Daniel Ubalde

danielubaldelaguia@gmail.com

Descripción breve

Curso de especialización en ciberseguridad 2022

Estructura Lógica



**ÍNDICE DE CONTENIDOS**

1. INTRODUCCIÓN 6

1.1 Estructura lógica 7

2. Estructura física y cableado estructurado 8

2.1 Tipos de medios de transmisión 8

2.2 Armarios de distribución o racks y pasacables 8

2.3 Pach-panels 8

2.4 Cableado horizontal 8

2.5 Cableado vertical 8

3. Estructura lógica 9

3.1 Diseño de la red 9

3.2 Protocolo IP empleado 9

3.3 Direccionamiento IP y subredes 10

4. Administración de servidores 11

4.1 Sistemas operativos y software 11

4.1.1 Servidores 11

4.1.1 Estaciones de trabajo 11

4.2 Servicios en red 11

4.2.1 DNS 11

4.2.2 DHCP 11

4.2.3 VPN 11

4.3 Sistemas de seguridad 11

5. Ciberseguridad 12

5.1 Inventario de Activos 12

5.2 Firewall 13

5.3 DNS 13

5.4 DHCP 13

5.5 VPN 13

5.6 IPS 13

5.7 XDR 13

5.8 Switches 13

5.9 Copias de seguridad 14

5.9.1 Análisis 14

5.9.2 Diseño 14

5.10 Normativa Puestos de trabajo 14

ANEXO 1. Diagrama Packet tracer 15

ANEXO 2. Conexionado Físico 16

ANEXO 3. Plan de ciberseguridad Puestos de trabajo 21

ANEXO 4. Pulseway 22

A1.1 Administración de dispositivos 22

A1.1.1 DESCUBRIMIENTO Y DESPLIEGUE 22

A1.1.2 Monitorización y administración 23

A1.1.3 Automatización y auto remediación 24

A1.1.4 Administración de parches de seguridad 25

A1.1.5 Detección de Ransomware y AV integrado 26

A1.2 Backup & Disaster Recovery 27

A1.3 Protección contra Ransomware 28

A1.3.1 Protección contra Phishing 28

A1.3.2 Planes de concienciación 29

A1.3.3 Escáner de vulnerabilidades 30

A1.3.4 Backup and Disaster Recovery 31

GLOSARIO 32

 ABREVIATURAS Y ACRÓNIMOS 32

 DEFINICIONES 32

CONTROL DE CAMBIOS 33

**ÍNDICE DE TABLAS:**

Tabla 1‑1 Departamentos 6

Tabla 3‑1 Direccionamiento 10

Tabla 5‑1 Conexionado Físico 20

**ÍNDICE DE FIGURAS:**

Figura 1‑1 Topología Híbrida 7

Figura 5‑1 Diagrama Físico planta superior 15

Figura 5‑2 Diagrama Físico planta inferior 15

Figura 5‑3 Pulseway endpoint discovery 22

Figura 5‑3 Monitorización y Administración 23

Figura 5‑3 Automatizaciones 24

Figura 5‑3 Parches de Seguridad 25

Figura 5‑3 Detección de Ransomware 26

Figura 5‑3 Backup & Disaster Recovery 27

Figura 5‑3 Phishing 28

Figura 5‑3 Planes de concienciación 29

Figura 5‑3 Escáner de vulnerabilidades 30

Figura 5‑3 Backup & Disaster Recovery 31

# INTRODUCCIÓN

En este documento se va a detallar la estructura lógica de la empresa Bionica Automations.

La empresa estará ubicada en el polígono de Plaza Zaragoza, sitio elegido por ser un enclave logístico sin igual.

A continuación, vamos a realizar el diseño de una red informática de la empresa.

La empresa tiene un edificio de 2 plantas donde hay que realizar el diseño de la red para los departamentos que confirman la empresa y dimensionar las redes acordes a las necesidades requeridas:

|  |  |
| --- | --- |
| Departamento | Personal |
| Sistemas | 5 |
| Comercial | 6 |
| Soporte | 8 |
| Contabilidad | 6 |
| Dirección | 4 |
| Recursos Humanos | 4 |
| I+D | 36 |

Tabla 1‑1 Departamentos

## Estructura lógica

La topología de la red es una topología mixta o híbrida.

Existe una VLAN por departamento con su propio direccionamiento y servidor DHCP, el acceso a internet está garantizado gracias a dos Reuters configurados con el protocolo HSRP, también hay redundancia en el primer salto, todas las bocas que no están en uso están deshabilitadas y asignadas a una VLAN donde no hay nada, para maximizar la seguridad.

Los departamentos que lo necesiten tendrán disponibles en su subred los servicios necesarios para desempeñar su trabajo, como las impresoras en cado de los comerciales o contabilidad o también un NAS para los programadores y desarrolladores.

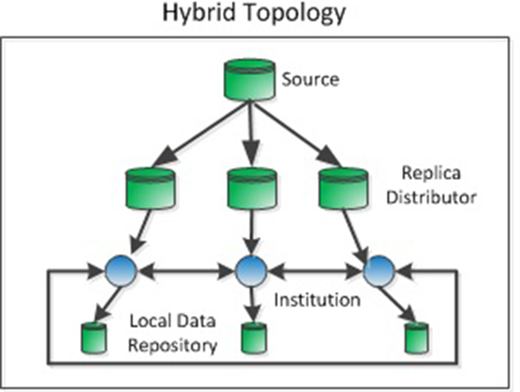


Figura 1‑1 Topología Híbrida

# Estructura física y cableado estructurado

## Tipos de medios de transmisión

Los medios de transmisión escogidos para el proyecto han sido: fibra óptica de 10 Gb para las comunicaciones entre los dispositivos del CPD y el cableado vertical, cable de par trenzado CAT-7 para el cableado horizontal y el aire (WiFi): bandas de 2.4 estándar IEEE 802.11n y 5 GHz IEEE 802.11ac.

## Armarios de distribución o racks y pasacables

Para el CPD hay un rack donde están todos los equipos junto con 2 pasacables laterales que recorren el rack de arriba abajo con 3 paneles de parcheo.

Para la planta baja hay un armario de distribución que contiene un panel de parcheo y un switch para abastecer a la planta.

## Pach-panels

En el siguiente documento está el mapeado de las bocas del panel de parcheo a las respectivas bocas de las rosetas identificadas por “S1, S2, S3” en caso de que pertenezcan a la planta superior o “B1, B2, B3” si son de la planta baja.

## Cableado horizontal

Para el cableado horizontal vamos a utilizar cable de par trenzado CAT-6 con rosetas en cada zona de trabajo numeradas con la nomenclatura.

Todos los cables se pasarán por el suelo o techo técnicos, dependiendo de lo que haya disponible con sus respectivos aislantes para evitar las interferencias, eso supone canaletas especiales dependiendo si los cables pasan al lado de los cables eléctricos.

## Cableado vertical

Para el cableado vertical hemos optado por cables de fibra plástica de 10 Gb de ancho de banda para evitar cuellos de botella en la red y porque es fácil de manejar debido a que no necesitan de canalizaciones especiales como el cable de par trenzado, al no ser impulsos eléctricos le que va a viajar por esos cables, se pueden ubicar justo al lado de los cables eléctricos sin que haya ninguna interferencia, por lo que se pueden aprovechar las canalizaciones ya existentes.

# Estructura lógica

## Diseño de la red

La red está formada por dos routers conectados a un core de dos switches que están conectados entre sí para garantizar la alta disponibilidad, ambos routers están en una configuración de Activo-Pasivo.

Luego tenemos los switches de cada plata conectados con los switches principales por fibra plástica de 10 Gb, con sus respectivos paneles de parcheo de RJ45 de CAT-6 conectado a las rosetas de las plantas, y estas a los dispositivos finales.

Los servidores están conectados a un switch central a través de cables CAT-6 RJ45.

Todas las conexiones con los equipos de trabajo se realizan bajo cable de par trenzado CAT-6 de 1Gb, las rosetas por supuesto son CAT-6 también.

