

# BPA Executive Summary

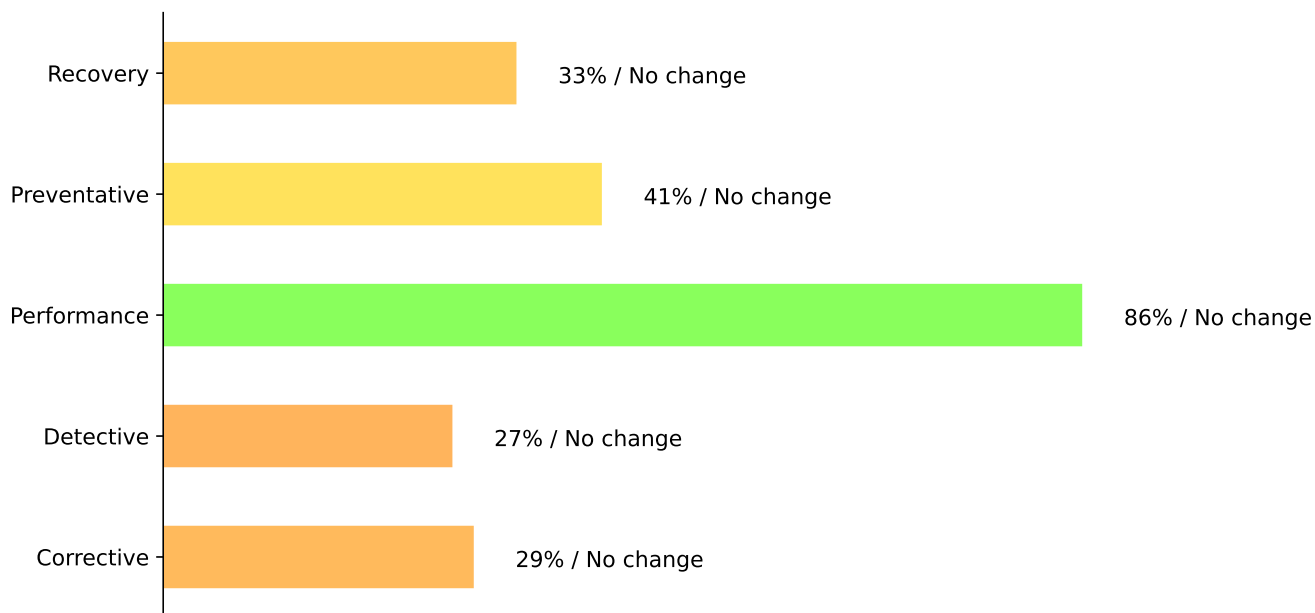
Generated On: Sep 27, 2022 @ 01:50:26 AM PDT

Device: PA-460-1 (\*\*1008539)

