A1 Digital

WHITE PAPER

Providing the best possible protection for decentralized networks

How enterprises use SD-WAN, microsegmentation, zero trust and AI to create the highest level of security for their IT and OT infrastructures, processes, and applications – freeing themselves from technical and monetary constraints by using NaaS (Network as a Service).

By Philipp von Strobl-Albeg

Content

Foreword

Author Philipp von Strobl-Albeg explains the security improvements resulting from the use of up-to-date safety concepts, technologies and services, and highlights underlying processes to provide a top-down perspective useful for decision makers.

Technology should make life easier but often doesn't quite do its job. Good examples are traditional networks and security structures, which are increasingly overwhelmed by the way we work today. As digital transformation progresses, companies are confronted with immense technical challenges, most notably the massively increasing complexity caused by a wide variety of systems, platforms and processes intended to cooperate seamlessly. And then there are the various messenger services and other apps on the devices of employees.

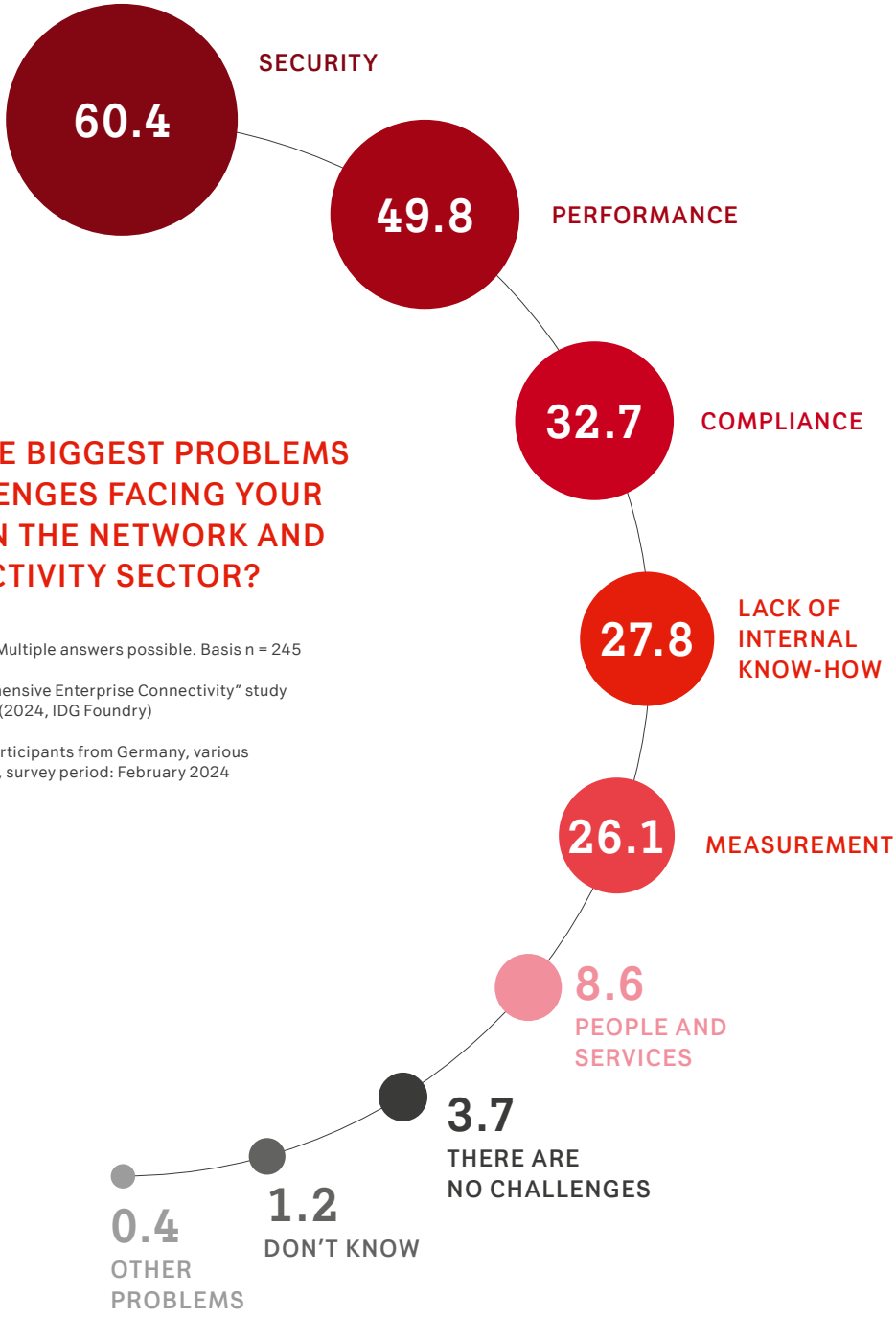
Keeping all of this monitored and secure is pushing network administrators to their limits. Complexity pressure keeps increasing with every new virtualization, every additional cloud service and networked site, not to mention all the current remote work and mobile applications requiring administration as well as security.

