Foro AAPP

Reforzando la seguridad y el cumplimiento en la Administración Pública

Gloria Tamayo

WatchGuard en el Mundo

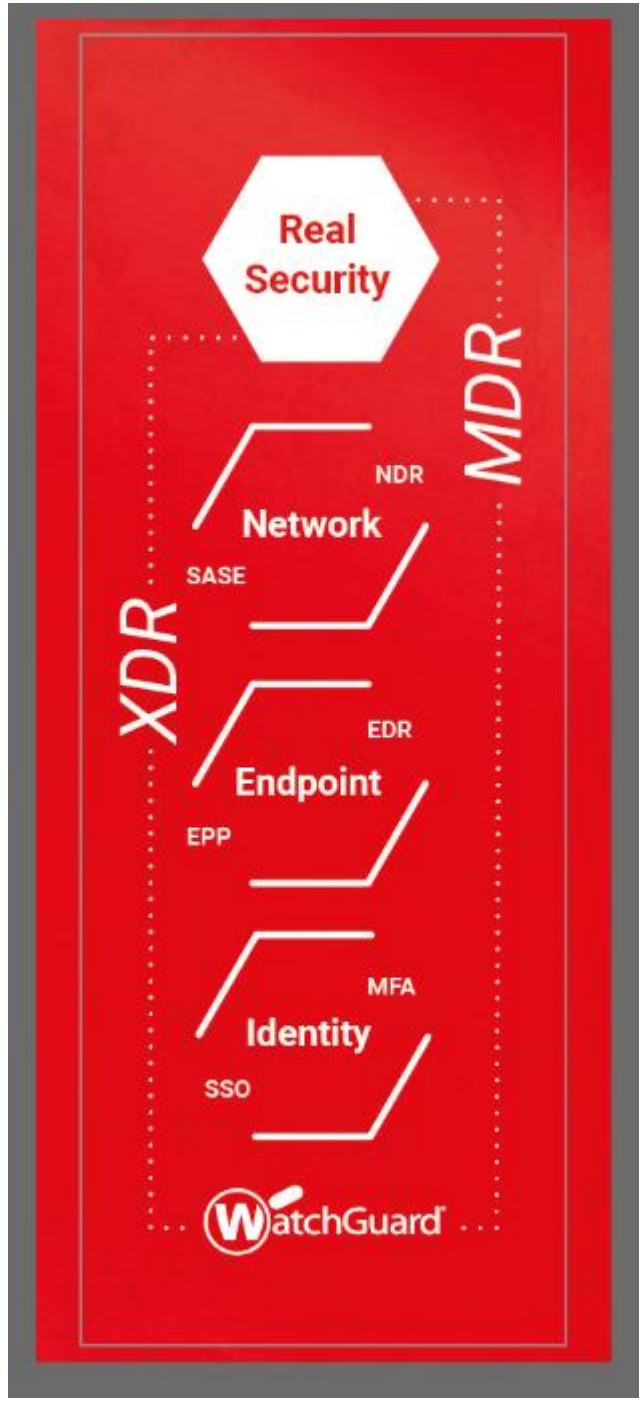
WatchGuard fundada en **1996**
Panda Security fundada en **1990**

Operaciones en **7** países;
Presencia directa en **21**

1,200 Empleados

1.5M Clientes

100+ Mayoristas
25,000 Partners



WatchGuard en España

Empresa de ciberseguridad con mayor presencia en España: más de **400** profesionales

Distribución por funciones en España:

- Más de **300** Técnicos
- **45** Ventas
- **55** Otros

R&D + Laboratorio Empresa con mayor presencia en I&D en ciberseguridad

Centro Mundial de Seguridad Gestionada en España

SOC 24x7 con Threat Hunters en España

Soporte L1, L2 y L3 con soporte en español

Reconocimientos WatchGuard - Cytomic

Premios y certificaciones

Enterprise Evaluation 2024 y 2025

La clasificación “ENS Alto”
del Centro Criptológico Nacional

Producto de Seguridad TIC Cualificado
del Centro Criptológico Nacional**

Nube avalada por el CCN
del Centro Criptológico Nacional ***

Producto de Seguridad TIC CCN

7.3 Seguridad en la explotación

7.3.1 Anti-virus / EPP (Endpoint Protection Platform)

7.3.2 EDR (Endpoint Detection and Response)

WatchGuard EPDR/WatchGuard Advanced EPDR

Versión	EPDR 4.60, Manag. Agent. 1.21, Protect. Agent 8.00
Fabricante	WatchGuard Technologies
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	27/06/2025
Revisión de Validez	31/05/2027