## Protocolo IP empleado

Solo se implementa el protocolo IPv4 ya que como máximo vamos a escalar la red hasta los 255 equipos y no necesitamos más.

IPv6 estará deshabilitado por seguridad.

## Direccionamiento IP y subredes

En la siguiente tabla se lleva a cabo el direccionamiento de las redes de la empresa dividida por departamentos

|  |  |  |  |
| --- | --- | --- | --- |
| VLAN | Name | Network IP | DHCP |
| 10 | WiFi Empleados | 192.168.10.0/24 | 192.168.10. 11 - 50  40 IPs |
| 15 | WiFi Guest | 192.168.15.0/24 | 192.168.15.11-230  240 IPs |
| 20 | Demo\_Area | 192.168.20.0/24 | 192.168.20. 11 - 50  40 IPs |
| 30 | I+D | 192.168.30.0/24 | 192.168.30. 11 - 70  60 IPs |
| 49 | Native-Trunk | N/A | N/A |
| 50 | Systems | 192.168.50.0/24 | 192.168.50.11 - 50  40 IPs |
| 60 | Commercial | 192.168.60.0/24 | 192.168.60.11 - 50  40 IPs |
| 70 | Accounting | 192.168.70.0/24 | 192.168.60.11 - 50  40 IPs |
| 80 | Support | 192.168.80.0/24 | 192.168.70.11 - 50  40 IPs |
| 90 | R-H | 192.168.90.0/24 | 192.168.90.11 - 50  40 IPs |
| 99 | Management | 192.168.99.0/24 | N/A |
| 100 | Direction | 192.168.100.0/24 | 192.168.100.11 - 50  40 IPs |
| 110 | Testing | 192.168.110.0/24 | N/A |
| 120 | Printers | 192.168.120.0/24 | N/A |
| 150 | Internal Services | 192.168.150.0/24 | N/A |
| 200 | DMZ | 192.168.200.0/24 | N/A |
| 555 | Black-Hole | N/A | N/A |

Tabla 3‑1 Direccionamiento

# Administración de servidores

## Sistemas operativos y software

### Servidores

Como software de virtualización se usará VMware vSphere Hypervisor (ESXi) junto con VMware vCenter.

Se dispondrá de un Windows Server 2022 standard como controlador de dominio con redundancia en Azure.

### Estaciones de trabajo

Los ordenadores de los trabajadores llevan Windows 10 Pro y se administrarán con el controlador de dominio además de Pulseway.

## Servicios en red

### DNS

### DHCP

### VPN

Los servicios presentes son los siguientes: DNS, DHCP, SMB para los trabajadores que tengan que almacenar sus datos de trabajo, además de las copias de seguridad, una VPN y RDP por si los trabajadores tienen que trabajar desde casa, Active Directory para la gestión de los usuarios, para las actualizaciones de Windows WSUS y para la autentificación de los empleados en las redes corporativas RADIUS.

## Sistemas de seguridad

Para evitar los inicios de sesión no autorizado contaremos con una autentificación en 2 factores.

Los usuarios deberán cambiar la contraseña cada 2 meses

Se activarán las horas activas para que no se pueda iniciar sesión cuando estas fuera del horario establecido.

Los discos duros de los ordenadores de trabajo estarán cifrados.

Los trabajadores no pueden modificar ningún parámetro de los sistemas de seguridad tales como antivirus, firewall.

Se van a grabar las acciones de un usuario o un grupo en el registro de eventos.

# Ciberseguridad

## Inventario de Activos

El software que va a emplear Bionica Automations para mantener un seguimiento de los equipos informáticos de la empresa va a ser [Pulseway](https://www.pulseway.com).

Pulseway es una herramienta no solo ofrece la posibilidad de hacer un inventario de inventariado, sino que también monitoriza, automatiza, protege y gestiona los activos de la empresa.

Esta herramienta es de pago, se pueden consultar sus precios por dispositivo en su [calculadora online.](https://www.pulseway.com/pricing)

Entre las características que incluye este software están las siguientes:

* [Administración de dispositivos](https://www.pulseway.com/it-management-software)
* [Backup & Disaster Recovery](https://www.pulseway.com/backup-software)
* [Protección contra Ransomware](https://www.pulseway.com/ransomware-protection-software)

Para más información consultar el **ANEXO 4 Pulseway**

## Firewall

Las conexiones de fuera hacia dentro están bloqueadas y las conexiones salientes permitidas.

Si permitimos que los trabajadores trabajen desde casa se dispondrá de una VPN a los recursos de la empresa.

## DNS

## DHCP

## VPN

## IPS

## XDR

## Switches

Los switches tendrán un faltado por Mac que va por puerto, si conectas un ordenador con distinta Mac que el que había antes, el puerto de deshabilitará.

## Copias de seguridad

El software de copias de seguridad que vamos a utilizar es Easeus la edición Advanced Server.

### Análisis

Los datos más importantes que podemos tener son los siguientes:

* Sistema operativo de Windows Server de Active Directory (aunque sea una VM, la copia se hará aparte).
* El resto de los servicios que están en otras máquinas virtuales asociadas a los proyectos.

La información de los proyectos puede cambiar seriamente cada hora, los datos de contabilidad cada día, los datos de los clientes cada media hora, el sistema operativo de Windows server de Active Directory cada 1 semanas, el resto de las máquinas virtuales cada 1 semanas también.

Los datos de los proyectos se almacenarán durante 6 meses, los de contabilidad durante 3 años, los datos de los clientes durante 1 año, el S.O. del Windows Server de Active Diectory se almacenará durante 4 meses, el resto de los servicios de otras máquinas virtuales de proyectos se almacenarán durante otros 6 meses.

### Diseño

En el siguiente esquema relacionado con el horario en el que se van a ejecutar las copias de seguridad y su ubicación, no están incluidas las copias de los datos de los clientes (Base de datos de clientes), ya que esto hay que hablarlo con la empresa que contratemos para dichos servicios para acordar un plan de copias de seguridad.

## Normativa Puestos de trabajo

Consultar el Anexo 3 documento:

UBALDE\_Plan\_de\_Ciberseguridad\_en\_puestos\_de\_trabajo

1. Diagrama Packet tracer

El esquema está en formato Packet Tracert [Diagrama Packet Tracer](Anexos/Anexo%201%20-%20Diagrama%20Packet%20Tracer)

