UltiMaker white paper

Secure 3D printing: Safeguarding IP and mission-critical operations

Contents

EN 09/2025

Introduction

With additive manufacturing moving from a prototyping tool to a core manufacturing technology used in various sectors, such as defense, aerospace, and healthcare, the need for secure solutions is increasing.

While such a transformation brings speed, flexibility, and new dimensional opportunities, it also presents new vulnerabilities. Confidential prototypes, designs, and intellectual property (IP) can now be shared, stolen, or at risk of being compromised. Choosing an additive manufacturing solution that supports the safekeeping of intellectual property, both on a software and physical level, is crucial to ensure operational continuity.

In this white paper, we will present the most important aspects of security in 3D printing and how to adopt a secure 3D printing ecosystem to your organization. We will also deep-dive into how UltiMaker tackles the current security challenges that defense, manufacturing, and other sectors might face.

Part 1

The security landscape for 3D printing

When talking about security in the realm of additive manufacturing, there are several factors to consider before adopting 3D printing technology, especially in high-security sectors. Ensuring the confidentiality, integrity, and availability of both digital assets and printed parts is critical, particularly when producing functional components for aerospace, medical, or defense applications.

Software security

In the context of 3D printing, software security means ensuring that every stage of the digital manufacturing chain – from CAD design to slicer software to printer firmware – is safeguarded against cyber threats. Poorly secured software can expose organizations to theft of sensitive IP, sabotage of production files, or insertion of hidden defects into parts.

Software security considerations include:
- Encryption of design files and print data
- Access control and authentication
- Regular software updates and patch management

Hardware security

Hardware security refers to the tangible product security. Ensuring robust hardware security and sound manufacturing practices is essential to maintain the integrity of devices and their outputs. Given the risks of tampering, unauthorized access, and compromised production, hardware security safeguards the printer's physical and operational reliability, helping prevent disruptions from malicious interference or errors and reducing vulnerabilities within the supply chain.

Hardware security considerations include:
- Manufacturing certifications
- Tamper resistance
- Firewall Integration

1.3 Compliance & regulatory requirements

Compliance and regulatory requirements ensure that additive manufacturing processes and outputs meet industry-specific standards for safety, reliability, and traceability. In high-security or highly regulated sectors (e.g., aerospace, medical, defense), following these requirements is not just a legal obligation but a safeguard against operational and reputational risks.