Descripción

WatchGuard Advanced EPDR integra en una única solución un conjunto completo de tecnologías preventivas en el endpoint, con capacidades EDR y el Servicio Zero-Trust Application. Extiende las capacidades de prevención, detección y respuesta con una gama completa de capacidades de protección del endpoint necesarias para evitar que las amenazas lleguen a los dispositivos y servidores y reducir la superficie de ataque. Sus capacidades de protección avanzada cubren todas las fases de la Seguridad Adaptativa: Prevención, Detección, Respuesta y Remediación, gracias a los servicios gestionados: servicio de clasificación del 100% de los programas, procesos y ejecutables en los endpoints y servicios de Threat Hunting y Análisis Forense, que permite enforzar la seguridad corporativa de forma continua.

Observaciones

CCN-STIC-1213 Procedimiento de Empleo Seguro en Proceso de Actualización

Cytomic EPDR

Versión	v4.6
Fabricante	WatchGuard Technologies
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	07/08/2025
Revisión de Validez	31/07/2027

Descripción

Cytomic EPDR integra en una única solución un conjunto completo de tecnologías preventivas en el endpoint, con capacidades EDR y el Servicio Zero-Trust Application. Extiende las capacidades de prevención, detección y respuesta con una gama completa de capacidades de protección del endpoint necesarias para evitar que las amenazas lleguen a los dispositivos y servidores y reducir la superficie de ataque. Sus capacidades de protección avanzada cubren todas fases de la Seguridad Adaptativa: Prevención, Detección, Respuesta y Remediación, gracias a los servicios gestionados: servicio de clasificación del 100% de los programas, procesos y ejecutables en los endpoints y el servicio de Threat Hunting y Análisis Forense, que permite una enforzamiento de la seguridad corporativa continua.

Observaciones

CCN-STIC-1213 Procedimiento de Empleo Seguro en Proceso de Actualización

Panda Adaptive Defense 360

Versión	v4.6
Fabricante	WatchGuard Technologies
Familia	Anti-virus / EPP (Endpoint Protection Platform)
Tipo	Servicio
Categoría ENS	ALTA
Fecha Inclusión	07/08/2025
Revisión de Validez	31/07/2027

Descripción

Panda Adaptive Defense 360 integra en una única solución un conjunto completo de tecnologías preventivas en el endpoint, con capacidades EDR y el Servicio Zero-Trust Application. Extiende las capacidades de prevención, detección y respuesta con una gama completa de capacidades de protección del endpoint necesarias para evitar que las amenazas lleguen a los dispositivos y servidores y reducir la superficie de ataque. Sus capacidades de protección avanzada cubren todas fases de la Seguridad Adaptativa: Prevención, Detección, Respuesta y Remediación, gracias a los servicios gestionados: servicio de clasificación del 100% de los programas, procesos y ejecutables en los endpoints y el servicio de Threat Hunting y Análisis Forense, que permite una enforzamiento de la seguridad corporativa continua.

Observaciones

CCN-STIC-1213 Procedimiento de Empleo Seguro en Proceso de Actualización

7.5 Protección de las comunicaciones

7.6.4 Redes privadas virtuales: IPSEC

WatchGuard Fireware on Firebox NGFWs (T35, T40, T80, T55, M270, M370, M470, M570, M670, M4600 y M5600)

Versión	FirewareOS 12.10
Fabricante	WatchGuard Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/03/2023
Revisión de Validez	31/05/2026

Descripción

Los equipos UTM de WatchGuard están enfocados en ofrecer la mejor seguridad para cualquier empresa y entorno corporativo distribuido. Nuestros dispositivos de seguridad de red están diseñados, desde el inicio, para enfocarse en facilitar el despliegue, el uso y la administración continua. Proporcionan protección contra ataques de malware avanzado y phishing, así como las protecciones de seguridad tradicionales: prevención de intrusiones (IPS), filtrado de URL, control de aplicaciones, antispam y antivirus, … ofreciendo en todo momento visibilidad del entorno (productividad y seguridad) Cuentan con capacidades SD-WAN, y VPN. Están disponibles tanto en equipos físicos como virtuales. https://www.watchguard.com/es/wgrd-products/network-security

Observaciones

CCN-STIC-1421 Procedimiento de empleo seguro WatchGuard Fireware

WatchGuard Fireware on Firebox NGFWs (T25, T45, T85, M290, M390, M590, M590, M690, M4800, M5800)