Imagen que contiene interior, edificio, computadora, montón

Descripción generada automáticamente

Figura 5‑1 Diagrama Físico planta superior

Diagrama, Dibujo de ingeniería

Descripción generada automáticamente

Figura 5‑2 Diagrama Físico planta inferior

1. Conexionado Físico

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Device | **Port** | **VLAN** | **Use** | **Conected Device** | **Target Port** | **Patch Panel** | **Patch Panel Port** |
| R\_Movistar | g0/0/0 | N/A | WAN 1 | N/A | N/A | N/A | N/A |
| R\_Movistar | g0/0/1 | N/A | N/A | N/A | N/A | N/A | N/A |
| R\_Movistar | g0/0/2 | N/A | N/A | N/A | N/A | N/A | N/A |
| R\_Movistar | g0/1/0 | Trunk 49 | Internet | SW\_C1 | g1/1/4 | N/A | N/A |
| R\_Movistar | g0/1/1 | N/A | N/A | N/A | N/A | N/A | N/A |
| R\_Movistar | g0/1/2 | N/A | N/A | N/A | N/A | N/A | N/A |
| R\_Movistar | g0/1/3 | N/A | N/A | N/A | N/A | N/A | N/A |
| R\_Vodafone | g0/0/0 | N/A | WAN 2 | N/A | N/A | N/A | N/A |
| R\_Vodafone | g0/0/1 | N/A | N/A | N/A | N/A | N/A | N/A |
| R\_Vodafone | g0/0/2 | N/A | N/A | N/A | N/A | N/A | N/A |
| R\_Vodafone | g0/1/0 | Trunk 49 | Internet | SW\_C2 | g1/1/4 | N/A | N/A |
| R\_Vodafone | g0/1/1 | N/A | N/A | N/A | N/A | N/A | N/A |
| R\_Vodafone | g0/1/2 | N/A | N/A | N/A | N/A | N/A | N/A |
| R\_Vodafone | g0/1/3 | N/A | N/A | N/A | N/A | N/A | N/A |
| SW\_C1 | g1/0/1 | Trunk | Connunication | SW\_P1-1 | g1/1/1 | N/A | N/A |
| SW\_C1 | g1/0/2 | Trunk | Connunication | SW\_P1-2 | g1/1/1 | N/A | N/A |
| SW\_C1 | g1/0/3 | Trunk | Connunication | SW\_P1-3 | g1/1/1 | N/A | N/A |
| SW\_C1 | g1/0/4 | Trunk | Connunication | SW\_P0-1 | g1/1/1 | N/A | N/A |
| SW\_C1 | g1/0/5 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C1 | g1/0/6 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C1 | g1/0/7 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C1 | g1/0/8 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C1 | g1/0/9 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C1 | g1/0/10 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C1 | g1/0/11 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C1 | g1/0/12 | 99 | MGM ESXi | ESXi\_1 | g0 | N/A | N/A |
| SW\_C1 | g1/0/13 | 150 | Internal Services | ESXi\_1 | g1 | N/A | N/A |
| SW\_C1 | g1/0/14 | 150 | Servers | NAS | g0 | N/A | N/A |
| SW\_C1 | g1/0/15 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C1 | g1/0/16 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C1 | g1/0/17 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C1 | g1/0/18 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C1 | g1/0/19 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C1 | g1/0/20 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C1 | g1/0/21 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C1 | g1/0/22 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C1 | g1/0/23 | Trunk | Communication | SW\_C2 | g1/0/23 | N/A | N/A |
| SW\_C1 | g1/0/24 | Trunk | Communication | SW\_C2 | g1/0/24 | N/A | N/A |
| SW\_C1 | g1/1/1 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C1 | g1/1/2 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C1 | g1/1/3 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C1 | g1/1/4 | Trunk | Connunication | Router\_Movistar | g0/0/1 | N/A | N/A |
| SW\_C2 | g1/0/1 | Trunk | Connunication | SW\_P1-1 | g1/1/2 | N/A | N/A |
| SW\_C2 | g1/0/2 | Trunk | Connunication | SW\_P1-2 | g1/1/2 | N/A | N/A |
| SW\_C2 | g1/0/3 | Trunk | Connunication | SW\_P1-3 | g1/1/2 | N/A | N/A |
| SW\_C2 | g1/0/4 | Trunk | Connunication | SW\_P0-1 | g1/1/2 | N/A | N/A |
| SW\_C2 | g1/0/5 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/0/6 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/0/7 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/0/8 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/0/9 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/0/10 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/0/11 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/0/12 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/0/13 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/0/14 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/0/15 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/0/16 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/0/17 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/0/18 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/0/19 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/0/20 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/0/21 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/0/22 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/0/23 | Trunk | Communication | SW\_C1 | g1/0/23 | N/A | N/A |
| SW\_C2 | g1/0/24 | Trunk | Communication | SW\_C1 | g1/0/24 | N/A | N/A |
| SW\_C2 | g1/1/1 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/1/2 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/1/3 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_C2 | g1/1/4 | Trunk | Communication | Router\_Vodafone | g0/0/1 | N/A | N/A |
| SW\_P1-1 | g1/0/1 | 30 | Developers | Roseta\_S9 | 0 | Patch\_Panel\_S1 | 1 |
| SW\_P1-1 | g1/0/2 | 30 | Developers | Roseta\_S9 | 1 | Patch\_Panel\_S1 | 2 |
| SW\_P1-1 | g1/0/3 | 30 | Developers | Roseta\_S9 | 2 | Patch\_Panel\_S1 | 3 |
| SW\_P1-1 | g1/0/4 | 30 | Developers | Roseta\_S9 | 3 | Patch\_Panel\_S1 | 4 |
| SW\_P1-1 | g1/0/5 | 30 | Developers | Roseta\_S10 | 0 | Patch\_Panel\_S1 | 5 |
| SW\_P1-1 | g1/0/6 | 30 | Developers | Roseta\_S10 | 1 | Patch\_Panel\_S1 | 6 |
| SW\_P1-1 | g1/0/7 | 30 | Developers | Roseta\_S10 | 0 | Patch\_Panel\_S1 | 7 |
| SW\_P1-1 | g1/0/8 | 30 | Developers | Roseta\_S11 | 0 | Patch\_Panel\_S1 | 8 |
| SW\_P1-1 | g1/0/9 | 30 | Developers | Roseta\_S11 | 0 | Patch\_Panel\_S1 | 9 |
| SW\_P1-1 | g1/0/10 | 30 | Developers | Roseta\_S11 | 0 | Patch\_Panel\_S1 | 10 |
| SW\_P1-1 | g1/0/11 | 30 | Developers | Roseta\_S12 | 0 | Patch\_Panel\_S1 | 11 |
| SW\_P1-1 | g1/0/12 | 30 | Developers | Roseta\_S12 | 1 | Patch\_Panel\_S1 | 12 |
| SW\_P1-1 | g1/0/13 | 30 | Developers | Roseta\_S12 | 2 | Patch\_Panel\_S1 | 13 |
| SW\_P1-1 | g1/0/14 | 30 | Developers | Roseta\_S12 | 3 | Patch\_Panel\_S1 | 14 |
| SW\_P1-1 | g1/0/15 | 30 | Developers | Roseta\_S13 | 0 | Patch\_Panel\_S1 | 15 |
| SW\_P1-1 | g1/0/16 | 30 | Developers | Roseta\_S13 | 1 | Patch\_Panel\_S1 | 16 |
| SW\_P1-1 | g1/0/17 | 30 | Developers | Roseta\_S13 | 2 | Patch\_Panel\_S1 | 17 |
| SW\_P1-1 | g1/0/18 | 30 | Developers | Roseta\_S13 | 3 | Patch\_Panel\_S1 | 18 |
| SW\_P1-1 | g1/0/19 |  | Phones | Roseta\_S14 | 0 | Patch\_Panel\_S1 | 19 |
| SW\_P1-1 | g1/0/20 |  | Phones | Roseta\_S14 | 1 | Patch\_Panel\_S1 | 20 |
| SW\_P1-1 | g1/0/21 | N/A | Not Used | N/A | N/A | N/A | N/A |
| SW\_P1-1 | g1/0/22 | N/A | Not Used | N/A | N/A | N/A | N/A |
