

# La persistencia del RANSOMWARE

Horatiu BANDOIU

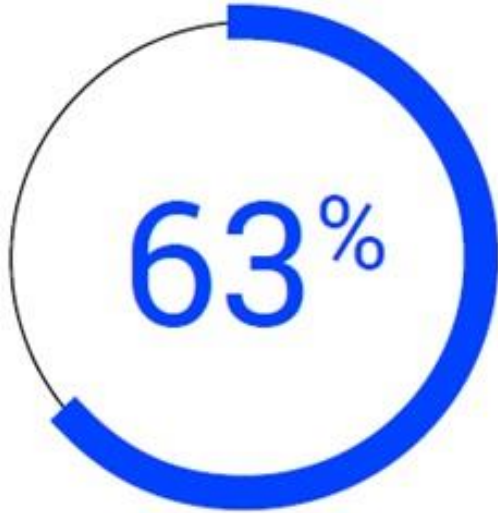
Channel Marketing Manager, España & LATAM

ISO 27001 Lead Auditor



Bitdefender®  
**10 in 10**  
2020

## Bitdefender 10 in 10



**63%**

consideran que estamos en una ciber guerra que les puede afectar



**27%**

de las empresas cuestionadas **no tienen una estrategia de seguridad**



**72%**

creen que hay necesidad de **un tipo más diverso de habilidades** en la ciberseguridad

# RISE AND FALL (AND RISE AGAIN) OF RANSOMWARE

Why has ransomware fluxed in popularity, and is it here to stay? Infosec professionals explore how ransomware has changed over the last few years and whether companies know how to deal with it.

# Ransomware is here to stay

The resurgence of ransomware is a huge concern for infosec professionals and recent events have only made it easier for cybercriminals

43% of infosec professionals agree that they are seeing a resurgence in ransomware attacks, but protection against them hasn't advanced much over the last five years. Just under half (49%) also stated that with increasing numbers of people working from home, their main cybersecurity concern is the business suffering a large-scale ransomware attack.



43%

seeing a resurgence in ransomware attacks

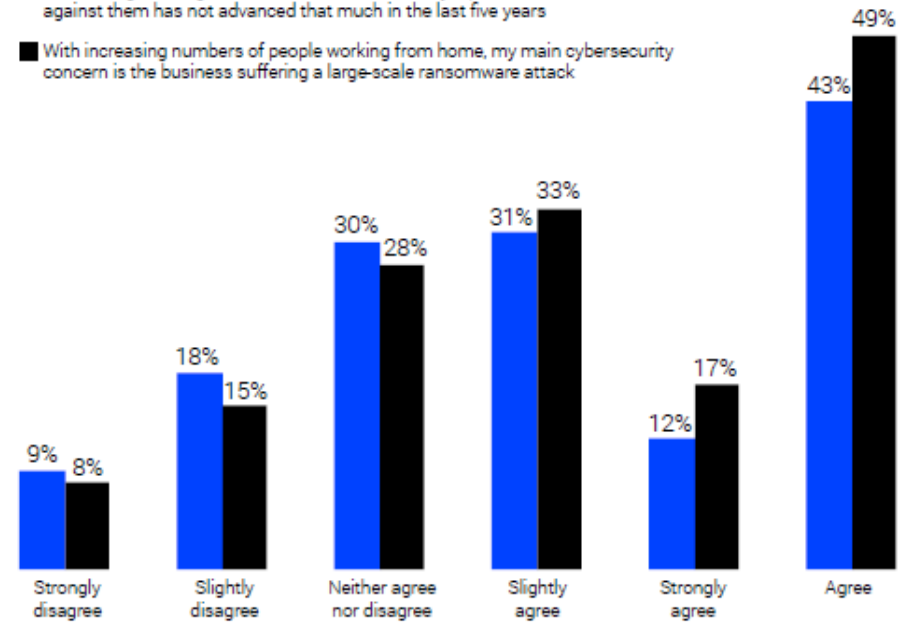


49%

concern is suffering a large-scale attack

Please indicate to what degree you agree or disagree with the following statements:

- I am seeing a resurgence in ransomware attacks, yet protection against them has not advanced that much in the last five years
- With increasing numbers of people working from home, my main cybersecurity concern is the business suffering a large-scale ransomware attack



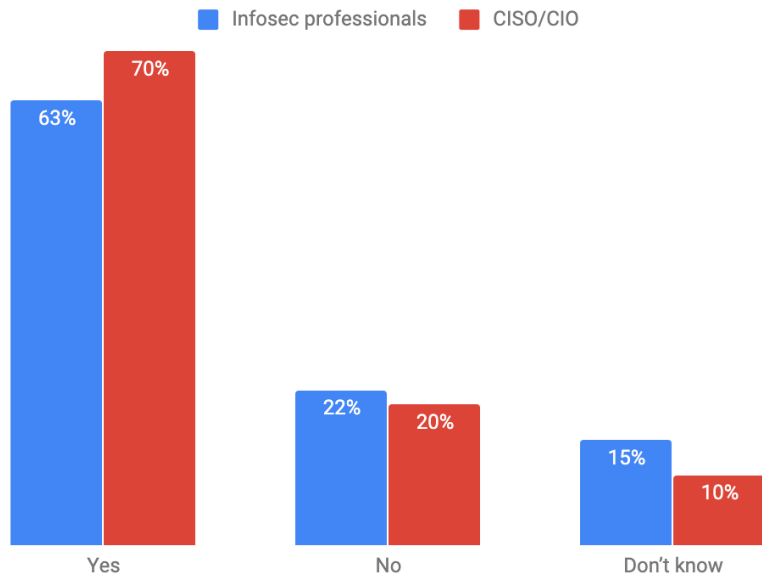
# LA PERSISTENCIA DEL RANSOMWARE

## Puede empeorar

La mayoría de los profesionales de ciberseguridad consideran que el ransomware va a empeorar

