key resource(s) to handle the reported security incidents.



1222

Users Record

Password Last Set

07/04/2011 | 09/10/2023

Active Directory Accounts Summary

	User Count
Enabled Accounts	717
Disabled Accounts	505
Enabled Accounts no login more than 30 days	189
Enabled Accounts no login more than 90 days	179
Enabled Accounts never logged in	93
Users with Bad Password Attempts (>5)	3
Enabled Accounts with AdminCount attribute	55

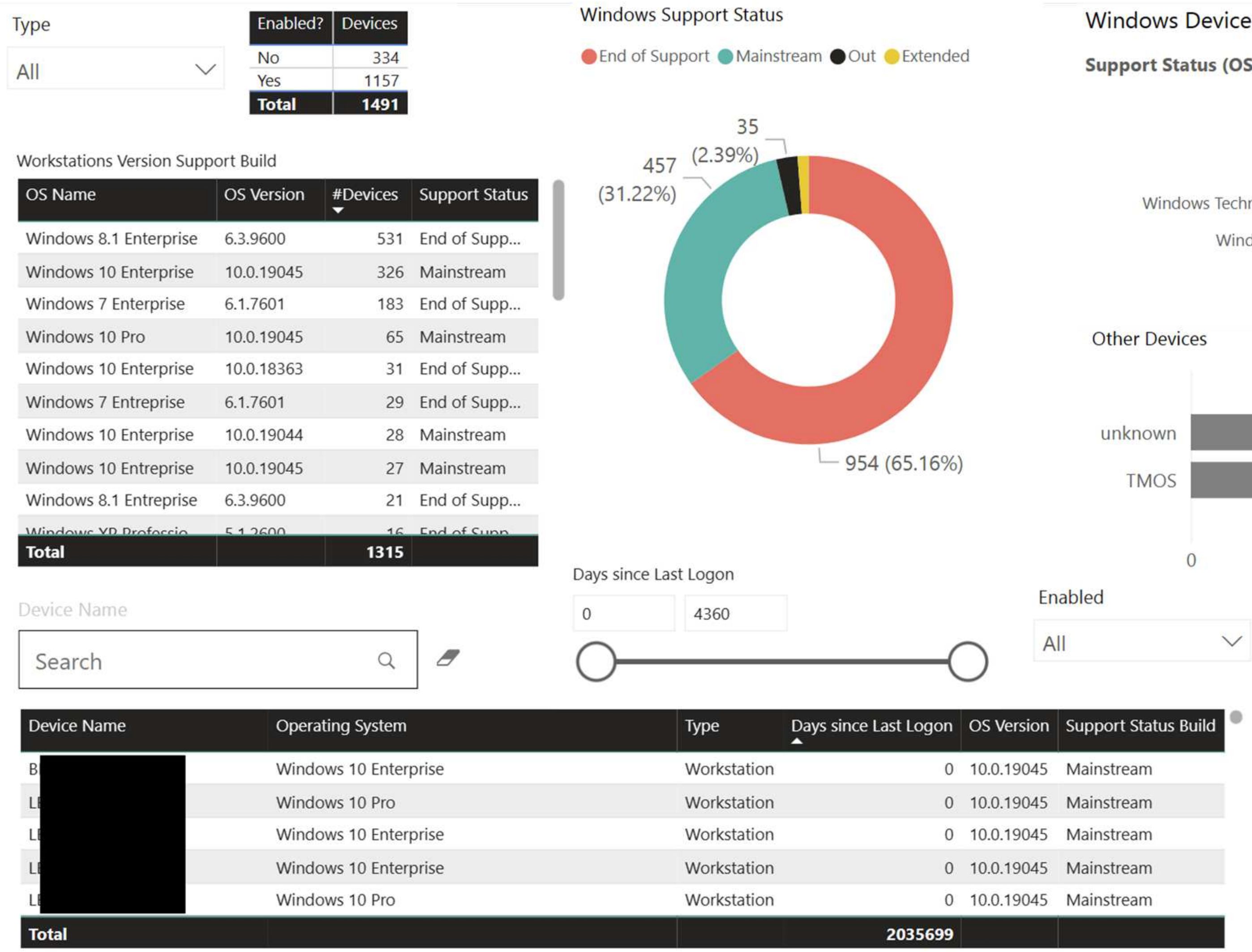
Active Directory User Account Control Flags (Enabled)

	User Count
Password is not Required	19
Don't Require PreAuthorization	0
Reversible Text Password	0
Password is not going to expire	339
Smartcard Required	0
Use DES Key Only	0
Trusted to Authenticate For Delegation	3
Partial Secrets Account	0

