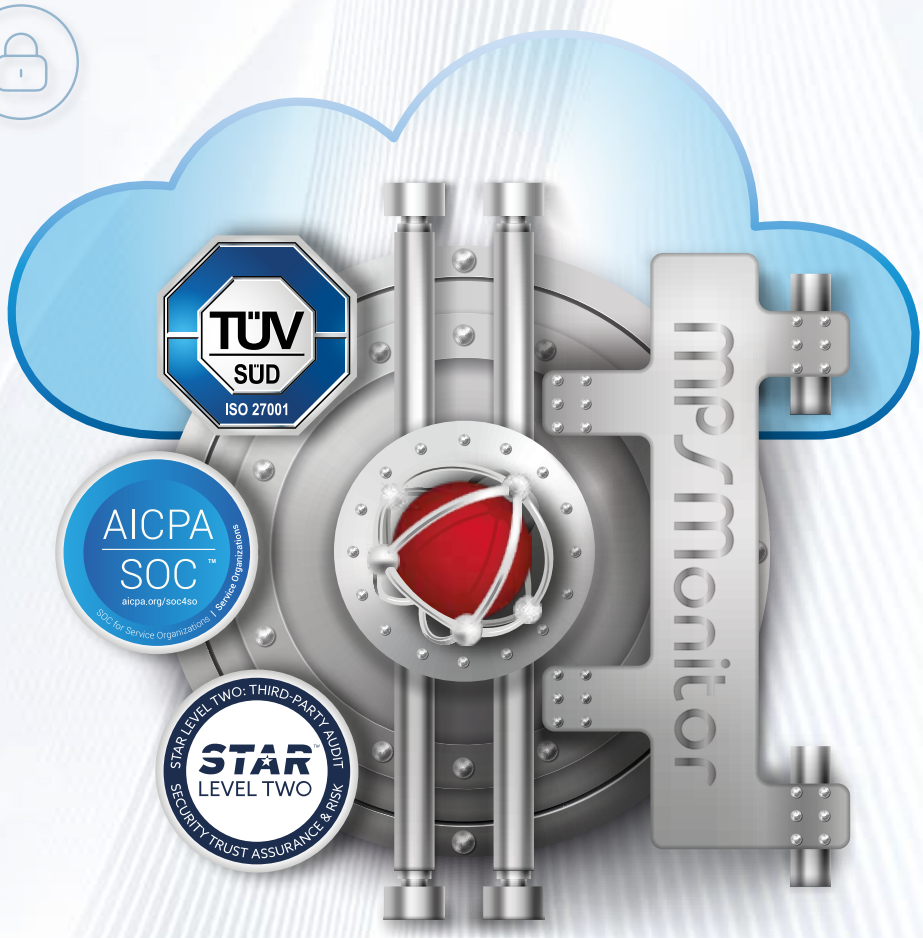
The Importance of **Cybersecurity** for **SaaS Companies** and **How MPS Monitor Maintains its Strong Security Posture**

Software-as-a-service (SaaS) companies are unique because they provide software to millions of users. Specifically, remote monitoring SaaS platforms like MPS Monitor also install Data Collection Agents (DCAs) on hundreds of thousands of computers and other devices across the world. Managed Service Providers like Impact Networking install these agents and provide access to these platforms to their customers of any size and industry.

SaaS delivers incredibly useful services to businesses but also exposes a great risk: **if a cyberattack compromises the SaaS company, attackers can gain access to every computer that has a copy of their software, and from there, to any device connected to the customer's internal network**.

These risks are even more relevant in the Managed Print industry: according to Quocirca's Print Maturity Index 2024, **only 20% of companies are classified as having six or more security measures in place**. Because so few companies take cyber threats seriously, it's vital for any organization to thoroughly assess SaaS providers to confirm their cybersecurity protocols are robust enough to provide adequate protection.



MPSMonitor
Printer Monitoring in the Cloud

impact

DOT Security

Setting New Benchmarks for SaaS Cybersecurity

To meet this growing requirement, MPS Monitor in the last ten years has been developing and improving its own cybersecurity posture, by implementing a **comprehensive approach and a holistic strategy**, which include:

- **User Account Security Features like Single Sign On and Multi-Factor Authentication**
- **Third-party Code Reviews before each DCA release**

- **24x7 System Monitoring, Log Analytics and Alerting**
- **Physical Security, Disaster Recovery and Incident Management**

- **Routine 3rd Party Penetration Testing and Security Assessment with DOT Security**
- **Compliance to International Security Standards**

ISO27001 | **SOC 2 Type 2** | **CSA Star Level 2**

Keeping Up with Threats with DOT Security

With one of the most **robust security postures** among SaaS solutions in the Print industry — and an unwavering commitment to maintaining compliance with security standards — MPS Monitor has emerged as a benchmark in shaping and adopting newly established cybersecurity frameworks. This is evident in the assessments published recently by several prominent analysts and evaluators.

To maintain its edge, MPS Monitor regularly partners with **cybersecurity experts like DOT Security, Impact's cybersecurity partner**, to conduct ongoing penetration tests.
DOT Security's red team — composed of specialists who employ **real-world hacking tactics** — uses the latest methods to "attack" MPS Monitor's systems and uncover potential vulnerabilities. By taking this **proactive approach**, MPS Monitor is able to address weaknesses quickly, long before cybercriminals can exploit them.

During the latest penetration tests performed by DOT Security in November 2024, MPS Monitor's portal applications, distributed architecture, and surrounding infrastructure demonstrated **exceptional resilience**, successfully withstanding some of the most common and sophisticated attacks targeting modern web platforms and the organizations that develop them. Also, a review of the DCA's latest code was performed, and the auditor determined that the source code was **skillfully crafted, well-documented, and securely built**.

MPS Monitor has emerged as a benchmark in shaping and adopting newly established cybersecurity frameworks

MPSMonitor
Printer Monitoring in the Cloud

impact

DOT Security

FAQs

What Happens if MPS Monitor Fails a Test?

If a test fails and a vulnerability is found, the company's policy allows a maximum of 30 days to fix, retest, and repeat until the security tests show that the problem is fixed.

How Often Do Tests Occur?

MPS Monitor performs penetration tests alongside partners like DOT Security, twice a year, alternating between cybersecurity teams.

Why Test So Often?

Vulnerabilities can be created at any time. Every new feature, update, or installation can inadvertently create an entry point for cybercriminals. We run tests to ensure that no new vulnerabilities arise and, if they do, we can promptly remediate them.

Why Use Two Teams?

MPS Monitor works with two cybersecurity teams to ensure fresh eyes and new perspectives are used each time. It's the best way to guarantee that the platform's security is effectively tested.

Why Comply with Three Security Standards?

Each Standard addresses different requirements:

ISO27001 ensures maximum Confidentiality, Availability and Integrity of data

SOC 2 Type 2 ensures that more than 390 Security Controls are in place and effective

CSA STAR Level 2 provides a standardized framework for evaluating the security posture of SaaS / Cloud platforms

Why Perform a Code Review before each DCA release?

The DCA is the most sensitive component of the MPS Monitor platform, as it is installed inside the customer network and constantly communicates with the SaaS platform. Testing before each release ensures that the DCA code does not contain malware or bugs that may create security risks to the customer's network.

MPSMonitor
Printer Monitoring in the Cloud