NEWS

Strategic Solutions Unlimited
910-222-8138
info@ssuinc.us

CIGENT, AVANAN, PC MATIC AND STRATEGIC SOLUTIONS UNLIMITED JOIN FORCES TO PROVIDE ONE-STOP SHOP FOR CYBERSECURITY MATURITY MODEL CERTIFICATION

Cybersecurity Innovators Offer Compliance Solutions To Organizations Serving DoD Defense Industry Base

FORT MYERS, FLA. – (April 28, 2021) – Four key players representing critical areas of cybersecurity technology have joined forces to offer a "one-stop-shop" for organizations seeking Cybersecurity Maturity Model Certifications (CMMC) required to do business with the DoD Defense Industrial Base (DIB). The Cigent, Avanan, PC Matic and Strategic Solutions Unlimited partnership provides a comprehensive CMMC compliance service backed by years of industry expertise and government/military-grade technology that defends government- created or -owned Controlled Unclassified Information (CUI) against any cyberthreat vector.

CMMC was established to enhance the protection of sensitive information through five cyber hygiene levels. Each level builds on the previous one and has its own domain requirements. The Department of Defense (DoD) specifies the required level needed for suppliers to participate in specific contracts that require them to handle both CUI and Federal Contract Information (FCI). CMMC compliance also requires vendors to have an approved "technology stack" – a set of cybersecurity products that, along with other hygiene requirements, protect CUI and FCI. Developing the stack and achieving compliance can prove difficult for many organizations which led to the formation of the "one-stop-shop" approach. Complete information on the one-stop-shop and overall CMMC compliance can be found here.

Through the partnership, Cigent, Avanan, PC Matic and Strategic Solutions provide affordable, cloud managed, solutions that target exact requirements for any desired level of compliance. The partnership also enables organizations to efficiently put technology stacks in place that are compatible and properly integrated. This approach enables organizations to affordably achieve compliance at the highest of CMMC levels without the burden of searching for, deploying, and managing one-off solutions.

"This one-stop-shop managed solution provides DIBs with an easy-to-implement, affordable cyber stack that will allow them to more efficiently pursue CMMC compliance," said Bradley A. Rowe, Cigent CEO and co-founder. "We're excited to partner with cyber industry leaders Avanan, PC Matic and SSU to offer this unique approach to what can often be a complicated and challenging compliance processed."

Avanan – Email and File Share Security

The #1 breach threat for users is phishing emails that aim to steal sensitive information. Malware incidence also occurs often where viruses hide in emails and act upon opening. Avanan recognizes these urgent dangers and tackles cyber-attacks through proactive email security that captures, scans, and remediates targeted issues before attacks get to your inbox. If the email is not malicious, it gets delivered. To ensure you're not exposed from any angle, these security measures extend to internal, inbound, and outbound emails, as well as collaboration on file share apps. Avanan's "Complete Malware" service option covers level 3email protections and sandboxing for the following domain: System and Information Integrity (SI)

Cigent – CUI Protection and Network Security Monitoring

Cigent's Dynamic Data Defense Engine™ (D³E): Protection of CUI is a critical requirement of CMMC level 3. Cigent's Dynamic Data Defense Engine™ (D³E) Zero Trust file access controls utilize multi-factor authentication to protect CUI from data theft and ransomware, even if a system is compromised. Its authentication capabilities also allow individuals or organizations of all sizes to encrypt and control access to sensitive files. Those files can be securely stored in any location and shared with only trusted users.

Cigent Secure SSD™: Cigent Secure SSDs also protect CUI. This first and only family of self-defending storage devices have cybersecurity built into the firmware itself. They include a dedicated security processor that relies on machine learning to detect and respond to ransomware, a keep-alive sensor that automatically encrypts sensitive files if security software is bypassed, and a "safe room" that makes data invisible to any attacker. When paired withD³E, sensitive data stays protected throughout the entire device lifecycle

Cigent for Networks™ (C4N): The C4N service offers network security monitoring and features several layers of advanced network detection and response technology, fully managed by Cigent cybersecurity experts 24/7.Best of all, C4N is affordable, easy to install, and immediately effective.

Cigent technology meets CMMC controls for levels 1-3 and addresses the following domains: Access Control (AC), Audit and Accountability (AU), Security Assessment (CA), Configuration Management (CM), Identification and Authentication (IA), Incident Response (IR), Maintenance (MA), Media Protection (MP), Risk Management (RM), System and Communications Protection (SC), System and Information Integrity (SI).