- **179** Accounts have **not logged on for 90 days** and **93** accounts have **never logged on**. Review these accounts and disable the unused accounts.
- **505** Accounts are **disabled**, clean these accounts up.
- **0** Accounts **do not require Kerberos pre-authentication** for logon. Kerberos pre-authentication enables protection against password-guessing attacks. Review this accounts and check if there is a requirement to use this setting.
- **19** Accounts have the setting **Password Not Required** enabled. This flag enables an account to logon with a blank password. Review these accounts and remove this setting if possible. To change this setting an IT administrator should use PowerShell.
- **339** Accounts have the settings **Password not going to expire**. Older passwords are more vulnerable to being hacked. Review these accounts and remove this setting if possible.
- **0** Accounts have the setting **Reversible Text Passwords** enabled, this means that the encrypted passwords can be decrypted. Review these accounts and remove this setting.
- **0** Accounts have the setting **Smartcard required**, this flag forces the user to log on using a smartcard. In case the smartcard is stolen or lost, this could potentially result into a security breach.
- **0** Accounts use DES Key Only, this encryption method uses 56-bit keys. Its short key length makes it vulnerable to a brute-force attack. Therefore, it is advised to review these accounts and disable this UAC flag. It is advised to apply the **AES (Advanced Encryption Standard)** on all accounts.
- **3** Accounts presented a high number of failed password attempts (greater than 5). To mitigate the risk of becoming compromised through stolen identities, suspicious logons should be monitored.

UAC Overview (Enabled Accounts)

UAC Description	User Count	AdminCount Users	Description
Interdomain Trust Account	1	0	It's a permit to trust an account for a system domain that trusts other domains. Normally, the name account is the NetBIOS name of the domain with a '$' at the end. This flag should never be set for a account.
Normal Account	728	55	It's a default account type that represents a typical user.To distinguish this type of account from othe types is necessary because not only user objects have a userAccountControl attribute, but also comp objects and others representing domain controllers or trust relationships.
Password Doesn't Expire	339	44	Represents the password, which should never expire on the account. The user is not subject to an ex policy regarding a forced password change interval: The password of this account never expires.
Password Not Required	19	1	No password is required. The user is not subject to a possibly existing policy regarding the length of



Type

All

Enabled?	Devices
No	334
Yes	1157
Total	**1491**

Workstations Version Support Build

OS Name	OS Version	#Devices	Support Status
Windows 8.1 Enterprise	6.3.9600	531	End of Supp...
Windows 10 Enterprise	10.0.19045	326	Mainstream
Windows 7 Enterprise	6.1.7601	183	End of Supp...
Windows 10 Pro	10.0.19045	65	Mainstream
Windows 10 Enterprise	10.0.18363	31	End of Supp...
Windows 7 Entreprise	6.1.7601	29	End of Supp...
Windows 10 Enterprise	10.0.19044	28	Mainstream
Windows 10 Entreprise	10.0.19045	27	Mainstream
Windows 8.1 Entreprise	6.3.9600	21	End of Supp...
Windows XP Professio	5.1.2600	16	End of Supp...
Total		**1315**	

Windows Devices
Support Status (OS) ● End of Support ● Extended ● Mainstream ● Out
Windows 7 Entreprise
32
Windows XP Professional
Windows Technical Preview for Enterprise
Windows Server 2022 Standard
0
200
400
600
#Devices