Versión	FirewareOS 12.10
Fabricante	WatchGuard Technologies
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/05/2024
Revisión de Validez	30/06/2026

Descripción

Los equipos UTM de WatchGuard están enfocados en ofrecer la mejor seguridad para cualquier empresa y entorno corporativo distribuido. Nuestros dispositivos de seguridad de red están diseñados, desde el inicio, para enfocarse en facilitar el despliegue, el uso y la administración continua. Proporcionan protección contra ataques de malware avanzado y phishing, así como las protecciones de seguridad tradicionales: prevención de intrusiones (IPS), filtrado de URL, control de aplicaciones, antispam y antivirus, … ofreciendo en todo momento visibilidad del entorno (productividad y seguridad) Cuentan con capacidades SD-WAN, y VPN. Están disponibles tanto en equipos físicos como virtuales. https://www.watchguard.com/es/wgrd-products/network-security

Observaciones

CCN-STIC-1421 Procedimiento de empleo seguro WatchGuard Fireware

CIS SECURITY PRODUCT — CCN Centro Criptológico Nacional — QUALIFIED

Proceso de certificación continua

PROXIMAMENTE Solución MFA: WatchGuard AuthPoint (EN PROCESO DE CERTIFICACIÓN)

WatchGuard-Cytomic en ENS | Medidas de protección

EndPoint

Gestión del personal [mp.per]

- Formación

Protección de los equipos [mp.eq]

- Protección de dispositivos portátiles - **WatchGuard Encryption**

Protección de los soportes de información [mp.si]

- Criptografía - **WatchGuard Encryption y WatchGuard Data Control**

Protección de la información [mp.info]

- Datos personales - **WatchGuard DataControl**

Protección de los servicios [mp.s]

- Protección del correo electrónico - **WatchGuard Email Protection**
- Protección de servicios y aplicaciones web - **WatchGuard EDR/EPDR/Advanced EPDR**
- Protección de la navegación web - **WatchGuard EDR/EPDR/Advanced EPDR**

Network

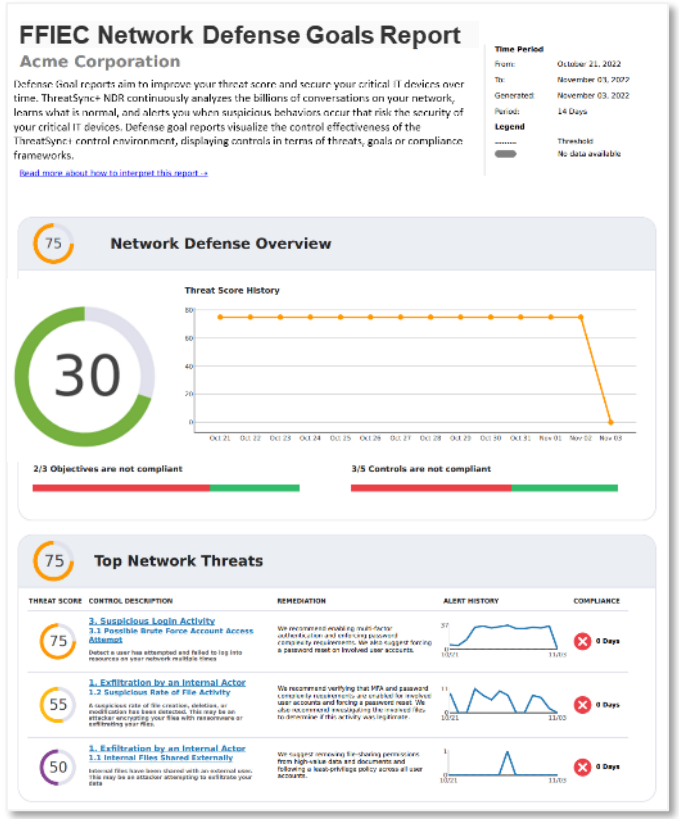
- **Protección de las comunicaciones [mp.com]**
  - Perímetro seguro – **WatchGuard Firebox**
  - Protección de la confidencialidad - **WatchGuard Firebox**
  - Protección de la integridad y de la autenticidad - **WatchGuard Firebox**
  - Separación de flujos de información en la red - **WatchGuard Firebox**
- **Protección de los servicios [mp.s]**
  - Protección de servicios y aplicaciones web - **WatchGuard Firebox**
  - Protección de la navegación web - WatchGuard Firebox

