BEST PRACTICE ASSESSMENT PRIVACY

The Best Practice Assessment (BPA) evaluates Palo Alto Networks next-generation firewall (NGFW) and Panorama™ network security management configurations to identify risks and provide recommendations on how a customer can remediate issues. It consists of two components: the Best Practice Assessment itself and the Security Policy Capability Adoption Heatmap.

The BPA compares current configurations against best practices and produces a report on which best practices are—and are not—being followed. Each policy, security profile, and configuration is parsed to see if it aligns with best practices. If any do not, the BPA provides guidance on how to remediate the issue.

The Security Policy Capability Adoption Heatmap analyzes Panorama and individual NGFW configurations to determine how the customer is leveraging our prevention capabilities. The tool analyzes the rule base to identify whether our capabilities are applied where relevant. Shown in a matrix form with color coding, the Adoption Heatmap can help drive effective capability adoption on existing infrastructure. The Adoption Heatmap offers different ways to consume the information, such as filtering data by device groups, serial numbers, zones, areas of architecture, tags, and other categories. It also provides various filter options to narrow the data search to specific device groups, specific traffic between source and destination zones, to or from an area of architecture, one or more tags, etc. The Adoption Heatmap also shows trending information that tracks historical capability adoption, which helps to identify progress and rate of improvement in security posture.

Summary views provide an executive report on overall adoption, comparison to the industry average, and alignment with industry security standards, such as the NIST Cybersecurity Framework and CIS Critical Security Controls.

Information Processed by BPA

The Best Practice Assessment tool receives the Technical Support file (TSF), which is used to generate the BPA report. The TSF contains a configuration file, management and data plane program files, a few command outputs, etc.

Category	Info Sent to BPA (Based on Customer Configuration)	Example	May Be Considered or Contain Personal Information
User info	Username or User ID	jdoe	Yes
	User group name	companyA\Eng-users or companyA\domain-admins	Yes
	Admin name	srich or vsys-admin1	Yes
	Email address of recipient of report	srich@company.com	Yes
Network address	IP address (v4 or v6)	10.16.72.42	Yes
	FQDN	www.srv1.ntp.org	No

Device info	Serial number	002190357401	No
	MAC address	00:50:56:81:6f:23	No
	Hostname	FW-Dallas	No
	Zone names or names used in configuration	Trust-zone or Dmz or Vsys3	No
	UUID or CPUID	4201E4DB-4C25-BA4D-DD31-C137C718D30E or ESX:D20602003FFBA51F	No
	URL categories	Shopping, military, health-and-medicine	No

How the BPA Fits with EU Data Protection Laws

Processing personal data to ensure network and information security, including through a cloud-based data processor, is broadly recognized as a "legitimate interest" and specifically called out as such in the EU General Data Protection Regulation:

> *(49) The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned.*
>
> *This could, for example, include preventing unauthorized access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.*

Where a service provider like Palo Alto Networks processes personal data to ensure network and information security, this is a legitimate interest of the service provider and its customers. Such legitimate interest provides a basis for the processing of personal data by Palo Alto Networks under EU data protection laws.

How Palo Alto Networks Complies with Data Protection Rules

Palo Alto Networks is committed to protecting personal data stored and processed in the BPA tool. Access to the data is restricted to the Customer Experience Automation team. Access is allowed for the purpose of solving issues, troubleshooting, and improving the effectiveness of the BPA. We will not access the information in such a way as to learn meaningful information about natural persons unless necessary for the purpose of troubleshooting issues with the BPA report or its findings. The TSF is uploaded and processed in memory and never captured or stored by the BPA tool.

The BPA report is never shared with any third parties. Any data stored on or processed by Palo Alto Networks systems is secured with state-of-the-art technologies, and Palo Alto Networks operates rigorous technical and organizational security controls.

Retention

BPA reports are not retained for access at a later time. BPA data from the TSF is retained in JSON format for five years after the report is produced. Customers also have an option to "soft delete" or archive themselves any data processed by the tool to exclude it from trending and benchmarking metrics. If a customer requests to purge their data, Palo Alto Networks will do so by the next business day. Heatmap and BPA adoption aggregate data is also retained for five years.

Access by Customer

Customers can view assessment history for each TSF uploaded in the past. The assessment report contains best practice checks mapped to industry security standards, overall security posture, industry benchmarking, and detailed feature adoption views. Customers can generate a BPA report by uploading a TSF to the BPA tool.

Resources

More information about the BPA and other assessment tools is available on our Optimizing Prevention webpage.

About This Datasheet

Please note that the information provided with this paper that concerns technical or professional subject matter is for general awareness only, may be subject to change, and does not constitute legal or professional advice, warranty of fitness for a particular purpose, or compliance with applicable laws.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

best-practice-assessment-privacy-ds-031219