SOFTICS INGENIEROS

RESPALDO TECNOLÓGICO PARA UN ENTORNO DIGITAL SEGURO

Reporte Implementación TrendAI

Fecha: 27 de julio de 2026

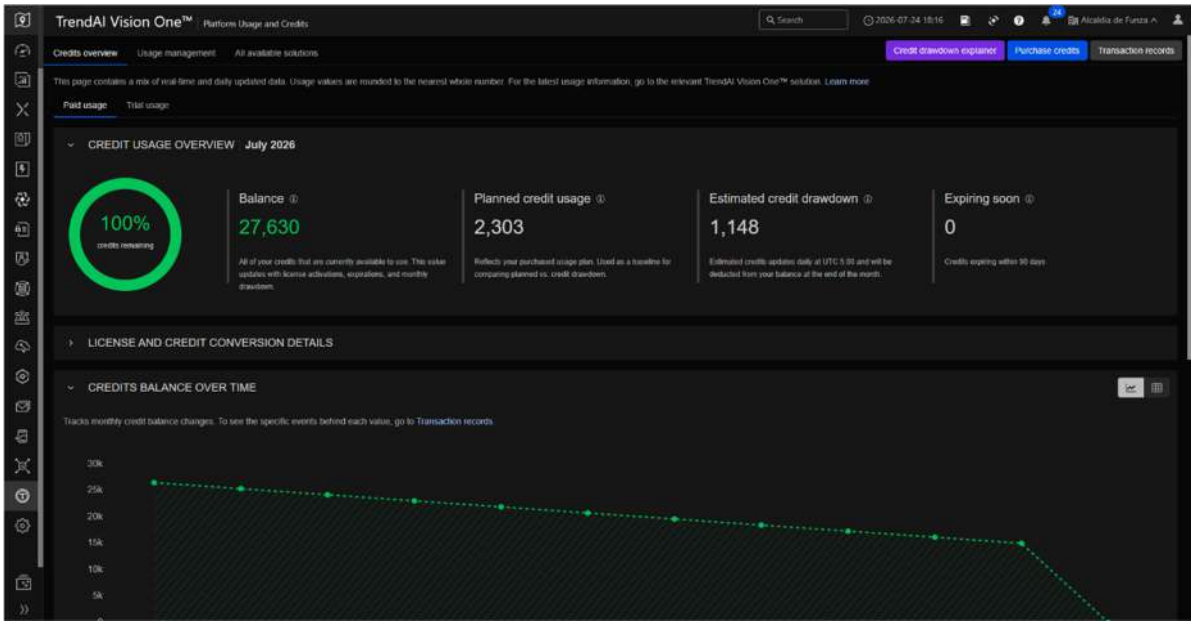
TrendAI Vision One

1. Introducción

En este reporte encontramos en detalle el estado actual de la solución adquirida por la Alcaldía municipal de Funza, adicional se menciona el proceso de implementación de cada uno de los productos adquiridos y un porcentaje del avance de cada uno de estos.

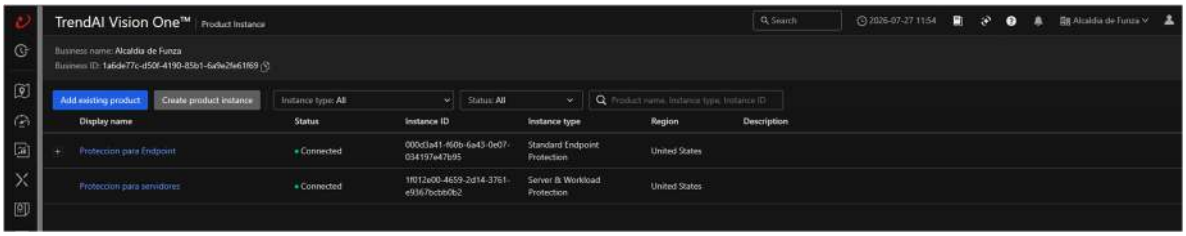
2. Resumen de actividades

- **Validación de las licencias en la consola (100%):** Se valida en consola que los productos adquiridos en consola se encuentras 100% activos y disponibles.