Part 2

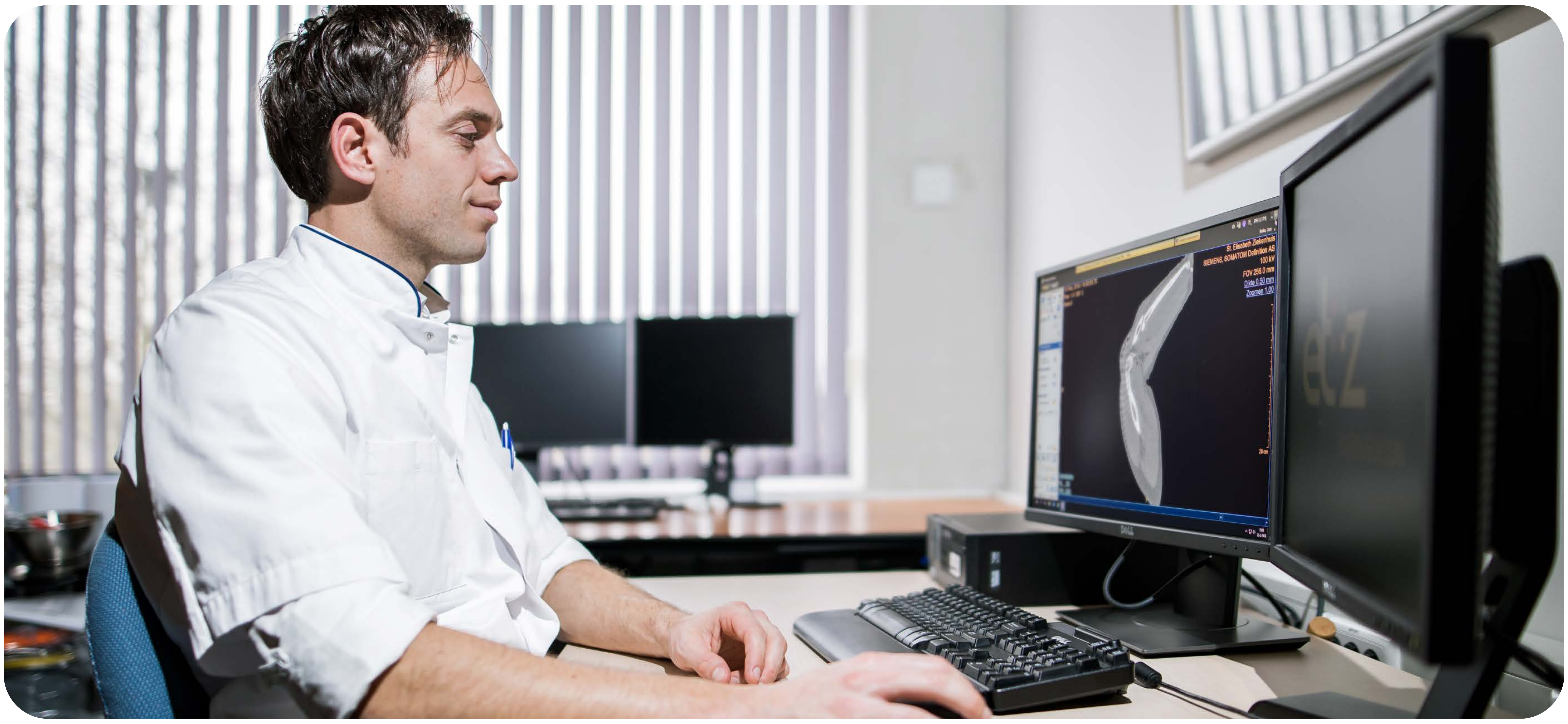
Security needs of high-risk and data-sensitive sectors

When adopting additive manufacturing in industries where failure is not an option, security is not just a feature – it's a requirement. Defense, aerospace, healthcare, and highly regulated manufacturing sectors deal with sensitive designs, intellectual property, and mission-critical parts. Any compromise – whether digital or physical – can result in safety risks, financial losses, or operational setbacks.

Defense

Key security needs. Protection of proprietary designs, prevention of sabotage, traceability of parts, compliance with classified data regulations, and technological sovereignty. In these sectors, maintaining full control over sensitive data and production processes is critical.

Risks if neglected. Unauthorized access to digital part libraries, malicious alterations that could cause part failure, or loss of readiness due to tampered maintenance workflows. Without sovereignty, organizations risk exposing confidential data to foreign jurisdictions or external providers, undermining both national security and operational independence.



Healthcare & medical devices

Key security needs. Patient data protection, compliance with GDPR and medical device regulations, and ensuring sterility and integrity.

Risks if neglected. Breaches of sensitive patient data, compromised tools or implants, and loss of trust in digital health solutions.

General manufacturing & supply chain

Key security needs. Intellectual property (IP) protection, secure workflows across distributed production networks, and safeguarding proprietary tooling or fixtures.

Risks if neglected. Counterfeiting, IP theft, or maliciously modified parts entering the production line, potentially halting manufacturing processes or lowering product quality.

Common threads across high-risk industries

Despite operating in different environments, these sectors share four overarching security priorities:

Confidentiality
Ensuring sensitive design files and data remain protected.

Integrity
Making sure parts are printed as intended, without tampering or hidden defects.

Availability
Securing systems and printers against downtime that could disrupt critical operations.