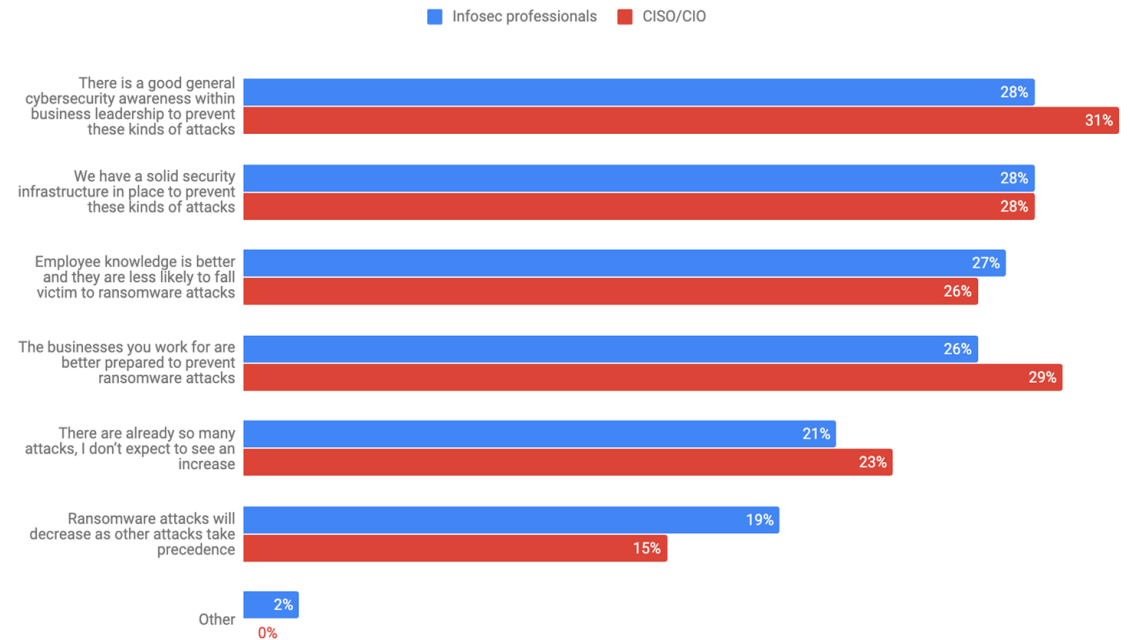
70% de los CISOs/CIOs creen que vamos a ver un incremento de los ataques ransomware en las siguientes 12-18 meses. Es una opinión que han expresado también 63% de los profesionales infosec.

**Do you expect to see an increase in ransomware attacks in the next 12-18 months?**



De los que no opinan que van a incrementar los ataques ransomware en los próximos 12-18 meses, 3 de 5 afirman que no van a ser afectados porque han reforzado sus infraestructuras y educan a los empleados en ciberseguridad.

**Why do you think that will be the case?**



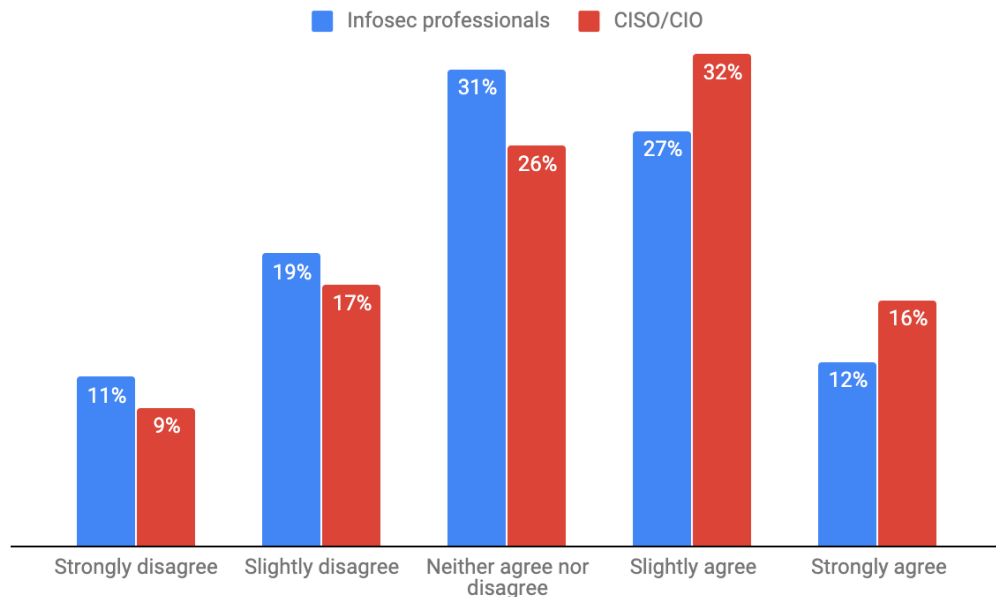
# LA PERSISTENCIA DEL RANSOMWARE

## Viviendo con las consecuencias

## Caiendo victima de un ransomware tiene un gran impacto en el negocio

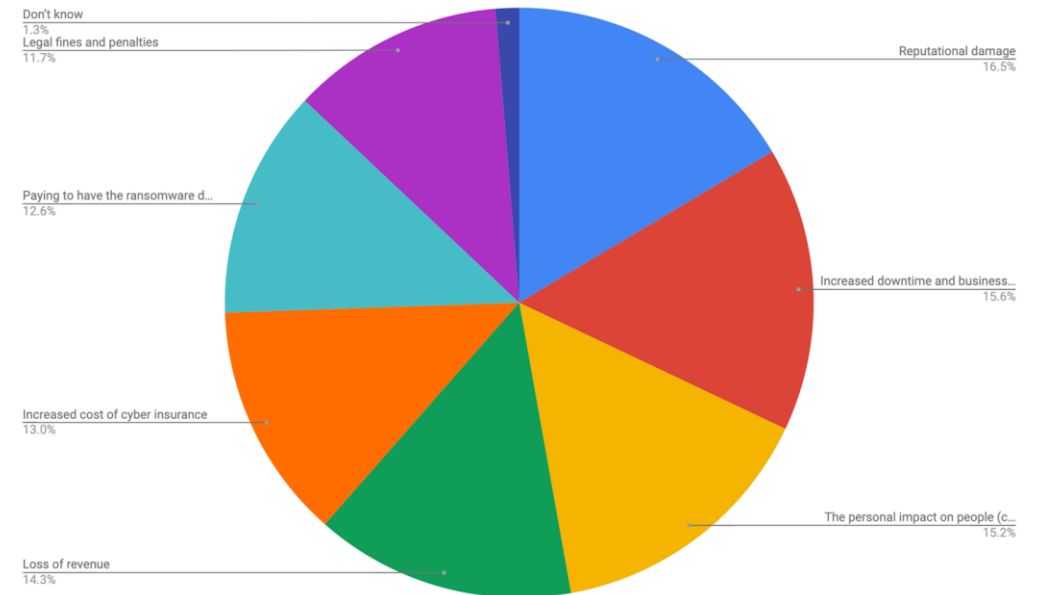
Casi la mitad de los CISOs/CIOs (49%) y más de un tercio de los profesionales en infosec (42%) se muestran preocupados que un ataque de ransomware los puede echar del negocio en 12-18 meses si no se protegen adecuadamente.