Version: 6.4.0

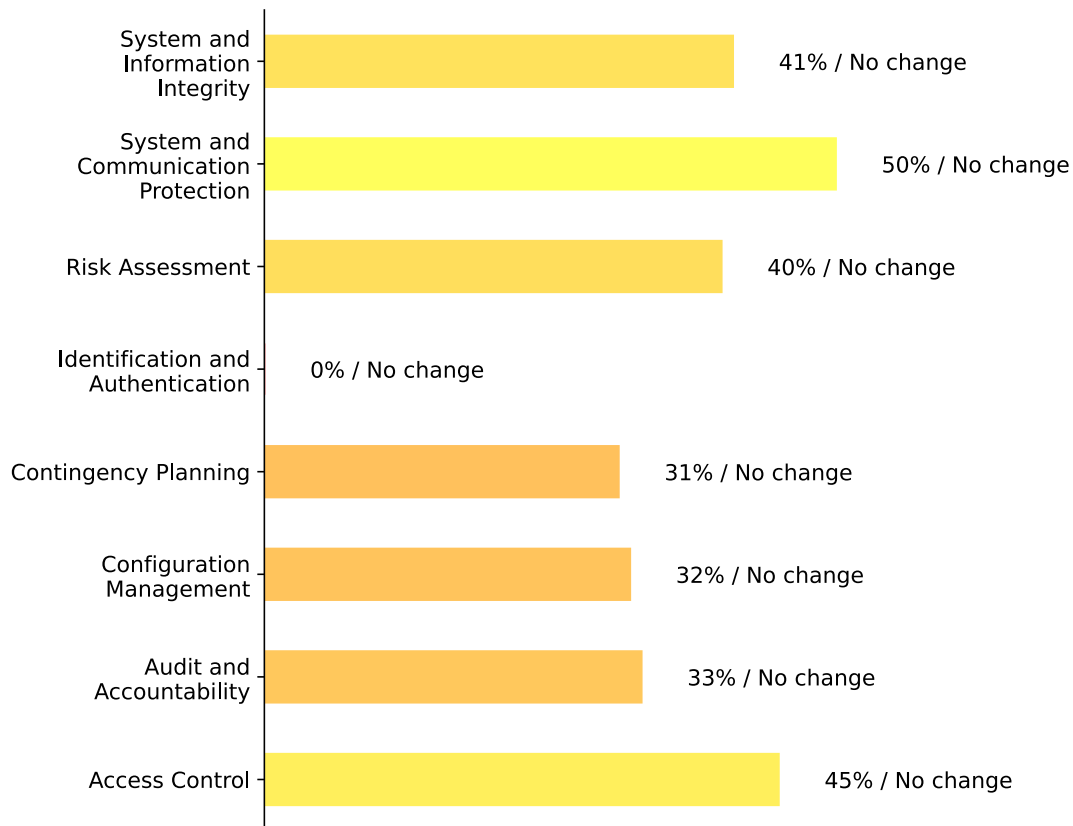
## BPA Summary

### Capability Summary



Security controls are safeguards or countermeasures put into place to reduce overall risk. Additional information available at <https://www.microsoftpressstore.com/articles/article.aspx?p=2201319>.

### NIST Security Controls

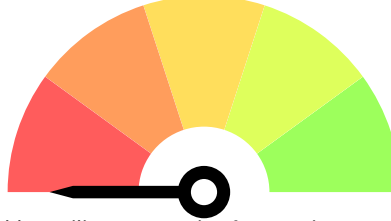


Security controls and assessment procedures for federal information systems and organizations. Additional information available at [NIST Security Controls](#).

## Class Summary

### Connectivity

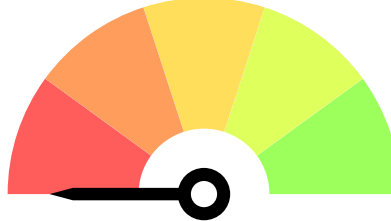
0% No change



Achieve a reliable, resilient connection from perimeter to Prisma Access.

### Infrastructure

0% No change



Optimize the Implementation, Integration and Scaling of the product.

### Management

40% No change



Management controls use planning and assessment methods to reduce and manage risk. Many provide an ongoing review of an organization's risk management capabilities.

### Operational

43% No change



Operational controls help ensure that day-to-day operations of an organization comply with their overall security plan. People (not technology) implement these controls.

### Security

0% No change



A birds eye view into Security Posture and guidance for enhancements.

