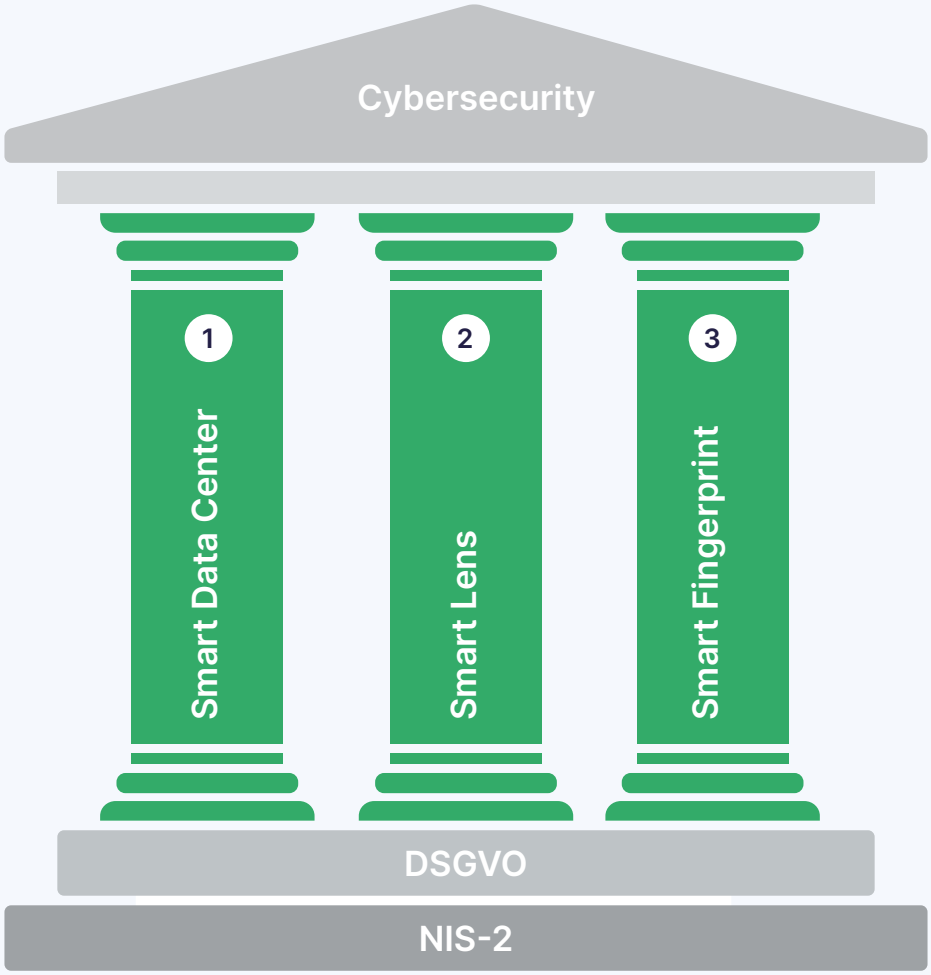
The Three Pillars of Your Cybersecurity Strategy

