





WHO WE ARE?

After years of experience managing computer networks, attending customer requests who needed to know in a simple way what was happening in the network of their company and have the ability to quickly take the necessary corrective actions, the idea arose to develop an easy to install and use product that allows you to take control and increase security levels of the network even when whoever manages it does not have advanced technical knowledge.

The initial product was incubated between 2014 and 2016 by INGENIO (LATU Business Incubator) and supported by ANII (National Research and Innovation Agency), which allowed its growth both at a technical and business level.

Currently our GuardiaN product is installed in several companies and institutions of different sectors (financial, health, import & logistics, commerce, tvcable, etc.) who not only found in it a reliable, robust and user-friendly solution, but also thanks to their requests of new functionalities, collaborate in maintaining the constant growth of GuardiaN given the new technologies and threats that arise every day.

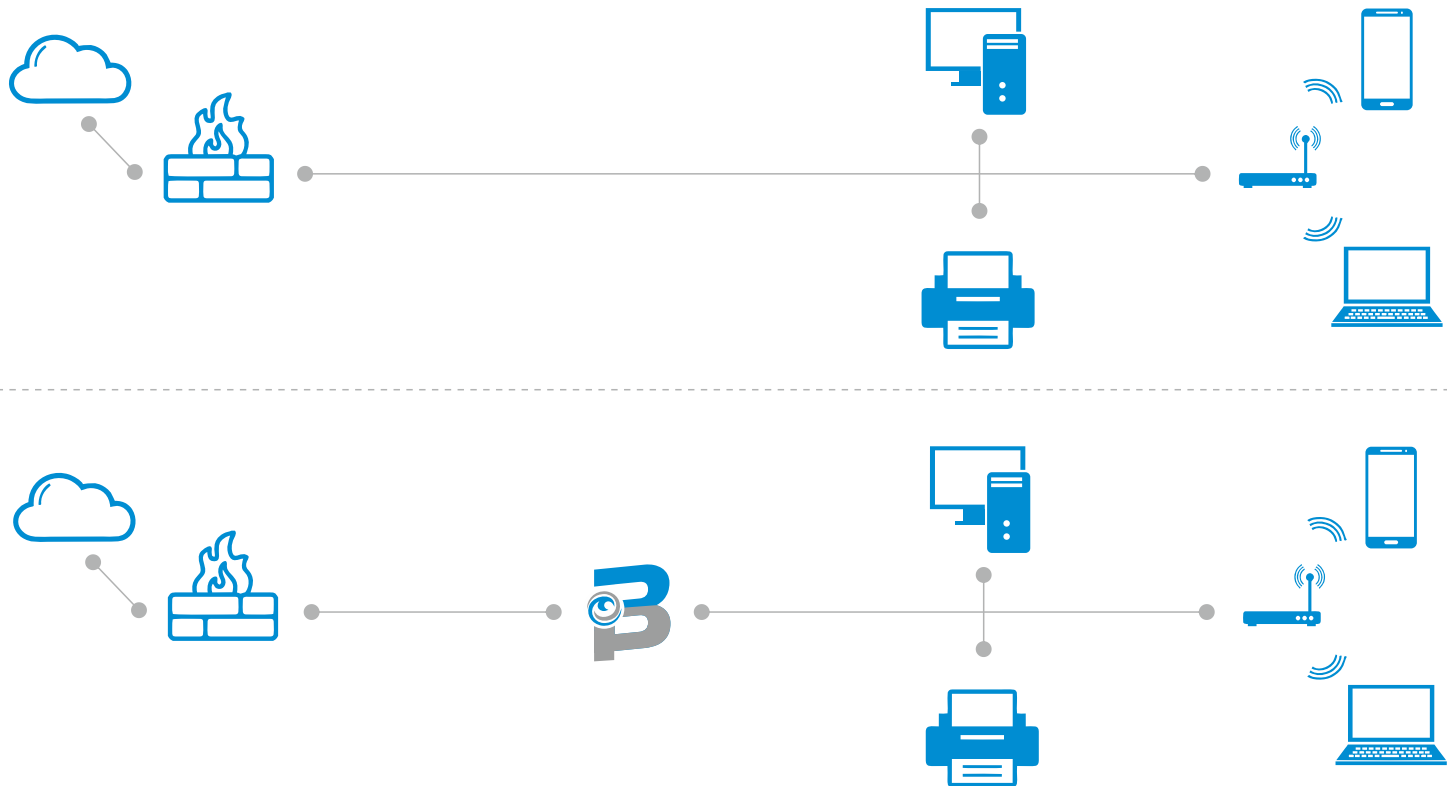
TEAM

We have a team of constantly trained professionals, who are updated on new technologies and trends related to security. This allows us to continuously offer a service and product in constant growth and evolution.

WHAT DO WE DO?