Device Name

Search

Days since Last Logon

0 4360

Enabled

All

OS Version

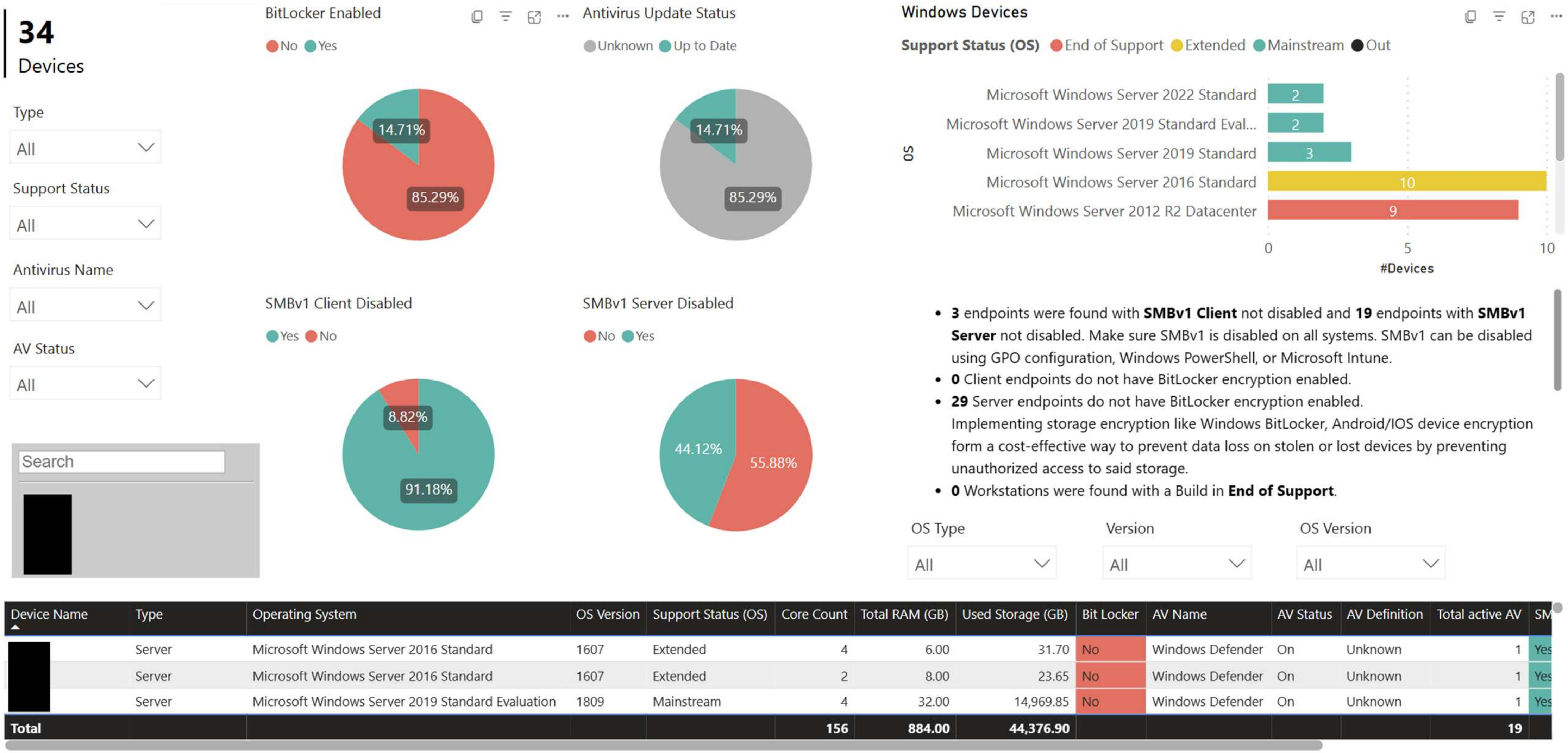
All

OS Name

All

Device Name	Operating System	Type	Days since Last Logon	OS Version	Support Status Build
[redacted]	Windows 10 Enterprise	Workstation	0	10.0.19045	Mainstream
[redacted]	Windows 10 Pro	Workstation	0	10.0.19045	Mainstream
[redacted]	Windows 10 Enterprise	Workstation	0	10.0.19045	Mainstream
[redacted]	Windows 10 Enterprise	Workstation	0	10.0.19045	Mainstream
[redacted]	Windows 10 Pro	Workstation	0	10.0.19045	Mainstream
Total			**2035699**		

