proactivanet

High Performer Mid-Market SPRING 2024 · High Performer Latin America SPRING 2024 · High Performer SPRING 2024 · Gartner Peer Insights Customers' Choice 2024

PRODUCT SHEET

CyberITAM by Proactivanet

In a fully digitalized world, where organizations depend almost entirely on IT services and infrastructure, **cybersecurity has become essential**—not only **to protect data** but also **to safeguard reputation and business continuity.** Cyber threats are constantly evolving, and attacks often have a devastating impact, not just financially but also on an organization's reputation, eroding customer trust and disrupting continuity.

As such, implementing proactive and effective cybersecurity measures is no longer optional; it is a necessity for businesses seeking to minimize risks in an increasingly vulnerable environment.

In this context, the **integration of cybersecurity practices and IT Asset Management (ITAM) into a single platform,** is key to ensuring **effective and comprehensive protection of corporate IT infrastructure.** By gaining complete, **up-to-date visibility of all IT assets** —from any hardware device to software, including cloud services—the security team can **proactively identify vulnerabilities and manage threats.**

This visibility allows for the identification of unpatched devices, outdated third-party software, or misconfigurations, which might otherwise go unnoticed and become entry points for attackers.

With a **unified approach,** organizations can **respond more quickly and efficiently to incidents,** reducing complexity and the costs associated with managing multiple IT and security tools. An integrated platform also fosters collaboration between IT and security teams, aligning asset management and security policies with the organization's strategic needs, significantly reducing the risk of security breaches. Ultimately, having a single source of truth that consolidates strategic cybersecurity information enables both the CISO and CIO to make informed decisions.

You are not doing cybersecurity if you are not doing ITAM

> The cost of cyberattacks for Spanish companies **increased by 43% in 2022** compared to the previous year [...] Corporations with more than 1,000 employees experienced an **average cost** increase of 34%, reaching **€333,939.**
>
> EuropaPress

INCLUDES:

- NATIVE INTEGRATION WITH ITAM AND CMDB
- NATIVE INTEGRATION WITH SERVICE DESK
- REAL-TIME INTRUSION DETECTION
- REAL-TIME MULTICHANNEL NOTIFICATIONS
- WINDOWS UPDATE AND THIRD-PARTY SOFTWARE MONITORING
- REAL-TIME CYBERSECURITY DASHBOARDS
- REGULATORY AUDIT EVIDENCE (ENS, NIS2, DORA)
- CENTRALIZED VULNERABILITY DATABASE (NVD, MITRE)
- AUTOMATED SOFTWARE PATCHING AND UPDATES
- SMART ASSET-VULNERABILITY MAPPING
- RISK MANAGEMENT BASED ON MAGERIT
- REAL-TIME MULTICHANNEL NOTIFICATIONS (WHATSAPP, MS TEAMS, TELEGRAM, SMS, EMAIL, ...).
- API AND WEBHOOKS FOR INTEGRATION WITH SOCS AND SIEMS

ens Esquema Nacional de Seguridad · NIS2 · DORA · ISO 27000

Key features of this module

Real-time intrusion detection and notification

Real-time detection of the networks to which corporate equipment is connected, showing the use of corporate networks, or "external" networks for which there are no security details. Additionally, for corporate networks, intrusion detection and notification can be activated in real time or deferred (WhatsApp, MS Teams, SMS, email) when non-inventoried equipment is detected.

	STANDARD	ADVANCED	PREMIUM
Subnet detection	✓	✓	✓
Real-time intrusion detection	✓	✓	✓
Communication pattern analysis	✗	✗	✓

Windows Update

Detection of the patches pending application on each Windows computer, with global vision (given a patch, where it needs to be applied) or individual (given a computer, which patches it has pending application), with the option to deploy them automatically and unattended. Dashboard to visualize the current status, patches with more pending updates, more critical patches pending to deploy, ...