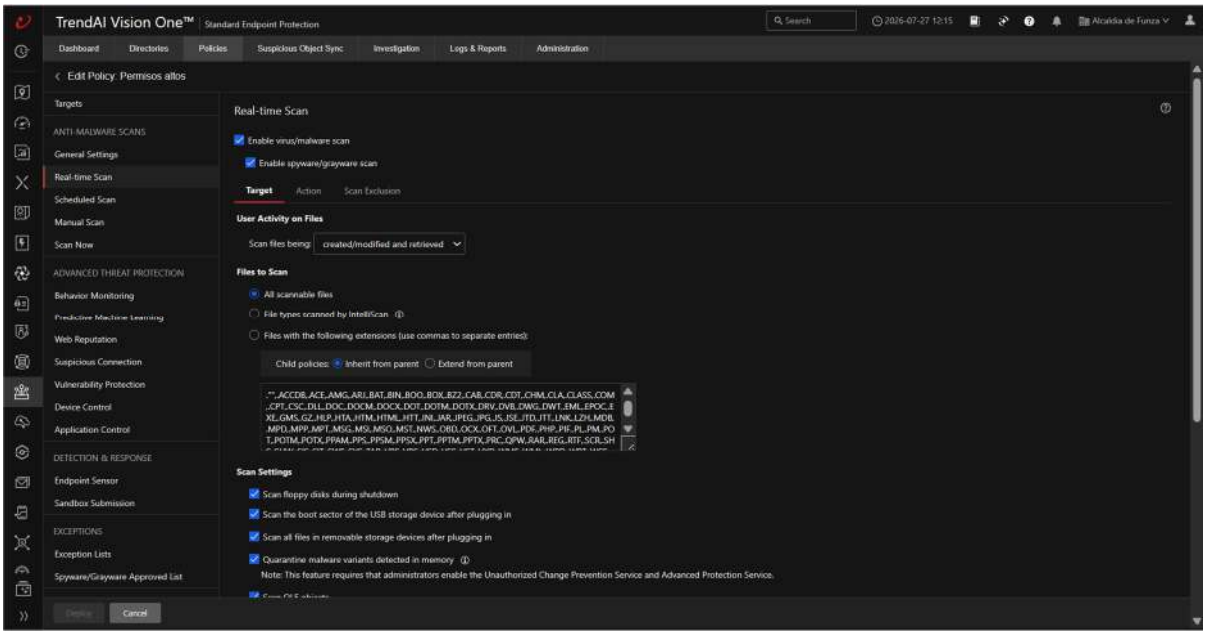


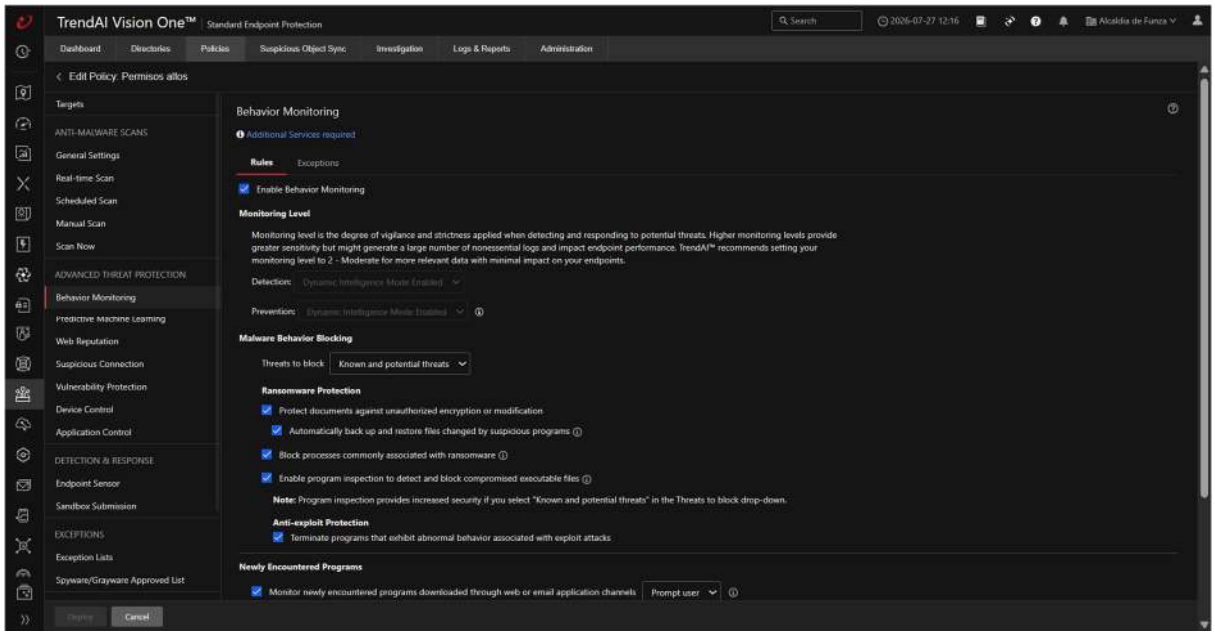


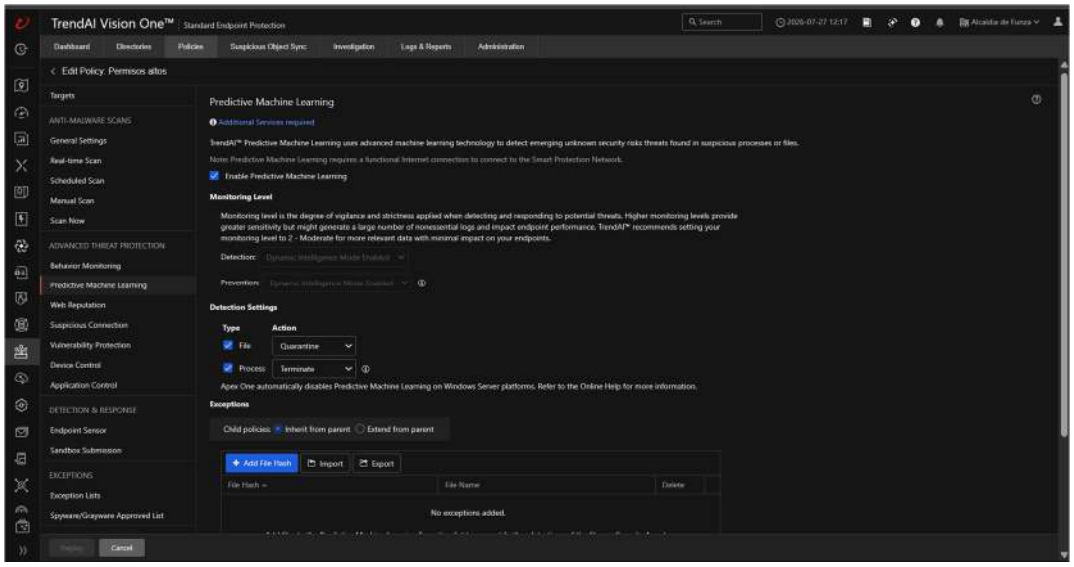
- **Creación de las instancias de producto (100%):** Para realizar la activación e implementación de la solución se realizó la creación de las instancias de producto donde se realizar la creación de las políticas de seguridad y la visualización de los eventos generados.

