Advanced Reporting Tool

Automated Advanced Security
Put an end to cyber threats

panda
a WatchGuard brand

THE INCREASE IN THE VOLUME OF SECURITY DATA HANDLED BY ORGANIZATIONS PREVENTS IT DEPARTMENTS FROM ADEQUATELY FOCUSING ON IMPORTANT DETAILS

This information can be used to detect security issues and breaches caused by both external factors and company insiders.

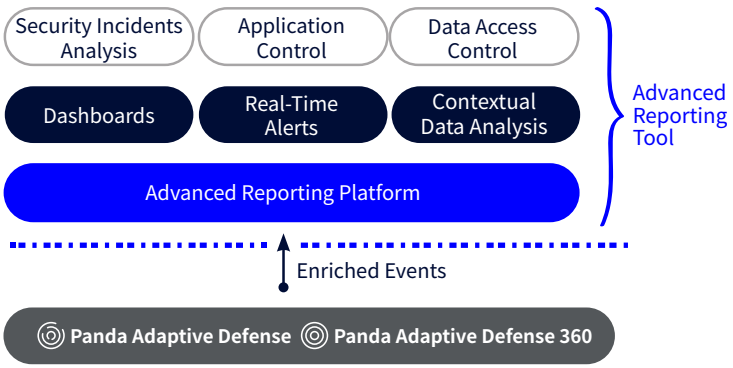
IT departments are overwhelmed: The large volumes of information handled and the appearance of next-generation malware causes many details to be **overlooked or simply not registered at all,** compromising the security of the entire system.

THE SOLUTION: PANDA ADAPTIVE DEFENSE 360 AND ADVANCED REPORTING TOOL

Advanced Reporting Tool 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.

The **Advanced Reporting Tool** provides organizations with the capacity to search, explore and analyze, offering IT and security insights without having to invest 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 **more 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 everything that occurs on every device 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, 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.

panda
a WatchGuard brand

FLEXIBLE ANALYSES ADAPTED TO YOUR NEEDS

The **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**

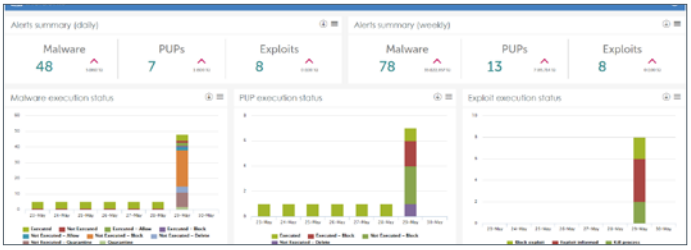
Adapt searches and key information alerts to your business needs.

SECURITY INCIDENT INFORMATION

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

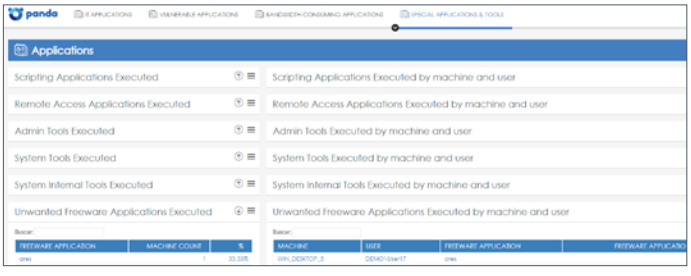
- Calendar charts showing the malware, PUPs and exploits detected over the last year.
- Computers with most infection attempts and malware specimens detected.
- Pinpoint computers with vulnerable applications.
- Malware, PUPs and exploit execution status.

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

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

- Find the corporate and non-corporate applications run on your network.
- Vulnerable applications run or installed on the network that may lead to infections, 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.
- Which users have accessed certain computers on the network.
- Countries that receive the most 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 systems requirements for ADVANCED REPORTING TOOL:
http://go.pandasecurity.com/reporting-tool/requirements

Special application and tool tables in ADVANCED REPORTING TOOL - SHADOW IT:
http://go.pandasecurity.com/reporting-tool/tools

WatchGuard

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