Please indicate to what degree you agree or disagree with the following statements: *“I am worried that a ransomware attack could wipe out the business in the next 12-18 months if we don’t increase investment in security.”*



Casi 2 de 5 profesionales creen que un ransomware les va a producir daño reputacional(38%), interrupción del negocio y afectación de su continuidad (36%). Las penas y multas legales son las que más preocupan, pero solo un 27% las ve como el motivo principal de preocupación

What would be the main consequences of your company suffering a ransomware attack? Select all that apply



## Paying up

A surprising amount of infosec professionals believe their organisation would pay up should they be attacked with ransomware

Almost one in six CISOs/CIOs (59%) and half of infosec professionals (50%) believe that the business they work for would pay the ransom in order to prevent its data/information from being published. And a further 18% of infosec professionals, don't know whether the business they work for would pay the ransom.



1 in 6

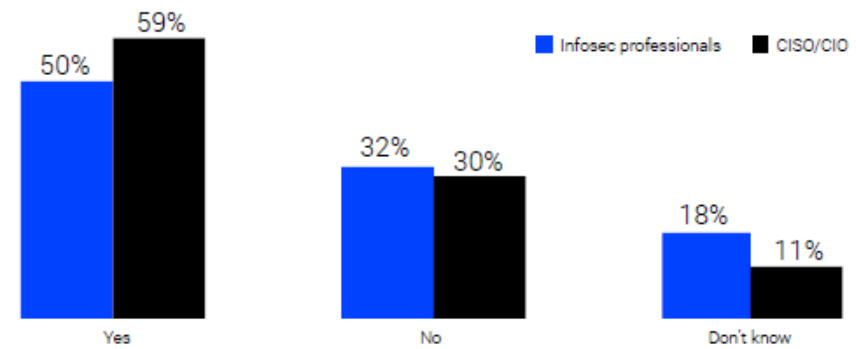
CISOs and CIOs believe that the business they work for would pay the ransom



50%

infosec professionals believe that the business they work for would pay the ransom

Should the business you work for suffer a ransomware attack, do you believe it would pay their ransomware in order to prevent its data/information from being published?



Those in the UK and Denmark are most likely to expect their organisation to pay a ransomware order (both 56%)



## GARMIN CASE – FACTS & LESSONS

### FACTS:

23.07.2020

GARMIN Connect secuestrado  
Servicios importantes de conectividad  
parados – call centers, redes internas, online  
chat

Apps para móvil y wearables que no han  
funcionado

Los mapas para los sistemas de navegación  
no se han podido actualizar

### WastedLocker by Evil Corp - GARMINLOCKED

25.07.2020

Pagaron unos millones a través de **Coveware**  
Recibieron la llave y trabajaron con **Emsisoft**  
para un tool para todas las máquinas

**GARMIN.** SUBSCRIBE TO UPDATES

### Service Outage

**Update** - We are currently experiencing an outage that affects flyGarmin and as a result, the flyGarmin website and mobile app are down at this time. This outage also affects our call centers, and we are currently unavailable to receive any calls, emails, and chats. We are working to resolve this issue as quickly as possible and apologize for this inconvenience.

**Connect Services:**

- Down: weather, CMC, position reports
- Up: phone/SMS via Iridium

**FitPlan:**

- Fully operational with exception of Mexican eAPIS

**Garmin Pilot Apps:**

- Down: Flight plan filing unless connected to FitPlan, account syncing, database concierge
- Up: largely functional - weather and other real-time aeronautical data are operational

**FlyGarmin: Down**  
Jul 23, 13:56 EDT

**Update** - We are continuing to investigate this issue.  
Jul 23, 08:49 EDT

**Investigating** - We are currently experiencing an outage that affects flyGarmin and as a result, the flyGarmin website and mobile app are down at this time. This outage also affects our call centers, and we are currently unavailable to receive any calls, emails, and chats. We are working to resolve this issue as quickly as possible and apologize for this inconvenience.  
Jul 23, 08:43 EDT

## GARMIN CASE – FACTS & LESSONS

### LESSONS:

1. Los cibercriminales vienen a por cualquier organización
2. Ataque dirigido. EvilCorp no ha escogido Garmin al azar
3. Han afectado las operaciones, no los satélites u otros sectores. Y esto ha sido visible y ha dolido más.
4. Ellos lo dan todo. ¿Y tus empleados?
5. La prevención les ha fallado. Y la EDR?
6. GARMIN tenia muchas tecnologías de seguridad instaladas. Pero aún asi...
7. TO PAY OR NOT TO PAY
8. La necesidad de tecnologías integradas en una **plataforma de ciber-resiliencia**

