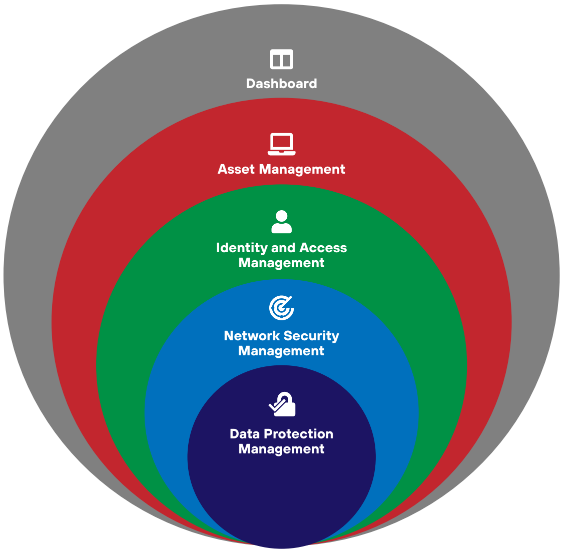
Software Asset Management

There is a solution to defeating and preventing ransomware. It is called Software Asset Management, fully funded through the Department of Homeland Security and mandated by law for civilian agencies.

Continuous Diagnostics and Mitigation

Through the CDM Program, all civilian agencies are required to deploy Software Asset Management Solutions to meet NIST 800-53 CM 7 (5) (b) Employ a deny-all, permit-by-exception policy.


Dashboard
Asset Management
Identity and Access Management
Network Security Management
Data Protection Management

The CDM Program was developed by DHS in 2012 to support government-wide and agency-specific efforts to provide risk-based, consistent, and cost-effective cybersecurity solutions to protect federal civilian networks across all organizational tiers.

DHS's goal, now implemented through CISA, is to provide an additional layer of standardized tools to enhance each agency's security and governance of cybersecurity without increasing the agency's budget.

The first two years of SWAM adoption are fully funded through the CDM Program. Without cost inhibiting this decision, civilian agencies are free from the largest barrier to adding SWAM and quickly slowing the ransomware spread.

What is SWAM?

Software Asset Management puts each agency's IT organization squarely in control by strictly allowing authorized applications to execute on the network. If any program attempts to run without prior approval, it is blocked and hence no ransomware can enter the network.

Despite a superior security architecture that prevents ransomware, SWAM solutions created governance challenges in blocking too many good applications reducing user productivity while increasing IT frustration.

Lower Costs

A focus on prevention using a default-deny approach through SWAM can drastically lower security costs and human hours needed to investigate and contain rogue applications. Permitting only by exception means less activity on the network, less alerts inside the SOC, and less time spent reacting to events.

PC Matic solves historical SWAM governance issues through our global allowlist and state-of-the-art remediation

NIST

In August 2020, NIST selected PC Matic to be one of 18 cybersecurity companies to design its Zero Trust Center of Excellence, the security operations center (SOC) of the future. PC Matic is the only application allowlisting company on the team.

For over a decade, PC Matic has curated a master list of 26M commonly used, high prevalence good applications which reduces the governance challenges allowing IT to focus on the lower prevalence, and custom software running in its user base. In the event that a good application is indeed blocked, PC Matic employs the latest web technologies allowing the block to be remediated in seconds facilitating superior governance while reducing IT and user frustration.

With Application Allowlisting, our agent provides a deny-all permit-by-exception environment to control what can run on each endpoint. Backed by our Global Allowlist Intelligence, it comes without governance headaches from traditional Application Allowlisting.

PC Matic is FedRAMP approved and available through the FedRAMP Marketplace in an On-Prem and Gov Cloud offering to allow complete flexibility to meet the needs of all civilian agencies.

Contact Us

TONY GAGE
Director, Federal Sales
443-983-5347
tony@pcmatic.com

ZACK AUSTIN
Vice President
352-530-6199
zack@pcmatic.com

PC Matic

PC Matic is 100% developed and supported in the USA, delivering products with a secure supply chain.

Learn more at pcmatic.com