WHAT ARE THE BIGGEST PROBLEMS AND CHALLENGES FACING YOUR COMPANY IN THE NETWORK AND CONNECTIVITY SECTOR?

Figures in percent. Multiple answers possible. Basis n = 245

Source: "Comprehensive Enterprise Connectivity" study (2024, IDG Foundry)

305 study participants from Germany, various industries, survey period: February 2024



Networks under complex pressure

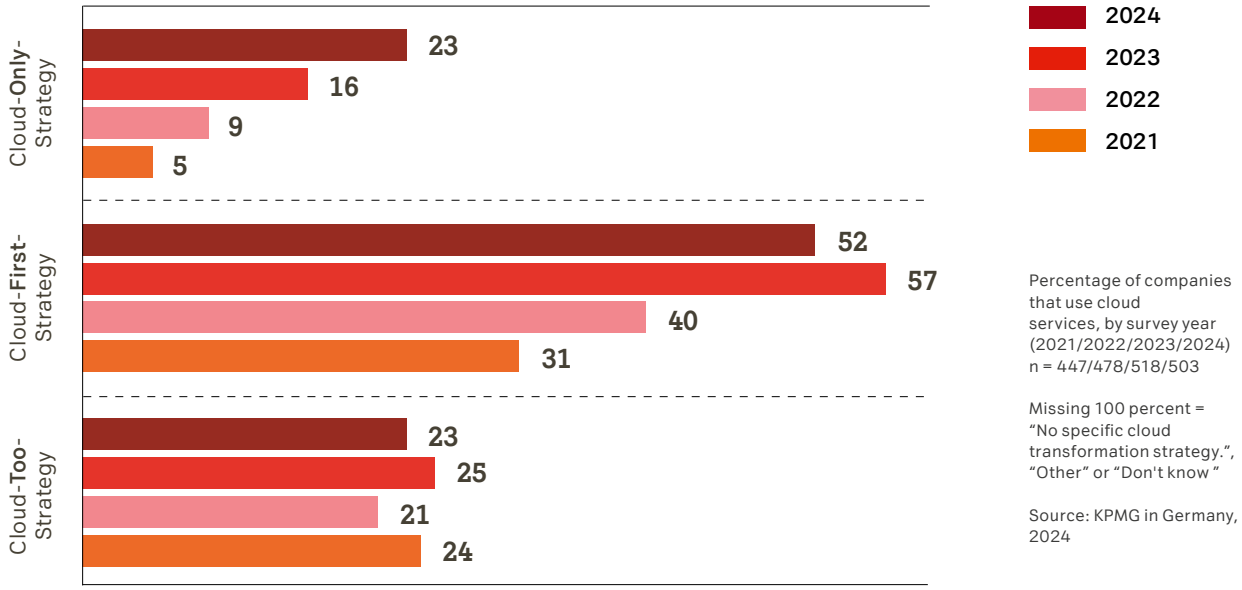
The more organizations decentralize their resources and move them to the cloud, with more work being done outside of company headquarters, the greater the control and management requirements, and therefore, security risks grow exponentially.

As a matter of fact, traditionally designed networks and their corresponding policies more often than not turn out to be roadblocks in the forward-looking, scalable, cloud-supported evolution of businesses. Today, tried-and-tested methods for managing and securing infrastructure, data and applications are only partially or not at all effective anymore.