Sovereignty
Having full control over the entire process.

Part 3

Building security into 3D printing systems

Security is more than just a feature – it's a foundation. In professional 3D printing, where intellectual property and sensitive data are central to daily operations, trust in the technology depends on how well it protects users and their work.

UltiMaker incorporates industry-recognized standards and independent security testing into both hardware and software, while manufacturing in Europe under strict quality controls. From protecting digital workflows in the cloud to safeguarding hardware against tampering, UltiMaker ensures that every layer of its ecosystem is designed to give organizations confidence that their data, processes, and devices remain secure.

Software security measures

When proprietary designs and sensitive workflows are at stake, robust software security is essential. UltiMaker aligns its security practices with globally recognized standards and regulations, including ISO/IEC 27001 for Information Security Management, ISA/IEC 62443-4-2 for industrial cybersecurity, and the General Data Protection Regulation (GDPR) to ensure that customer data is processed transparently, securely, and without third-party interference.

- **Principle of Least Privilege (PoLP).** Applied across UltiMaker Digital Factory and UltiMaker Cura Enterprise, PoLP restricts access based on roles (admin, member, and guest), ensuring only authorized users can perform sensitive operations
- **Third-party security assessments.** UltiMaker has conducted independent audits to identify vulnerabilities and prioritize fixes for medium and high-risk issues
- **No network security dependency.** UltiMaker printers are designed with support for offline operation

> "Using UltiMaker, we have actually saved €350,000 in our production facilities by increasing the yield of our products and eliminating a number of safety hazards."
>
> – Job van de Sande, Head of Technology Sealing and Polymer at ERIKS

Hardware security measures

By combining European manufacturing excellence, rigorous quality standards, and robust hardware, we ensure the highest possible degree of security and quality in our manufacturing processes by incorporating tamper-resistant designs, secure firmware, and compliance with regulations like the Machinery Directive (2006/42/EC).

- **Tamper resistance.** UltiMaker printers are designed for trusted environments but include features to minimize unauthorized physical access, such as:
  - Restricted access to certain settings via PIN codes (S and Factor series printers)
  - Secure firmware updates signed with private GPG keys to verify authenticity and prevent malicious installations.
- **Firewall integration.** Both S and Factor series printers allow administrators to activate a built-in firewall, adding an additional layer of security by limiting access to authorized users.
- **Separation of critical functions.** Printers differentiate between process data (how an object is printed) and product data (the design itself), ensuring sensitive information is safeguarded even during physical access.
- **Removed camera for extra security.** With the UltiMaker Secure line, there is no built-in camera for an extra layer of security.

Transparent system design and operations

Security and transparency should extend beyond data protection into the way systems are built, supported, and used. By combining the strengths of a tightly integrated ecosystem with the freedom of an open system, UltiMaker ensures customers retain both reliability and flexibility.

- **Hybrid ecosystem.** UltiMaker systems are designed to work together, including Cura, Digital Factory, and the hardware. At the same time, they support the use of third-party materials and slicers, so users are not limited to proprietary options
- **User autonomy.** With regular firmware and software updates, UltiMaker ensures printers remain secure and up to date. At the same time, customers retain full control over how and when to use their systems, ensuring printers remain entirely theirs
- **Component sourcing and transparency.** UltiMaker uses secure, high-quality components from trusted suppliers to mitigate hardware vulnerabilities, and provides visibility into how systems are built and maintained
- **Local support.** Through an extensive partner network, UltiMaker ensures that issues are addressed quickly and workflows experience minimal disruption

This approach balances the reliability of an integrated system with the flexibility of an open one.

> “We wanted to have a variety of different printers, but we paid close attention to the reputation of the manufacturer, the long-standing reliability of its service, and how easy to use its products are. Undeniably, UltiMaker did fit all the criteria.”