	STANDARD	ADVANCED	PREMIUM
Detection and listing of Windows patches pending deployment	✓	✓	✓
Automatic update of Windows Update patches	✗	✓	✓

Third-party Windows SW update

Detection of pending updates for third party applications running on Windows platform (Adobe software, Audodesk, compressors, office tools, collaborative tools, ...), Audodesk, compressors, office tools, collaborative tools, ...). The Premium mode can also launch its own pending updates automatically and unattended. Dashboard for automatic control of the patching status of the park.

	STANDARD	ADVANCED	PREMIUM
Detection of SW due for update	✗	✓	✓
Automatic SW Windows update pending update	✗	✗	✓

Cybersecurity monitoring controls

Detection of other key cybersecurity aspects such as antivirus status, antispyware, firewall, HD encryption, remote control tools, VPN connectivity, ... The Standard version will offer basic capabilities on these aspects that will be more complete and multiplatform in the Premium and Advance levels. The higher levels of CyberITAM provide more information on the life cycle of the OS and its obsolescence, graphical data exploitation on the status and evolution in real time, generation of evidence for compliance with ENS, NIS2, DORA, ...

	STANDARD	ADVANCED	PREMIUM
Antivirus & antispyware deployment status	Only Win Client	✓	✓
Firewall deployment status	Only Win Client	✓	✓
VPNs deployment status	✗	✓	✓
HD (bitlocker) encryption status	✗	✓	✓
Remote control tools deployment status	✗	✗	✓
Deployment status of other configurable SW	✗	✗	✓
Historical evolution of cyber security status	✗	✗	✓
ENS, NIS2, DORA compliance listings	✗	✗	✓

