WHITE PAPER

Velo3D Sapphire Printers

Pioneering Secure Metal Additive Manufacturing with DoD Green-Level STIG Compliance

VELO 3D

Velo3D.com

Table of Contents:

Introduction	03
Understanding the Significance of STIG Compliance	04
Green-Level STIG Compliance: A Milestone for Velo3D	05
Securing the Future of Metal Additive Manufacturing	05
Technical Deep Dive: Velo3D's STIG Compliance Journey	06
Benefits of STIG Compliance for Velo3D Customers	08
Conclusion	10

Introduction

The landscape of metal additive manufacturing (AM) is rapidly evolving, revolutionizing the production of complex, high-performance parts for critical applications.

However, with this advancement comes the growing need to secure these systems and processes against increasingly sophisticated cyber threats. Velo3D is a leading innovator in this field, offering a unique metal 3D printing solution that delivers superior performance and unmatched security.

This white paper focuses on the groundbreaking achievement of Velo3D's Sapphire family of printers: becoming the first and only AM printer to achieve the U.S. Department of Defense's (DoD) Green-level Security Technical Implementation Guide (STIG) compliance.

> With AM advancement growing comes the need to secure systems and process against sophisticated cyber threats."

Understanding the Significance of STIG Compliance

Developed by the Defense Information Systems Agency (DISA), STIGs are comprehensive documents outlining secure configuration standards for a wide range of information systems and devices. They encompass various aspects, including operating systems, applications, network configurations, and security tools.

Achieving STIG compliance, particularly a high score, signifies a system's robust security posture and alignment with the DoD's stringent cybersecurity requirements.

Green-Level STIG Compliance: A Milestone for Velo3D

Velo3D's Sapphire family of metal 3D printers holds the distinction of being the first to achieve Green-level STIG compliance. Velo3D's achievement is particularly noteworthy because it surpasses the Green-level threshold of 90% with an average score of 97%.

This exceptional outcome demonstrates the company's commitment to building printers using the security by design principles.

Securing the Future of Metal Additive Manufacturing

As metal AM plays an increasingly critical role in producing defense components and other sensitive parts, cybersecurity becomes paramount. STIG compliance provides a validated framework to mitigate cyber vulnerabilities inherent in metal AM, such as:

- **Protecting Digital Design Files**: These files contain vital intellectual property and sensitive data. If compromised, they could lead to significant national security risks. STIGs provide guidelines for secure storage, transmission, and access control of these digital assets.

- **Networked AM Systems:** Modern AM systems often involve remote monitoring and control capabilities, introducing potential vulnerabilities to cyberattacks. STIGs help safeguard against unauthorized access, data breaches, distributed denial-of-service attacks (DDoS), and potential damage to AM machines.

Technical Deep Dive: Velo3D's STIG Compliance Journey

Velo3D's achievement of Green-level STIG compliance underscores its dedication to building secure metal AM solutions. Key aspects of this accomplishment include:

Rigorous Evaluation Process:

- A comprehensive assessment was conducted against established STIG benchmarks. This in-depth evaluation provided a clear picture of the printers' security posture.

Exceptional Score:

- Velo3D surpassed the DoD's Green-level threshold of 90% by achieving an average score of 97% across the entire Sapphire printer family (Sapphire, Sapphire 1MZ, Sapphire XC, and Sapphire XC 1MZ).

SCAP Test:

- Scope for Security Content Automation Protocol (SCAP) tests included Build PC and Motion PC. SCAP Compliance Checker 5.6 was run locally on the printers for conducting the STIG compliance tests.

  - STIGs were applied to the printer using the Microsoft Powershell desired state configuration as well as local security policy.
  - No errors or warnings were discovered during the SCAP audit. See figure 2 below for STIG compliance scores.

STIG checklists evaluated included:

- MS_Dot_Net_Framework: This relates to the Microsoft .NET framework
- MS_Edge_STIG: This relates to the Microsoft Edge web browser
- Windows_10_STIG: This relates to the Windows 10 Operating Systems
- Windows_Defender_Antivirus: This relates to the Windows Defender Anti-virus
- Windows_Firewall_with_Advanced_Security: This relates to the Windows Firewall