— Dr. Orlando Ayala, EMIC Director

How to implement a secure 3D printing ecosystem in high-security environments

Adopting additive manufacturing in high-security environments requires more than simply selecting the right hardware and software. It requires a structured approach to build a secure ecosystem – one that protects data, ensures reliable output, and supports compliance with sector-specific regulations. Whether in defense, aerospace, healthcare, or other regulated industries, organizations can follow a set of practical steps to safeguard their operations.

Assess and classify security requirements

The first step is understanding what needs to be protected. Not all parts or design files carry the same level of sensitivity. Organizations should classify assets – from confidential prototypes to mission-critical replacement parts – and define the security level each requires. This process helps align resources with the principles of confidentiality, integrity, availability, and sovereignty, which underpin security in additive manufacturing.

Establish secure digital workflows

Sensitive designs should be protected at every step of the digital manufacturing chain. This includes:

- Encrypting design files and printing data end-to-end
- Implementing role-based access control so that only authorized users can access or modify files
- Ensuring compliance with data regulations relevant to the sector

Protect physical infrastructure

High-security printing environments benefit from strict facility controls. Printers should be installed in restricted areas, with access only to cleared personnel. Additional safeguards – such as tamper detection, firewall integration, or environmental monitoring – reduce the risk of unauthorized use or interference. For mobile or distributed production units, hardened enclosures and monitoring can help maintain trust in the production process.