### GARMIN®

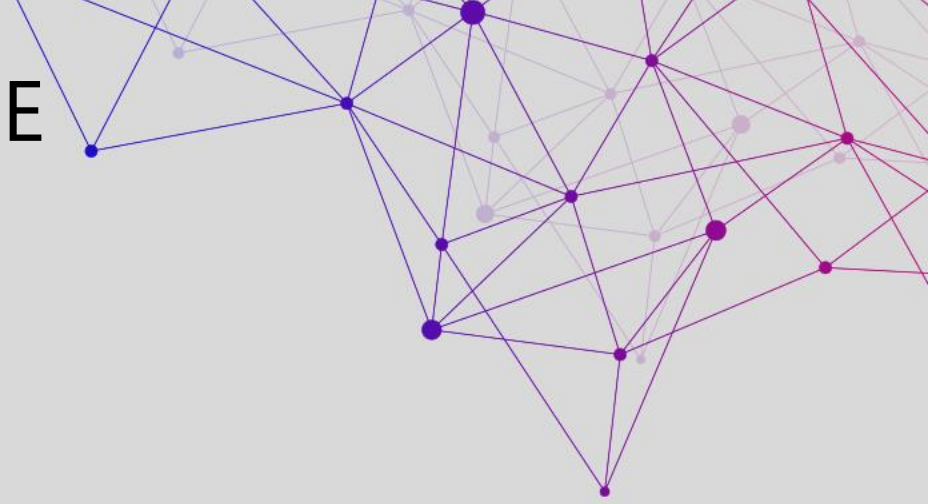
We're sorry.

We are currently experiencing an outage that affects [Garmin.com](https://www.garmin.com) and Garmin Connect. This outage also affects our call centers, and we are currently unable to receive any calls, emails or online chats. We are working to resolve this issue as quickly as possible and apologize for this inconvenience.

# Bitdefender<sup>®</sup>



# LA RESPUESTA ADECUADA REQUIERE DE TECNOLOGÍAS INTEGRADAS



# LA RESPUESTA ADECUADA REQUIERE DE TECNOLOGÍAS INTEGRADAS

## PREVENCIÓN DESTACADA

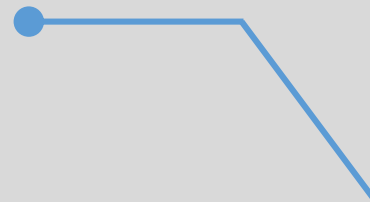
Para parar lo máximo  
que puedas



# LA RESPUESTA ADECUADA REQUIERE DE TECNOLOGÍAS INTEGRADAS

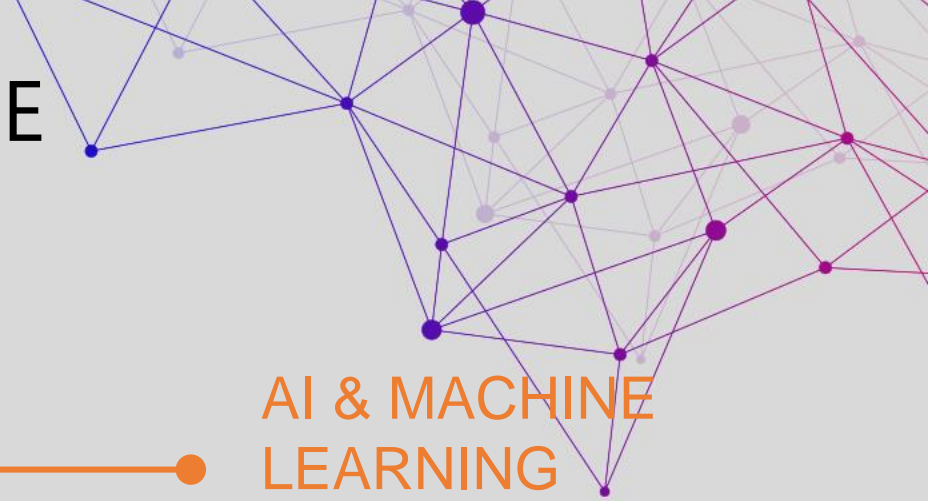
## PREVENCIÓN DESTACADA

Para parar lo máximo  
que puedas



## AI & MACHINE LEARNING

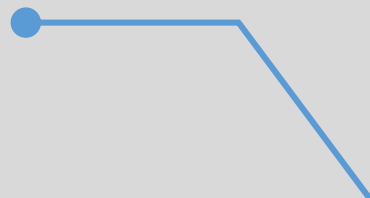
Para detectar  
amenazas  
desconocidas y  
ataques avanzados



# LA RESPUESTA ADECUADA REQUIERE DE TECNOLOGÍAS INTEGRADAS

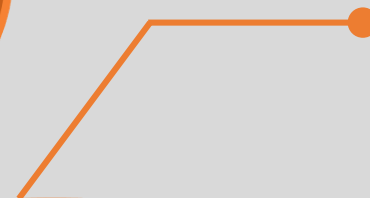
## PREVENCIÓN DESTACADA

Para parar lo máximo  
que puedas



## AI & MACHINE LEARNING

Para detectar  
amenazas  
desconocidas y  
ataques avanzados



## INVESTIGACIÓN AUTOMATIZADA

Para acelerar la  
respuesta



# LA RESPUESTA ADECUADA REQUIERE DE TECNOLOGÍAS INTEGRADAS

## PREVENCIÓN DESTACADA

Para parar lo máximo que puedas

## AI & MACHINE LEARNING

Para detectar amenazas desconocidas y ataques avanzados

## RESPUESTA AUTOMATIZADA

Efectiva y con sugerencias de mejora de la postura de seguridad

## INVESTIGACIÓN AUTOMATIZADA

Para acelerar la respuesta



**ENDPOINT, NETWORK, CLOUD & HUMAN**



# EL CICLO DE LA SEGURIDAD



# EL CICLO DE LA SEGURIDAD

**PREVENIR**

La mejor prevención  
a nivel del Endpoint,  
Network, Cloud y el  
Humano



# EL CICLO DE LA SEGURIDAD

**DETECTAR**

Análisis comportamental,  
Machine Learning, Detección  
personalizada, Threat  
Hunting Automatizado

**PREVENIR**

La mejor prevención  
a nivel del Endpoint,  
Network, Cloud y el  
Humano



# EL CICLO DE LA SEGURIDAD

**INVESTIGAR**

Análisis de la causa raíz,  
Análisis histórico  
Threat Intelligence  
integrado

**DETECTAR**

Análisis comportamental,  
Machine Learning, Detección  
personalizada, Threat  
Hunting Automatizado