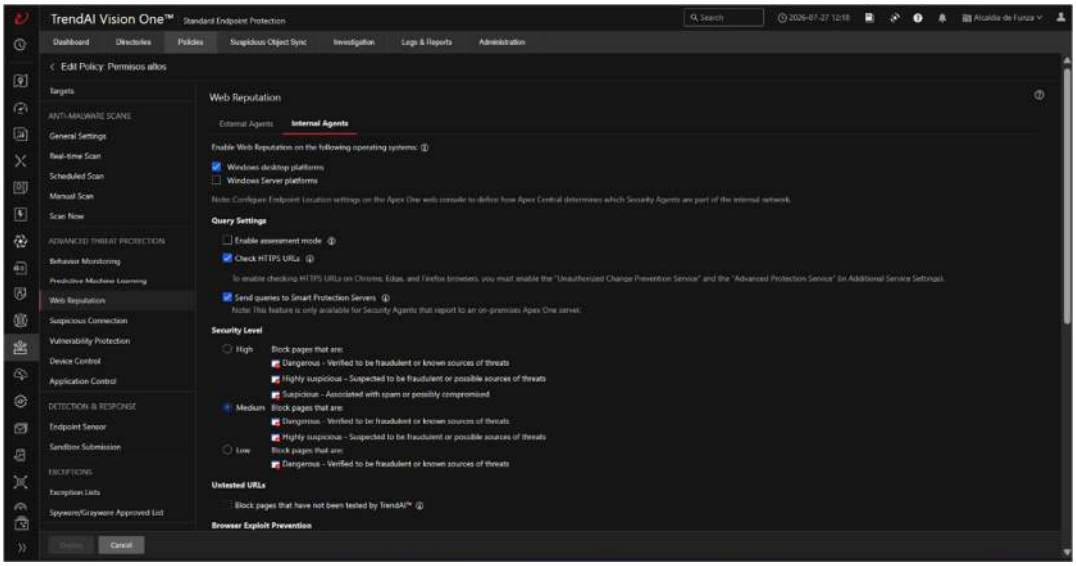


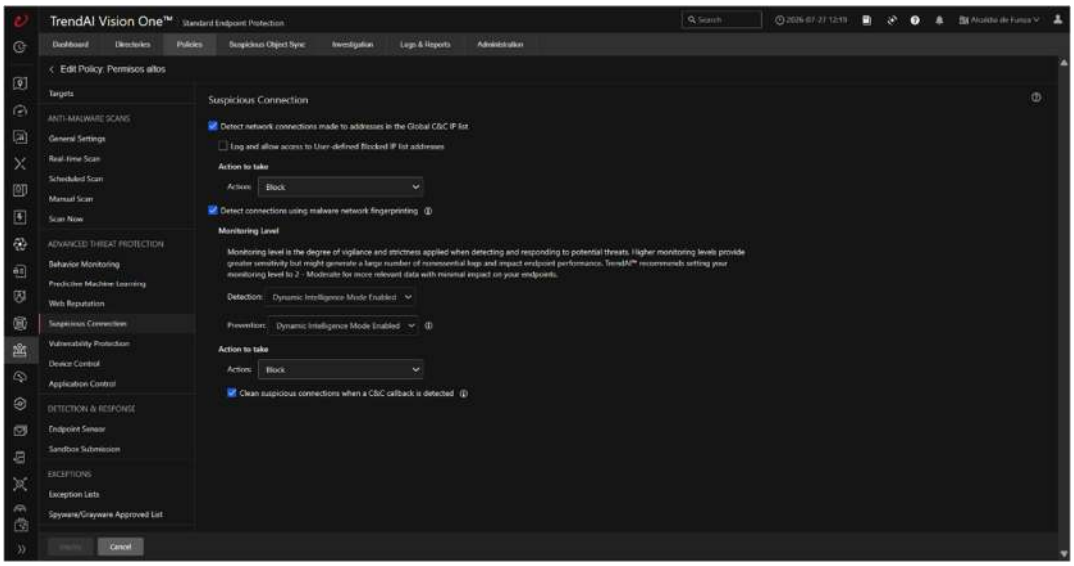
- **Creación de las políticas de seguridad Endpoint (100%):** Se realiza la creación de las políticas de seguridad según la guía de buenas prácticas del fabricante, dentro de estas se configuran 3 políticas diferentes, estas relacionadas a los permisos a nivel de dispositivos extraíbles “device control”, a nivel de antimalware, web reputation, Behavior Monitoring, Predictive Machine Learning, Suspicious Connection, Vulnerability Protection y Application Control la configuración de las políticas es la misma.