| SW\_P1-1 | g1/0/23 | N/A | Not Used | N/A | N/A | N/A | N/A |
| SW\_P1-1 | g1/0/24 | N/A | Not Used | N/A | N/A | N/A | N/A |
| SW\_P1-1 | g1/1/1 | Trunk | Communication | SW\_C1 | g1/0/1 | N/A | N/A |
| SW\_P1-1 | g1/1/2 | Trunk | Communication | SW\_C2 | g1/0/1 | N/A | N/A |
| SW\_P1-1 | g1/1/3 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P1-1 | g1/1/4 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P1-2 | g1/0/1 | 50 | Systems-Admin | Roseta\_S0 | 0 | Patch\_Panel\_S2 | 1 |
| SW\_P1-2 | g1/0/2 | 50 | Systems-Admin | Roseta\_S0 | 1 | Patch\_Panel\_S2 | 2 |
| SW\_P1-2 | g1/0/3 | 50 | Systems-Admin | Roseta\_S0 | 2 | Patch\_Panel\_S2 | 3 |
| SW\_P1-2 | g1/0/4 | 50 | Systems-Admin | Roseta\_S0 | 3 | Patch\_Panel\_S2 | 4 |
| SW\_P1-2 | g1/0/5 | 50 | Systems-Admin | Roseta\_S1 | 0 | Patch\_Panel\_S2 | 5 |
| SW\_P1-2 | g1/0/6 | 555 | Not Used | Roseta\_S1 | 1 | Patch\_Panel\_S2 | 6 |
| SW\_P1-2 | g1/0/7 | 110 | Testing | Roseta\_S2 | 0 | Patch\_Panel\_S2 | 7 |
| SW\_P1-2 | g1/0/8 | 110 | Testing | Roseta\_S3 | 0 | Patch\_Panel\_S2 | 8 |
| SW\_P1-2 | g1/0/9 | 110 | Testing | Roseta\_S4 | 0 | Patch\_Panel\_S2 | 9 |
| SW\_P1-2 | g1/0/10 | 90 | R-H | Roseta\_S5 | 0 | Patch\_Panel\_S2 | 10 |
| SW\_P1-2 | g1/0/11 | 80 | Call-Center | Roseta\_S6 | 0 | Patch\_Panel\_S2 | 11 |
| SW\_P1-2 | g1/0/12 | 80 | Call-Center | Roseta\_S6 | 1 | Patch\_Panel\_S2 | 12 |
| SW\_P1-2 | g1/0/13 | 80 | Call-Center | Roseta\_S6 | 2 | Patch\_Panel\_S2 | 13 |
| SW\_P1-2 | g1/0/14 | 80 | Call-Center | Roseta\_S6 | 3 | Patch\_Panel\_S2 | 14 |
| SW\_P1-2 | g1/0/15 | 80 | Call-Center | Roseta\_S7 | 0 | Patch\_Panel\_S2 | 15 |
| SW\_P1-2 | g1/0/16 | 80 | Call-Center | Roseta\_S7 | 1 | Patch\_Panel\_S2 | 16 |
| SW\_P1-2 | g1/0/17 | 80 | Call-Center | Roseta\_S7 | 2 | Patch\_Panel\_S2 | 17 |
| SW\_P1-2 | g1/0/18 | 80 | Call-Center | Roseta\_S7 | 3 | Patch\_Panel\_S2 | 18 |
| SW\_P1-2 | g1/0/19 | 70 | Accounting | Roseta\_S8 | 0 | Patch\_Panel\_S2 | 19 |
| SW\_P1-2 | g1/0/20 | 70 | Accounting | Roseta\_S8 | 1 | Patch\_Panel\_S2 | 20 |
| SW\_P1-2 | g1/0/21 | 70 | Accounting | Roseta\_S8 | 2 | Patch\_Panel\_S2 | 21 |
| SW\_P1-2 | g1/0/22 | 70 | Accounting | Roseta\_S8 | 3 | Patch\_Panel\_S2 | 22 |
| SW\_P1-2 | g1/0/23 | 70 | Accounting | Roseta\_S20 | 0 | Patch\_Panel\_S2 | 23 |
| SW\_P1-2 | g1/0/24 | 70 | Accounting | Roseta\_S20 | 1 | Patch\_Panel\_S2 | 24 |
| SW\_P1-2 | g1/1/1 | Trunk | Connunication | SW\_C1 | g1/0/2 | N/A | N/A |
| SW\_P1-2 | g1/1/2 | Trunk | Communication | SW\_C2 | g1/0/2 | N/A | N/A |
| SW\_P1-2 | g1/1/3 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P1-2 | g1/1/4 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P1-3 | g1/0/1 | 40 | Programers | Roseta\_S15 | 0 | Patch\_Panel\_S3 | 1 |
| SW\_P1-3 | g1/0/2 | 40 | Programers | Roseta\_S15 | 1 | Patch\_Panel\_S3 | 2 |
| SW\_P1-3 | g1/0/3 | 40 | Programers | Roseta\_S15 | 2 | Patch\_Panel\_S3 | 3 |
| SW\_P1-3 | g1/0/4 | 40 | Programers | Roseta\_S15 | 3 | Patch\_Panel\_S3 | 4 |
| SW\_P1-3 | g1/0/5 | 40 | Programers | Roseta\_S16 | 0 | Patch\_Panel\_S3 | 5 |
| SW\_P1-3 | g1/0/6 | 40 | Programers | Roseta\_S16 | 1 | Patch\_Panel\_S3 | 6 |
| SW\_P1-3 | g1/0/7 | 40 | Programers | Roseta\_S16 | 2 | Patch\_Panel\_S3 | 7 |
| SW\_P1-3 | g1/0/8 | 40 | Programers | Roseta\_S16 | 3 | Patch\_Panel\_S3 | 8 |
| SW\_P1-3 | g1/0/9 | 40 | Programers | Roseta\_S17 | 0 | Patch\_Panel\_S3 | 9 |
| SW\_P1-3 | g1/0/10 | 40 | Programers | Roseta\_S17 | 1 | Patch\_Panel\_S3 | 10 |
| SW\_P1-3 | g1/0/11 | 40 | Programers | Roseta\_S17 | 2 | Patch\_Panel\_S3 | 11 |
| SW\_P1-3 | g1/0/12 | 40 | Programers | Roseta\_S18 | 0 | Patch\_Panel\_S3 | 12 |
| SW\_P1-3 | g1/0/13 | 40 | Programers | Roseta\_S18 | 1 | Patch\_Panel\_S3 | 13 |
| SW\_P1-3 | g1/0/14 | 40 | Programers | Roseta\_S18 | 2 | Patch\_Panel\_S3 | 14 |
| SW\_P1-3 | g1/0/15 | 40 | Programers | Roseta\_S19 | 0 | Patch\_Panel\_S3 | 15 |
| SW\_P1-3 | g1/0/16 | 40 | Programers | Roseta\_S19 | 1 | Patch\_Panel\_S3 | 16 |
| SW\_P1-3 | g1/0/17 | 40 | Programers | Roseta\_S19 | 2 | Patch\_Panel\_S3 | 17 |
| SW\_P1-3 | g1/0/18 | 40 | Programers | Roseta\_S19 | 3 | Patch\_Panel\_S3 | 18 |
| SW\_P1-3 | g1/0/19 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P1-3 | g1/0/20 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P1-3 | g1/0/21 | 120 | Printers | Roseta\_S21 | 0 | Patch\_Panel\_S3 | 21 |
| SW\_P1-3 | g1/0/22 | 120 | Printers | Roseta\_S21 | 1 | Patch\_Panel\_S3 | 22 |
| SW\_P1-3 | g1/0/23 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P1-3 | g1/0/24 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P1-3 | g1/1/1 | Trunk | Communication | SW\_C1 | g1/0/3 | N/A | N/A |
| SW\_P1-3 | g1/1/2 | Trunk | Communication | SW\_C2 | g1/0/3 | N/A | N/A |
| SW\_P1-3 | g1/1/3 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P1-3 | g1/1/4 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P0-1 | g1/0/1 | 130 | Recepcion | Roseta\_B0 | 0 | Patch\_Panel\_B1 | 1 |
| SW\_P0-1 | g1/0/2 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P0-1 | g1/0/3 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P0-1 | g1/0/4 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P0-1 | g1/0/5 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P0-1 | g1/0/6 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P0-1 | g1/0/7 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P0-1 | g1/0/8 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P0-1 | g1/0/9 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P0-1 | g1/0/10 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P0-1 | g1/0/11 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P0-1 | g1/0/12 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P0-1 | g1/0/13 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P0-1 | g1/0/14 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P0-1 | g1/0/15 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P0-1 | g1/0/16 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P0-1 | g1/0/17 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P0-1 | g1/0/18 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P0-1 | g1/0/19 | 10 | WiFi\_Empleados | Access\_Points | g0 | N/A | N/A |
| SW\_P0-1 | g1/0/20 | 10 | WiFi\_Empleados | Access\_Points | g0 | N/A | N/A |
| SW\_P0-1 | g1/0/21 | 10 | WiFi\_Empleados | Access\_Points | g0 | N/A | N/A |
| SW\_P0-1 | g1/0/22 | 10 | WiFi\_Empleados | Access\_Points | g0 | N/A | N/A |
| SW\_P0-1 | g1/0/23 | 10 | WiFi\_Empleados | Access\_Points | g0 | N/A | N/A |
| SW\_P0-1 | g1/0/24 | 10 | WiFi\_Empleados | Access\_Points | g0 | N/A | N/A |
| SW\_P0-1 | g1/1/1 | Trunk | Communication | SW\_C1 | g1/0/4 | N/A | N/A |
| SW\_P0-1 | g1/1/2 | Trunk | Communication | SW\_C2 | g1/0/4 | N/A | N/A |
| SW\_P0-1 | g1/1/3 | 555 | Not Used | N/A | N/A | N/A | N/A |
| SW\_P0-1 | g1/1/4 | 555 | Not Used | N/A | N/A | N/A | N/A |