The dilemma starts at the connection stage. Often, for current traditional WAN ports, the task of prioritizing data paths and applications is already too complex. This results in delayed accessibility, slow download speeds, disruptions in video communications with customers, partners and colleagues, and frustrated IT staff.

CLOUD TRANSFORMATION STRATEGY OVER TIME

Which of the following strategies best applies to the cloud transformation in your company?



Percentage of companies that use cloud services, by survey year (2021/2022/2023/2024) n = 447/478/518/503

Missing 100 percent = "No specific cloud transformation strategy.", "Other" or "Don't know "

Source: KPMG in Germany, 2024

And that's just the tip of the iceberg. Given the variety of internet connections, apps and cloud platforms in use, network segments set up as demilitarized zones, for example, hardly provide any effective security in an emergency. As it stands, once an attacker has a foot in the door of the network, they can easily move around and cause significant damage.

It is not only analysts and ICT providers, who have recognized how weak network security and performance really are in an increasingly digitalized world. Many affected businesses also see an urgent need for action. The requirements for a secure future are a flexible, resilient network infrastructure, simpler regulatory planning and implementation, and of course more effective safety concepts, explained on the following pages of this paper.

Network security and performance: many affected companies recognise the urgent need for action.

Zero trust – never trust anything or anyone

The most optimistic solution to a comprehensive protection of proprietary IT and data is Zero Trust Network Access (also known as "ZTNA" or "ZT"). This approach works off the premise that every system, every device, every user and every connection – inside and outside any network – can be attacked and compromised at any time.

Subsequently, nothing and no one is allowed to access networked resources without first confirming their identity and "trustworthiness".

Consistently applied, ZTNA will extend to any

- **infrastructure** and its **component**
- **devices**
- **network equipment**
- **virtual servers and storage facilities**
- **cloud components and services** (such as PaaS, IaaS, SaaS etc.)
- **applications**
- **workloads**

... and every individual user inside and outside the organization who accesses parts of the physical and virtual network or any applications.

The foundation for effective ZTNA is a granular network segmentation across all components and applications. This is called **microsegmentation** (see info box on page 6). It finely divides a company's entire physical and virtual infrastructure and at the same time registers the applications and workloads of individual users and groups.

Microsegmentation enables continuous security validation by applying multiple checks of each ID and verifying regulatory compliance as well as automatically scanning all network activity for any suspicious irregularities.

Micro-segmentation enables continuous testing and examination of safety-related harmlessness.

What microsegmentation achieves

Microsegmentation breaks down infrastructure assets into small units, making it easier to secure devices, endpoints, applications and workloads, rendering unauthorized access to proprietary company systems virtually impossible. If it does occur, damage will be restricted to a single, isolated area.

This is how microsegmentation applied to transport rules (routing/forwarding) helps to protect resources such as smartphones, laptops and emails, quickly, easily and in a targeted manner. These kinds of resources often run on their own operating systems and have vulnerabilities that can't be eliminated or patched automatically by a central network administrator.

Microsegmentation is also recommended for production facilities (OT devices), medical technology and industrial equipment/robots that are integrated into workflows or processes. In other words: the finer the segmentation, the smaller the target areas.

BENEFITS OF ZTNA

- Protection of individual applications and workloads, even across dispersed infrastructure such as multi-cloud environments. Granular connection restriction keeps out potential attackers and avoids internal errors.
- Savings of time and resources through integration via interfaces, centralization, and reusable security policy templates (i.e.pre-defined and pre-approved connections).
- Simplified regulatory compliance through the option of implementing automated cross-platform processes, which can quickly be adjusted on demand to match new compliance requirements.
- Infrastructure-independent segmentation and environmental segregation of systems, for example: productive infrastructure data residing on-premise can be granularly separated from systems and development environments in the public cloud.
- Real-time transparency through a centralized overview of all network connections reduces the time required to assess and eliminate issues. Attacks can be detected and averted more quickly.

Zero Trust protection results via the multiple authentication/authorization of finely segmented access points and user accounts, but especially via easily adaptable access regulations.

Subsequently, neither connection paths nor applications are visible from the outside, and hackers have significantly fewer target areas. They can also no longer move laterally throughout the entire network.

Instead, they remain stuck in the small segment through which they have gained initial access, and there, are only able to cause short-term damage, if any.