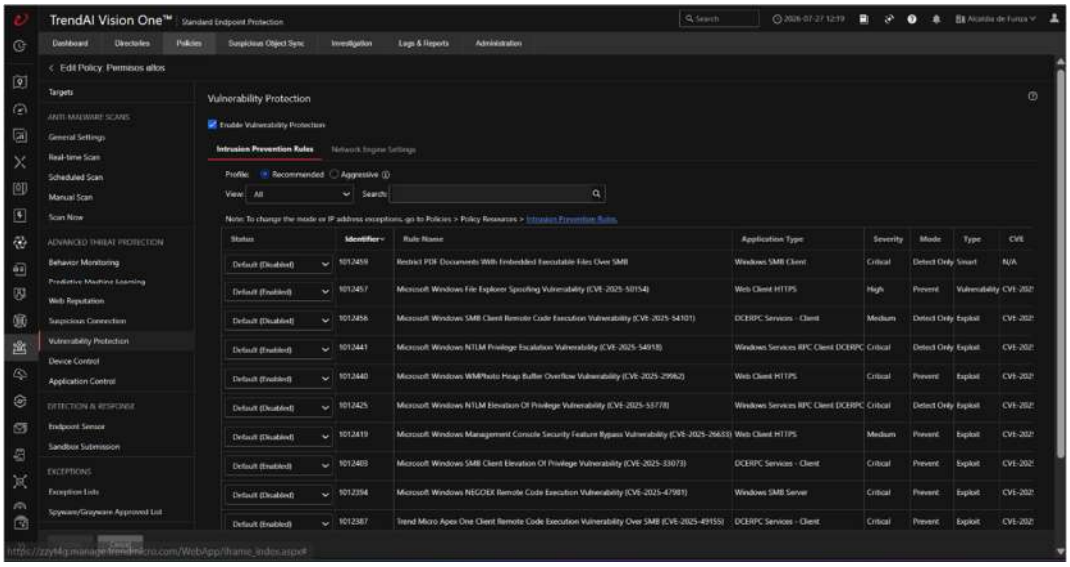


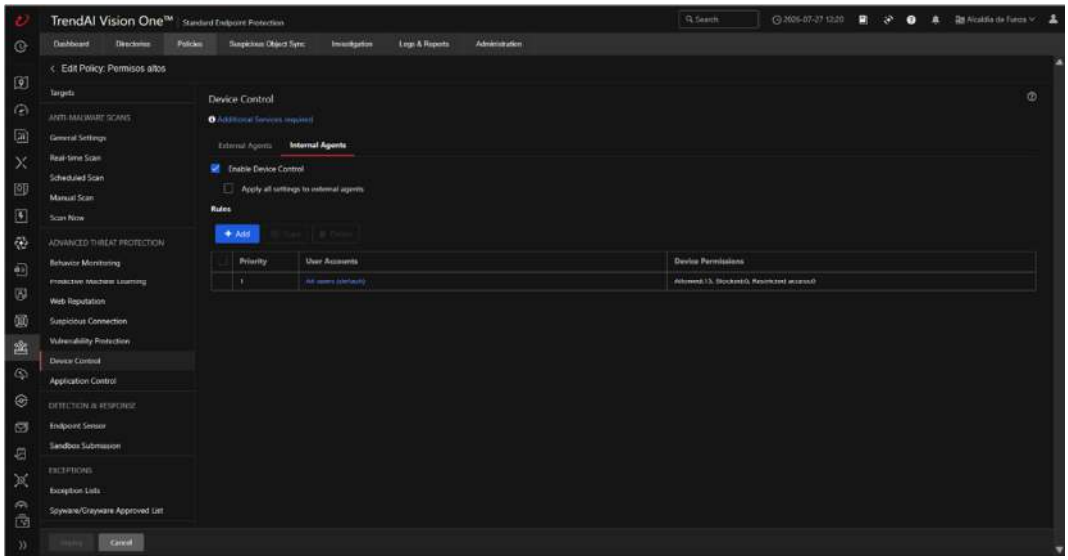


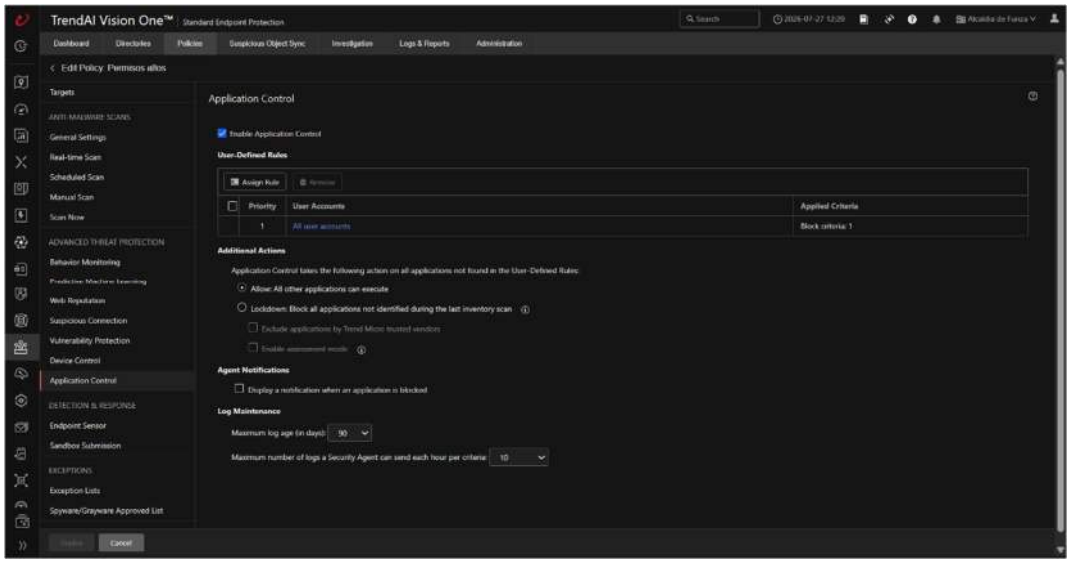

TrendAI Vision One™ Standard Endpoint Protection
Dashboard
Directories
Policies
Suspicious Object Sync
Investigation
Logs & Reports
Administration
Edit Policy: Permisos altos
Targets
ANTI-MALWARE SCANS
General Settings
Real-time Scan
Scheduled Scan
Manual Scan
Scan Now
ADVANCED THREAT PROTECTION
Behavior Monitoring
Predictive Machine Learning
Web Reputation
Suspicious Connection
Vulnerability Protection
Device Control
Application Control
DETECTION & RESPONSE
Endpoint Sensor
Sandbox Submission
EXCEPTIONS
Exception Lists
Spyware/Grayware Approved List
Predictive Machine Learning
Additional Services required
TrendAI™ Predictive Machine Learning uses advanced machine learning technology to detect emerging unknown security risks threats found in suspicious processes or files.
Note: Predictive Machine Learning requires a functional Internet connection to connect to the Smart Protection Network.
Enable Predictive Machine Learning
Monitoring Level
Monitoring level is the degree of vigilance and strictness applied when detecting and responding to potential threats. Higher monitoring levels provide greater sensitivity but might generate a large number of nonessential logs and impact endpoint performance. TrendAI™ recommends setting your monitoring level to 2 - Moderate for more relevant data with minimal impact on your endpoints.
Detection:
Prevention:
Detection Settings
Type
Action
File
Quarantine
Process
Terminate
Apex One automatically disables Predictive Machine Learning on Windows Server platforms. Refer to the Online Help for more information.
Exceptions
Child policies:
Inherit from parent
Extend from parent
Add File Hash
Import
Export
File Hash
File Name
Delete
No exceptions added.
Cancel


TrendAI Vision One™ Standard Endpoint Protection
Dashboard
Directories
Policies
Suspicious Object Sync
Investigation
Logs & Reports
Administration
Edit Policy: Permisos altos
Targets
ANTI-MALWARE SCANS
General Settings
Real-time Scan
Scheduled Scan
Manual Scan
Scan Now
ADVANCED THREAT PROTECTION
Behavior Monitoring
Predictive Machine Learning
Web Reputation
Suspicious Connection
Vulnerability Protection
Device Control
Application Control
DETECTION & RESPONSE
Endpoint Sensor
Sandbox Submission
EXCEPTIONS
Exception Lists
Spyware/Grayware Approved List
Web Reputation
External Agents
Internal Agents
Enable Web Reputation on the following operating systems:
Windows desktop platforms
Windows Server platforms
Note: Configure Endpoint Location settings on the Apex One web console to define how Apex Central determines which Security Agents are part of the internal network.
Query Settings
Enable assessment mode
Check HTTPS URLs
To enable checking HTTPS URLs on Chrome, Edge, and Firefox browsers, you must enable the "Unauthorized Change Prevention Service" and the "Advanced Protection Service" on Additional Service Settings.
Send queries to Smart Protection Servers
Note: This feature is only available for Security Agents that report to an on-premises Apex One server.
Security Level
High
Block pages that are:
Dangerous - Verified to be fraudulent or known sources of threats
Highly suspicious - Suspected to be fraudulent or possible sources of threats
Suspicious - Associated with spam or possibly compromised
Medium
Block pages that are:
Dangerous - Verified to be fraudulent or known sources of threats
Highly suspicious - Suspected to be fraudulent or possible sources of threats
Low
Block pages that are:
Dangerous - Verified to be fraudulent or known sources of threats
Untested URLs
Block pages that have not been tested by TrendAI™
Browser Exploit Prevention
Cancel