Tabla 5‑1 Conexionado Físico

1. Plan de ciberseguridad Puestos de trabajo

[Ciberseguridad](Anexos/Anexo%203%20-%20Ciberseguridad)

1. Pulseway

Administración de dispositivos

Dentro de este apartado se engloba todas las funcionalidades que tienen que ver con la administración IT de activos:

* + 1. DESCUBRIMIENTO Y DESPLIEGUE

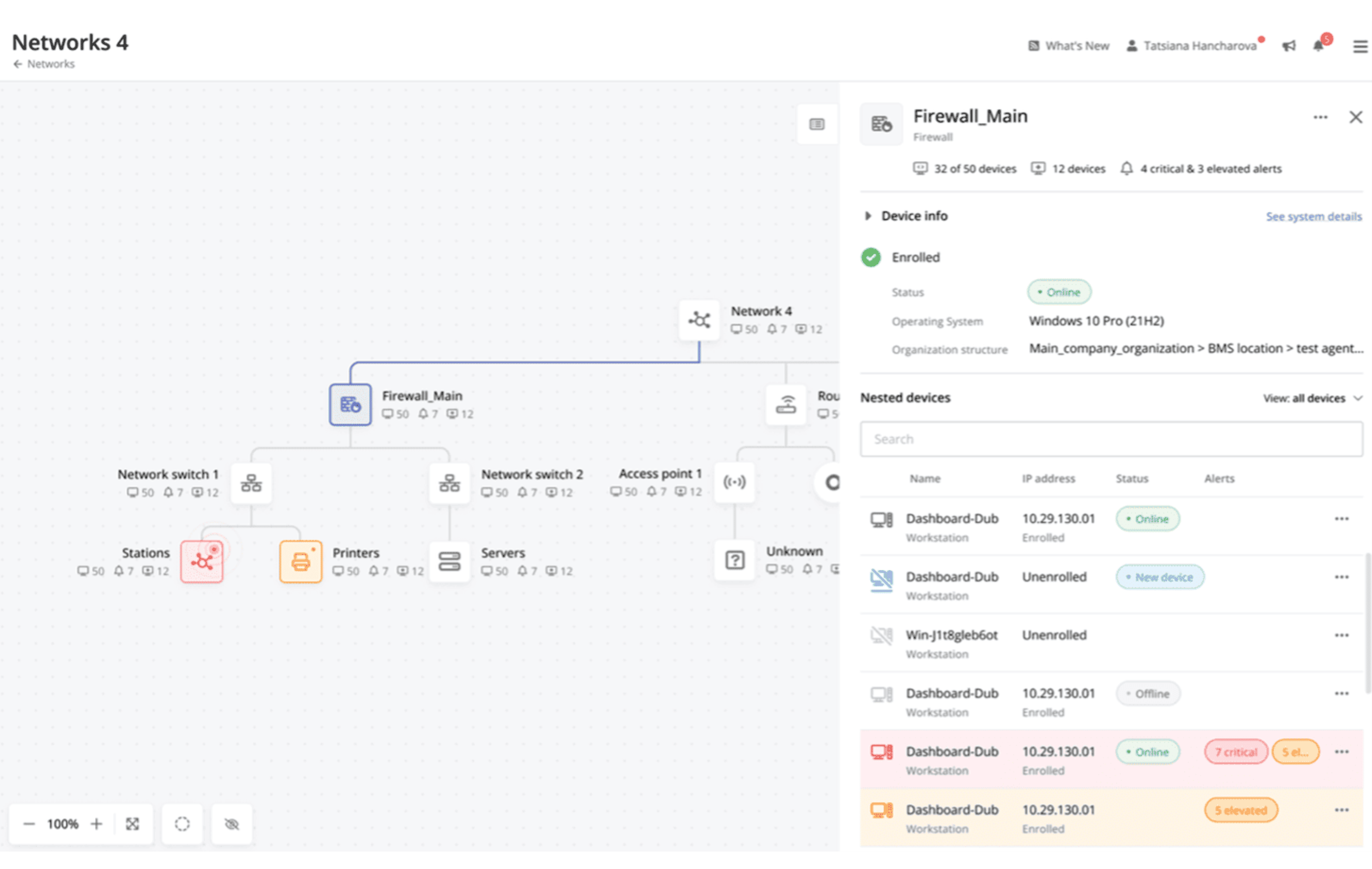


Figura 5‑3 Pulseway endpoint discovery

En minutos, verá rápidamente todos los endpoints se muestran en la herramienta. A continuación, puede implementar fácilmente Pulseway en masa con políticas preconfiguradas integradas. Comience rápidamente a dar soporte a sus clientes sin la necesidad de una incorporación o capacitación costosa y que consume mucho tiempo.