SD-WAN in a nutshell

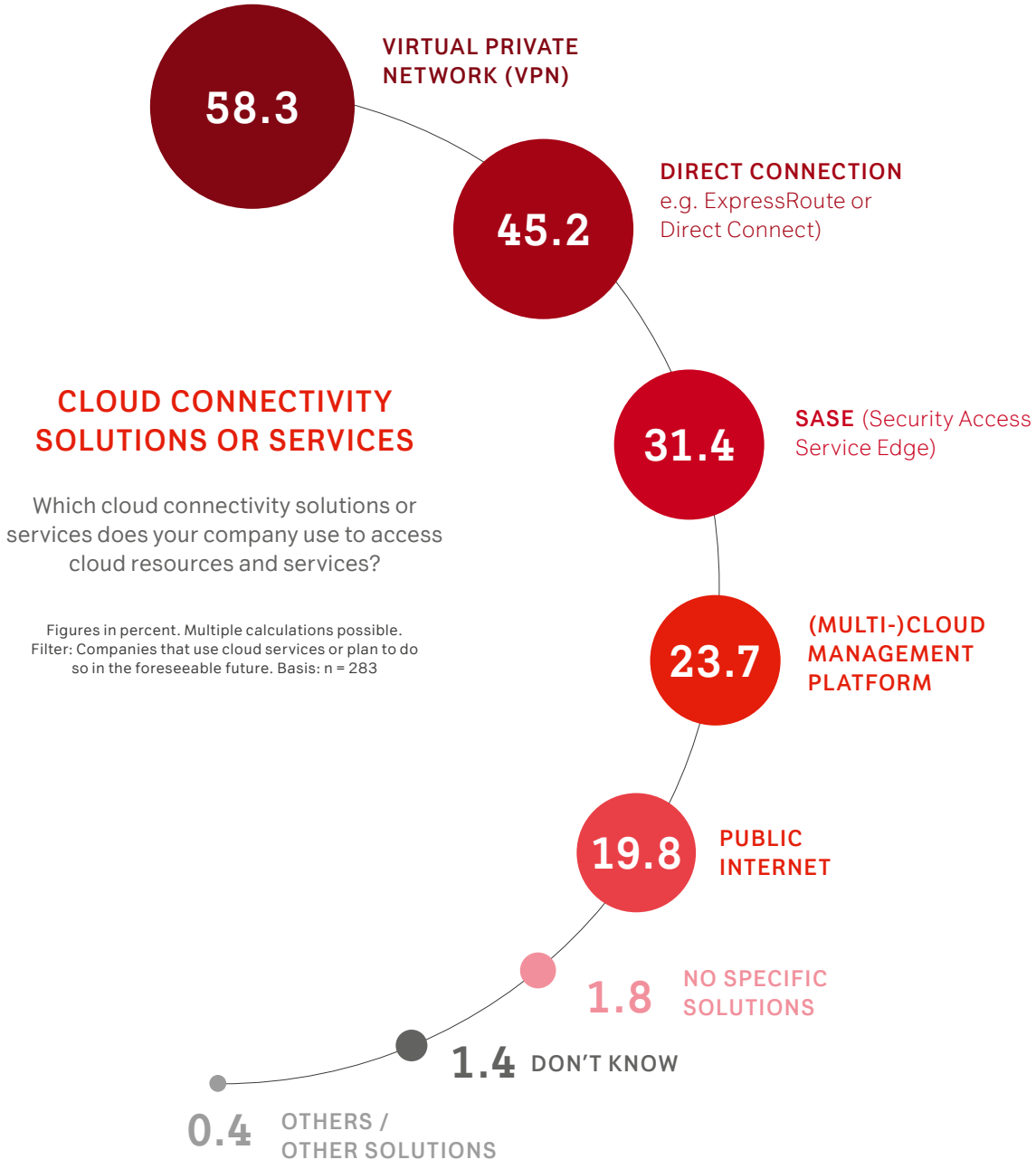
In recent years, SD-WAN technology has proven to be an effective and cost-efficient tool for connecting network locations and hybrid IT, while at the same time preventing and averting various cyberattacks, and it has increased in popularity among businesses.