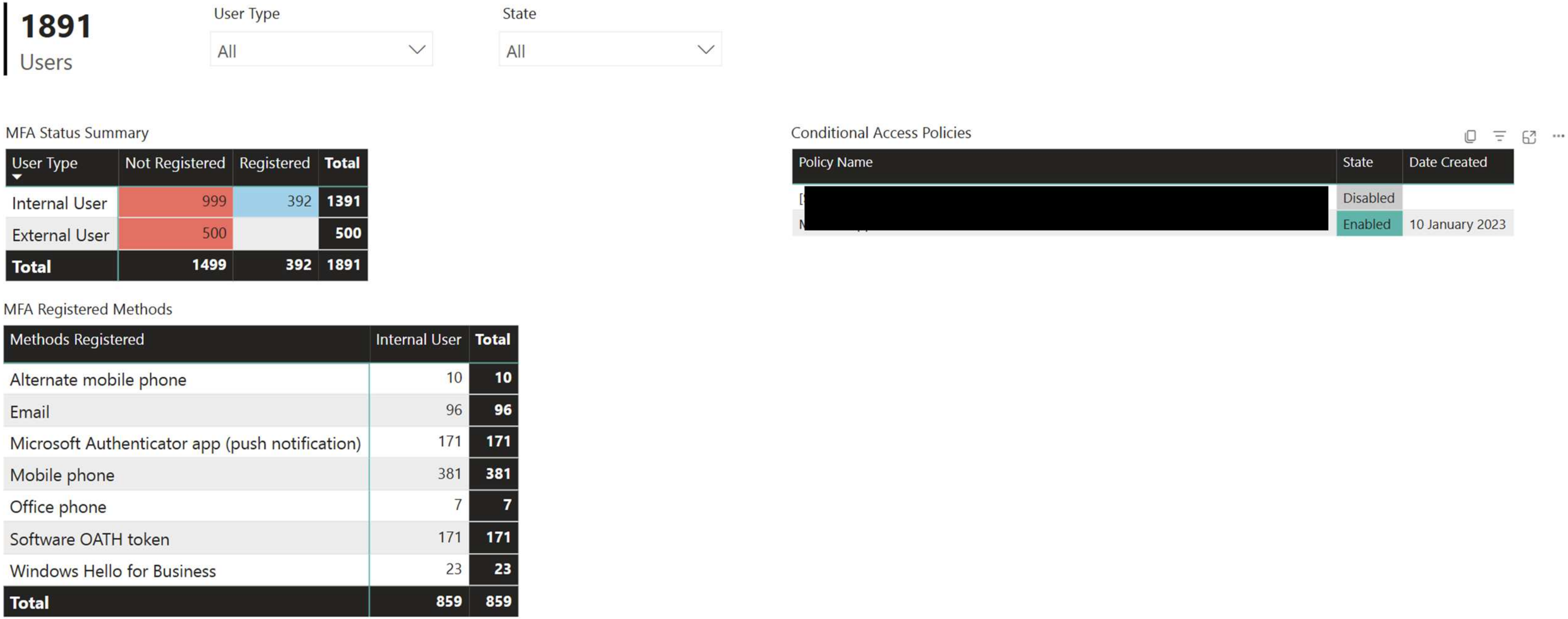
- There are **1157** Enabled Accounts and **334** Disabled Accounts. Clean up the disabled accounts.
- There are **740** Enabled Accounts with inactivity beyond 30 days (**78** Servers and **639** Workstations).
- **65** Enabled Workstations have Windows 10 Installations with a current unsupported build. Update to the latest version of Windows 10 **(19045 build)** or to **Windows 11**.



[redacted]

- **3** endpoints were found with **SMBv1 Client** not disabled and **19** endpoints with **SMBv1 Server** not disabled. Make sure SMBv1 is disabled on all systems. SMBv1 can be disabled using GPO configuration, Windows PowerShell, or Microsoft Intune.
- **0** Client endpoints do not have BitLocker encryption enabled.
- **29** Server endpoints do not have BitLocker encryption enabled.
  Implementing storage encryption like Windows BitLocker, Android/IOS device encryption form a cost-effective way to prevent data loss on stolen or lost devices by preventing unauthorized access to said storage.
- **0** Workstations were found with a Build in **End of Support**.

Device Name	Type	Operating System	OS Version	Support Status (OS)	Core Count	Total RAM (GB)	Used Storage (GB)	Bit Locker	AV Name	AV Status	AV Definition	Total active AV	SM
[redacted]	Server	Microsoft Windows Server 2016 Standard	1607	Extended	4	6.00	31.70	No	Windows Defender	On	Unknown	1	Yes
[redacted]	Server	Microsoft Windows Server 2016 Standard	1607	Extended	2	8.00	23.65	No	Windows Defender	On	Unknown	1	Yes
[redacted]	Server	Microsoft Windows Server 2019 Standard Evaluation	1809	Mainstream	4	32.00	14,969.85	No	Windows Defender	On	Unknown	1	Yes
Total					**156**	**884.00**	**44,376.90**					**19**	



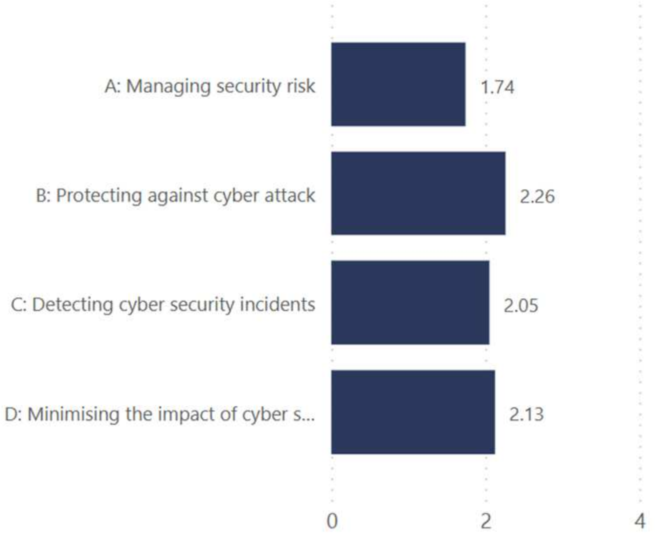
The **NIS 2 Directive** is the EU-wide legislation on cybersecurity. The goal of NIS 2 is to enhance the security level in the same level across the EU. Some of the key benefits of the NIS 2 Directive:

- Improve the cybersecurity posture of your businesses across EU, making it more resilient to cyberattacks.
- Promote a more harmonized approach to cybersecurity, making it easier for businesses to operate across borders.
- Strengthen the EU's ability to respond to cyberattacks and other cybersecurity threats.