* + 1. Monitorización y administración

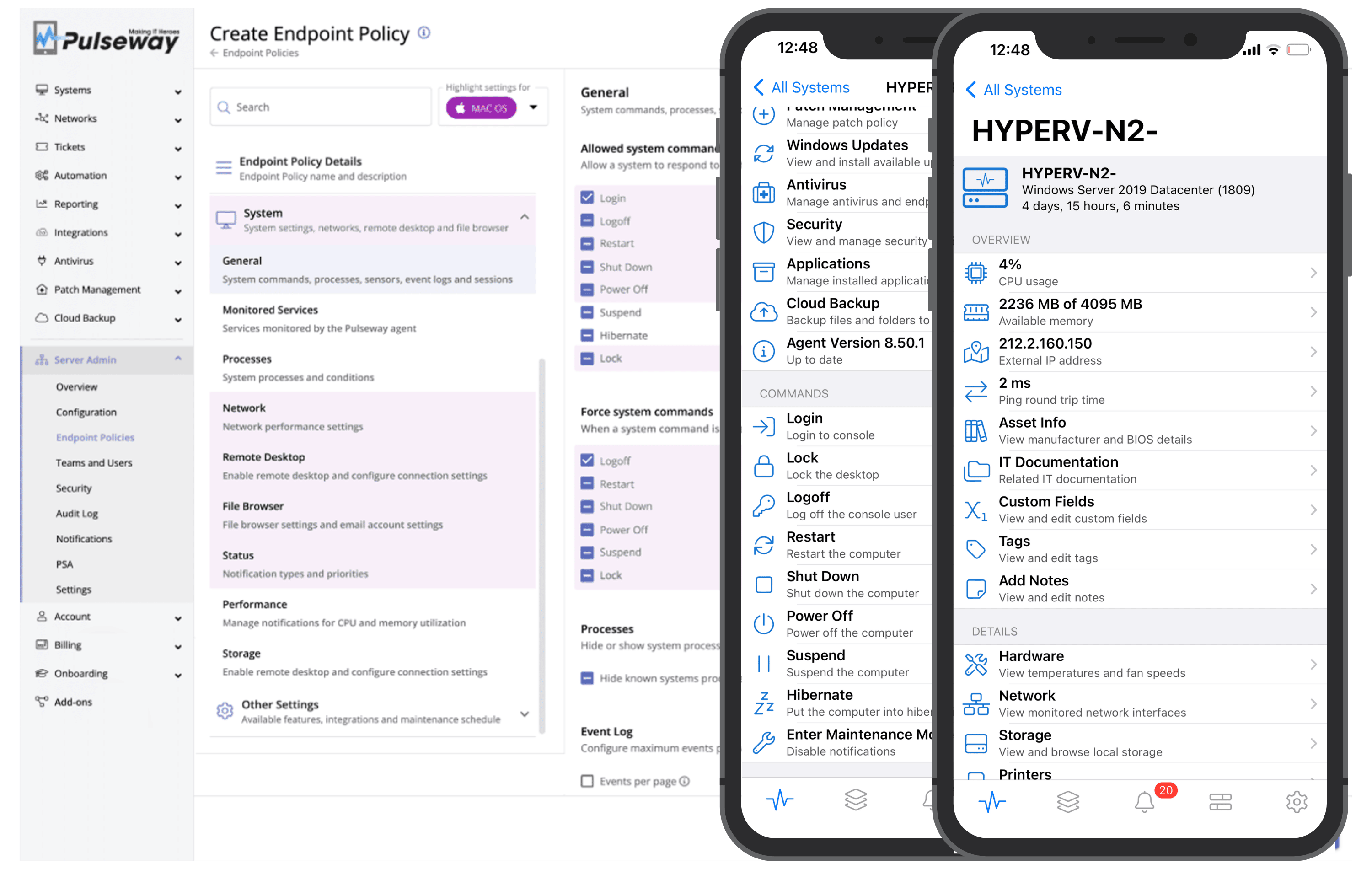


Figura 5‑4 Monitorización y Administración

La interfaz intuitiva de Pulseway significa que cualquier técnico puede ser productivo instantáneamente con información detallada, procesable y en tiempo real en servidores, estaciones de trabajo y dispositivos de red. Combinado con alertas personalizables, puede identificar rápidamente problemas, comunicarse con los clientes y resolver problemas con comandos y scripts integrados, incluso desde su dispositivo móvil.

Desea ofrecer el mismo nivel de servicio a todos sus clientes y con la aplicación de administración de TI móvil más rica en funciones de la industria, puede hacerlo. Su equipo ahora puede hacer su trabajo desde cualquier lugar para que puedan responder rápidamente a cualquier problema, de cualquier cliente, directamente desde sus teléfonos inteligentes.

* + 1. Automatización y auto remediación



Figura 5‑5 Automatizaciones

Haga más haciendo menos, con el potente motor de automatización de Pulseway. Al combinar la tecnología de flujo de trabajo con una interfaz de usuario intuitiva, puede configurar activadores inteligentes para solucionar automáticamente los problemas de TI de inmediato antes de que tengan la oportunidad de convertirse en un problema, lo que le ayuda a cumplir o superar sus SLA. Puede ahorrar aún más el valioso tiempo de su equipo automatizando tareas repetitivas y cotidianas utilizando nuestra amplia biblioteca de scripts integrados, plantillas y automatización específica de funciones, liberándolos para centrarse en actividades de mayor valor.

* + 1. Administración de parches de seguridad

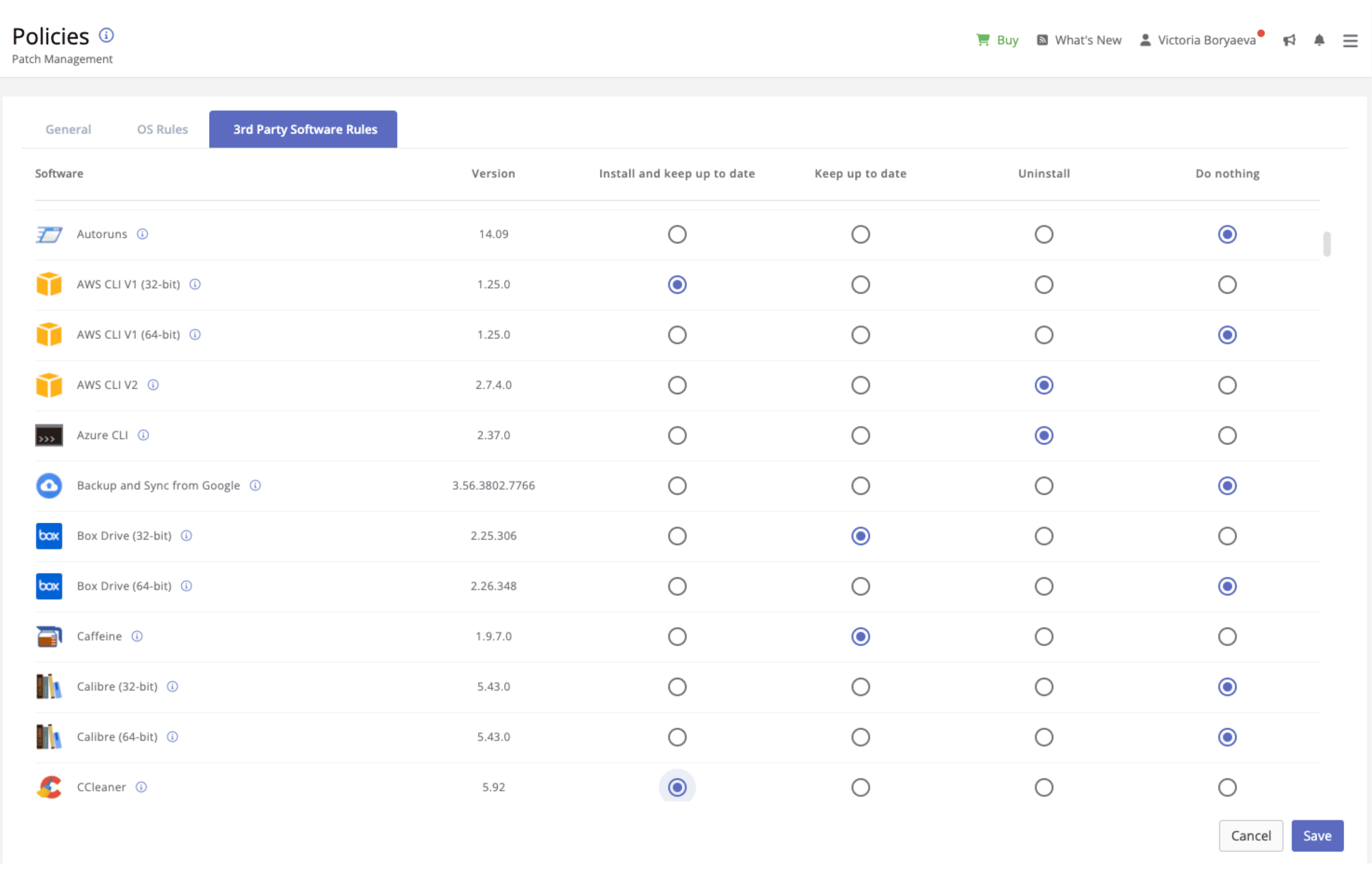


Figura 5‑6 Parches de Seguridad

La administración de parches puede ser una pérdida de tiempo y recursos a medida que intenta mantenerse al tanto de la aplicación de parches en todos sus clientes, especialmente cuando intenta garantizar que se prioricen los críticos. El potente software de administración de parches de Pulseway automatiza el descubrimiento y la aplicación de parches de aplicaciones de terceros y sistemas operativos. Las políticas de parches integrales le permiten definir el qué, dónde y cuándo de la aplicación de parches por adelantado. Más de 220 aplicaciones de terceros de uso común son compatibles de fábrica, pero puede agregar fácilmente aplicaciones especializadas con nuestra función de aplicaciones personalizadas para garantizar que todas sus aplicaciones se mantengan actualizadas.