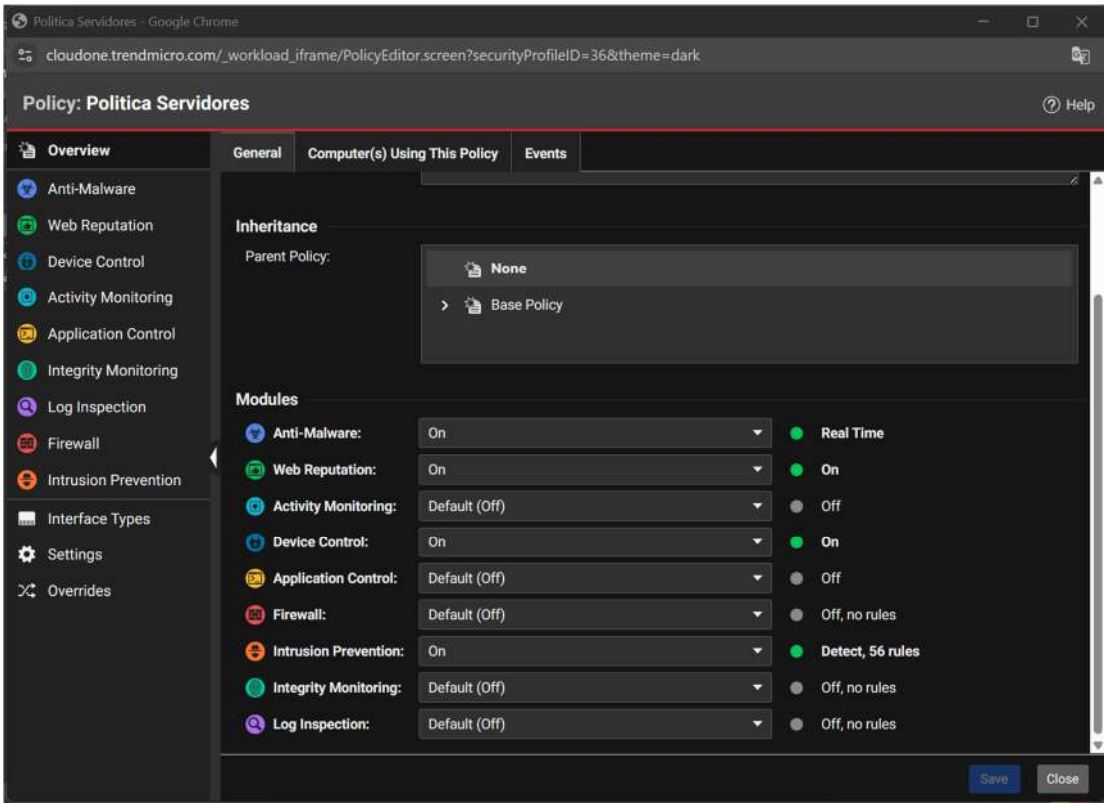

TrendAI Vision One™ Standard Endpoint Protection
Dashboard
Directories
Policies
Suspicious Object Sync
Investigation
Logs & Reports
Administration
Edit Policy: Permisos altos
Targets
ANTI-MALWARE SCANS
General Settings
Real-time Scan
Scheduled Scan
Manual Scan
Scan Now
ADVANCED THREAT PROTECTION
Behavior Monitoring
Predictive Machine Learning
Web Reputation
Suspicious Connection
Vulnerability Protection
Device Control
Application Control
DETECTION & RESPONSE
Endpoint Sensor
Sandbox Submission
EXCEPTIONS
Exception Lists
Spyware/Grayware Approved List
Suspicious Connection
Detect network connections made to addresses in the Global C&C IP list
Log and allow access to User-defined Blocked IP list addresses
Action to take
Action:
Block
Detect connections using malware network fingerprinting
Monitoring Level
Monitoring level is the degree of vigilance and strictness applied when detecting and responding to potential threats. Higher monitoring levels provide greater sensitivity but might generate a large number of nonessential logs and impact endpoint performance. TrendAI™ recommends setting your monitoring level to 2 - Moderate for more relevant data with minimal impact on your endpoints.
Detection:
Dynamic Intelligence Mode Enabled
Prevention:
Dynamic Intelligence Mode Enabled
Action to take
Action:
Block
Clean suspicious connections when a C&C callback is detected
Cancel