**PREVENIR**

La mejor prevención  
a nivel del Endpoint,  
Network, Cloud y el  
Humano



# EL CICLO DE LA SEGURIDAD

**INVESTIGAR**

Análisis de la causa raíz,  
Análisis histórico  
Threat Intelligence  
integrado

**DETECTAR**

Análisis comportamental,  
Machine Learning, Detección  
personalizada, Threat  
Hunting Automatizado

**PREVENIR**

La mejor prevención  
a nivel del Endpoint,  
Network, Cloud y el  
Humano

**RESPONDER**

Respuesta  
adecuada y  
efectiva



# EL CICLO DE LA SEGURIDAD

## INVESTIGAR

Análisis de la causa raíz,  
Análisis histórico  
Threat Intelligence  
integrado

## DETECTAR

Análisis comportamental,  
Machine Learning, Detección  
personalizada, Threat  
Hunting Automatizado

## PREVENIR

La mejor prevención  
a nivel del Endpoint,  
Network, Cloud y el  
Humano

## REFORZAR

Reducir la  
superficie de  
ataque

## RESPONDER

Respuesta  
adecuada y  
efectiva



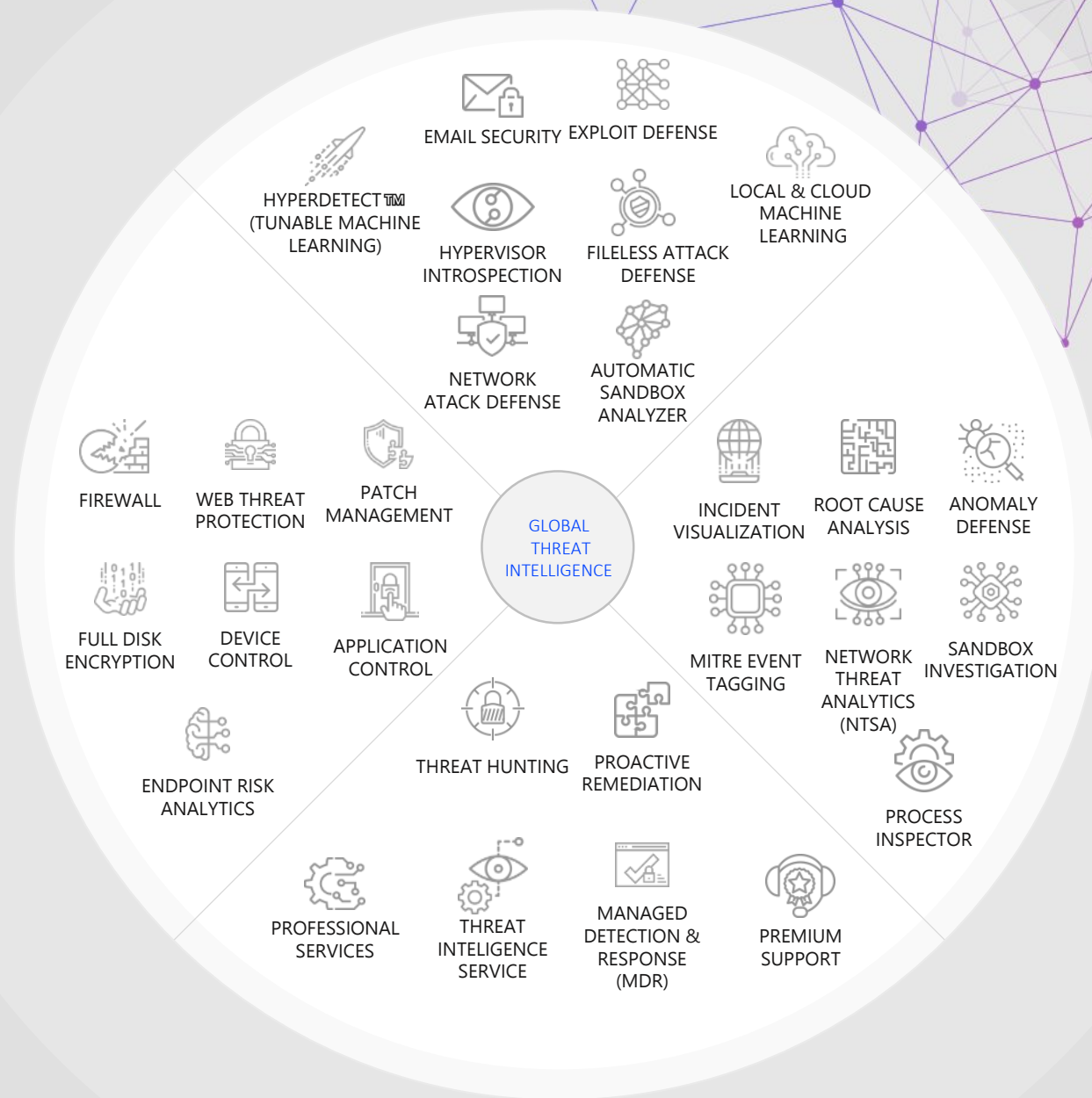
# TECNOLOGIAS & SERVICIOS INTEGRADOS PARA EVITAR LAS BRECHAS

Bitdefender GravityZone es una plataforma de seguridad de próxima generación que les permite proteger todos los endpoints de una empresa, incluido los que los empleados traen en la red empresarial, tanto físicos como virtuales, en el datacenter o instancias en la nube.