* + 1. Detección de Ransomware y AV integrado

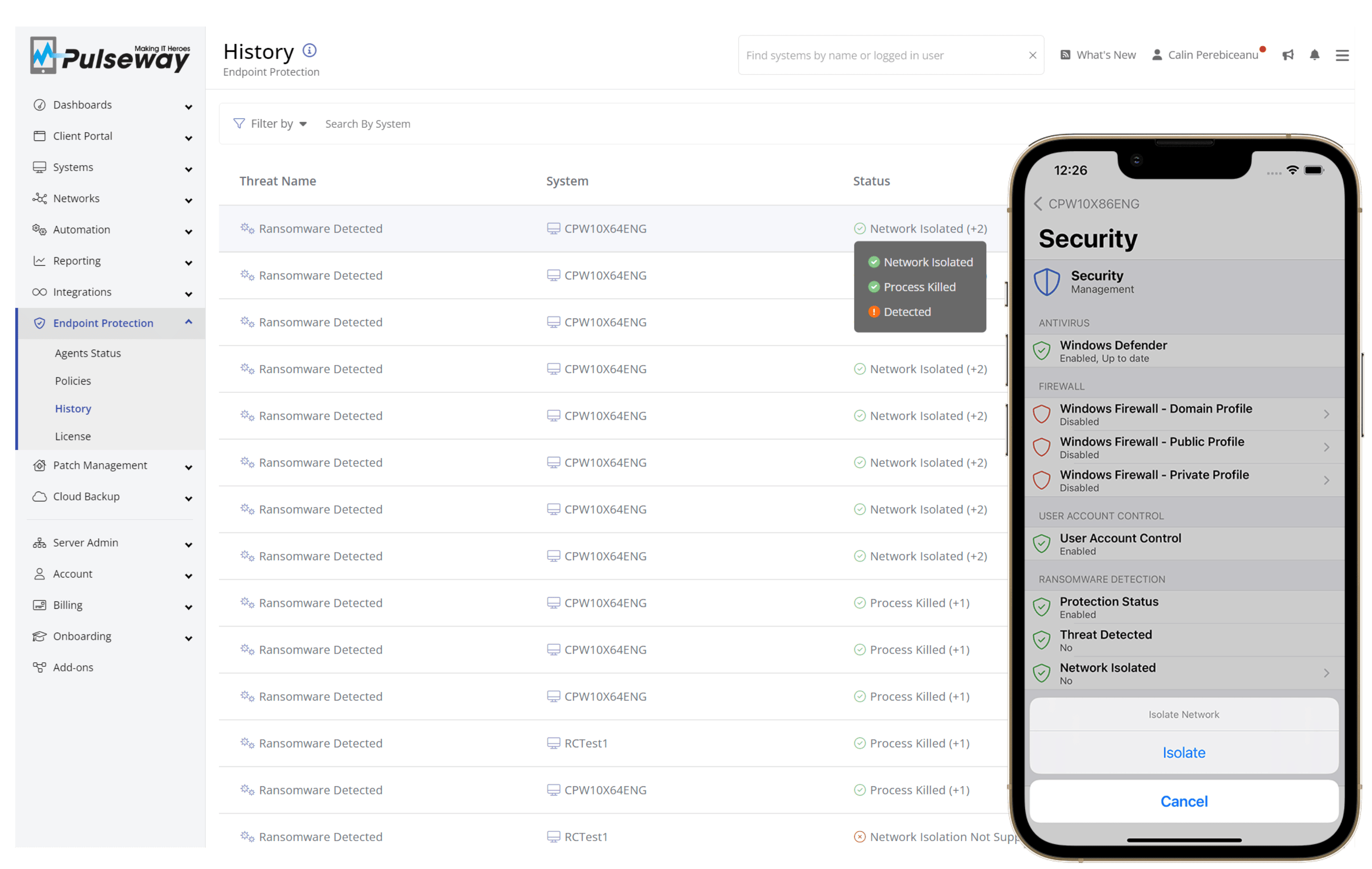


Figura 5‑7 Detección de Ransomware

Supervise, detecte, detenga y elimine de forma proactiva la actividad de ransomware en dispositivos Windows administrados con Pulseway Ransomware Detection integrado de forma nativa en los agentes de Pulseway. Además, la solución AV integrada de Pulseway le permite administrar Bitdefender o Webroot directamente desde la consola RMM. Además de simplificar la implementación, también habilitamos la inscripción automática para que cualquier dispositivo nuevo agregado a la red se inscriba automáticamente en el AV.

* 1. Backup & Disaster Recovery

El sistema de copias de seguridad que posee Pulseway esta desarrollada por Unitrends y es capaz de hacer copias de seguridad de entornos SaaS como Microsoft 365, Google Workspace o Salesforce.

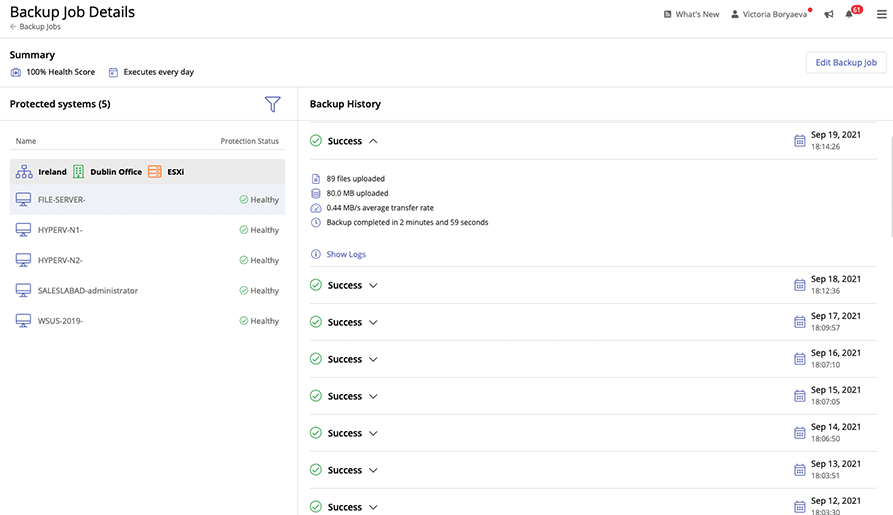


Figura 5‑8 Backup & Disaster Recovery

Muchos usuarios de estas plataformas no se dan cuenta de que no están protegidos contra la pérdida de datos causada por una acción accidental o maliciosa del usuario, y necesitan hacer sus propios arreglos de copia de seguridad.

* 1. Protección contra Ransomware

Pulseway posee características esenciales para detectar, prevenir y remediar cualquier incidente de Ransomware.

Además, incluye planes de concienciación para los empleados de la compañía para evitar el Phishing, además de incluir una protección ante este tipo de ataques.

* + 1. Protección contra Phishing

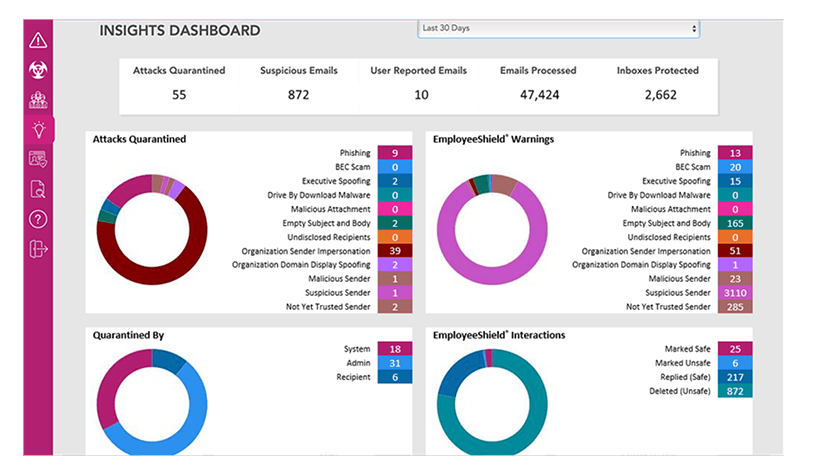


Figura 5‑9 Phishing

**El 91% de todos los ataques cibernéticos comienzan a partir de correos electrónicos de phishing** Pulseway combate eso con una solución basada en la nube que detecta y bloquea el 99.9% de los ataques sofisticados de correo electrónico antes de que lleguen a las bandejas de entrada de los empleados.