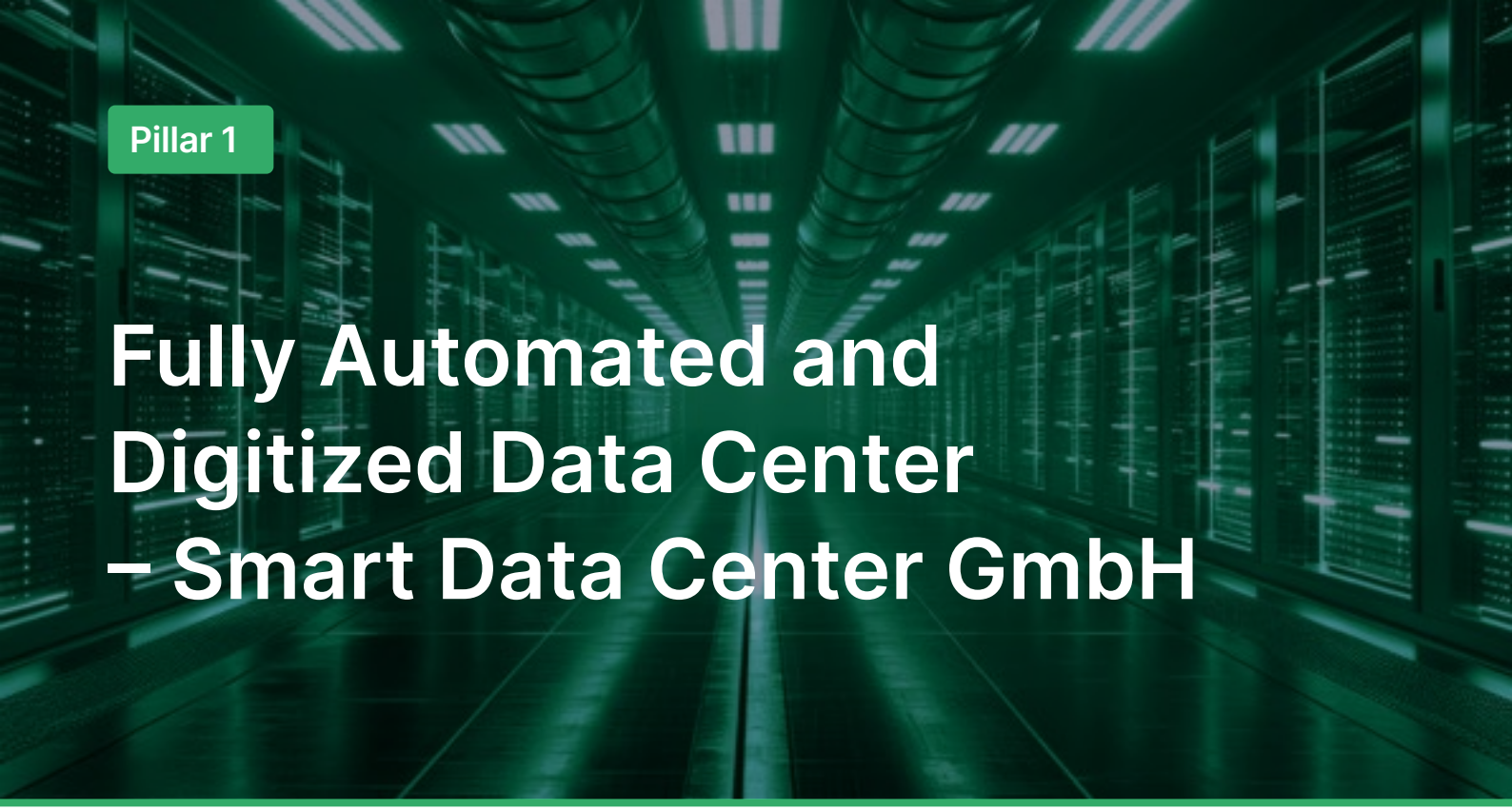
Smart DataCenter

The Pillars of Cybersecurity

Cybersecurity is a term that is frequently discussed. However, instead of focusing on what cybersecurity is, we should be aware of what it is not: dispensable. In the digital world, adequate security measures are essential; otherwise, companies risk their data, reputation, and existence.

Our solutions provide your company with the highest security, seamlessly integrated into your IT infrastructure, ensuring comprehensive protection against daily digital threats. With our solutions, we ensure that your company is always protected against the latest cyber threats. Cybersecurity is not just a technical challenge but also a strategic necessity. Protect your business operations and company values with our comprehensive cybersecurity strategy.





Pillar 1

Fully Automated and Digitized Data Center – Smart Data Center GmbH

With the Smart Data Center, we offer the world‘s first fully automated and completely digitized data center. The key unique selling point of this product is the fully automated process for backups, including a comprehensive backup strategy (disaster recovery test), which allows you to test your own backups completely for the first time.

Thanks to this technology, which would not be technically available without a fully automated data center, you have the assurance that in the worst case of a successful hacker attack, you can get back on your feet 100% securely without paying a ransom, despite all security measures.

Since no one can ever achieve 100% security against a successful attack, even with the measures mentioned in pillars one and two, the personal verification of the restoration of all data and systems has gained the utmost importance in today‘s world.

Pillar 2

Reducing the Likelihood of Being Hacked – Smart Lens

With Smart Lens, you can register and continuously monitor all desired attack surfaces, such as your website, online shop, databases, or intranet. Our software performs automated checks and detects potential threats at the moment they arise (optionally in real-time).

A user-friendly dashboard provides you with a clear overview of the current threat situation. For all new and existing vulnerabilities, you automatically receive detailed reports via email, allowing you to react immediately.

Our solution ensures that you receive clear and easily understandable reports for each attack surface. Additionally, a risk score from 1 to 10 is provided, allowing you to evaluate the severity, damage potential, and exploitability of the analyzed security risks based on international CVSS (Common Vulnerability Scoring System) values. With these features, you, as a managing director, can transparently, precisely, and objectively assess the security status of your company and take the right actions.

Pillar 3

Security Through a Third Biometric Factor – Smart Fingerprint

Thanks to our „Smart Fingerprint“ software (expected to be available from 10/2024), you can introduce a third biometric factor in your company. With our AI, you can monitor browser usage and detect successfully infiltrated hackers one second before they strike.

How does it work? If a malicious hacker manages to obtain the administrator password despite all precautions and attempts to enter critical commands such as „delete everything,“ „encrypt everything,“ or „give me a new super-admin password,“ the AI recognizes through the browser, keyboard, and mouse usage that the access is not by the legitimate user but by a hacker. The way we surf the internet is a completely unique biometric characteristic. Smart Cyber Security GmbH is the first international company to recognize this and implement it in highly intelligent AI software. This allows us to stop an intruder in real-time, even if they have already breached the system.

As soon as unauthorized use is suspected, the AI immediately revokes all rights of the account and, if configured by you, requests authorization via two-factor authentication from both the legitimate user and a third factor (e.g., your IT manager or CEO) via SMS. Until both authorizations are provided, the usage rights remain revoked, and the hacker attack is effectively rendered harmless.

Smart Data Center GmbH
Südportal 3
22848 Norderstedt

+49 40 741 24 16 0
kontakt@smart-datacenter.de
www.smart-datacenter.de

Smart DataCenter