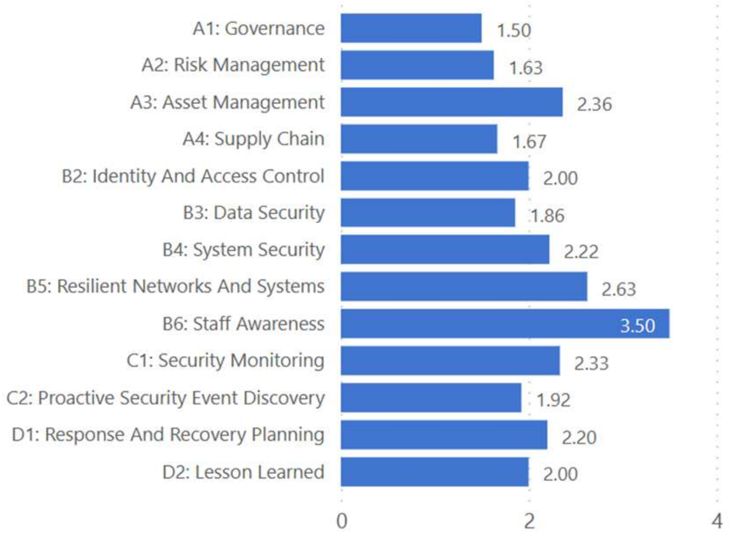
NIS 2 Principles have been linked with the questionnaire to provide a current state based on the **NIS Regulations - Compliance Framework** (some questions may apply to more than one Principle)