RISK ANALYTICS & HARDENING

PREVENCIÓN

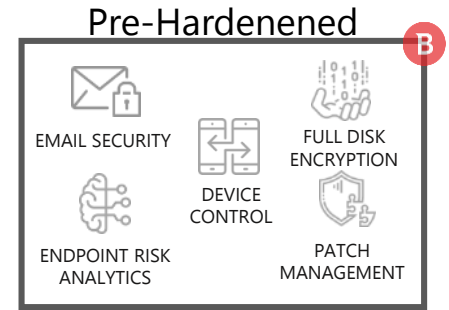
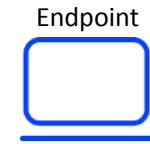
DETECCIÓN & RESPUESTA



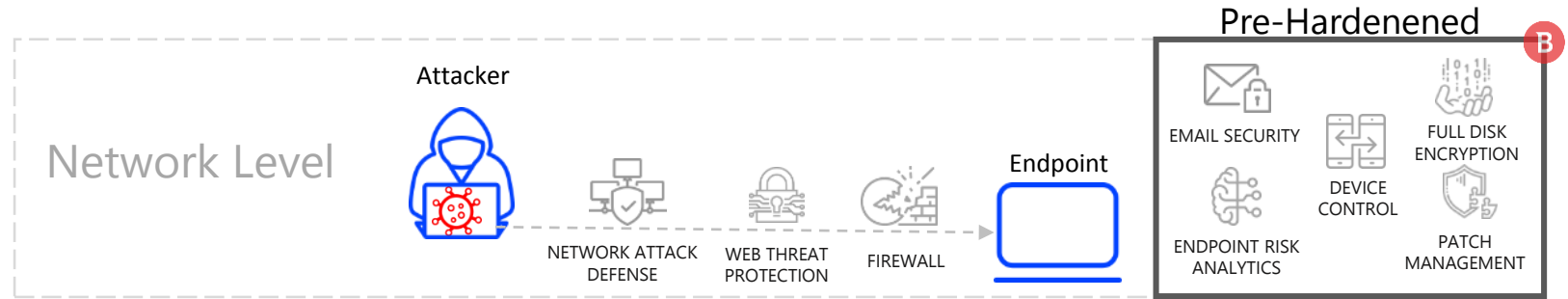
# LAS CAPAS DE PROTECCIÓN PARA UNA EMPRESA CIBER- RESILIENTE



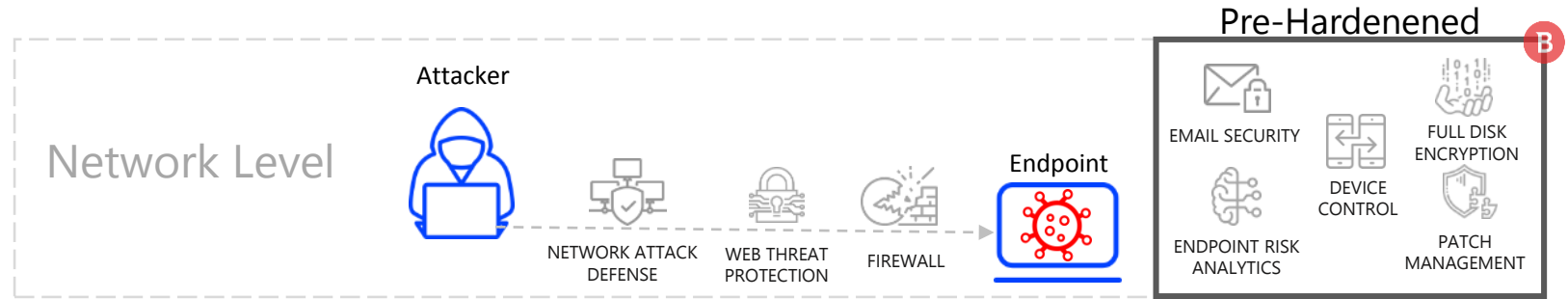
# LAS CAPAS DE PROTECCIÓN PARA UNA EMPRESA CIBER-RESILIENTE



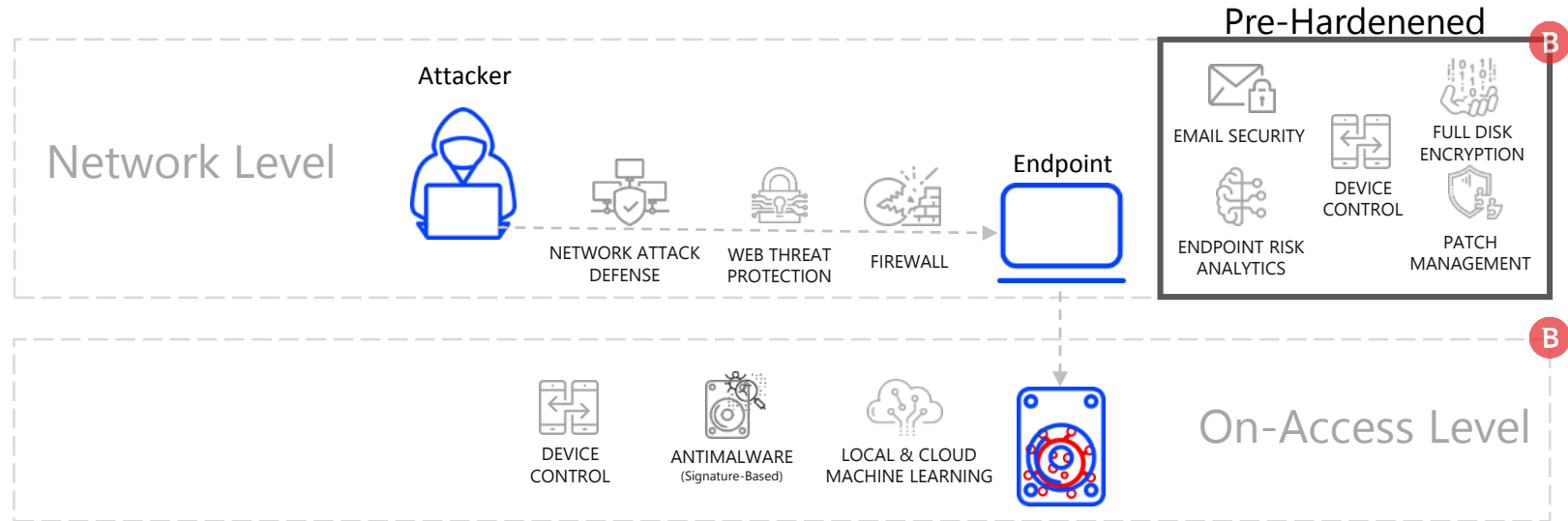