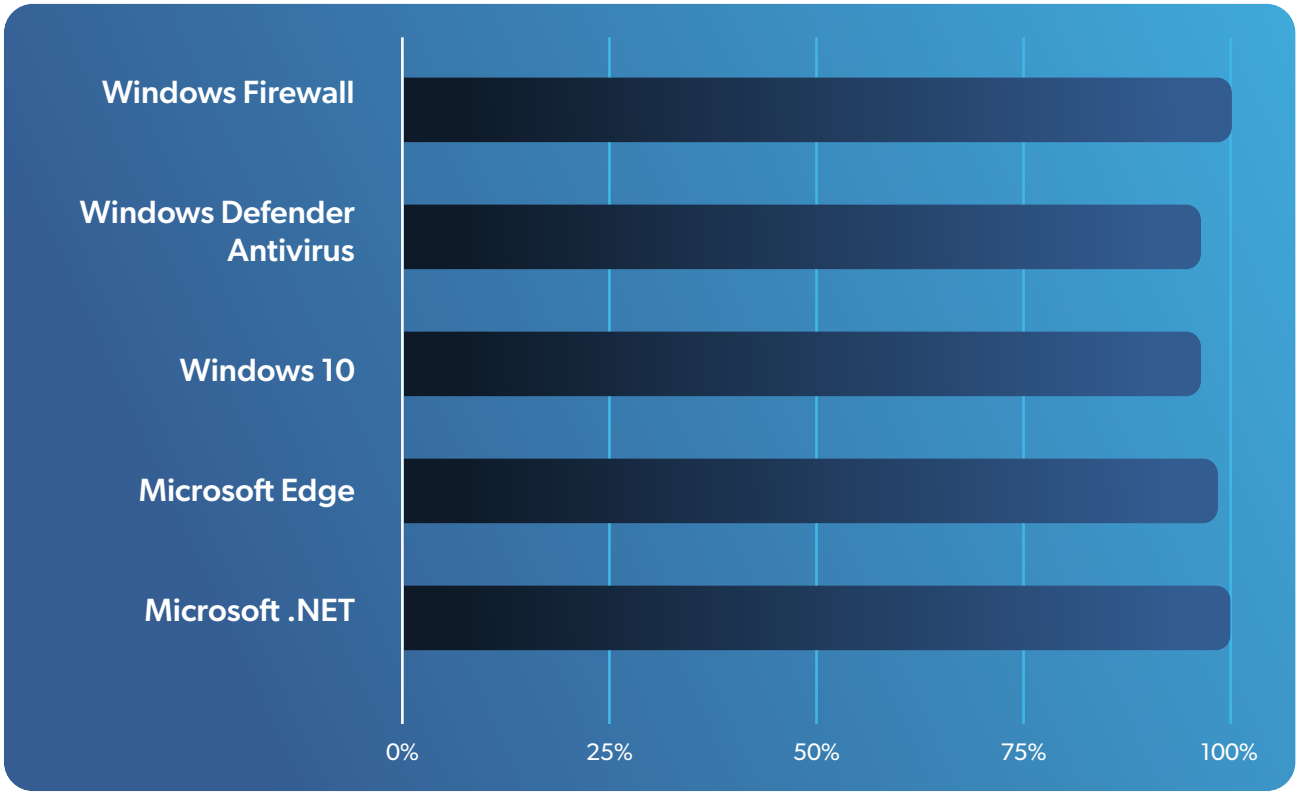

Figure 1: Bar graph representation of STIG scores

Stream	Score	Errors	Warnings
MS_Dot_Net_Framework	100	0	0
MS_Edge_STIG	97.96	0	0
Windows_10_STIG	93.33	0	0
Windows_Defender_Antivirus	92.68	0	0
Windows_Firewall_with_Advanced_Security	100	0	0

Figure 2: STIG compliance scores

Benefits of STIG Compliance for Velo3D Customers

Velo3D's Sapphire printers, with Green-level STIG compliance (90% - 99% score), unlock significant advantages for its customers, particularly government agencies, defense contractors, and other security-conscious organizations:

ENHANCED NETWORK CONNECTIVITY

Without STIG compliance, government agencies and contractors using metal 3D printers were required to keep them disconnected from network connections. This technique commonly referred to as Air-gapping, can complicate the process of managing printers. In the case of Velo3D, engineers and printer operators could not fully leverage the capabilities of its fully integrated solution, which enables users to easily monitor the printing of parts, analyze the data generated in the printing process, and transfer print files to and from printers.

- Green-level STIG compliance allows Velo3D printers to connect securely to the DoD's classified SIPRNet and non-classified NIPRNet networks. This eliminates the need for air-gapping, enabling users to leverage the full potential of Velo3D's fully integrated solution for improved efficiency and streamlined workflows.

- Now, with Velo3D, engineers can utilize all aspects of metal additive manufacturing technology when manufacturing parts that are classified or International Traffic in Arms Regulation (ITAR) protected, without risking stolen intellectual property or other cyberattacks.

STREAMLINED ACQUISITION

DoD agencies and contractors often face complex procurement processes when acquiring technology that doesn't meet stringent security standards. Non-compliant equipment typically requires special exceptions or waivers, leading to delays and administrative hurdles.

Green-level STIG compliance removes this obstacle for Defense contractors and agencies to purchase Sapphire printers as they will no longer have to obtain exceptions and other approvals that are required for non-compliant printers.

ELEVATED SECURITY POSTURE

Cybersecurity threats are a constant concern for organizations handling sensitive data. Green-level STIG compliance signifies that Velo3D printers are fortified against cyberattacks, protecting critical information used in defense applications and intellectual property related to cutting-edge technologies.

This alignment with stringent security requirements also ensures compliance with International Traffic in Arms Regulations (ITAR) for safeguarding technology with national security implications.

INDUSTRY BENCHMARK

Beyond the immediate benefits for defense and government agencies, Velo3D's STIG compliance serves as a valuable security benchmark for various industries.

Organizations across diverse sectors that utilize metal AM technology can leverage this achievement as a reference point when assessing the security posture of their own systems and devices. This demonstrates Velo3D's commitment to prioritizing robust cybersecurity practices across the metal AM landscape.

UPGRADE PATH FOR EXISTING CUSTOMERS:

Velo3D recognizes the value proposition of STIG compliance for all its customers. Current Velo3D customers can easily upgrade their existing Sapphire printers to achieve STIG Green-level security. The software upgrade can be completed with minimal impact on the customer.

Conclusion

Velo3D has achieved a major milestone by reaching Green-level STIG compliance for its Sapphire family of metal 3D printers, marking a turning point in the industry. This achievement enables government agencies, contractors, and all security-conscious customers to confidently utilize the full potential of our metal AM technology. With printers hardened against cyberattacks and critical data secured, they can concentrate on innovation and manufacturing excellence.

Ready to Learn More About Velo3D?

Let us help you with your most challenging and innovative projects.

Contact us today to schedule a consultation or to learn more about our fully integrated metal AM solution.

Without Compromise

Headquarters
2710 Lakeview Court
Fremont, CA 94538

Contact Us:
velo3d.com
info@velo3d.com