We develop products aimed at managing networks, increasing security levels and taking control of the use that users give the Internet taking into account three fundamental points:

- Ease of installation and use of our products.
- Development of functionalities requested by clients.
- After-sales support service.



FEATURES



E-MAIL

Control the emails that enter and leave your company in real time. Define protection rules, get detailed reports. Know if you have viruses on your network.

NETWORK

Learn why the network is slow. Protection and alerts in real time of malicious activity. Block programs on demand. Secure teleworking. Get detailed reports.

WEB BROWSING

Control in real time browsing, sites accessed, time spent. Block access, get detailed reports. Automatic protection from fraudulent sites.

WEB APPLICATION

Protect your web applications from the most common attacks used today. Receive realtime alerts and get activity reports

NETWORK INVENTORY

Generate an inventory with detail of your network hardware and software. Receive alerts against configuration changes.

PROACTIVE SECURITY

Vulnerabilities analysis on demand or scheduled. Get a detailed knowledge of your weak points, before the attackers do.

USERS CONTROL

Get detailed employees activity. Time worked, programs used, screenshots, etc.



WEB BROWSING

Browse control:

See in real time the sites that your users are browsing.

Time spent on each website:

Get time spent on each site detailed by user.
Send reports to users with their internet activity to encourage self-regulation.

Monitor secure access:

The use of https to browse the Internet is a reality (social networks, music, banks, etc).
Bprot allows you to filter such sites without installing certificates or configuring a proxy server.

Optimize network speed:

improve Internet speed globally, filtering inappropriate sites or blocking mass consumption applications.

Information at your fingertips:

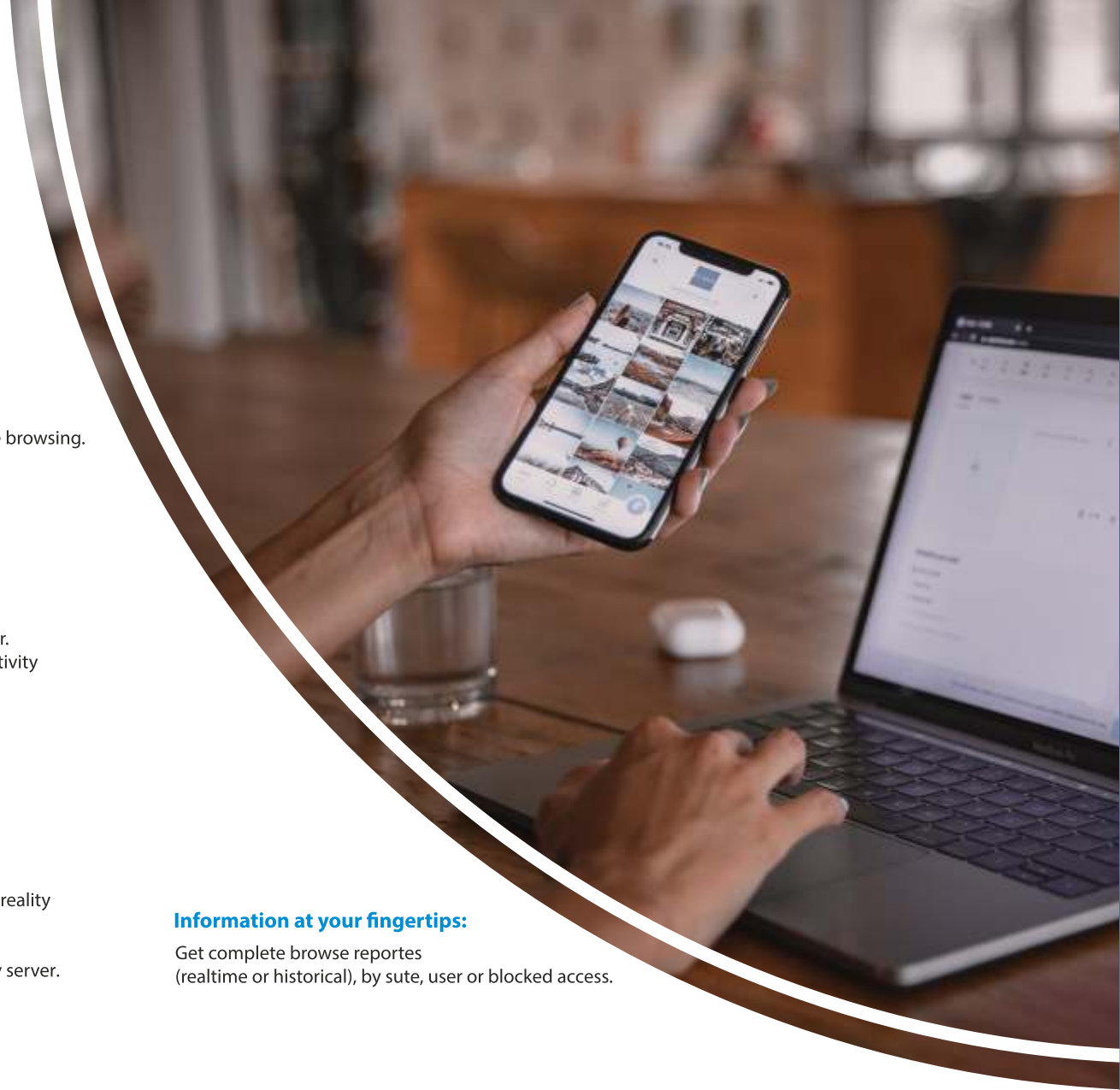
Get complete browse reportes (realtime or historical), by sute, user or blocked access.

