Advanced Reporting Tool

Transforming Data into Actionable IT and Security Insights

panda a WatchGuard brand

The Increase in the Volume of Data Managed By IT Departments Leaves Little Time to Focus on Other Critical Areas of Responsibility.

The bigger issue is that this data can be used to detect security issues and breaches caused by external factors and internal employees, but only if its managed appropriately.

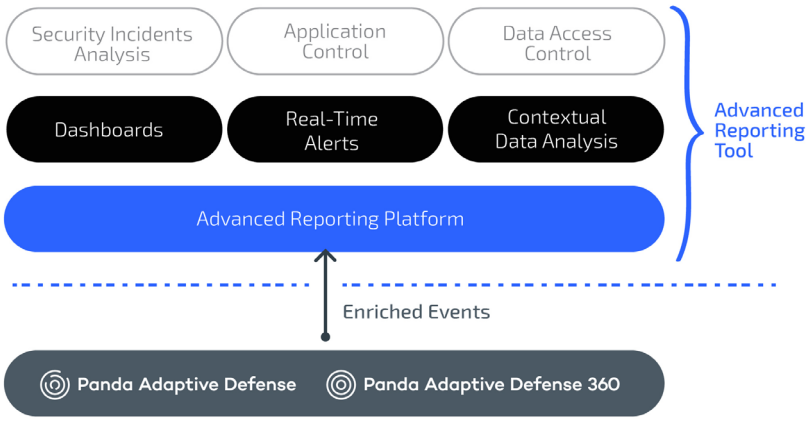
With IT departments short staffed and left to manage large volumes of data, not to mention combatting next-generation malware, it's no wonder why critical details are being overlooked. Unfortunately provides hackers the opening they need to compromise the security of the entire network. But what if there was a way to take this data and turn it into actionable tasks without overburdening the team?

The Solution: Panda Adaptive Defense 360 and Advanced Reporting Tool

The Advanced Reporting Platform automates the storage and correlation of information generated by the execution of processes and their context, extracted from endpoints by Panda Adaptive Defense 360.

This information enables **Advanced Reporting Tool** to automatically generate security intelligence and provide tools that allow organizations to **pinpoint attacks and unusual behaviors**, regardless of their origin, as well as **detecting internal misuse of the corporate network and systems**.

Advanced Reporting Tool provides organizations with the capacity to search, explore and analyze large volumes of data making IT and security insights possible in infrastructure, facilities or maintenance.



Advanced Reporting Tool provides the necessary data to draw informed conclusions about corporate IT and security management. These conclusions can then be used to define the basis of an action plan aimed at:

- **Determining the origin of security threats** and applying security measures to prevent future attacks.
- Implementing **restrictive policies for accessing critical business information**.
- Monitoring and controlling **misuse of corporate resources** that may have an impact on business and employee performance.
- **Correcting employee behavior** that is not in line with the company's usage policies.

KEY BENEFITS

1. Find Relevant Information

Maximize visibility into all events that occur on devices and increase IT department efficiency and productivity.

Access historical data to analyze corporate resource security and usage indicators.

Get in-depth information to identify security risks and insider misuse of the IT infrastructure.

2. Diagnose Network Issues

Reduce the number of tools and data sources required to fully understand what happens on devices and how this relates to the security and use of corporate assets.

Extract resource usage and user behavior patterns to demonstrate their potential business impact. Use this information to implement cost-saving policies.

3. Alert and Be Alerted

Transform anomaly detection into real-time alerts and reports.

Build business confidence by flagging security anomalies and employee misuse of IT resources in real-time.

4. Create Horizontal and Vertical Insights

Generate configurable detailed reports to perform methodical analyses of your company's security posture. Identify misuse of corporate assets and find behavioral anomalies.

Show the status of key security indicators and track their evolution over time as a consequence of the corrective actions taken.

