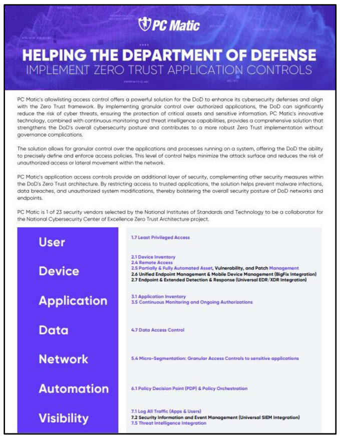

PC Matic

HELPING THE DEPARTMENT OF DEFENSE
IMPLEMENT ZERO TRUST APPLICATION CONTROLS

PC Matic's allowlisting access control offers a powerful solution for the DoD to enhance its cybersecurity defenses and align with the Zero Trust framework. By implementing granular control over authorized applications, the DoD can significantly reduce the risk of cyber threats, ensuring the protection of critical assets and sensitive information. PC Matic's innovative technology, combined with continuous monitoring and threat intelligence capabilities, provides a comprehensive solution that strengthens the DoD's overall cybersecurity posture and contributes to a more robust Zero Trust implementation without governance complications.

The solution allows for granular control over the applications and processes running on a system, offering the DoD the ability to precisely define and enforce access policies. This level of control helps minimize the attack surface and reduces the risk of unauthorized access or lateral movement within the network.

PC Matic's application access controls provide an additional layer of security, complementing other security measures within the DoD's Zero Trust architecture. By restricting access to trusted applications, the solution helps prevent malware infections, data breaches, and unauthorized system modifications, thereby bolstering the overall security posture of DoD networks and endpoints.

PC Matic is 1 of 23 security vendors selected by the National Institutes of Standards and Technology to be a collaborator for the National Cybersecurity Center of Excellence Zero Trust Architecture project.

User	1.7 Least Privileged Access
Device	2.1 Device Inventory 2.4 Remote Access 2.5 Partially & Fully Automated Asset, Vulnerability, and Patch Management 2.6 Unified Endpoint Management & Mobile Device Management (BigFix Integration) 2.7 Endpoint & Extended Detection & Response (Universal EDR/XDR Integration)
Application	3.1 Application Inventory 3.5 Continuous Monitoring and Ongoing Authorizations
Data	4.7 Data Access Control
Network	5.4 Micro-Segmentation: Granular Access Controls to sensitive applications
Automation	6.1 Policy Decision Point (PDP) & Policy Orchestration
Visibility	7.1 Log All Traffic (Apps & Users) 7.2 Security Information and Event Management (Universal SIEM Integration) 7.5 Threat Intelligence Integration

Helping the Department of Defense Implement Zero Trust Application Controls

Thank you for downloading this PC Matic product sheet. Carahsoft is the distributor for PC Matic cybersecurity solutions, available via NASA SEWP V, NCPA, ITES-SW2, and other contract vehicles.

To learn how to take the next step toward acquiring PC Matic's solutions, please check out the following resources and information:

For additional resources:
carah.io/pc-maticresources

For upcoming events:
carah.io/pc-maticevents

For additional PC Matic solutions:
carah.io/pc-maticsolutions

For additional cybersecurity solutions:
carah.io/cybersecuritysolutions

To set up a meeting:
PCMatic@Carahsoft.com

To purchase, check out the contract vehicles available for procurement:
carah.io/pc-maticcontracts

For more information, contact Carahsoft or our reseller partners:
PCMatic@Carahsoft.com | 703-889-9825

HELPING THE DEPARTMENT OF DEFENSE
IMPLEMENT ZERO TRUST APPLICATION CONTROLS

PC Matic's allowlisting access control offers a powerful solution for the DoD to enhance its cybersecurity defenses and align with the Zero Trust framework. By implementing granular control over authorized applications, the DoD can significantly reduce the risk of cyber threats, ensuring the protection of critical assets and sensitive information. PC Matic's innovative technology, combined with continuous monitoring and threat intelligence capabilities, provides a comprehensive solution that strengthens the DoD's overall cybersecurity posture and contributes to a more robust Zero Trust implementation without governance complications.

The solution allows for granular control over the applications and processes running on a system, offering the DoD the ability to precisely define and enforce access policies. This level of control helps minimize the attack surface and reduces the risk of unauthorized access or lateral movement within the network.