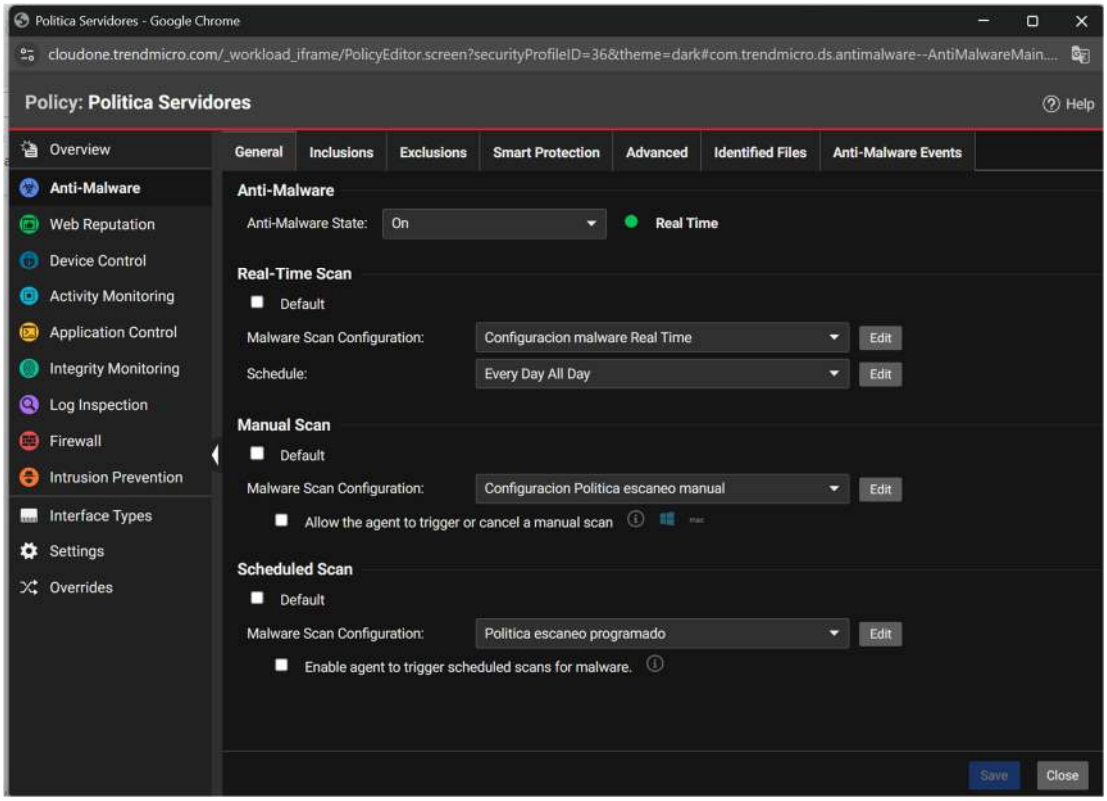

TrendAI Vision One™
Standard Endpoint Protection
Dashboard
Directories
Policies
Suspicious Object Sync
Investigation
Logs & Reports
Administration
Edit Policy: Permisos altos
Targets
ANTI-MALWARE SCANS
General Settings
Real-time Scan
Scheduled Scan
Manual Scan
Scan Now
ADVANCED THREAT PROTECTION
Behavior Monitoring
Predictive Machine Learning
Web Reputation
Suspicious Connection
Vulnerability Protection
Device Control
Application Control
DETECTION & RESPONSE
Endpoint Sensor
Sandbox Submission
EXCEPTIONS
Exception Lists
Spyware/Grayware Approved List
Vulnerability Protection
Enable Vulnerability Protection
Intrusion Prevention Rules
Network Engine Settings
Profile:
Recommended
Aggressive
View:
All
Search:
Status
Identifier
Rule Name
Application Type
Severity
Mode
Type
CVE

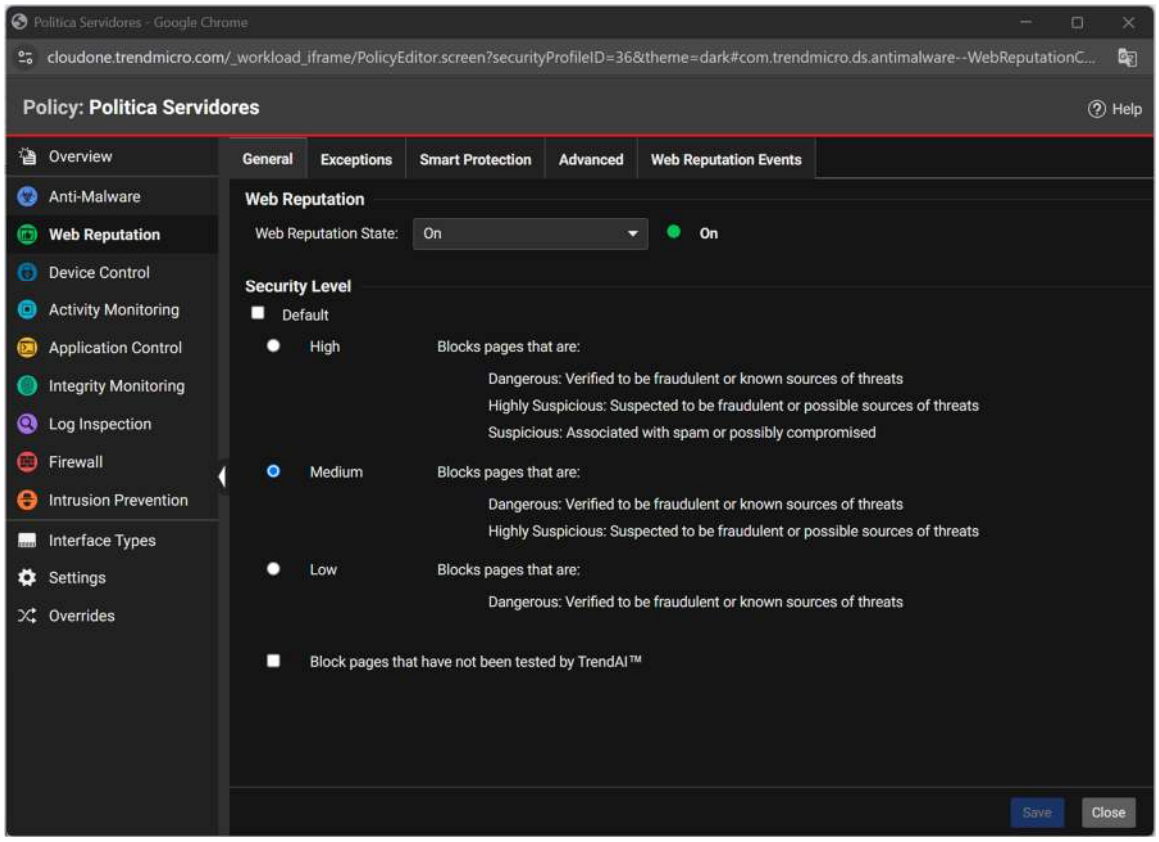

TrendAI Vision One™
Standard Endpoint Protection
Dashboard
Directories
Policies
Suspicious Object Sync
Investigation
Logs & Reports
Administration
Edit Policy: Permisos altos
Targets
ANTI-MALWARE SCANS
General Settings
Real-time Scan
Scheduled Scan
Manual Scan
Scan Now
ADVANCED THREAT PROTECTION
Behavior Monitoring
Predictive Machine Learning
Web Reputation
Suspicious Connection
Vulnerability Protection
Device Control
Application Control
DETECTION & RESPONSE
Endpoint Sensor
Sandbox Submission
EXCEPTIONS
Exception Lists
Spyware/Grayware Approved List
Device Control
Additional Services required
External Agents
Internal Agents
Enable Device Control
Apply all settings to external agents
Rules
Add
Priority
User Accounts
Device Permissions
All users (default)

