PT ADVANCED BORDER CONTROL: KEY BENEFITS

- Identify obsolete software versions
- Uncover evidence of unauthorized access
- Detect remote access interfaces
- Expose insecure protocols
- Reveal errors in access control and network traffic filtering

CONSTANT VIGILANCE FOR YOUR PERIMETER: UPGRADE YOUR SECURITY INSIGHT WITH PT ADVANCED BORDER CONTROL

Information security teams across every sector and in all sizes of enterprise face the same challenge: protecting a constantly shifting network perimeter from external attacks. For large enterprises, getting a clear picture of the software, protocols, and remote access interfaces being used across an ever-expanding border is a relentless task.

PT Advanced Border Control (PT ABC) is a service that tackles this challenge in a single weekly scan. It provides a regular, objective, and independent assessment of perimeter security as it changes over time. Results and recommendations for mitigating risks are presented both as a report and via a web portal.

PT Advanced Border Control is available as a hosted service in the Positive Technologies infrastructure for quick and easy deployment, or can be installed in an organization's own data center.

SEE YOUR NETWORK THE WAY A HACKER SEES IT

PT Advanced Border Control monitors and assesses an organization's level of protection against Internet-based attacks. The organization's Internet-facing systems are scanned regularly from the outside to obtain the same level of information that is available to external hackers. This includes data on available network services, versions, and the many types of systems in use on the organization's perimeter such as network infrastructure, servers, and endpoints. Each of these systems may be vulnerable in its own right, be unmonitored, or be running vulnerable services.

All scan data is checked against the Positive Technologies knowledge base, a continuously updated vulnerability database, to identify any flawed elements or misconfigurations that expose the organization to risk. These may include:

- **Unidentified hosts and services** — attackers constantly search enterprise perimeters for new or vulnerable hosts and services. Enterprises must implement their own continuous monitoring to discover and identify available hosts and services so that these can be effectively secured.
- **Outdated or vulnerable software versions** — newly detected vulnerabilities in popular software products do not stay secret, so it's essential that all software installed on perimeter hosts is promptly or properly configured to reduce risk levels. Identifying software that contains critical vulnerabilities enables organizations to effectively assess and manage risk.
- **Evidence of malware infections and vulnerability to unauthorized network access** — these can be discovered during monitoring of newly opened ports (including non-standard ports) that have not been added to whitelists provided by the organization's Information Security department.
- **Remote access interfaces (SSH, Telnet, web interfaces, etc.)** — an essential tool for administrators who need remote access to devices to perform their daily tasks, these interfaces can also create great risk. Telnet, for example, is unencrypted and should not be used on the perimeter, while vulnerable versions of SSHD or the use of weak passwords/compromised certificates etc. can also be exploited by attackers. Identifying accessible interfaces, particularly those set up in violation of administrator guidelines, is essential to prevent malicious behavior including brute force attacks and attempts to obtain user credentials through phishing or traffic sniffing.
- **Insecure protocols** — these can be used by attackers to eavesdrop on confidential information.
- **Errors in access control and network traffic filtering** — misconfigurations by administrators can result in internal services accidentally being made accessible to external networks or infrastructure information being disclosed.

Customers of the hosted PT ABC service receive detailed reports prepared by the analysts in the Positive Technologies Security Operation Center (SOC). Results can also be reviewed via a web-based portal. This allows authorized users to view and filter scan results as well as to observe the dynamics of security levels over time.

The diagram below shows PT Advanced Border Control functioning as a hosted service from the Positive Technologies SOC. For more details on using this service in your own infrastructure, please contact your local Positive Technologies sales office.

