DATASHEET

# WATCHGUARD ADVANCED REPORTING TOOL

**Actionable IT and Security Intelligence**

## STRENGTHEN YOUR SECURITY POSTURE PROACTIVELY

The increase in the volume of security data handled by organizations prevents IT Teams from adequately focusing on essential details. This information can be used to detect security issues and breaches caused by both external factors and company insiders.

Security professionals are overwhelmed with the amount of data. The large volumes of information handled and the appearance of next-generation malware causes many details to be overlooked or not registered, compromising the entire system's security.

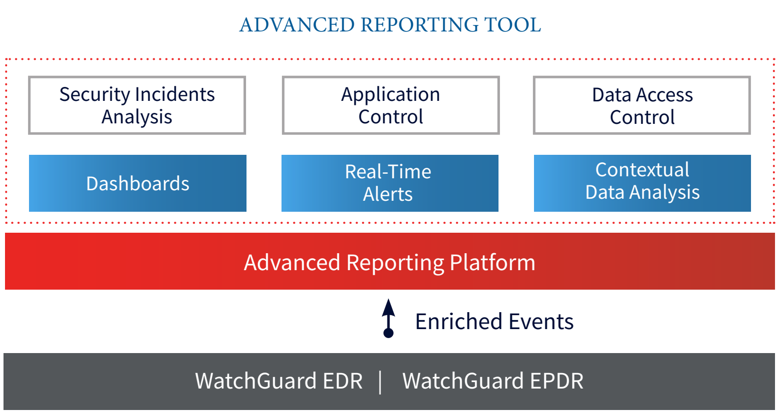
## WATCHGUARD ADVANCED REPORTING TOOL

**Advanced Reporting Tool** (ART) platform automates the storage and correlation of information generated by the execution of processes and their context, extracted from endpoints by WatchGuard EPDR and WatchGuard EDR without having to invest in infrastructure, facilities or maintenance.

This information enables **WatchGuard 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 such as:

- Determining the origin of security incidents 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

### Access to critical 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.

### Unravel network issues

- Extract resource usage and user behavior patterns. Use this information to educate users and implement cost-saving policies.
- Gain visibility into computers and applications running on your network to improve the security and control of your corporate assets.

### 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.

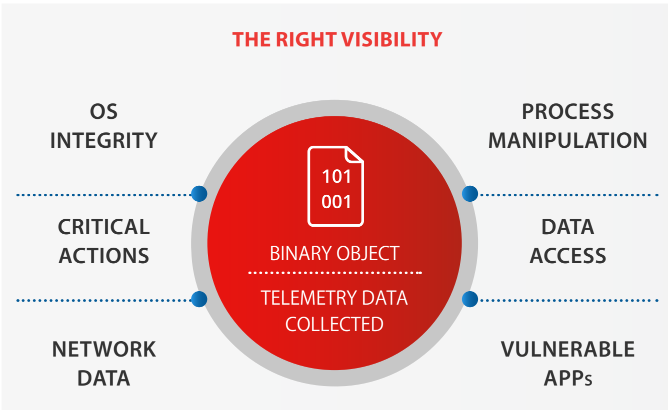
### Be prepared to face security incidents

- Generate configurable 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.

## FLEXIBLE ANALYSES ADAPTED TO YOUR NEEDS

The **Advanced Reporting Tool** incorporates dashboards with key indicators, search options and default alerts for three specific areas:

- Security incidents
- 365-day data retention storage
- Access to critical information
- Application and network resource usage
- Adapt searches and key information alerts to your business needs.



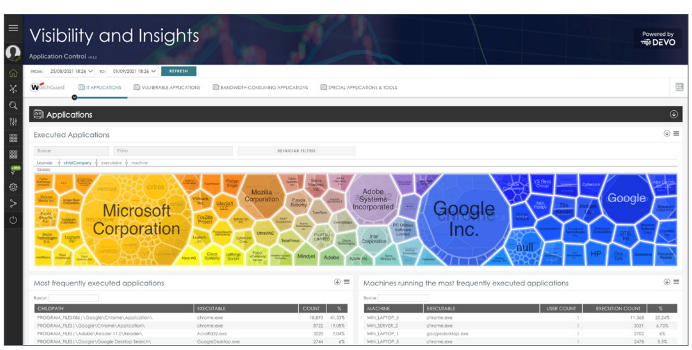

## SECURITY INCIDENT INFORMATION

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.

## SHADOW IT DISCOVERY

- 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

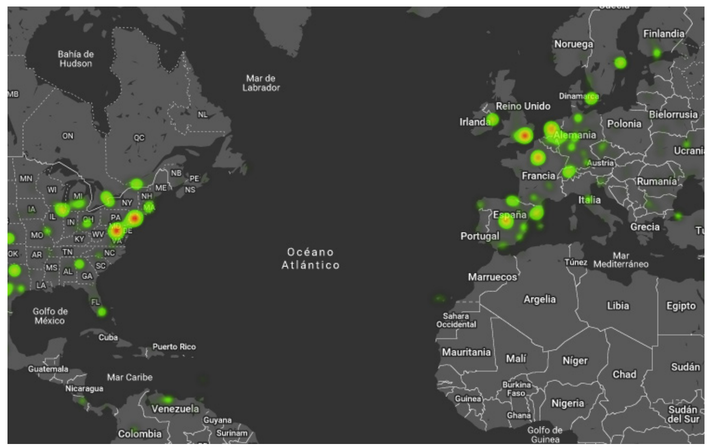
Discover IT resource usage patterns to define and enforce security policies:

- 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 of WatchGuard Advanced Reporting Tool**

**Compatible with the following solutions:** WatchGuard EDR, WatchGuard EPDR, and WatchGuard Advanced EPDR

**List of compatible browsers:**
Google Chrome and Mozilla Firefox (others may be compatible).