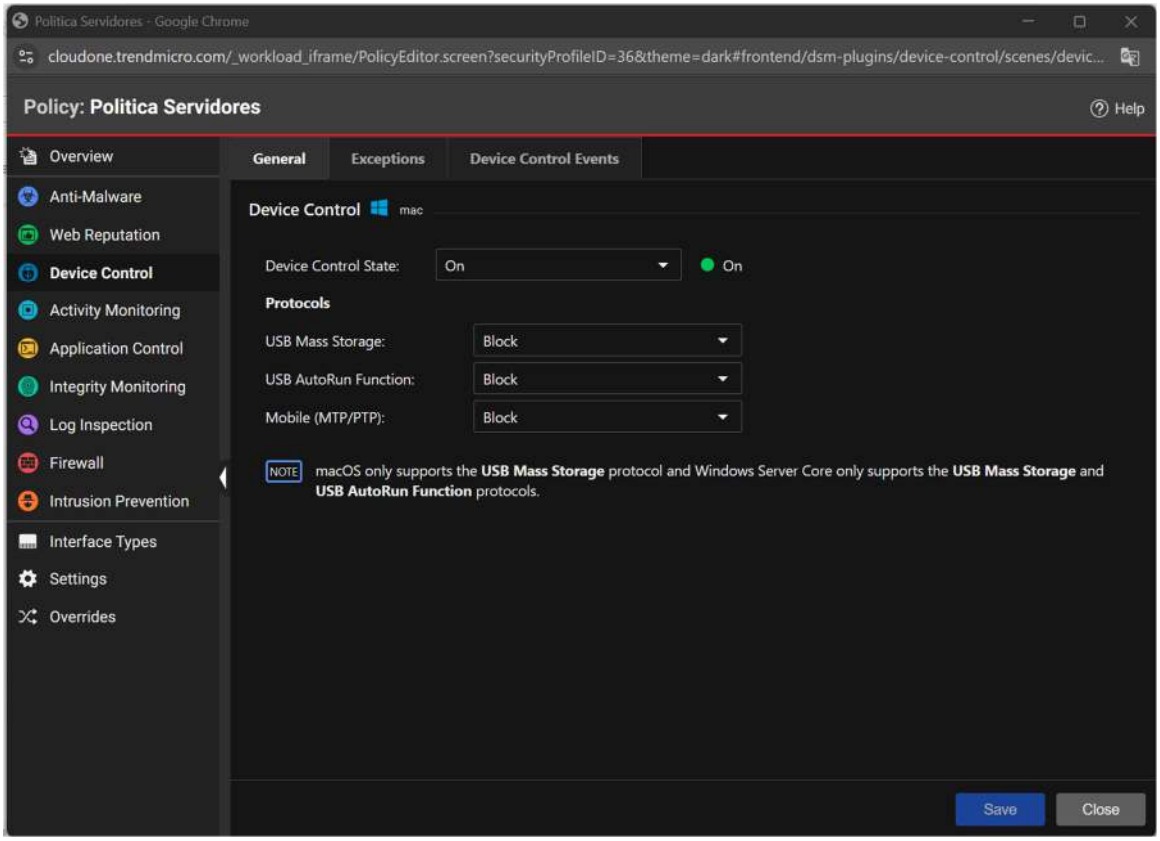

TrendAI Vision One™
Standard Endpoint Protection
Dashboard
Directories
Policies
Suspicious Object Sync
Investigation
Logs & Reports
Administration
Edit Policy: Permisos altos
Targets
ANTI-MALWARE SCANS
General Settings
Real-time Scan
Scheduled Scan
Manual Scan
Scan Now
ADVANCED THREAT PROTECTION
Behavior Monitoring
Predictive Machine Learning
Web Reputation
Suspicious Connection
Vulnerability Protection
Device Control
Application Control
DETECTION & RESPONSE
Endpoint Sensor
Sandbox Submission
EXCEPTIONS
Exception Lists
Spyware/Grayware Approved List
Application Control
Enable Application Control
User-Defined Rules
Assign Rule
Remove
Priority
User Accounts
Applied Criteria
All user accounts
Block criteria: 1
Additional Actions
Application Control takes the following action on all applications not found in the User-Defined Rules:
Allow: All other applications can execute
Lockdown: Block all applications not identified during the last inventory scan
Exclude applications by Trend Micro trusted vendors
Enable assessment mode
Agent Notifications
Display a notification when an application is blocked
Log Maintenance
Maximum log age (in days):
90
Maximum number of logs a Security Agent can send each hour per criteria:
10

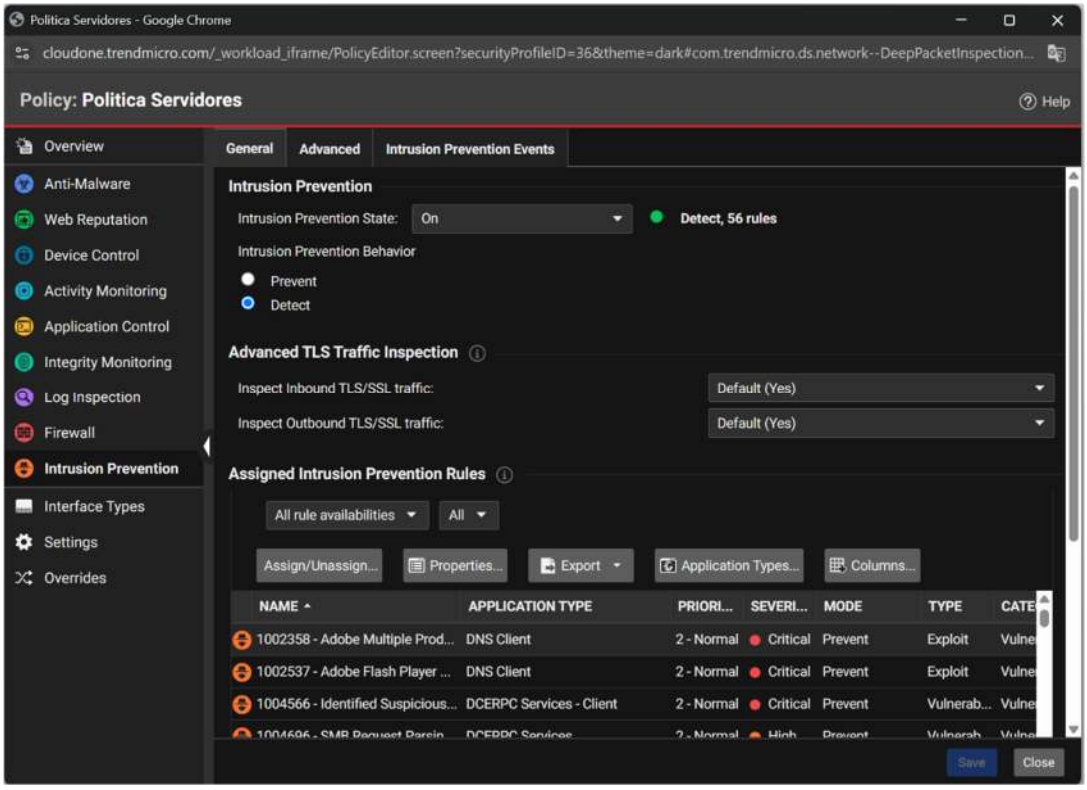
- **Creación de las políticas de seguridad servidores (100%):** Se realiza la creación de una política de seguridad para los servidores, donde se configura en motor de antimalware, web reputation, device control e intrusión prevention.



