Advanced Reporting Tool

From Data to Actionable IT and Security Insight

The increase in the security data volumes handled by organizations prevents IT departments from adequately focusing on important details

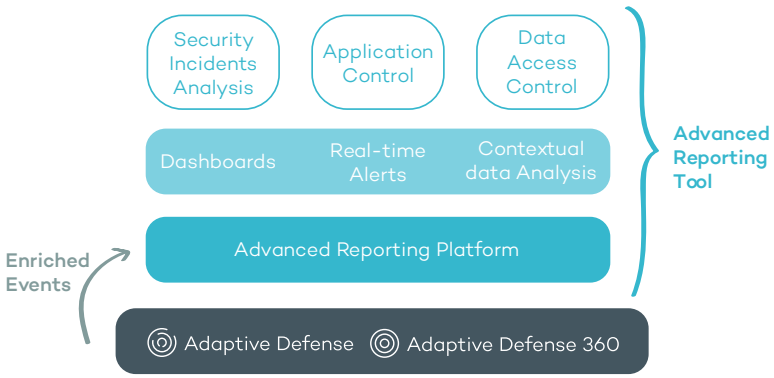
This information can be used to detect security issues and breaches caused by both external factors and company insiders.

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: Adaptive Defense and Advanced Reporting Tool

Advanced Reporting Platform automates the storage and correlation of the information related to process execution and its context extracted by **Adaptive Defense** from endpoints.

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



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 to access 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 usage policies defined.

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 its relation to the security and use of corporate assets.

Extract resource usage and user behavior patterns to demonstrate their potential business impact.

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. Report horizontally and vertically

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.

FLEXIBLE ANALYSES ADAPTED TO YOUR COMPANY'S NEEDS

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

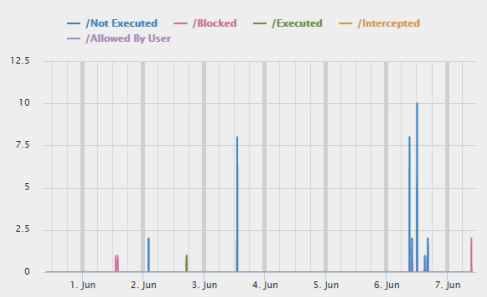
- Security incidents.
- Access to critical information.
- Application and network resource usage.

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.

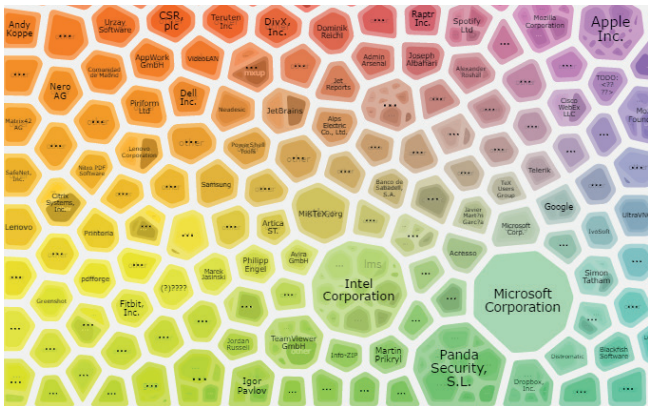
- Calendar charts showing the malware and PUPs detected over the last year.
- Computers with most infection attempts and malware specimens detected.
- Malware execution status on network computers.
- Pinpoint computers with vulnerable applications.



COST REDUCTION

Discover IT resource usage patterns to define and enforce cost reduction policies.

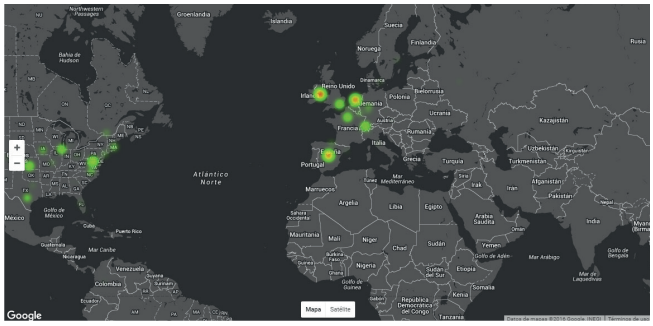
- Find the corporate and non-corporate applications run on your network.
- Office licenses used vs purchased.
- Applications with most bandwidth consumption.
- Vulnerable applications run or installed on the network that may lead to infections, have an impact on business performance or involve remediation costs.



CONTROL ACCESS TO BUSINESS DATA

Shows access to confidential data files and data leaks across the network.

- Countries that receive most connections from your network.
- Files most accessed and run by network users.
- Find out which users have accessed certain computers on the network.
- Calendar charts showing the data sent over the last year.



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).

FLEXIBLE, CONFIGURABLE, CLOUD-HOSTED BIG DATA SERVICE

- Adapted to the needs of network administrators, both regarding storage space as well as the ability to perform searches on historical data.
- Immediate startup. Doesn't require changes to the customer's network or installing additional infrastructures.
- Configurable environment, perfectly suited to the needs of the IT department.

TECHNICAL REQUIREMENTS

Supported browsers (others may also work):

- Mozilla Firefox.
- Google Chrome.

Internet connection and secure communication through port 443.

Minimum screen resolution 1280x1024 (1920x1080 recommended).

Compatible with:

- Adaptive Defense
- Adaptive Defense 360