* Analizar las relaciones comerciales de sus empleados (con quién trabajan, con qué frecuencia se comunican, etc.) para crear perfiles de confianza.
* Analizar en busca de irregularidades sospechosas en el contenido y los archivos adjuntos de los mensajes y compararlos con perfiles de confianza para detectar ataques.
* Aprender de la interacción y los comentarios del usuario para crecer de manera más inteligente y defenderlo mejor de las nuevas amenazas emergentes.
  + 1. Planes de concienciación

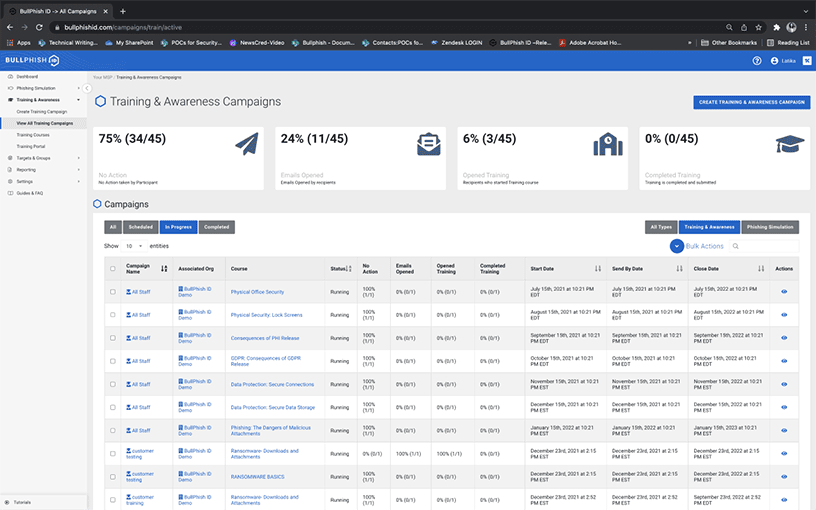


Figura 5‑10 Planes de concienciación

**El 90% de las violaciones de datos comienzan con un correo electrónico de phishing.** Reduzca las posibilidades de su organización de experimentar un desastre de ciberseguridad hasta en un 70% con capacitación en concientización sobre seguridad que incluye simulación de phishing.

* Agregue a todos los empleados a su equipo de seguridad con capacitación en concientización sobre seguridad que les permite detectar y detener las amenazas de phishing.
* Automatice las campañas de capacitación y los informes para obtener una capacitación consistente y sin estrés que obtenga resultados.
* Elija entre un amplio conjunto de kits de campaña anti-phishing plug-and-play.
  + 1. Escáner de vulnerabilidades

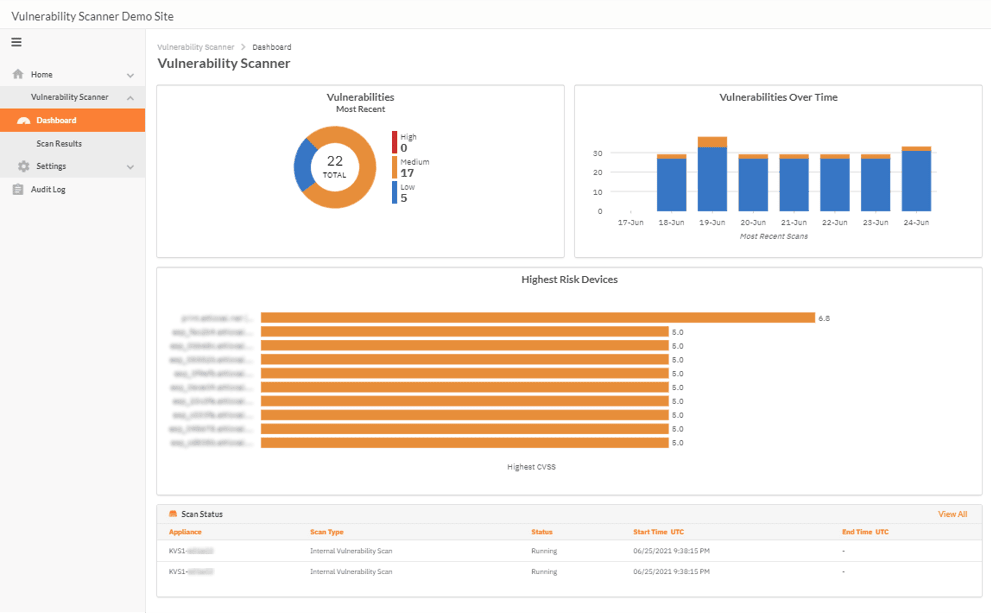


Figura 5‑11 Escáner de vulnerabilidades

El escáner de vulnerabilidades de Pulseway es un escáner de vulnerabilidades **automatizado y asequible que le alerta sobre vulnerabilidades en tiempo real.** Ofrece escaneo de vulnerabilidades internas y externas. Es fácil de usar y significa que cualquier organización ahora puede realizar fácilmente los escaneos de vulnerabilidad regulares que se consideran las mejores prácticas internacionales.

* + 1. Backup and Disaster Recovery

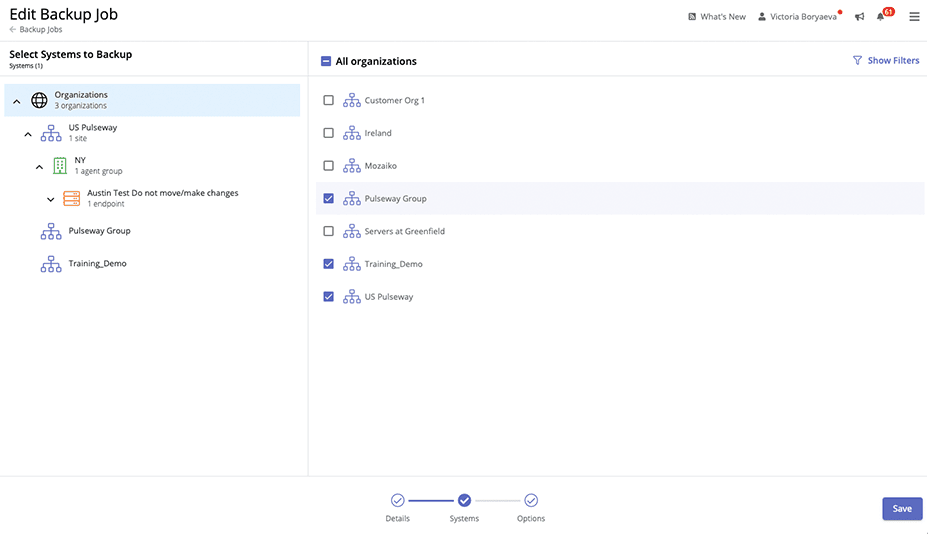


Figura 5‑12 Backup & Disaster Recovery

**Elimine la pérdida de datos y el tiempo de inactividad del ransomware** con detección integrada, protecciones de inmutabilidad y automatización que permite una recuperación rápida después de un ataque. Los datos viven en más lugares que nunca y están bajo ataque constante. Las copias de seguridad se encuentran entre las defensas más importantes contra el ransomware. Ahora es el momento de construir su plan de recuperación de ransomware para lograr la resiliencia cibernética.

# GLOSARIO

* ABREVIATURAS Y ACRÓNIMOS

| **Referencia** | **Descripción** |
| --- | --- |
|  |  |
|  |  |
|  |  |

* DEFINICIONES

| Referencia | Definición |
| --- | --- |
| VLAN | Red virtual |
| Active Directory | Para gestionar usuarios en entornos empresariales |
| CPD | Armario centrar para los dispositivos de red (Rack) |
| DHCP | Servicio para proveer de configuración de red a los dispositivos |
| HSRP | [Hot Standby Routing Protocol](https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/system-interface/ios-xe-17/systems-interfaces-book-xe-sdwan/m-hot-standby-router-protocol.html) |
| DNS | Servidor de nombres de dominio |
| IPS (Intrusion Prevention System) | Es una aplicación usada para detectar accesos no autorizados a un ordenador o a una red. |
| EDR (Endpoint Detection and Response) | Identificar comportamientos sospechosos y amenazas persistentes avanzadas en puntos finales en un entorno |

# CONTROL DE CAMBIOS

| **Edición** | **Fecha** | **Descripción** | **Colaboradores** | |
| --- | --- | --- | --- | --- |
| **Elaborado** | **Revisado** |
| 01.00 | 2023-03-09 | Primera edición | D. Ubalde |  |