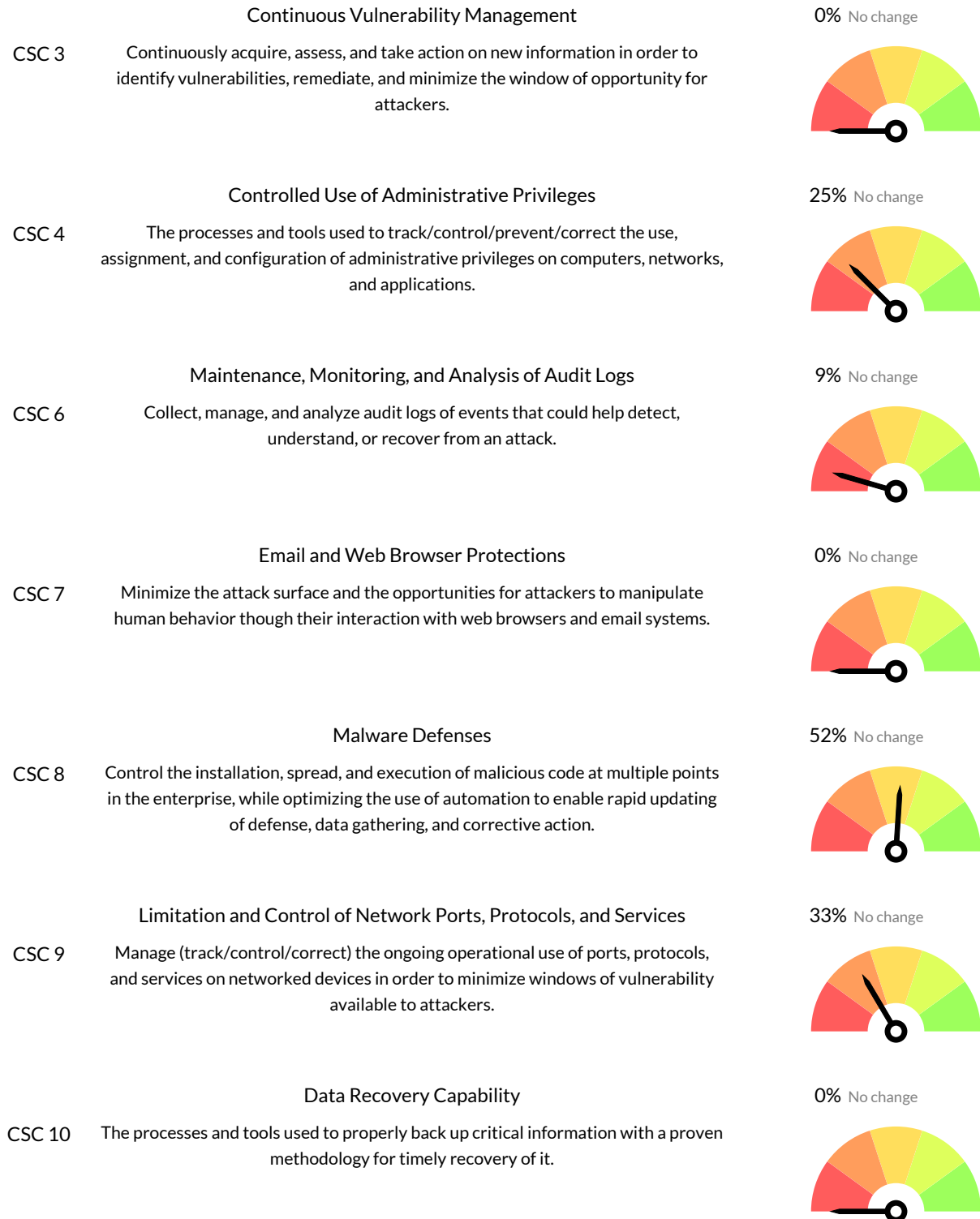
### Technical

44% No change



A technical control is one that uses technology to reduce vulnerabilities. An administrator installs and configures a technical control, and the technical control then provides the protection automatically.

## CIS Critical Security Control Summary



## Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

- CSC 11** Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

48% No change



## Boundary Defense

- CSC 12** Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

24% No change



## Data Protection

- CSC 13** The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

75% No change



## Controlled Access Based on the Need to Know

- CSC 14** The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

50% No change



## Account Monitoring and Control

- CSC 16** Actively manage the life cycle of system and application accounts - their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them.