Advanced Reporting Tool

Flexible Analytics Adapted to Your Needs

Advanced Reporting Tool (ART) incorporates dashboards with key indicators, search options and default alerts for three specific areas:

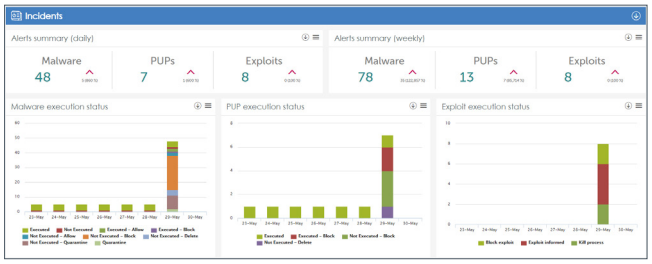
- **Security incidents**
- **Access to critical information**
- **Application and network resource usage**

Adapt **searches** and key information **alerts** to your business needs.

Security Incident Information

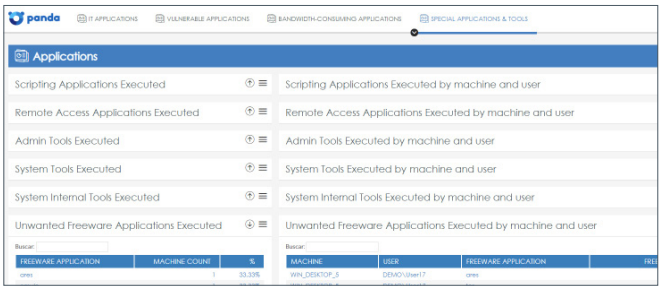
Generate security intelligence by processing and correlating the events generated during intrusion attempts:

- Calendar charts showing the Malware, PUPs and Exploits detected over the last year
- Computers with most infection attempts and malware specimens detected
- Pinpoint computers with vulnerable applications
- Malware, PUPs and exploit execution status



ART includes widgets for **Shadow IT**, giving visibility of applications executed that may be beyond the control of the IT department:

- Most and least frequently executed applications
- Scripting applications executed (PowerShell, Linux shell, Windows cmd, etc.)
- Remote access applications executed (TeamViewer, VNC, etc.)
- Unwanted freeware applications executed (Emule, torrent, etc.)



Network Resource Usage Patterns

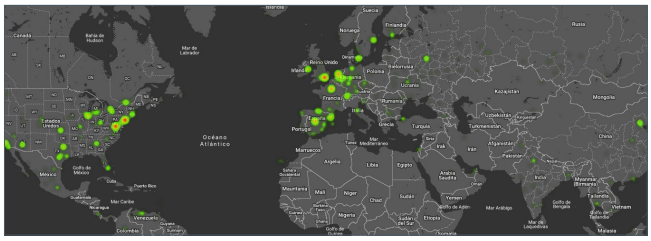
Track IT resource **usage patterns to define and enforce security policies**:

- Find the corporate and non-corporate applications running on your network
- Vulnerable applications running or installed on the network that may lead to infection or have an impact on business performance
- MS Office license control, used vs. purchased
- Applications with highest bandwidth consumption

Control Access to Business Data

Shows **access to confidential data files across the network**:

- Files most commonly accessed and run by network users
- Calendar charts and maps showing the data sent over the last year
- Find out which users have accessed specific computers on the network
- Countries receiving the highest number of connections from your network



Real-Time Alerts

Configure alerts based on events that can reveal a security breach or the infringement of a corporate data management policy:

- Default alerts indicating risk situations
- Define custom alerts based on user-created queries
- Seven delivery methods (on-screen and via email, JSON, Service Desk, Jira, Pushovery, and PagerDuty)

Supported Platforms and System Requirements for Advanced Reporting Tool:
http://go.pandasecurity.com/reporting-tool/requirements

Special applications and tool tables in Advanced Reporting Tool - Shadow IT:
http://go.pandasecurity.com/reporting-tool/tools

AWARDS AND CERTIFICATIONS

Panda Security regularly participates in and receives awards for protection and performance from Virus Bulletin, AV-Comparatives, AV-Test and NSSLabs. Panda Adaptive Defense achieved the EAL2+ certification in its evaluation for the Common Criteria standard.

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 www.watchguard.com | pandasecurity.com/business