SD-WAN enables a straightforward configuration of requirements and regulations for the secure transmission of all types of application. It works radically different to traditional network operating systems – most of which are centralized and operate on static settings across the entire wide area network (WAN). As a result, the more diverse and increasingly cloud-based the applications and platforms are, which network administrators have to connect, the more difficult their administration and control.

As the number of different, increasingly cloud-based applications and platforms that network administrators have to connect to grows, it becomes more difficult and time-consuming to control and manage them.

SD-WAN, on the other hand, is based on a cloud-native software platform with the flexibility to provide the required functions and specifications for all network layers – from orchestration down to the control of individual data packets. This eliminates the complicated route allocations, related performance issues and operational risks as we know them.

SD-WAN considerably simplifies the controlling and monitoring of internet connections and applications. Its high level of automation and intelligence increases data traffic stability, making applications more consistent in their availability and more resilient to disruptions. This translates into significant performance improvements, such as in video conferencing, collaborative activities or streaming. With SD-WAN, jittery connections, audio dropouts or even data loss are a thing of the past.



CLOUD CONNECTIVITY SOLUTIONS OR SERVICES

Which cloud connectivity solutions or services does your company use to access cloud resources and services?

Figures in percent. Multiple calculations possible.
Filter: Companies that use cloud services or plan to do so in the foreseeable future. Basis: n = 283

"Integrating a company-wide security solution with an application-centric approach into our network meets our expectations to a tee. With the deployment of A1 Digital SD-WAN, disruptions in voice and video communications across the entire business and all external sites are a thing of the past."

Hubert Willberger
Senior Systems Engineer at Arineo GmbH

ADVANTAGES OF SD-WAN

Businesses already working with SD-WAN or seriously considering a switch can expect to achieve the following improvements by using a software-defined network design:

- ✓ **Reliable, no-fuss site network connections**
- ✓ **Cost optimization for infrastructure, administration and personnel**
- ✓ **Simplified operational processes (IT and OT) with a high network reliability**
- ✓ **Intelligent orchestration and path routing**
- ✓ **Acceleration and stability of SaaS and other cloud applications (by minimizing latency, jitter and data loss)**
- ✓ **Increased agility**
- ✓ **Easier and deeper implantation of network regulations**
- ✓ **More security through granular regulatory control**
- ✓ **Better monitoring**
- ✓ **Easier application analyses**
- ✓ **Higher service quality and improved user experience**
- ✓ **Programmability, increased flexibility**
- ✓ **More automation**
- ✓ **More powerful, up-to-date interfaces/API**

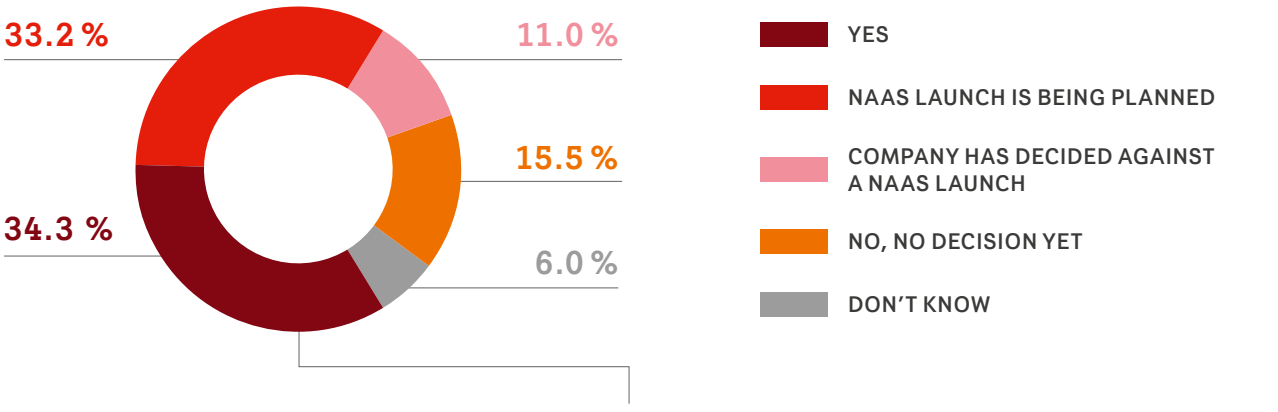
Network as a Service (NaaS)

With skilled labor shortages on the one hand, investment backlogs and budget constraints on the other, many businesses simply lack the resources to build a complete cybersecurity and network management team.