9% No change



## Adoption Summary

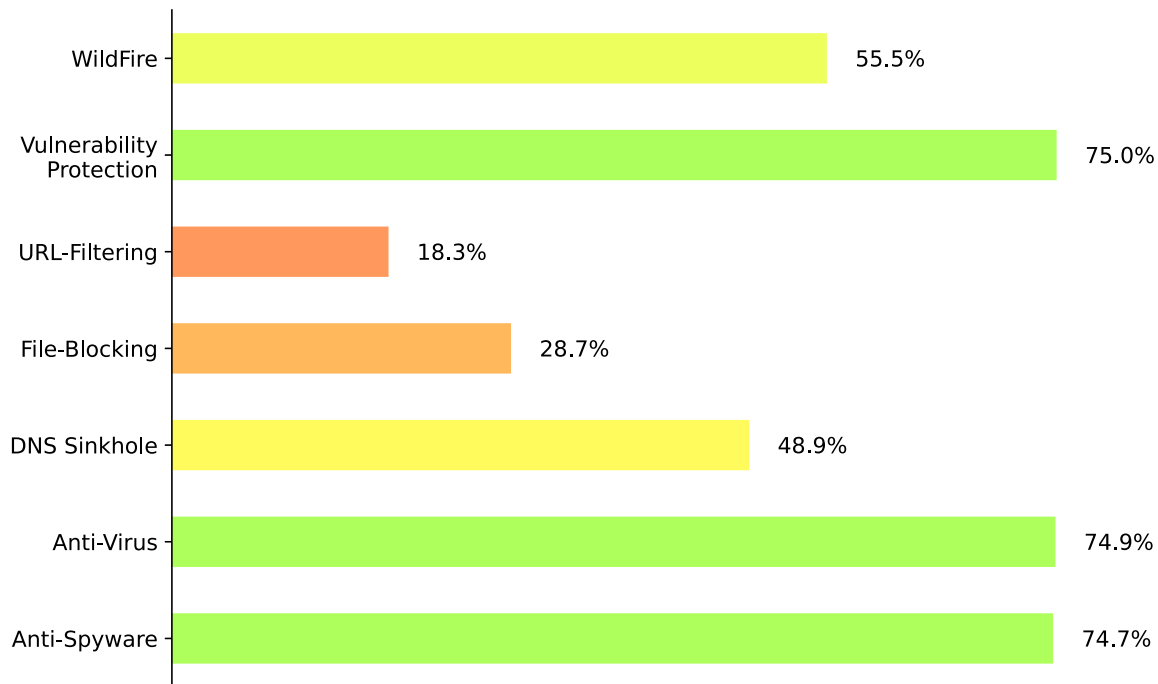
### Overall Adoption



This is the Heatmap results showing percentage of Adoption for all Security profiles applied on a firewall or Panorama.

### High Technology Adoption





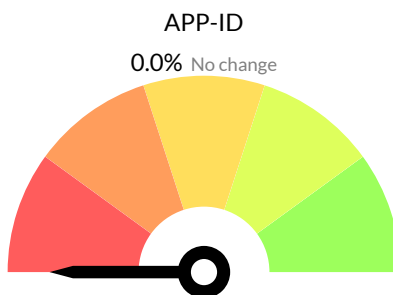
Industry Average results show how your area of business or industry is adopting security profiles on their firewall or Panorama. Industry Average data is obtained from the total Tech Support Files uploaded to Customer Success Tools. Only the Average % on Adoption is stored for providing the industry average guidance.

## BP Mode Adoption

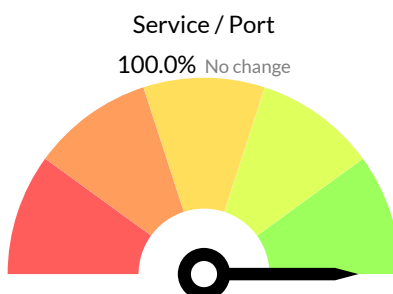


Best Practice Mode results show the effectiveness of the Security Profile Adoption. Results indicate how the security profiles adhere to Best Practice and provide the percentage of those security profiles adopting Best Practices.

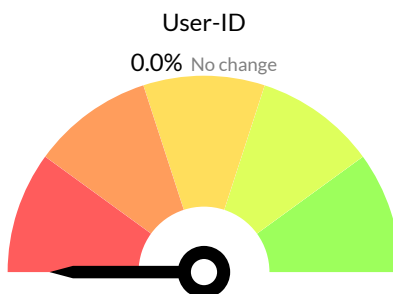
## Application & User Control Adoption



Shows adoption percentage on Application based policies in the firewall or Panorama.



Shows adoption percentage on Service or Ports on security policies in the firewall or Panorama.

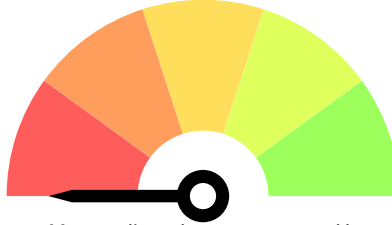


Shows adoption percentage on User or user-group based policies in the firewall or Panorama.

## Logging & Zone Protection Adoption

### Log Forwarding

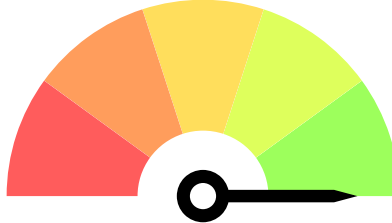
0.0% No change



Shows adoption percentage of forwarding a log to an external host. This is configured on each security policy on firewall or Panorama. Logs can be forwarded to external systems such as Panorama, Syslog server, snmp server, email server and http server.