PC Matic – Whitelist Management

Similar to how a firewall uses a deny-all, allow-by-exception approach to only allow approved traffic onto a network, whitelisting is the act of employing a deny-all, allow-by-exception security posture at the endpoint. A deny-all approach is the only way to proactively prevent threats; all other detect-and-respond approaches (e.g., EDR, MDR, TDR, XDR, etc.) require the threat to occur before they can counter it. Thanks to its global and patented digital-code-signing-certificate lists, PC Matic's whitelisting removes deployment and maintenance headaches that are common with other whitelisting technologies. PC Matic is available as a complete endpoint protection product or as a bolt-on complimentary product. It meets CMMC controls for levels 1-3 and addresses the following domains: Access Control (AC), Audit and Accountability (AU), Configuration Management (CM), Media Protection (MP), Risk Assessment (RM) and System and Information Integrity (SI).

ONE-STOP CMMC COMPLIANCE
2-2-2-2-2

SSU – Physical Security

Physical security protects physical assets that may reside in server rooms, private areas, or even in a home. If security measures are not up to par, there's no way to target threats and see their origination point. SSU understands physical security concerns and specializes in finding the right solutions for information systems and maintaining CMMC requirements. Through awareness training in security concepts such as situational response and threat analysis, SSU teaches organization how to mitigate risks. SSU also demonstrates how to develop programs to execute for finding and managing threats. SSU's services meet CMMC controls for levels 1-3 and address the following domains: Access Control (AC), Awareness and Training (AT), Media Protection (MP), Physical Protection (PE), Personnel Security (PS)

About Avanan

Avanan catches the advanced attacks that evade default and advanced security tools. Its invisible, multi-layer security enables full-suite protection for cloud collaboration solutions such as Office 365, G-Suite and Slack. The platform deploys in one click via API to prevent Business Email Compromise and block phishing, malware, data leakage, account takeover and shadow IT across the enterprise. Avanan replaces the need for multiple tools to secure the entire cloud collaboration suite, with a patented solution that goes far beyond any other Cloud Email Security Supplement.

About Cigent

Cigent is an In-Q-Tel-backed cybersecurity company founded by data recovery, storage, and cyber threat experts that protect businesses and individuals against any threat vector, even after a security breach. Cigent Data Defense solves more than three decades of failure by the cybersecurity industry to prevent ransomware, data theft, and insider theft by placing protection as close to the data as possible - inside the firmware of storage devices - and adds Zero Trust multi-factor authentication that protects data at the endpoint, on the network, in the cloud, or when shared with trusted users. Cigent Data Defense is comprised of Cigent's D^{3}E® (Dynamic Data Defense Engine™) Windows®-based software and Cigent's self-defending Secure Solid-State Drives (SSDs). For more information, please visit https://www.cigent.com/.

About PC Matic

About PC Matic: PC Matic was established in 1999 by its current CEO, Rob Cheng. The American company, with operations based across the United States, was established with the sole purpose of creating a better way to diagnose common computer problems. As cyber security threats began to evolve, PC Matic knew a new approach to thwart these attacks was critical. This led to the creation of its award-winning security software in 2011. Entirely developed, researched and supported in the United States, PC Matic features a globally automated whitelist technology, fileless malware detection, and RDP port protection from brute force attacks. Together, these technologies provide the best security protection for endpoint devices around the globe. For over 20 years, PC Matic has continued to evolve, making them an innovative provider of cloud-based security solutions for homes, businesses of all sizes, and government agencies.

About Strategic Solutions Unlimited

Strategic Solutions Unlimited, Inc. (SSU) was established to provide specialized support to the Intelligence and SOF communities. SSU provides world-class Intelligence, Electronic Security

Systems services, modular structures and SCIFs, information technology, network engineering, intelligence training, advisory services and other specialized OCONUS operations. SSU has since brought those refined capabilities to a broader client base throughout the Department of Defense and across Federal agencies.

# # #

Cigent, Secure SSD, D^{3}E, and Dynamic Data Defense Engine are registered trademarks of Cigent Technology, Inc. in the United States and other jurisdictions. All other trademarks, trade names, or service marks used or mentioned herein belong to their respective owners. The Cigent products mentioned in this release may be covered by one or more patents, including at least U.S. Patent Nos. 10437983, 10521611, 10282117, and 10095431 with additional patents pending in the U.S., Europe, Japan, Israel, and other jurisdictions.