PC Matic's application access controls provide an additional layer of security, complementing other security measures within the DoD's Zero Trust architecture. By restricting access to trusted applications, the solution helps prevent malware infections, data breaches, and unauthorized system modifications, thereby bolstering the overall security posture of DoD networks and endpoints.

PC Matic is 1 of 23 security vendors selected by the National Institutes of Standards and Technology to be a collaborator for the National Cybersecurity Center of Excellence Zero Trust Architecture project.

User	1.7 Least Privileged Access
Device	2.1 Device Inventory 2.4 Remote Access 2.5 Partially & Fully Automated Asset, Vulnerability, and Patch Management 2.6 Unified Endpoint Management & Mobile Device Management (BigFix Integration) 2.7 Endpoint & Extended Detection & Response (Universal EDR/XDR Integration)
Application	3.1 Application Inventory 3.5 Continuous Monitoring and Ongoing Authorizations
Data	4.7 Data Access Control
Network	5.4 Micro-Segmentation: Granular Access Controls to sensitive applications
Automation	6.1 Policy Decision Point (PDP) & Policy Orchestration
Visibility	7.1 Log All Traffic (Apps & Users) 7.2 Security Information and Event Management (Universal SIEM Integration) 7.5 Threat Intelligence Integration

PC Matic

Pillar 1

PC Matic's allowlisting allows agencies to control which applications and devices are allowed to access their networks, based on the identity of the user or device. Ensuring that only authorized users and devices can access sensitive data.

Pillar 2

PC Matic's trust nothing - verify everything approach to security, ensures that only trusted devices are allowed to connect to an agencies network of applications. If a device is found to be infected, compromised, or vulnerable, IT admin can swiftly remove allow policies to restrict that compromised device from accessing applications.

Pillar 3

PC Matic's default-deny approach to application security, helps with the implementation of micro-segmentation by allowing agencies to create granular access controls to applications found in different parts of their networks. This helps to isolate sensitive data and applications from other parts of the network, making it more difficult for attackers to gain access to them.
PC Matic's integrated software inventory scanner, allows agencies to have continuous visibility into what software assets are installed, authorized, and validly signed.

Pillar 4

PC Matic's allowlisting aides in implementing data access controls by allowing agencies to create authorization policies to applications containing sensitive data. Protecting sensitive data from being exposed to unauthorized users or devices.

Pillar 5

PC Matic incorporates granular access controls, allowing federal agencies to precisely define and enforce access policies for their sensitive applications. With granular controls, administrators can establish specific rules and restrictions on user access, such as defining authorized individuals or groups, time restrictions, and even geolocation-based access policies. This fine-grained access management assists in micro-segmentation efforts, and enhances security by ensuring that only authorized personnel can access critical applications, reducing the risk of data breaches or unauthorized modifications.

Pillar 6

PC Matic promotes automated monitoring by providing agencies with continuous visibility into all application traffic that is authorized across their networks. Allowing organizations to identify and respond to threats more quickly. PC Matic's policy orchestration grants agencies the ability to streamline authorization to individual users, departments, locations, and multiple facilities instantly with minimal effort required.

Pillar 7

PC Matic logging and reporting features enable heightened response tactics by providing agencies with the enhanced visibility and automated application reporting capabilities they need to quickly identify and respond to security incidents and suspicious lateral movement. This real-time and customizable reporting minimizes the impact of security incidents and to get back up and running quickly.

About Us

PC Matic provides organizations of all sizes with zero trust endpoint protection through a patented approach to application allowlisting that is developed and supported exclusively in the United States.

Contract Vehicles

- DOD ESI BPA
- CDM DEFEND
- GSA Schedules
- NASA SEWP V
- GSA 2GIT
- ITES-SW

Certifications

- FedRAMP Authorized
- NIST 800-171 Compliant
- FIPS 140-2 Compliant
- SVAR • STS
- NMSDC
- PCI-DSS Compliant

Available in FedRAMP Cloud and On-Premises
Protecting our Nations Windows, Mac, and Linux Devices

TEST
av-test.org
2022
AWARD
ADVANCED PROTECTION
PC Matic
Application Whitelisting

TEST
av-test.org
2022
AWARD
BEST PERFORMANCE
PC Matic
Application Whitelisting

Start your free trial today - to see why Federal agencies are layering PC Matic in their Zero Trust Architecture.

pcmatic.com

sales@pcmatic.com