### Logging

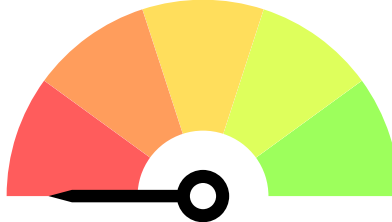
100.0% No change



Shows adoption percentage of security rule activity logging enabled at end of session on each security policy on firewall or Panorama.





### Zone Protection Profile

0.0% No change



Shows how many security policies have Zone protection profile enabled on the source zone and provides its adoption percentage.

## Decryption Summary

SSL Forward Proxy	Indicates if SSL Forward Proxy Decryption rule/s are configured on firewall or Panorama. Necessary to decrypt outbound traffic to internet for Layer 7 inspection to learn Application accurately and detect and block the threat.	 Not configured
SSL Inbound Inspection	Indicates if SSL Inbound Inspection Decryption rule/s are configured on firewall or Panorama. Necessary to decrypt inbound traffic to the servers in the company and identify applications and threat and take action as configured in policy.	 Not configured
SSH Proxy	Indicates if SSH Proxy Decryption rule/s are configured on firewall or Panorama. Necessary to block any SSH Tunnel traffic and just permit the legitimate SSH traffic in the environment.	 Not configured
Decryption Profile Used	Indicates if Decryption Profiles are applied on Decryption rule/s on firewall or Panorama. Necessary to inspect SSL/TLS protocol parameters and identify if the SSL communication is secure after reviewing the protocol version, cipher suites, Certificate verification and more.	 Not configured

URL Categories Exempted: None

URL predefined and custom categories that are being exempted from Decryption. This may be due to company policies such as compliance, privacy and other standards.

## Appendix

### Appendix - Capability

Capability	Definition
Corrective	Best Practice checks that modify the environment or fixes components after an incident has occurred to return to normal or expected working condition.
Preventative	Best Practice checks that attempts to prevent incidents before they occur. Steps taken to avoid unwanted or unauthorized activity from occurring.
Performance	Best Practice checks that intend to help increase the performance or help identify those causing performance degradation to help retain optimal performance.
Recovery	Best Practice checks that provide methods to recover from an incident.
Detective	Best Practice checks that help identify an incident's activities or help identify security violations after they have occurred.

## Appendix - NIST Security Controls

NIST Security Controls	Definition
Access Control	Best Practice checks that control access to services and resources. Security policies, Permitted IP address for management access, logon attempts, Service ports in policy etc.
Audit and Accountability	Best Practice checks that keep track of activity such as traffic flowing through the network or activity related to administrators logging into the system, changing configuration and so on.
Configuration Management	Best Practice checks that ensure baseline configuration are documented, reviewed and practiced. Checks that are part of set guidelines so the team members follow similar implementation standards that help achieve standardization, set a uniform process and help always align to the agreed process.
Contingency Planning	Best Practice checks that achieve business continuity by ensuring network devices and security controls function as expected even when process and systems gets compromised. Configuration components relating to monitoring profiles that provide fall back option if monitored system fails or High Availability functions that ensure traffic continuity without any existing sessions loss.
System and Information Integrity	Best Practice checks to ensure vulnerability and threat signatures are up to date, firmware and software are up to date, patches are always current and so on to protect the network systems from malware, exploitation and retain their integrity.
Identification and Authentication	Best Practice checks that provide access to resources only after correct identification and authentication of the users. Checks such as User based policies, Authentication policies, password complexity and so on.
System and Communication Protection	Best Practice checks that protect transmission, communication between systems, legitimate traffic and protocols only to be permitted, ensure protocol adherence, denial of service and flood protection.
Risk Assessment	Best Practice checks that take into account threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals.

## Appendix - Prior BPA Comparison

Comparison	Definition
No change	There was <u>no change</u> in the Best Practice passing percentage compared to the prior BPA report.
+ pts	There was <u>increase</u> in the Best Practice passing percentage compared to the prior BPA report.
- pts	There was <u>decrease</u> in the Best Practice passing percentage compared to the prior BPA report.