Identidad

- **Protección de los equipos [mp.eq]**
  - Bloqueo de puesto de trabajo - **AuthPoint**

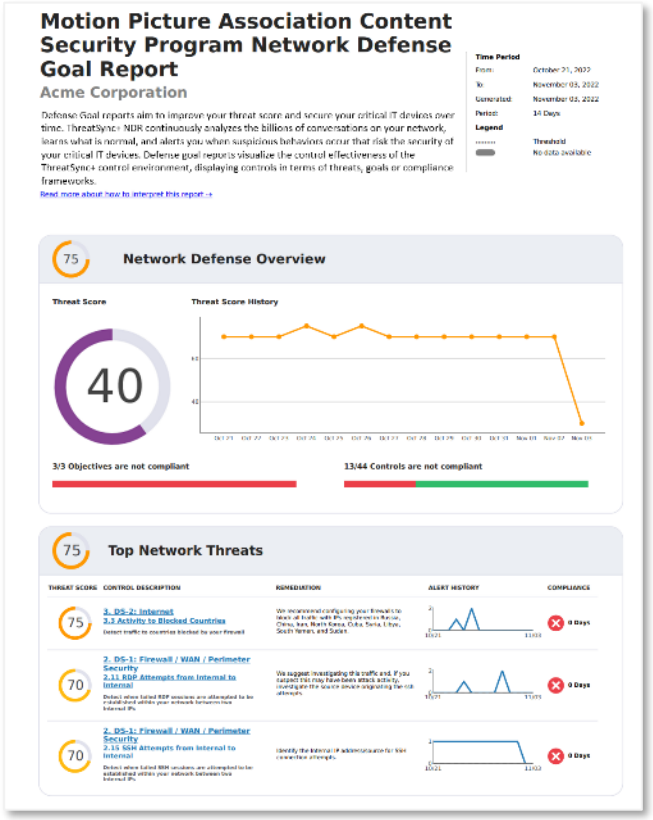
Evolución de la normativa y el cumplimiento

Compliance Reporting Examples



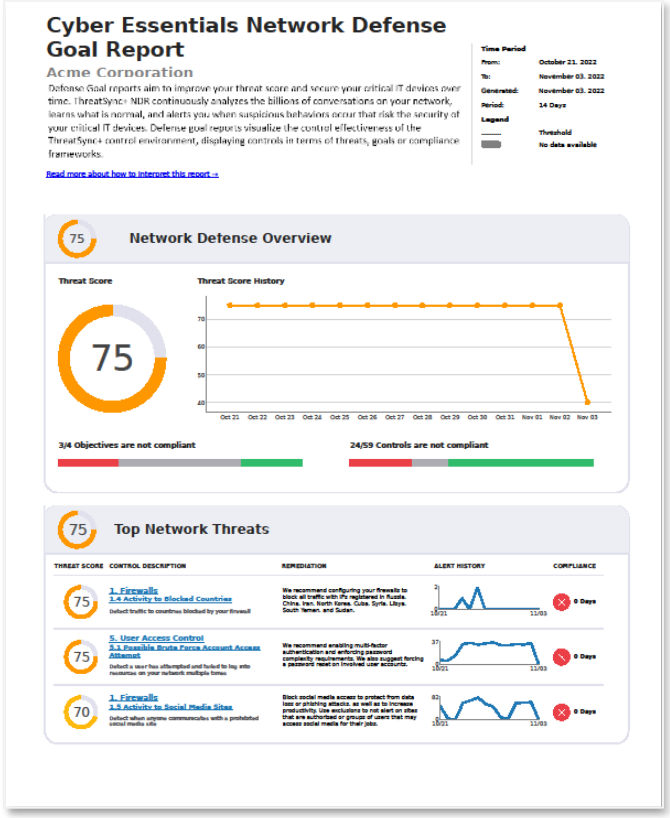
Regulatory Compliance Reporting

Instant report generation for regulatory compliance including: FFEIC, CMMC, NCUA, Build your own



Supply Chain Compliance Reporting

Build specialized compliance reports to prove ecosystem or vendor compliance with a click of a button



Best Practice Compliance Adoption

Implement and report against control framework adoption including: NIST-800.53, NIST 171, ISO 27001, and UK Essentials, or build your own