# LAS CAPAS DE PROTECCIÓN PARA UNA EMPRESA CIBER-RESILIENTE



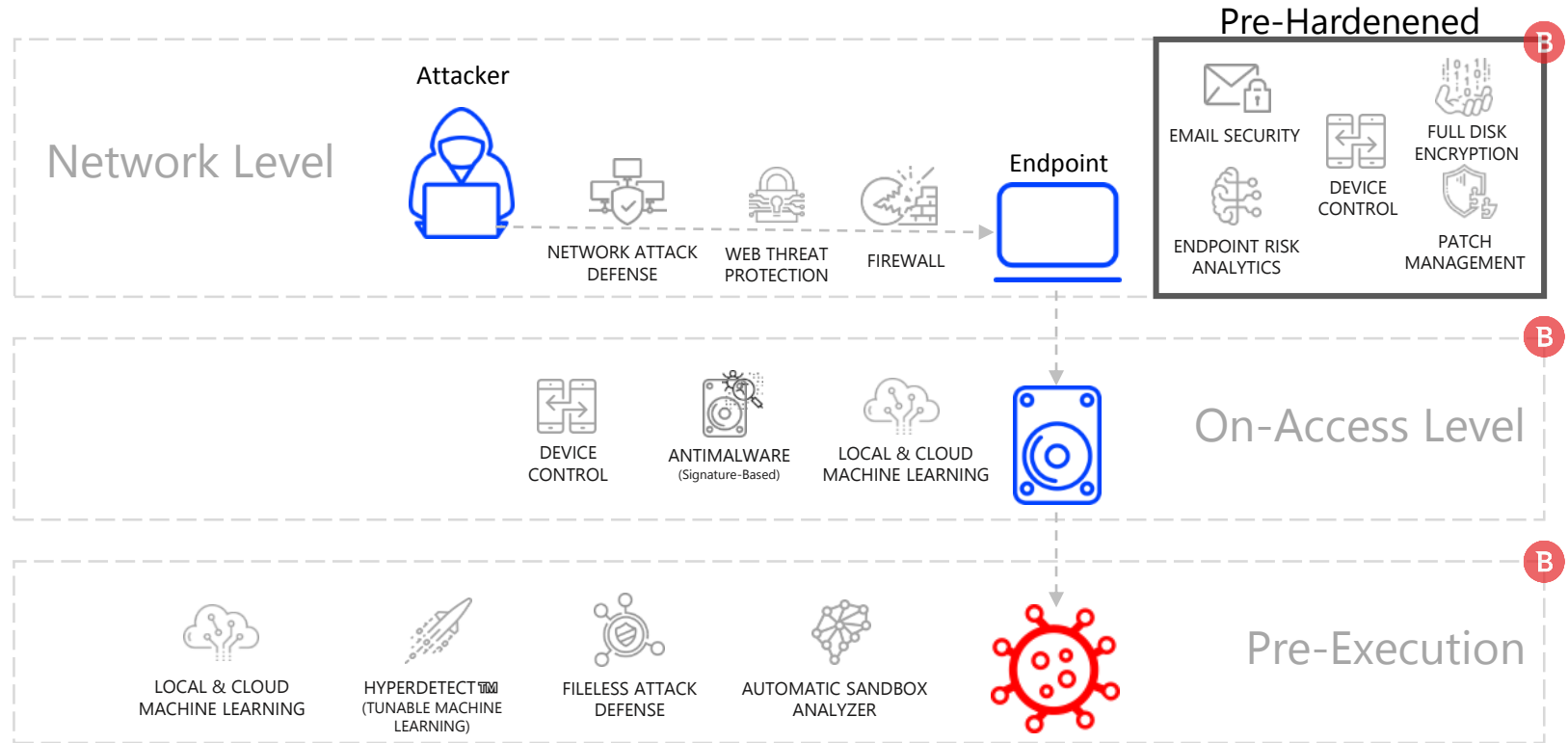
# LAS CAPAS DE PROTECCIÓN PARA UNA EMPRESA CIBER-RESILIENTE



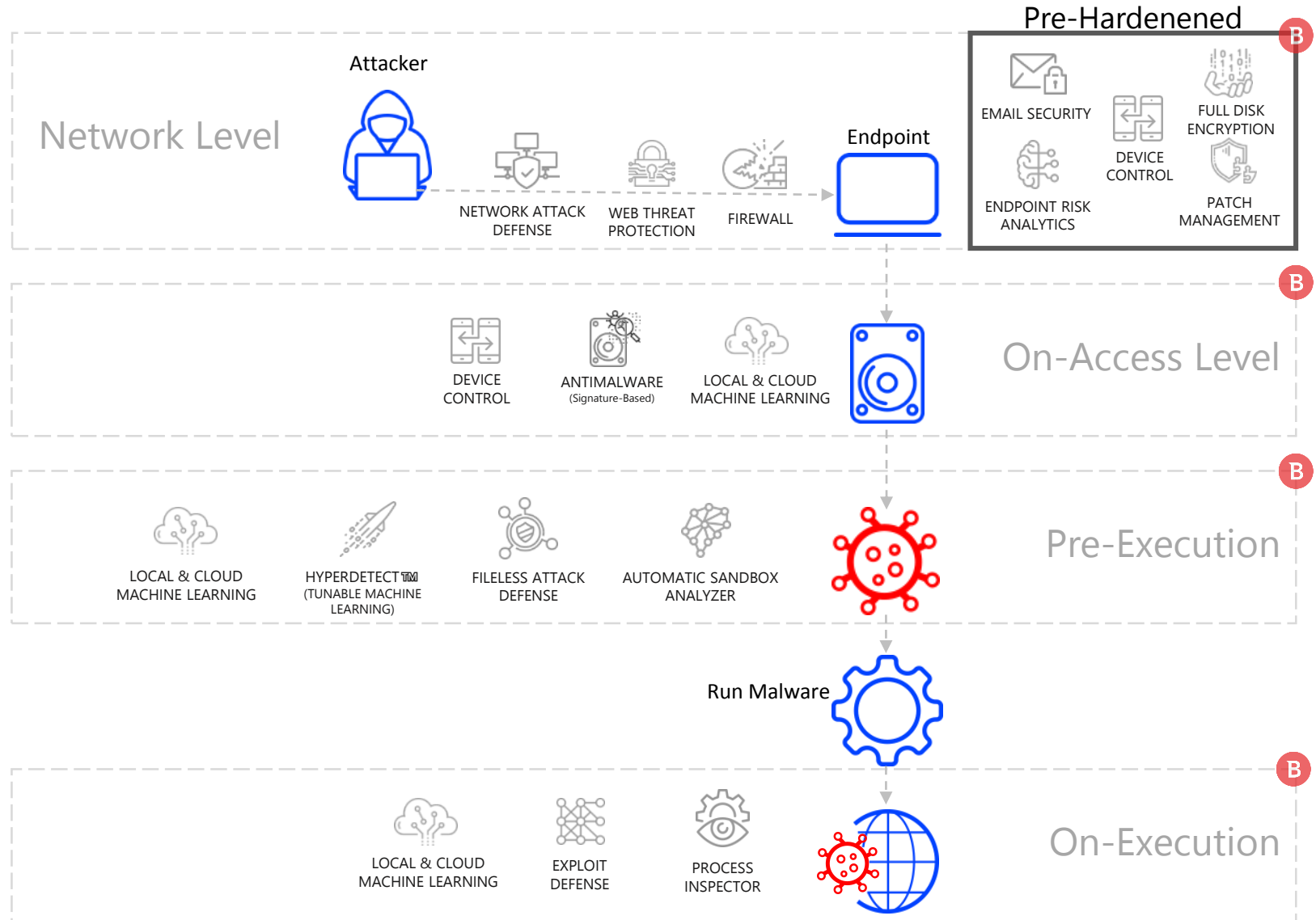
# LAS CAPAS DE PROTECCIÓN PARA UNA EMPRESA CIBER-RESILIENTE



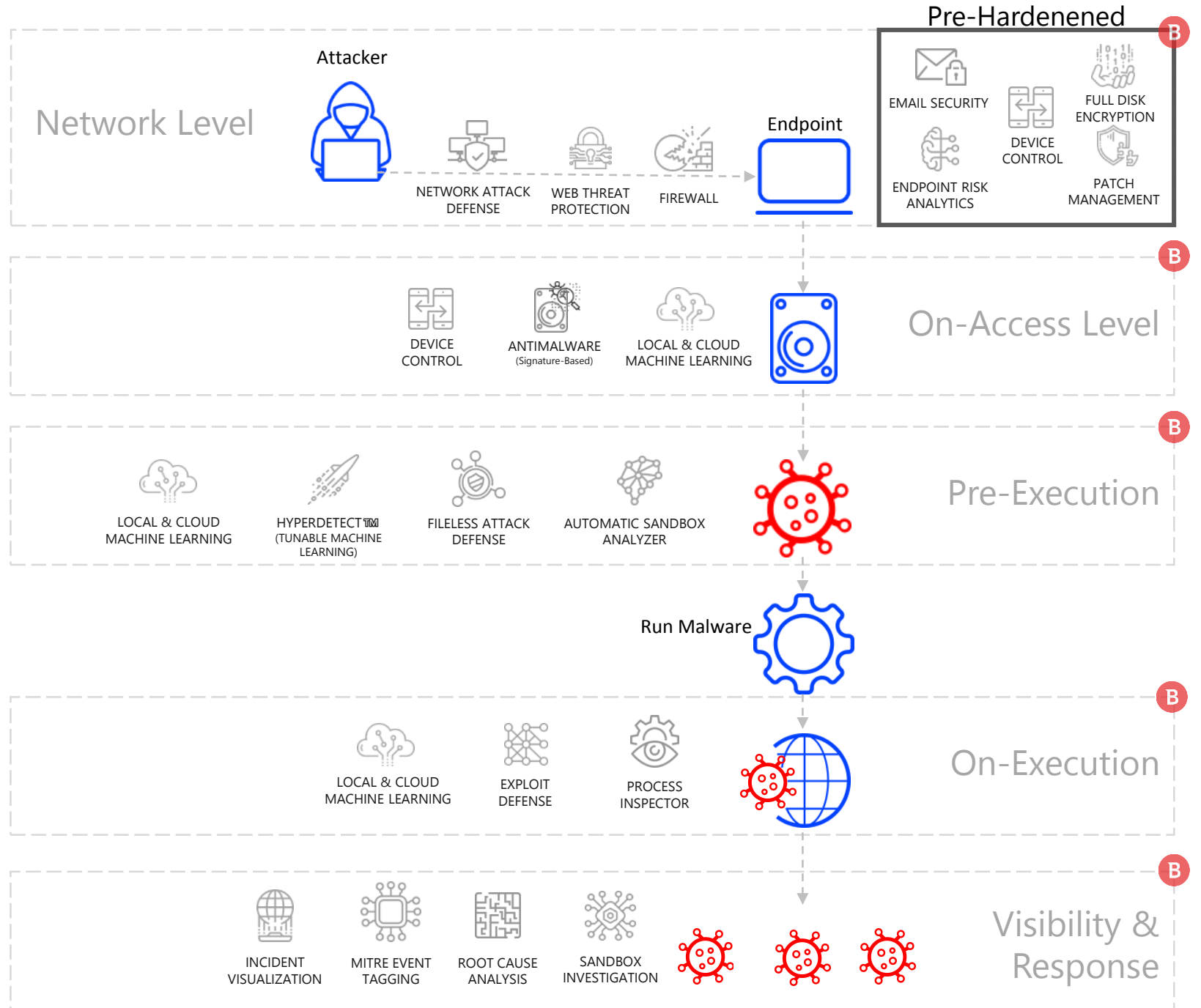
# LAS CAPAS DE PROTECCIÓN PARA UNA EMPRESA CIBER-RESILIENTE



# LAS CAPAS DE PROTECCIÓN PARA UNA EMPRESA CIBER-RESILIENTE



# LAS CAPAS DE PROTECCIÓN PARA UNA EMPRESA CIBER-RESILIENTE



# Bitdefender<sup>®</sup>

The background of the slide is a dark blue color with a grid of lighter blue rectangular panels. In the center-right area, there are silhouettes of three people standing and looking towards the right. The overall aesthetic is modern and tech-oriented.

¡MUCHAS GRACIAS!  
[hbandoiu@bitdefender.es](mailto:hbandoiu@bitdefender.es)