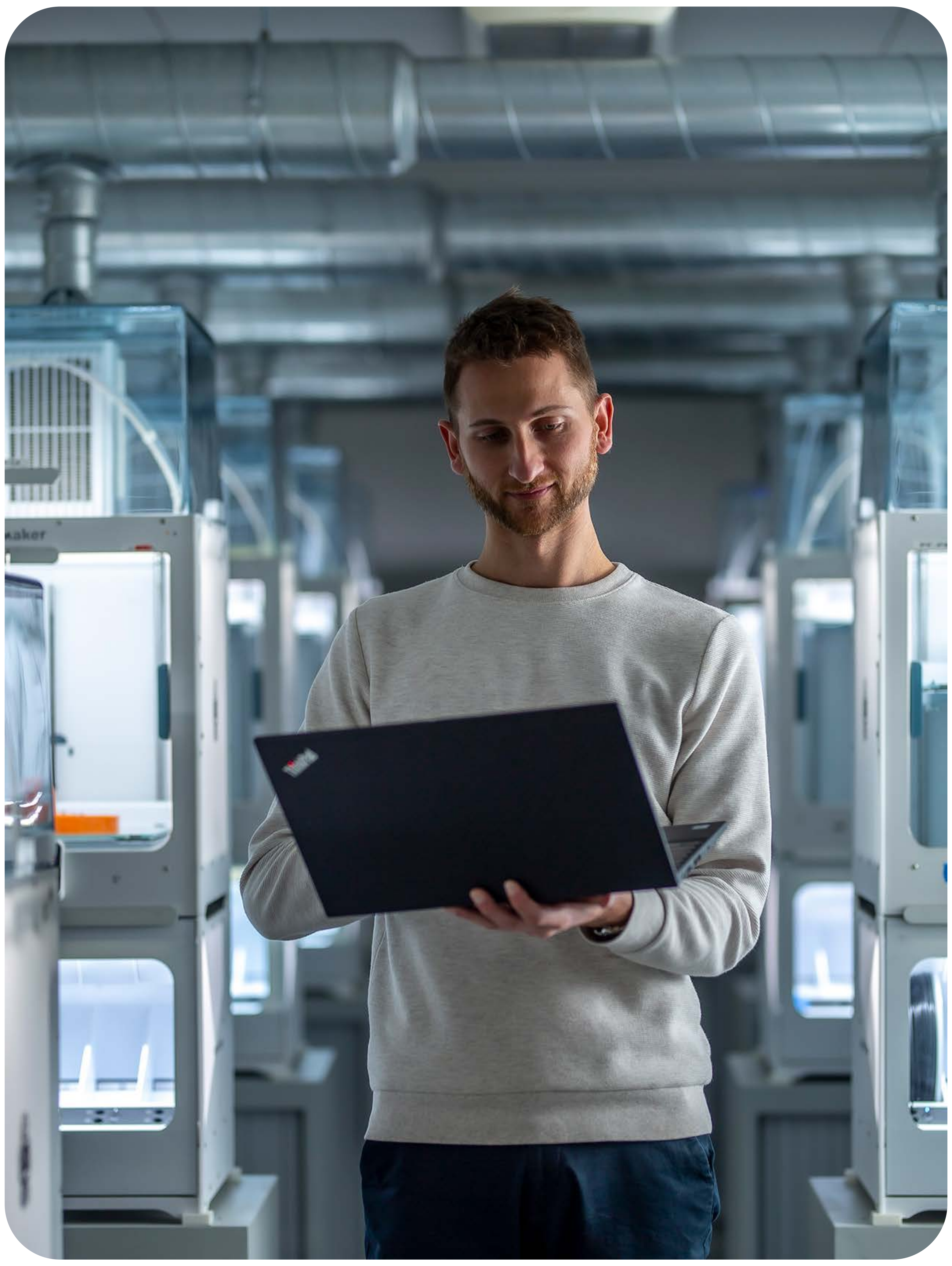
Secure the supply chain

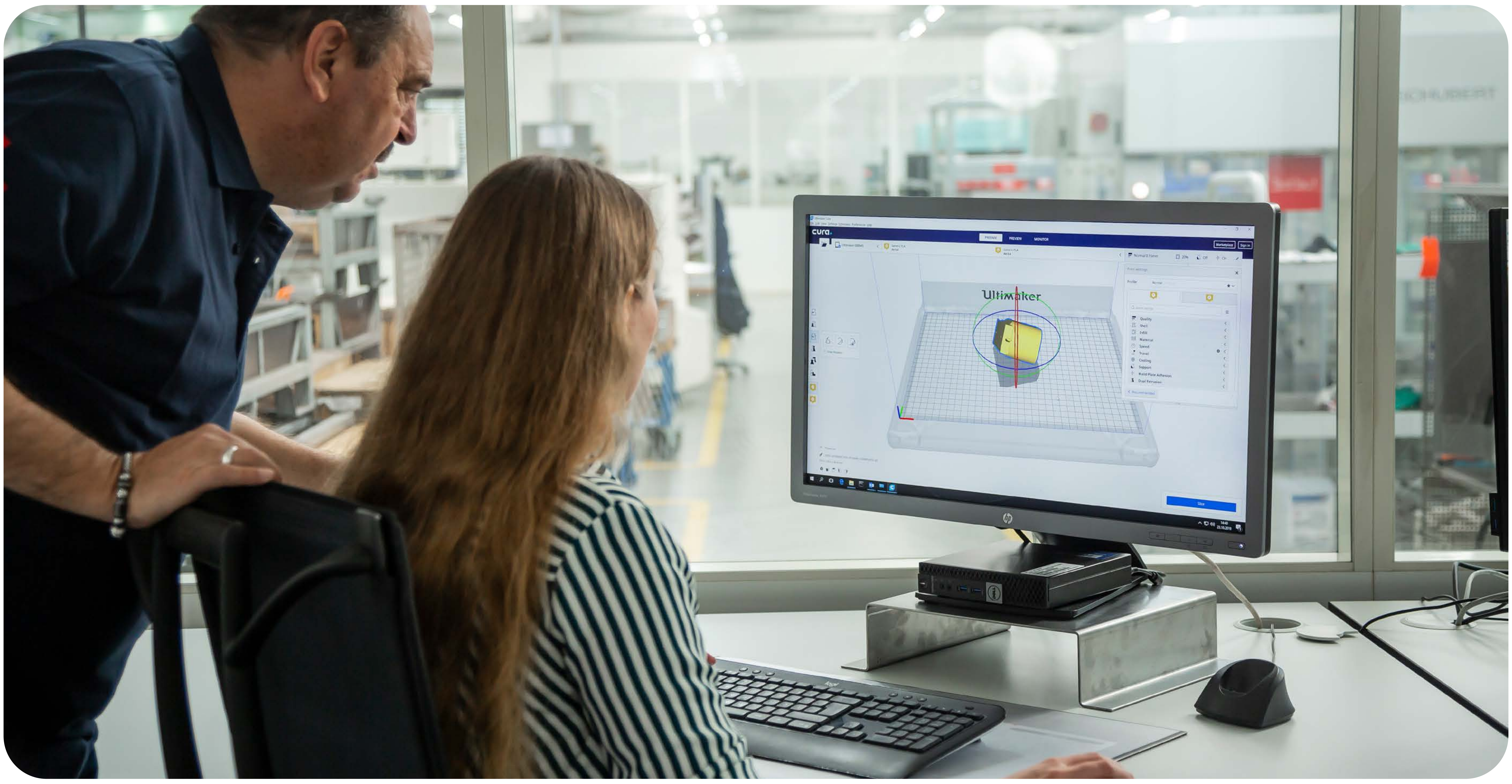
Security is only as strong as its weakest link. By sourcing materials, components, and hardware from trusted suppliers, organizations reduce the risk of compromised inputs.