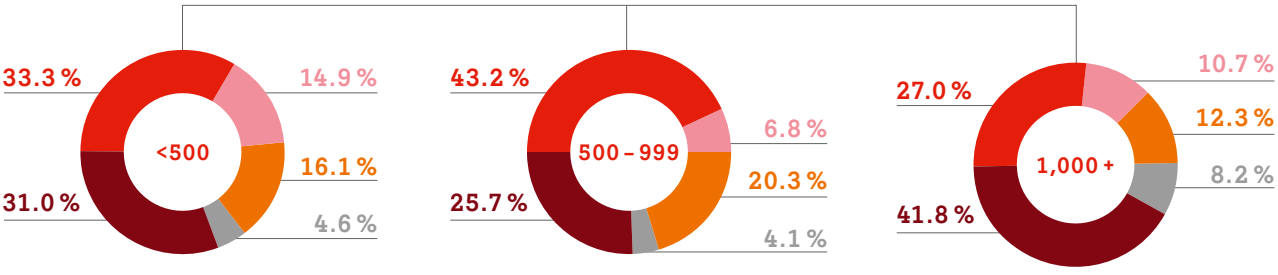
The solution is NaaS. With its services, companies can leverage cutting-edge, scalable, and future-proof technology and capabilities previously unattainable with traditional networks and understaffed IT teams – and they don't have to tie up investment capital to get it.

At A1 Digital, we see how much NaaS helps our clients to work more securely and flexibly. For them, NaaS is the key to powerful cloud structures, increased cyber security and satisfied users.

DOES YOUR COMPANY USE NETWORK AS A SERVICE (NAAS)?



SPLIT RESULT: COMPANY SIZE (NUMBER OF EMPLOYEES)



Figures in percent. Filter: Companies that use cloud services or plan to do so in the foreseeable future. Basis: n = 283

NaaS at your side

With A1 Digital's customized, intelligently automated workflows and highly trained service teams, businesses have the security and peace of mind of knowing their networks are being continuously monitored – without having to invest in additional personnel or IT equipment. We provide you with the experts and platforms for optimized network operations, and the services you use enter your balance sheet as Opex rather than Capex.

In the planning phase, our highly qualified specialists provide you with comprehensive support and then tailor the services precisely to your needs. Together with your commercial and technical decision makers, we determine which service model is best for your company and your cloud strategy. Ultimately, we can manage your entire network, including the internet and cloud providers you work with.

Let us advise you on how to reduce the effort and cost of your network infrastructure, how to better connect sites and employees, how to protect yourself successfully against cyberattacks, and how to work more efficiently!

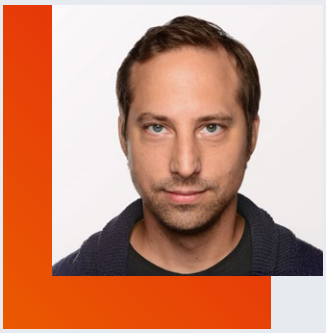
YOUR CONTACT

Holger Hartwig
Cybersecurity Expert

A1 Digital Deutschland GmbH
Unicorn Kustermannpark
Rosenheimer Str. 116
81669 Munich | Germany
M +49 162 338 08 39
holger.hartwig@a1.digital

The author

Philipp von Strobl-Albeg
Head of NaaS Delivery & Service Management



Philipp von Strobl-Albeg leads the NaaS Delivery & Service Management team at A1 Digital. He has many years of experience in the areas of SD-WAN and cybersecurity and has a deep understanding of service management, IT infrastructure and security by design. Philipp and his team support A1 Digital's customers and ensure a successful customer journey with Network as a Service and complementary products.