Key features of this module

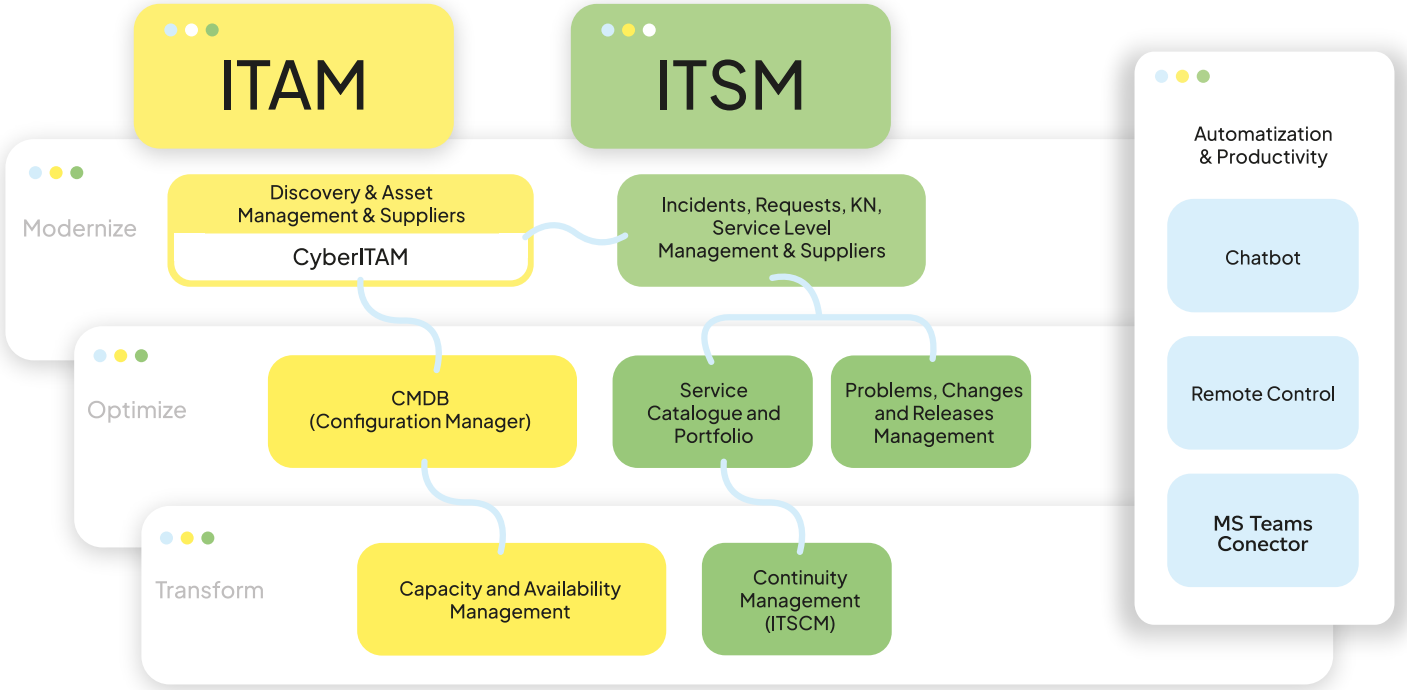
	STANDARD	ADVANCED	PREMIUM
CMDB and ITSM integration			
It allows the integration of CyberITAM natively with the rest of the Service Desk and CMDB processes, allowing the automatic creation of incidents in case of cybersecurity alerts and/or the visualization of such alerts directly in the CMDB graphs.			
Creation of automatic tickets for cybersecurity alerts	✓	✓	✓
Cybersecurity alerts in CMDB	✗	✓	✓
Vulnerability Management			
Centralized and always updated vulnerability database (Incibe, MITRE, NVD, ...), automatically linking each vulnerability with the assets in the inventory, eliminating false positives thanks to the integrated use of AISecOps.			
DDBB vulnerabilities	✗	✓	✓
Automatic detection of remediation	✗	✗	✓
Risk Management			
It facilitates the implementation of a Risk Management process following the Magerit methodology, according to the requirements established by the ENS, NIS2, DORA,... in a fully integrated way with the Inventory, CMDB and other Service Desk processes.			
Risk management according to Magerit methodology for ENS, NIS2, DORA	✗	✗	✓
Real-time multichannel alerts and notifications			
Configurable notification system, both in real time and deferred (e.g. daily/weekly summaries), using different communication channels depending on the criticality of the notification (SMS, WhatsApp, MS Teams, Email, Telegram, ...).			
Email alerts	✓	✓	✓
Advanced alerts (SMS, WhatsApp, MS Teams, ...)	✗	✓	✓
API and integrations			
Bidirectional integrations with 3rd party systems via REST API, as well as real time event notification to SOCs / SIEMs (notify the SOC immediately when an unknown computer is detected in a certain subnet, or notify the SIEM when a firewall is stopped in a computer, ...).			
Integration of external vulnerability scanners	✗	✗	✓
REST API	✓	✓	✓
Webhooks real-time security	✗	✓	✓

proactivanet

Proactivanet CyberITAM

TECHNICAL DATA SHEET

DEC 2024



DATA SHEET	
NAME OF MODULE	**CyberITAM**
DEPENDENCIES WITH OTHER MODULES	Discovery & IT Asset Management.
TYPES OF CONTRACTING	• **OnPremise Perpetual License.** • **Annual Leasing OnPremise** (includes support and subscription to versions). • **Software as a Service (Saas)** (includes support and subscription to versions).
FORM OF LICENSING	The module is licensed according to the number of assets with Operating System that are going to be inventoried automatically **(PCs, Servers and mobile devices).** Other devices with IP such as routers, printers, etc., as well as assets registered automatically, do not consume license.
LEVELS OF LICENSING	• **Standard** • **Advanced** • **Premium**

PinkVERIFY® Certified 16 PROCESSES

PinkVERIFY is a registered trademark of Pink Elephant.

15 PeopleCert ITIL®4 ACCREDITED TOOL VENDOR BRONZE Proactivanet v10