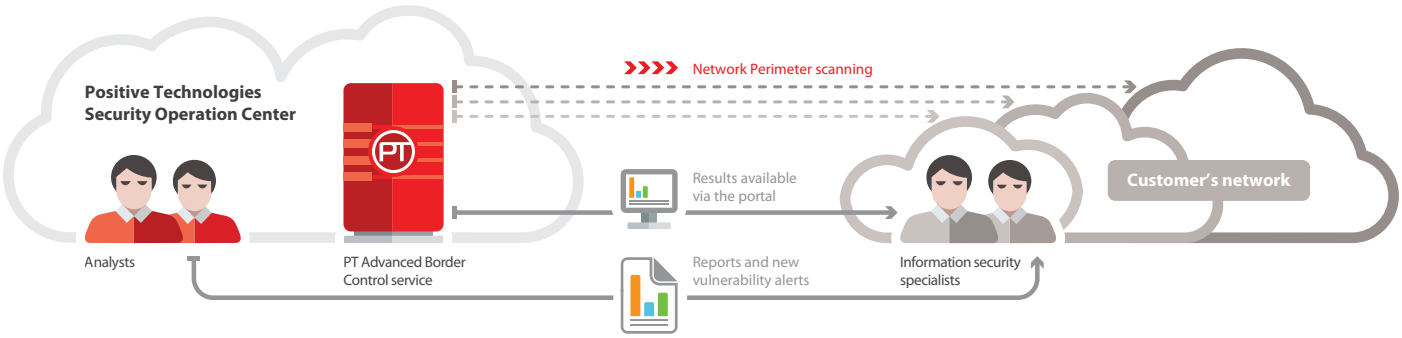

Figure 1. Architecture of Hosted Service

PT ADVANCED BORDER CONTROL SERVICE: HOW IT WORKS

Perimeter Scanning

The Positive Technologies experts work with each individual customer of PT Advanced Border Control to identify a weekly scanning schedule that meets the organization's specific needs. The scanning process for each network is divided into two stages:

1. **Identification of available network hosts.** To reduce the load on the communication channels in determining availability of network hosts, Positive Technologies sets a maximum number of packets sent per second.
2. **Identification of the available services and their versions.** Heuristic services checks are used to identify available services and their versions by fingerprints/banners. These are then compared with the database of known vulnerabilities. Vulnerability checks based on attempts to exploit the vulnerabilities are not performed to reduce scanning time and avoid possible denial of service. The Common Vulnerability Scoring System (CVSS v2) Base Score is used to calculate the risk levels of vulnerabilities.

The Positive Technologies Vulnerability Database

Whether the service is hosted by Positive Technologies or installed in a customer's data center, all scan results are compared against the unique and constantly updated Positive Technologies vulnerability database. To ensure that risks related to network services on the perimeter can be precisely assessed, the knowledge base reflects the most recent information from public sources, commercial databases, and limited-access resources as well as our own expert Positive Research team. Information is also included on known public and commercial exploits for various vulnerabilities. Additionally, all network services detected during perimeter scans are checked against a list of network services that have been deemed potentially unsafe and unsuitable for installation on the perimeter.

In the period between scans, a list of the network services currently being used by the customer is also checked regularly against the vulnerability database. If updates to the database include any new warnings about any of these services, Positive Technologies will inform the customer as soon as possible.

When information about a new critical vulnerability appears, Positive Technologies performs activities to identify services containing that vulnerability without additional scanning of the whole scope. Information on the identified vulnerabilities is provided to the customer along

with remediation recommendations. If detailed information about a new critical vulnerability is not yet available, Positive Technologies will provide information on the hosts where this potentially vulnerable service was found.

Scan Results and Reports

After each scan, the customer is provided with a differential report which allows them to track all changes on the perimeter, including those that were not authorized by the organization's Information Security department. It also contains recommendations for remediation of the identified risks.

The information is also presented in a web-based portal that provides both technical scanning details for every host and high-level security metrics. The images below provide an illustration of the graphics used to visualize the data within the web portal. These graphics can be customized according to an individual organization's needs.

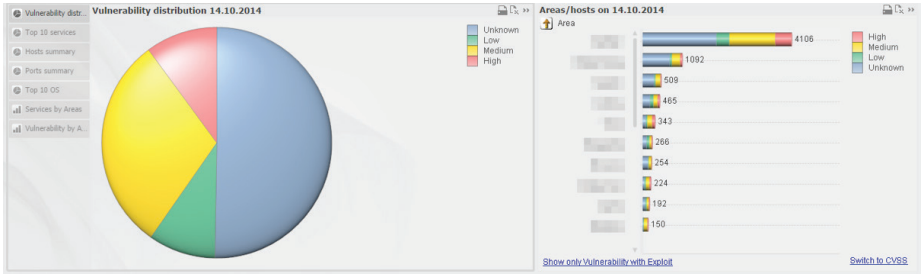

Figure 2. Samples of customizable graphics in scan results portal

In addition to the web-based portal, results from PT ABC can also be displayed and managed via a locally hosted application on the customer's site.

Classification and Filtering

All services detected during perimeter scanning are classified as either unidentified services, vulnerable services, or vulnerable services with public exploits.