NIS2 Directive

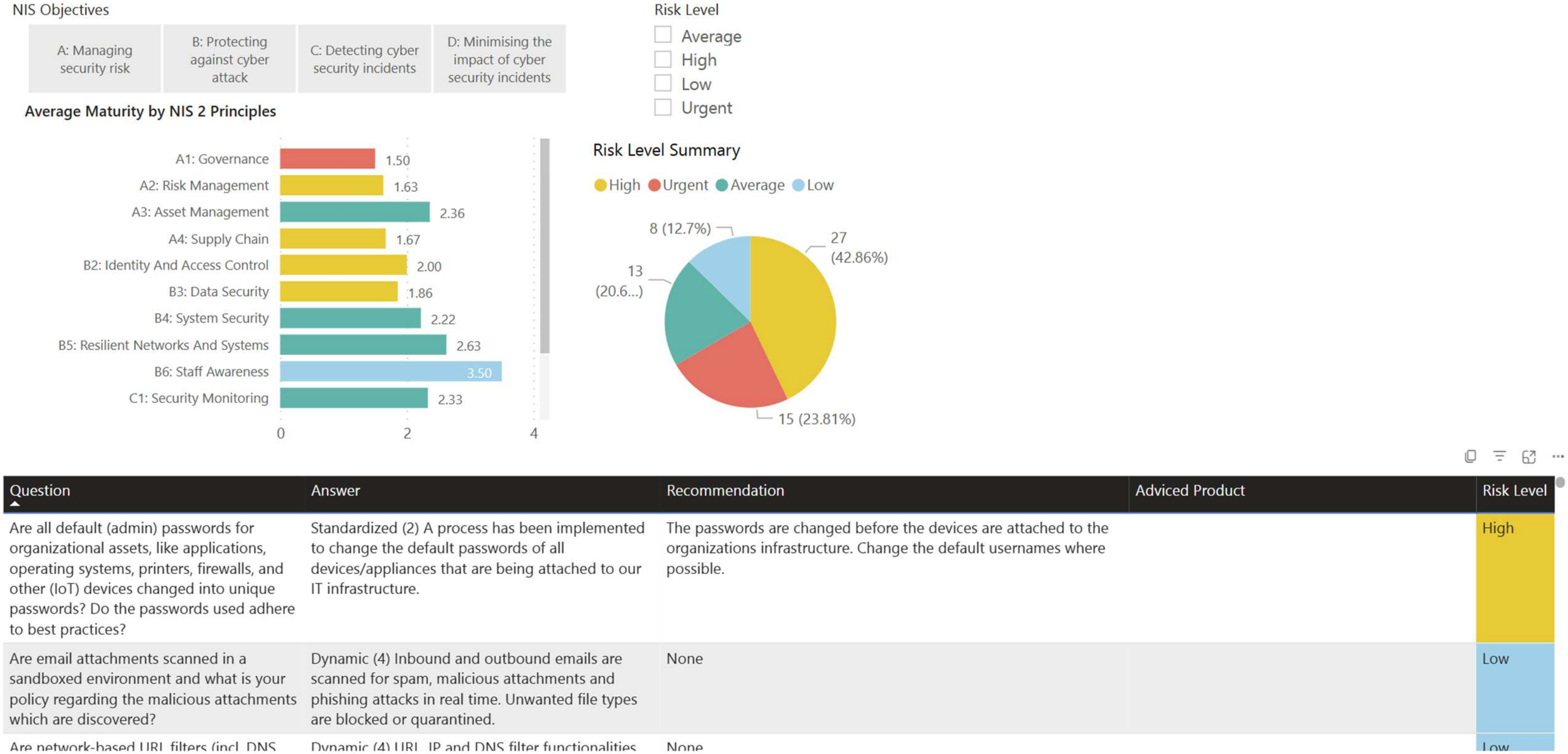
NIS 2 Objectives Average Maturity



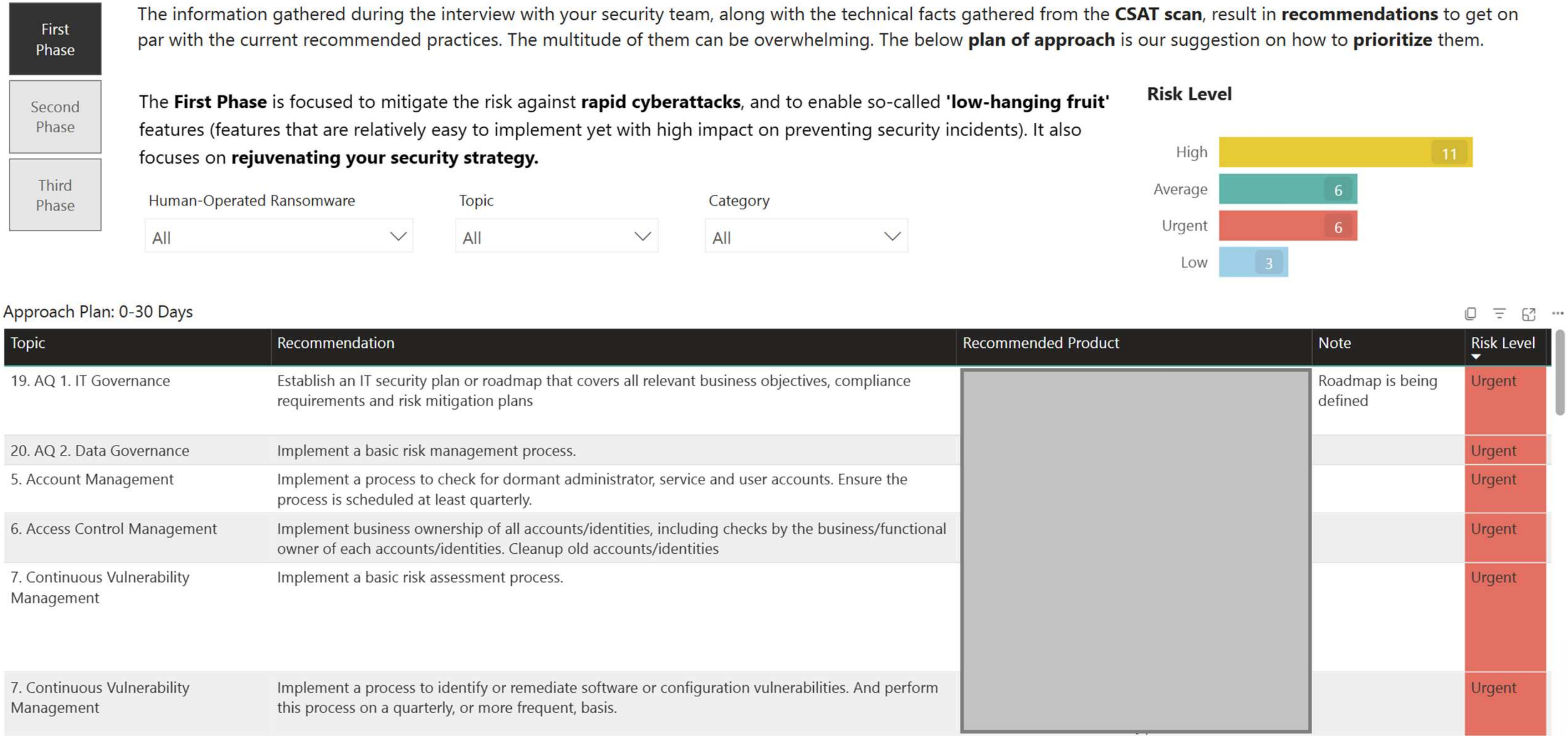
NIS 2 Principles Average Maturity



Questionnaire


NIS Objectives
A: Managing security risk
B: Protecting against cyber attack
C: Detecting cyber security incidents
D: Minimising the impact of cyber security incidents
Risk Level
□ Average
□ High
□ Low
□ Urgent
Average Maturity by NIS 2 Principles
A1: Governance 1.50
A2: Risk Management 1.63
A3: Asset Management 2.36
A4: Supply Chain 1.67
B2: Identity And Access Control 2.00
B3: Data Security 1.86
B4: System Security 2.22
B5: Resilient Networks And Systems 2.63
B6: Staff Awareness 3.50
C1: Security Monitoring 2.33
0
2
4
Risk Level Summary
● High ● Urgent ● Average ● Low
8 (12.7%)
27 (42.86%)
13 (20.6...)
15 (23.81%)

Question	Answer	Recommendation	Adviced Product	Risk Level
Are all default (admin) passwords for organizational assets, like applications, operating systems, printers, firewalls, and other (IoT) devices changed into unique passwords? Do the passwords used adhere to best practices?	Standardized (2) A process has been implemented to change the default passwords of all devices/appliances that are being attached to our IT infrastructure.	The passwords are changed before the devices are attached to the organizations infrastructure. Change the default usernames where possible.		High
Are email attachments scanned in a sandboxed environment and what is your policy regarding the malicious attachments which are discovered?	Dynamic (4) Inbound and outbound emails are scanned for spam, malicious attachments and phishing attacks in real time. Unwanted file types are blocked or quarantined.	None		Low
Are network-based URL filters (incl. DNS	Dynamic (4) URL, IP and DNS filter functionalities	None		Low



The information gathered during the interview with your security team, along with the technical facts gathered from the **CSAT scan**, result in **recommendations** to get on par with the current recommended practices. The multitude of them can be overwhelming. The below **plan of approach** is our suggestion on how to **prioritize** them.

The **First Phase** is focused to mitigate the risk against **rapid cyberattacks**, and to enable so-called **'low-hanging fruit'** features (features that are relatively easy to implement yet with high impact on preventing security incidents). It also focuses on **rejuvenating your security strategy.**