Infraestructura TI híbrida compleja y cambiante

El 96% de las empresas utiliza la nube pública

El 84% de las empresas utiliza la nube privada

El empleado medio utiliza 36 aplicaciones SaaS al día

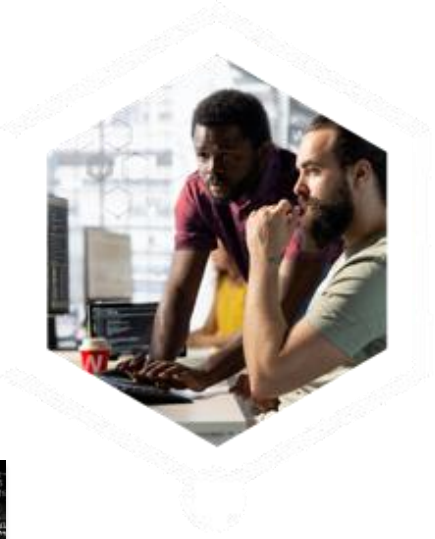
El 67% de las empresas tecnológicas de menos de 100 empleados trabajan a distancia

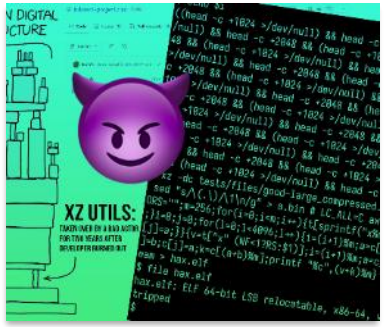
Ataques a la cadena de suministro de software

El 81% de las organizaciones mundiales sufren el impacto negativo de una brecha cibernética en la cadena de suministro

Aumento del 12% de los secretos de desarrollo y datos sensibles expuestos a través de repos de código abierto en 2024

El 45% de las organizaciones mundiales se verán afectadas por un ataque a la cadena de suministro este año - *Gartner*





XZ Utils Hack

Oracle Cloud Breach

Okta Support Breach

Intelligence Layer

Rai Insights Hub

Rai Control Modes

Rai Workers
- Analyst
- Auditor
- Admin

RED AI Intelligence
Unified intelligence | Real-time context | Orchestration
EndPoint 360/Elite | NDR | ThreatSync

Operations Layer

Operations Systems
CONNECTWISE · N-ABLE N-CENTRAL · ninjaOne · Autotask · Kaseya

OS & Cloud Systems
ANDROID · macOS · Office 365 · Azure · Linux · amazon web services · iOS · Windows · Google Cloud

Security Tools
CROWDSTRIKE · FORTINET · SentinelOne · Microsoft · CISCO · SOPHOS

Open APIs

WatchGuard Cloud
- Multi-Tenant Architecture
- Centralized provisioning
- Services Management
- Compliance and Reporting

WatchGuard Global PoP
- 16 Country Global Cloud Security Points
- Always-on Zero Trust Enforcement
- Optimized deliver, scalability & redundancy

WatchGuard Agent
- EDR/Identity/SASE
- Secure Comms
- Device Enforcement Point

WatchGuard MDR
Managed Detection and Response
Endpoint MDR | Defender MDR
Total MDR | Open MDR

Unified Security Core

NetSec

Firewalls
Firebox T Series
Firebox M Series
FireboxV
Firebox Cloud

Firewall Security
Intrusion Prevention
IntelligentAV
APT Blocker
DNSWatch

Wi-Fi Security & Services
Rogue AP detection
Captive Portal
Network Access Enforcement

Firewall Services
SD-WAN
VPN
Access Portal

Wi-Fi Access Points
Wi-Fi 6 AP
Rugged & Outdoor
PoE+

Endpoint

Endpoint Detection & Response
Basic | Prime | 360 | Elite

SOC Investigation
Orion

Endpoint Services
Patch Management
Full Encryption
Data Control (EMEA Only)
SIEM Feeder

Identity & SASE

Identity Security Services
Dark Web Monitoring
Credential Access
Zero Trust Validation

Multifactor Authentication
AuthPoint MFA
Hardware Token
Single Sign-on

SSE/SASE
FireCloud Internet Access
FireCloud Total Access

Cloud DR
Shadow IT Discovery
Misconfig Mgmt.
Identity Threat Detection

Zero Trust Identity Framework
Zero Trust Policies
Session Level Validation

XDR

ThreatSync XDR
Correlated Detection and Response

ThreatSync NDR
Hybird Network Detection and Response

ThreatSync SaaS
Cloud SaaS Detection and Response

Zero Trust Core

Gracias

gloria.tamayo@watchguard.com