A1 Digital

Contact Germany
A1 Digital Deutschland GmbH
Unicorn Kustermannpark
Rosenheimer Str. 116
81669 Munich | Germany

info@a1.digital
www.a1.digital

Contact Austria
A1 Digital International GmbH & Co KG
Lassallestrasse 9
1020 Vienna | Austria

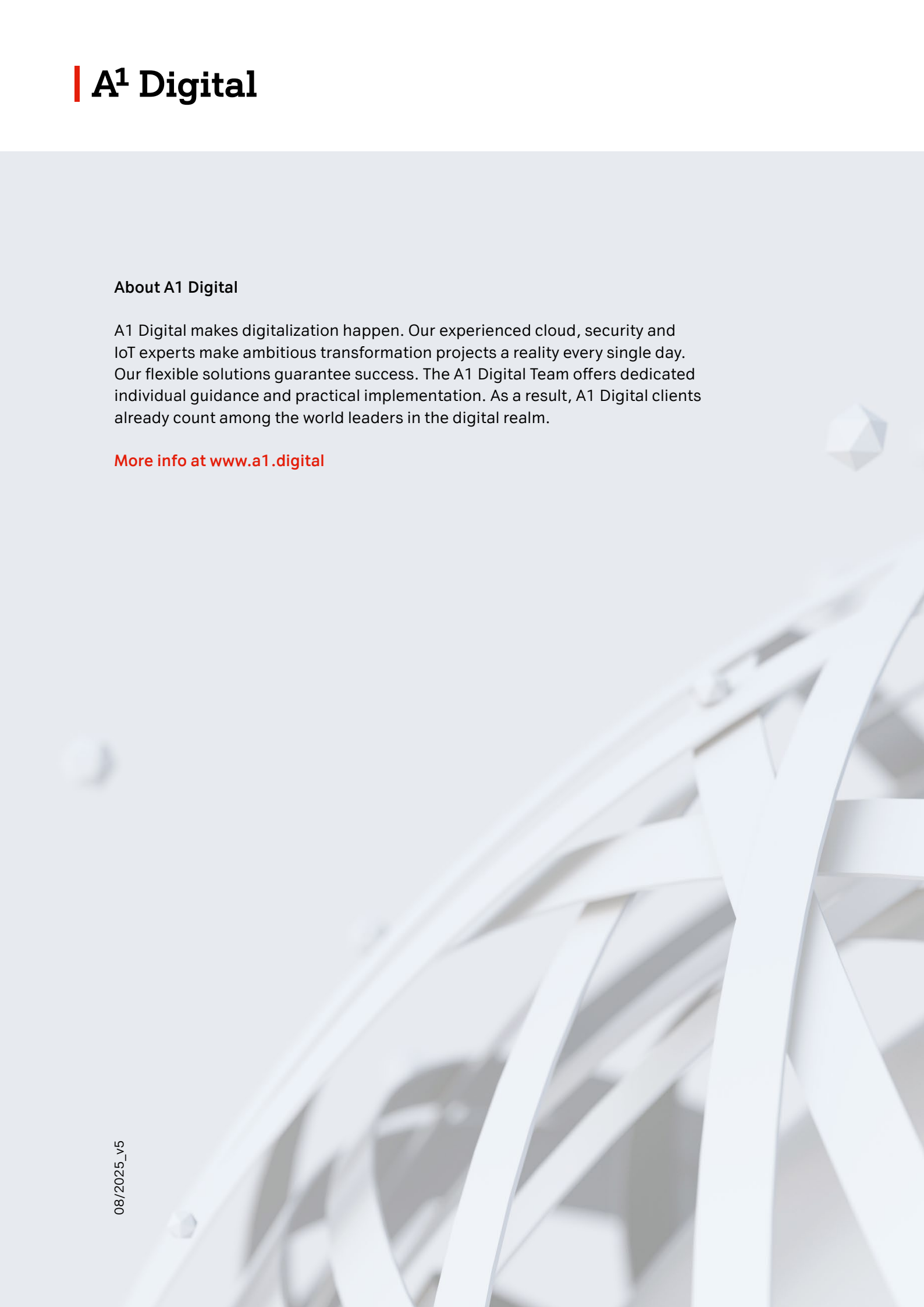
info@a1.digital
www.a1.digital

A1 Digital

About A1 Digital

A1 Digital makes digitalization happen. Our experienced cloud, security and IoT experts make ambitious transformation projects a reality every single day. Our flexible solutions guarantee success. The A1 Digital Team offers dedicated individual guidance and practical implementation. As a result, A1 Digital clients already count among the world leaders in the digital realm.

More info at www.a1.digital



08/2025_v5