The web-based portal offers various filters that can be used to view the detected network services by criteria such as protocol, port, service type, owner (operational unit), OS version, CVSS score, vulnerability, etc. The interface also allows users to set load levels for scanning.

Results are stored for the full duration of the organization's service contract, allowing users to view and filter events and changes throughout the contract period. The web portal can be used to generate differential reports using filters based on network resources or vulnerabilities. Such information can also be presented graphically as shown in the image below.

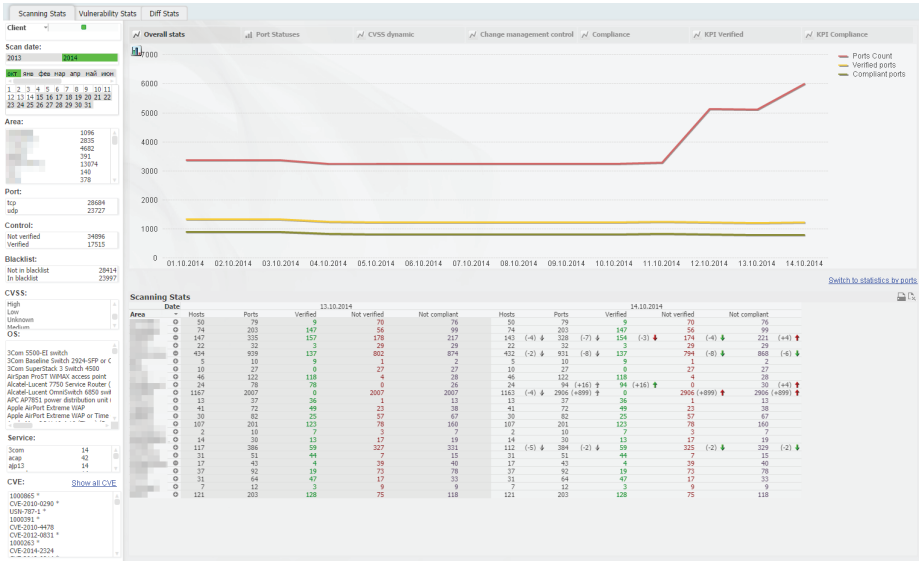

Figure 3. Scan results portal showing differential statistics over a defined date range

Compliance with Custom Requirements

Most organizations will have a set of unique requirements that they wish to use as a compliance benchmark for all hosts and services. These requirements may include the following:

- A service is not in a black list
- A service is verified
- A service does not contain critical vulnerabilities

PT Advanced Border Control automatically assesses each set of scan results for compliance with these requirements and provides an at-a-glance view of current performance.

Positive Technologies will gather information on these requirements and other important aspects of the customer's infrastructure using questionnaires prior to deployment of the service. Our experts can also provide recommendations for new requirements that should be added to your compliance regime. For example, based on our research in the field of radio telecommunication equipment security, we recommended our telecom customers to include GTP services into the scope of the monitoring service, since their availability from external networks is associated with severe risk. Similar industry-specific recommendations can be provided for customers in other sectors.

Performance and Scale

The scanning speed achieved depends on many external factors. The current scale of the Positive Technologies Security Operations Center allows us to scan several Class B networks (approximately 120,000+ hosts) per 24-hour period for a single customer. However, an unlimited number of additional scanners can be deployed if a customer requires further resources.

ADDITIONAL SERVICES

The following complementary services are available on request:

- **Detailed Vulnerability Testing of Specific Hosts —** the MaxPatrol™ vulnerability and compliance management solution is used in pentest mode to perform additional heuristic checks on a chosen set of hosts. Results are correlated and presented alongside PT ABC data in the same web portal.
- **Web Application Scanning —** detects errors in the application code and vulnerabilities related to obsolete software and misconfigurations. Identifies flaws such as SQL Injection, OS Commanding, Cross-Site Scripting, including errors leading to the threats listed in OWASP Top Ten 2013 and WASC Threat Classification.

About Positive Technologies

Positive Technologies is a leading global provider of enterprise security solutions for vulnerability and compliance management, incident and threat analysis, and application protection. Commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on Industrial Control System, Banking, Telecom, Web Application, and ERP security, supported by recognition from the analyst community. Learn more about Positive Technologies at ptsecurity.com.

POSITIVE TECHNOLOGIES

pt@ptsecurity.com ptsecurity.com