Automatic protection:

Block access to inappropriate sites in real time, without the need to activate extra policies.

Usage policies:

Define browsing permissions and restrictions by team, site or user.



Send Mail:

Monitor incoming and outgoing emails in realtime.

Detailed information:

Get most active users reports.

Remote cleaning:

Reduce the amount of spam that enters your mailbox.

Authorized addresses:

Know if someone is sending emails from external accounts through your company network.

Local protection:

Block inappropriate emails before they reach the mail server. Apply filters such as attachment size, viruses, blacklists, authorized senders, etc.

Virus identification:

Find out if your network is infected with viruses.





NETWORK INVENTORY

Equipment inventory:

Software and hardware inventory of Windows or *nix computers.
Detection of configuration changes and automatic notification to administrators.

Devices inventory:

Automatically detect and identify network assets (switches, routers, firewalls, etc.)

Change notifications:

Receive automatic alerts if there are changes in the devices configurations.

Infrastructure organization:

Automatic detection and classification of the network structure, according to detected roles (Databases, mail servers, etc).



NETWORK INVENTORY

Total control:

Apply strong controls without the need for technical knowledge.
Control access by team or user to applications (whatsapp, teamviewer, etc.), which generate loss of productivity and possible risks of exposing your information.

Realtime protection:

Protect your network from attacks, viruses, spam, malware, etc.
Get real-time and historical reports.

Network optimization:

Easily find the computers that are slowing down the Internet. See real-time and historical user activity.

Critical equipment monitor:

Monitor the status of critical equipment and services on your network.
Find out early problems.

Secure teleworking:

Access securely your company from anywhere in the world.

Simple interpretation:

Easy to understand charts.

Network Map:

Auto-generated map that allows to have a complete vision of the connected equipment.





USERS CONTROL

Programs usage:

Get detailed program usage, and knowledge of the time dedicated to work and time dedicated to non-work tasks.

in/out control:

Record everything the user did, obtaining a detailed record of their activity.

Screenshots:

Get screenshots when certain events occur.

Keyboard activity:

Keyboard activity

Controls even outside the company:

No matter if they work locally or remotely.

File activity:

Get file activity
(creation, editing, deletion, etc).



USERS CONTROL

Vulnerability scan:

Detect equipment and services with vulnerabilities avoiding possible unauthorized access by criminals.

Credentials check:

Find services with default credentials.

Knowledge to prevent attacks:

Get a clear view of the current state of network security.

Alerts:

Receive notifications in real time (email, telegram) when a vulnerable service is detected.

Simple visualization of results:

Dispositivos 318	Servicios 348	Tcp 264	Udp 84	Credenciales 0
-----------------------------------	--------------------------------	--------------------------	-------------------------	---------------------------------

Problemas 30	Problemas aceptados 0	Advertencias 54	Advertencias aceptadas 0
-------------------------------	--	----------------------------------	---



Permanent protection:

Protect your web applications from the most common attacks.

Real time monitoring:

Control in real time allowed and blocked access.

Alerts:

Get real time alerts (email, telegram).

Easy configuration:

Activate protection in seconds.

Simple activity reports:

Fecha/Hora	Origen	Destino	Bytes	Accion	Extra
2023-01-20 15:41:38	192.168.1.1	main_10000	8799	403	*GET /dwa/login.php?s HTTP/1.1"
2023-01-20 15:41:39	192.168.1.1	main_10000	8799	403	"POST /dwa/login.php?-d+allow_url_include%3d1+-d+auto_prepend_file%3dphp://input HTTP/1.1"
2023-01-20 15:41:39	192.168.1.1	main_10000	8799	403	"POST /dwa/login.php?-d+allow_url_include%3d1+-d+auto_prepend_file%3dphp://input HTTP/1.1"
2023-01-20 15:41:39	192.168.1.1	be_main_10000	1653	200	*GET /dwa/login.php HTTP/1.1"



Contact us:

info@bprot.com

<https://bprot.com>