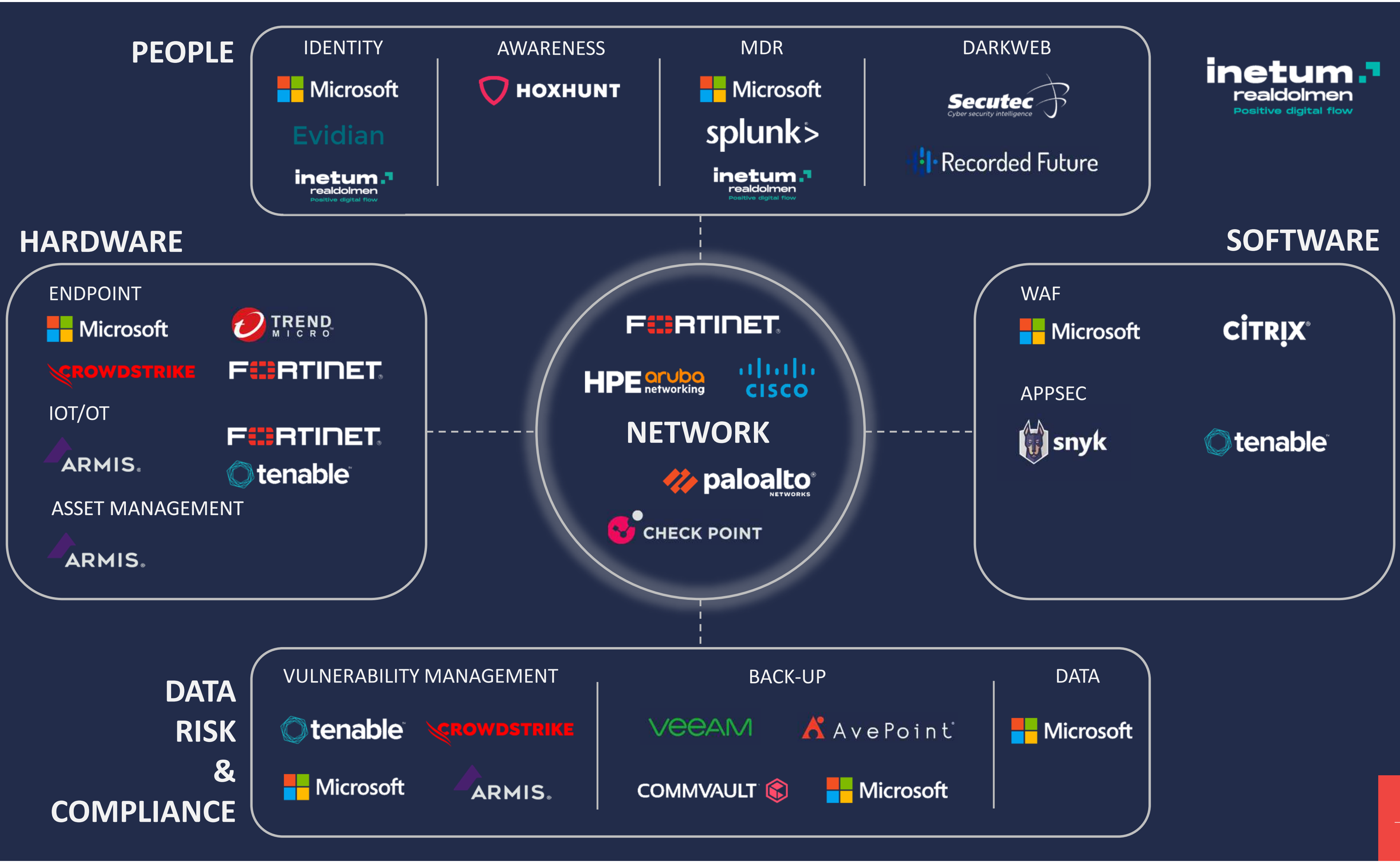
Human-Operated Ransomware: All

Topic: All

Category: All

Approach Plan: 0-30 Days

Topic	Recommendation	Recommended Product	Note	Risk Level
19. AQ 1. IT Governance	Establish an IT security plan or roadmap that covers all relevant business objectives, compliance requirements and risk mitigation plans	[redacted]	Roadmap is being defined	Urgent
20. AQ 2. Data Governance	Implement a basic risk management process.	[redacted]		Urgent
5. Account Management	Implement a process to check for dormant administrator, service and user accounts. Ensure the process is scheduled at least quarterly.	[redacted]		Urgent
6. Access Control Management	Implement business ownership of all accounts/identities, including checks by the business/functional owner of each accounts/identities. Cleanup old accounts/identities	[redacted]		Urgent
7. Continuous Vulnerability Management	Implement a basic risk assessment process.	[redacted]		Urgent
7. Continuous Vulnerability Management	Implement a process to identify or remediate software or configuration vulnerabilities. And perform this process on a quarterly, or more frequent, basis.	[redacted]		Urgent



inetum. realdolmen
Positive digital flow

PEOPLE

IDENTITY
Microsoft
Evidian
inetum. realdolmen Positive digital flow

AWARENESS
HOXHUNT

MDR
Microsoft
splunk>
inetum. realdolmen Positive digital flow

DARKWEB
Secutec Cyber security intelligence
Recorded Future

HARDWARE

ENDPOINT
Microsoft
TREND MICRO
CROWDSTRIKE
FORTINET

IOT/OT
ARMIS
FORTINET
tenable

ASSET MANAGEMENT
ARMIS

NETWORK
FORTINET
HPE aruba networking
CISCO
paloalto NETWORKS
CHECK POINT

SOFTWARE

WAF
Microsoft
CITRIX

APPSEC
snyk
tenable

DATA RISK & COMPLIANCE

VULNERABILITY MANAGEMENT
tenable
CROWDSTRIKE
Microsoft
ARMIS

BACK-UP
veeam
AvePoint
COMMVAULT
Microsoft

DATA
Microsoft

inetum.

realdolmen

Positive digital flow

inetum.world

FRANCE | SPAIN | PORTUGAL | BELGIUM | SWITZERLAND | LUXEMBOURG | ENGLAND |
POLAND | ROMANIA | MOROCCO | TUNISIA | SENEGAL | CÔTE D'IVOIRE | ANGOLA |
CAMEROON | USA | BRAZIL | COLOMBIA | MEXICO | RP OF PANAMA | PERU | CHILI |
COSTA RICA | DOMINICAN REPUBLIC | ARGENTINA | SINGAPORE | UAE