In sectors like defense and aerospace, domestic sourcing can also help maintain sovereignty and protection from external risks.

Maintain systems securely

Regular updates are essential for staying ahead of emerging threats. High-security organizations should adopt processes for securely applying firmware and software patches, including offline update options where cloud connectivity is restricted.





Train personnel and enforce policies

Technology alone cannot ensure security. Staff operating in high-risk environments must be trained in secure handling of sensitive design files, incident reporting, and adherence to strict data management policies. Establishing a clear chain of responsibility enables organizations to respond quickly and effectively when security concerns arise.

Work with trusted partners

Finally, building a secure ecosystem often means working with 3D printer manufacturers who can demonstrate compliance with sector-specific security standards.

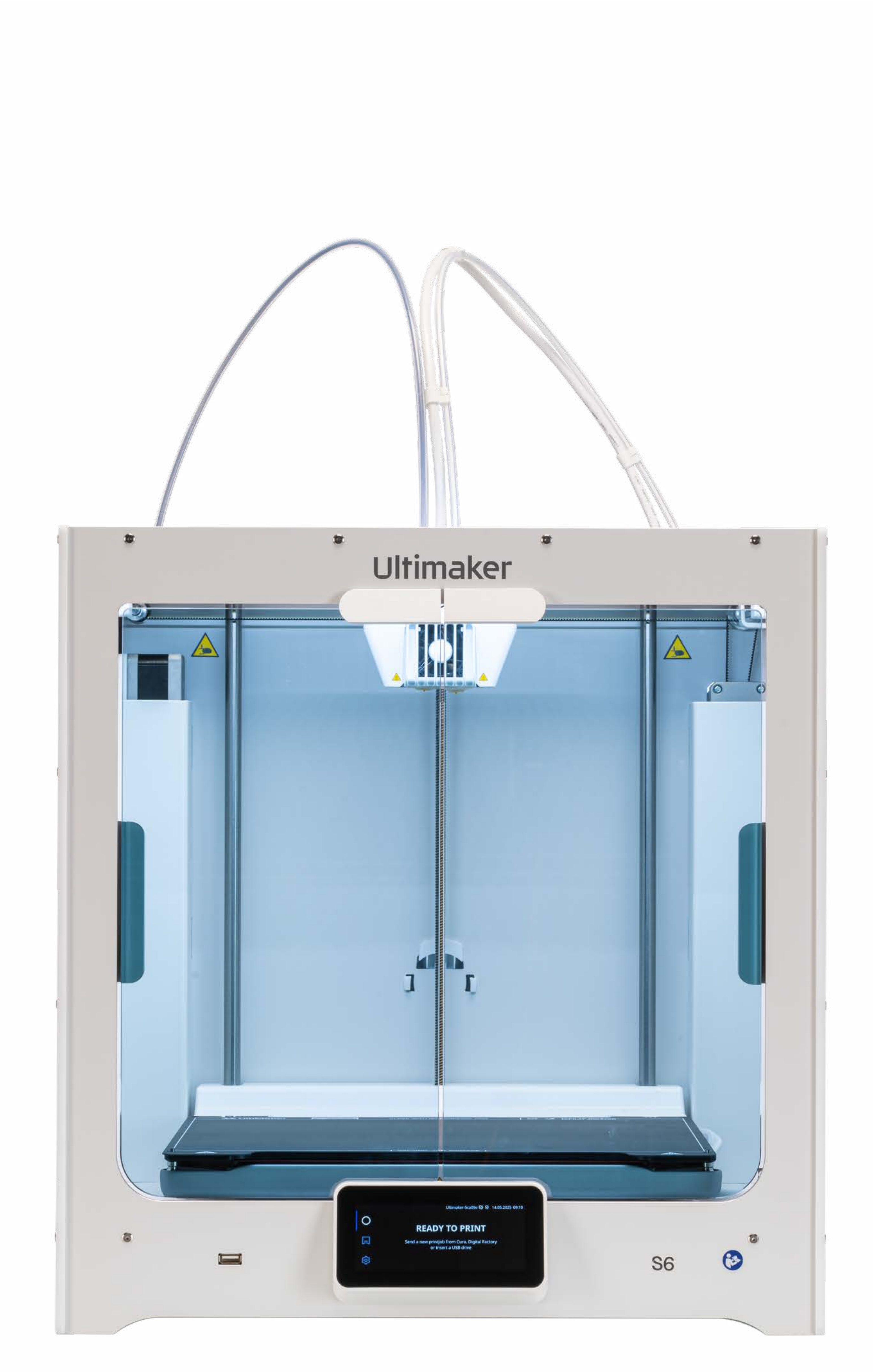
Solutions designed with transparency, offline operation, and independent audits assure organizations that their systems are both secure and flexible enough to adapt to changing needs.

UltiMaker Secure line

NATO-certified. EU-made. Mission-ready.

The UltiMaker Secure line is a portfolio of professional 3D printers optimized for defense and high-security environments. Built in the Netherlands, trusted by NATO-aligned organizations, and launching with the S6 Secure and S8 Secure.

Built for defense IT standards, Secure line printers remove entire classes of risks: no cloud dependency, no external attack surface, and factory-flashed firmware. The platform is fully auditable and tamper-resistant, ensuring data sovereignty and protection against file manipulation or denial-of-service attacks.



UltiMaker S6 Secure

UltiMaker S8 Secure

Choose the right 3D printing ecosystem for your business needs

Discover the UltiMaker ecosystem that will streamline your workflow and deliver the quality results you need.