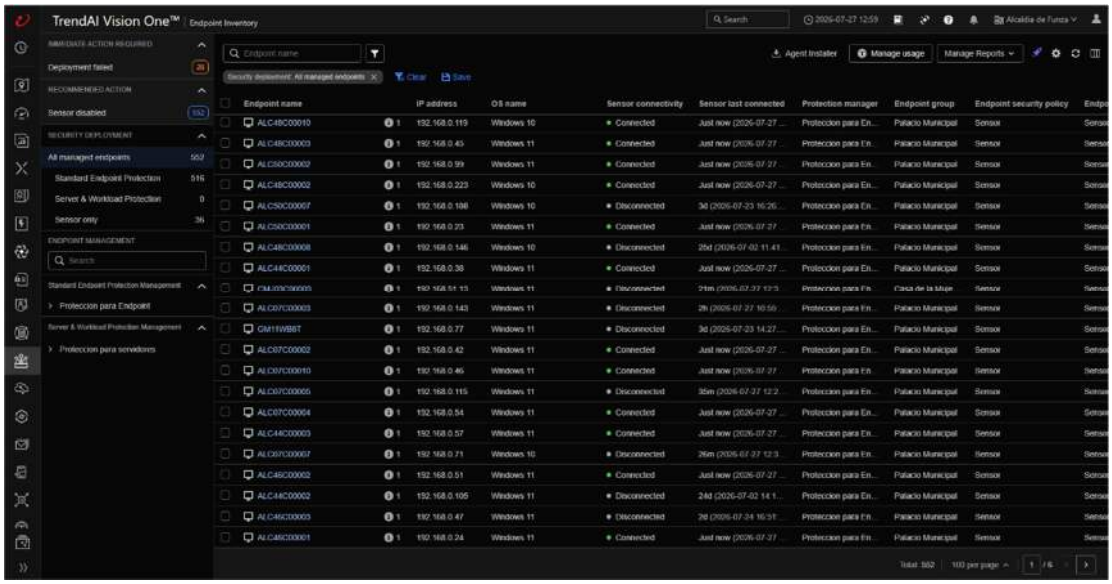



Politica Servidores - Google Chrome
cloudone.trendmicro.com/_workload_iframe/PolicyEditor.screen?securityProfileID=36&theme=dark#com.trendmicro.ds.antimalware--WebReputationC...
Policy: Politica Servidores
Help
Overview
Anti-Malware
Web Reputation
Device Control
Activity Monitoring
Application Control
Integrity Monitoring
Log Inspection
Firewall
Intrusion Prevention
Interface Types
Settings
Overrides
General
Exceptions
Smart Protection
Advanced
Web Reputation Events
Web Reputation
Web Reputation State:
On
On
Security Level
Default
High
Blocks pages that are:
Dangerous: Verified to be fraudulent or known sources of threats
Highly Suspicious: Suspected to be fraudulent or possible sources of threats
Suspicious: Associated with spam or possibly compromised
Medium
Blocks pages that are:
Dangerous: Verified to be fraudulent or known sources of threats
Highly Suspicious: Suspected to be fraudulent or possible sources of threats
Low
Blocks pages that are:
Dangerous: Verified to be fraudulent or known sources of threats
Block pages that have not been tested by TrendAI™
Save
Close


Politica Servidores - Google Chrome
cloudone.trendmicro.com/_workload_iframe/PolicyEditor.screen?securityProfileID=36&theme=dark#frontend/dsm-plugins/device-control/scenes/devic...
Policy: Politica Servidores
Help
Overview
Anti-Malware
Web Reputation
Device Control
Activity Monitoring
Application Control
Integrity Monitoring
Log Inspection
Firewall
Intrusion Prevention
Interface Types
Settings
Overrides
General
Exceptions
Device Control Events
Device Control
mac
Device Control State:
On
On
Protocols
USB Mass Storage:
Block
USB AutoRun Function:
Block
Mobile (MTP/PTP):
Block
NOTE
macOS only supports the USB Mass Storage protocol and Windows Server Core only supports the USB Mass Storage and USB AutoRun Function protocols.
Save
Close



- **Despliegue de agentes (100%):** Se realiza el proceso de implementación de los agentes de seguridad en las maquinas de la entidad, se despliega el agente sobre 552 máquinas, de las cuales 516 desplegaron con normalidad, 36 de ellas se deben aplicar parches de seguridad, retiro del antivirus anterior, y formateo.



4. Conclusiones

- Se realiza con éxito la implementación de la solución en las máquinas de la entidad.
- Se crean y despliegan con éxito las políticas de seguridad sobre las máquinas de la entidad.
- Se deben aplicar los parches de seguridad requeridos para el óptimo funcionamiento del agente sobre las maquinas con errores.
- Se debe realizar una trasferencia de conocimiento al equipo de seguridad de la entidad.

Samir Parra
Líder de Ingeniería
Softics Ingenieros

Juan Pablo Guazman
Oficina de Tecnología y Sistema
Alcaldía municipal de Funza