3D printers fit for every application

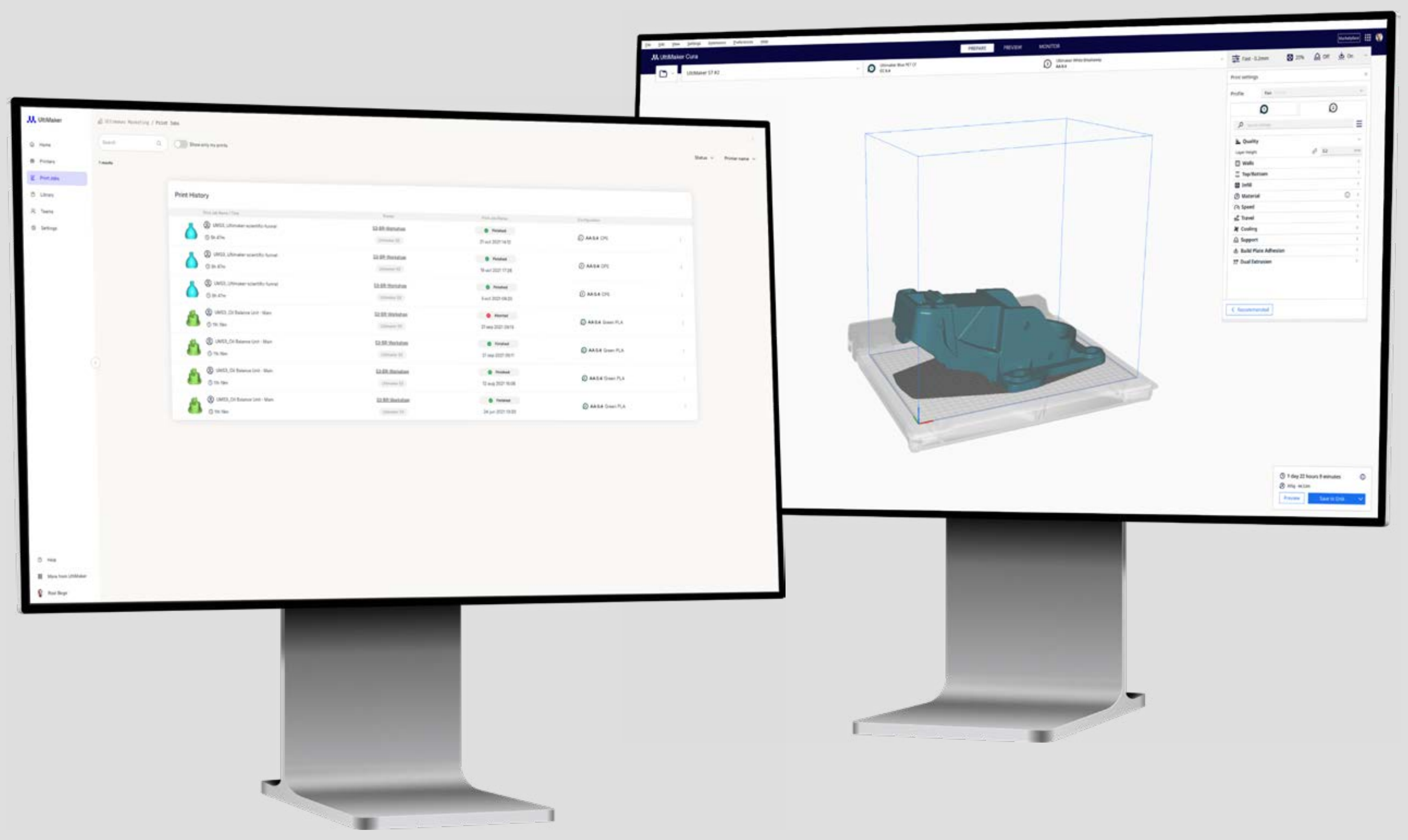
A comprehensive lineup of professional 3D printers designed to meet the needs of everything from design studios to factory floors. All our machines share the same UltiMaker DNA: reliability, quality and ease of use, while excelling in different applications.

One click print with over 240 materials

The widest range of materials on the market, enabling innovative and complex applications. Our high-performance materials are tested for reliability and accuracy, while the broad selection of certified options expands possibilities for various applications.

Secure cloud software for easy remote printing

A secure and streamlined platform for preparing, organizing and monitoring your 3D printing operations. 3D printing software trusted by millions of users. Fine-tune your 3D model with 400+ settings for the best slicing and printing results.



Support dedicated to your success

The expertise of hundreds of people with over 10 years of experience ready to help you. Our dedicated customer support and application engineer teams multiply the value of UltiMaker products with their knowledge.