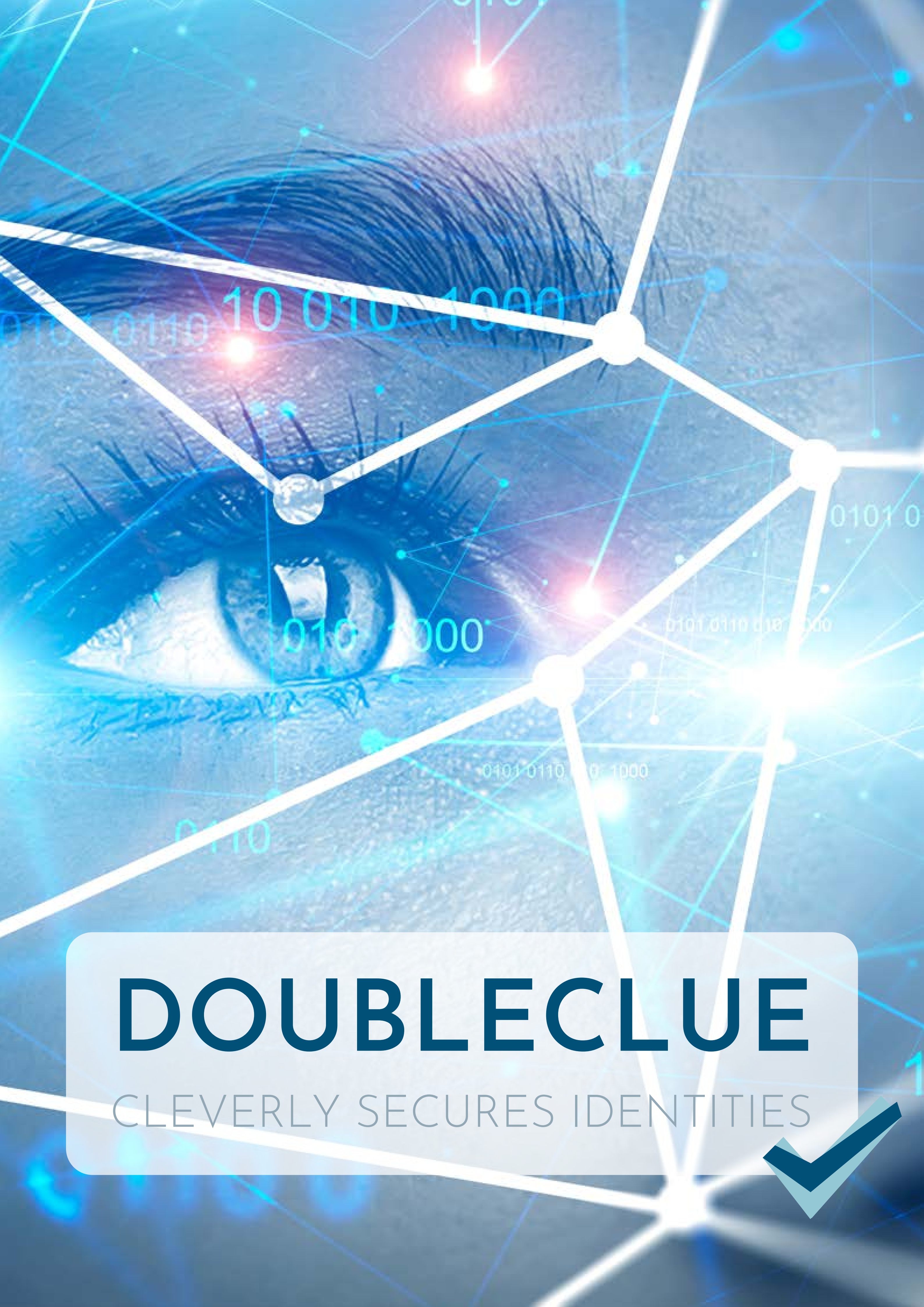


DOUBLECLUE

CLEVERLY SECURES IDENTITIES

CONTENTS

ABOUT DOUBLECLUE

DoubleClue reliably protects your corporate network from unauthorized and harmful third-party access. The software combines modern identity and access management (IAM) with state-of-the-art multifactor authentication (MFA). It comes standard also with additional security features that make your employees´ daily work and collaboration a lot easier.

IDENTITY AND ACCESS MANAGEMENT

The well-structured IAM platform allows you to centrally manage accounts, identities, passwords, data, and access. The core of the platform is access management to important systems and applications thanks to automated authorization management.

DoubleClue offers you eight options for authentication

- Push notification (passwordless)
- QR code (passwordless)
- OTP / One Time Passcode (also offline)
- OTP Hardware Token
- FIDO Token (including biometric)
- Voice Message
- SMS passcode
- Desktop App with passcode (no smartphone required)

TWO-FACTOR AUTHENTICATION

Easy-to-implement two-factor authentication prevents access to and intrusion into your network. DoubleClue offers you all the possibilities of a modern, password-free login: Choose the variant that best suits your company from eight different authentication options.

SINGLE SIGN ON (SSO)

Today, your employees work simultaneously in different applications. For the vast majority of them, they need to log in using a separate password. Thanks to Single Sign On, a single login to the DoubleClue UserPortal in the morning is enough to gain access to all the applications they need throughout the workday.

RIGHT ACCESS TO THE RIGHT DATA & APPLICATIONS BY THE RIGHT PEOPLE

PASSWORDSAFE WITH AUTOFILL-FUNCTIONALITY

With DoubleClue PasswordSafe, managing many, even complex passwords has become very simple: Easily store your (business) passwords in one place and access them in bundled form—directly from the DoubleClue UserPortal or the DoubleClue App. MFA ensures that passwords are kept safe in your virtual safe.

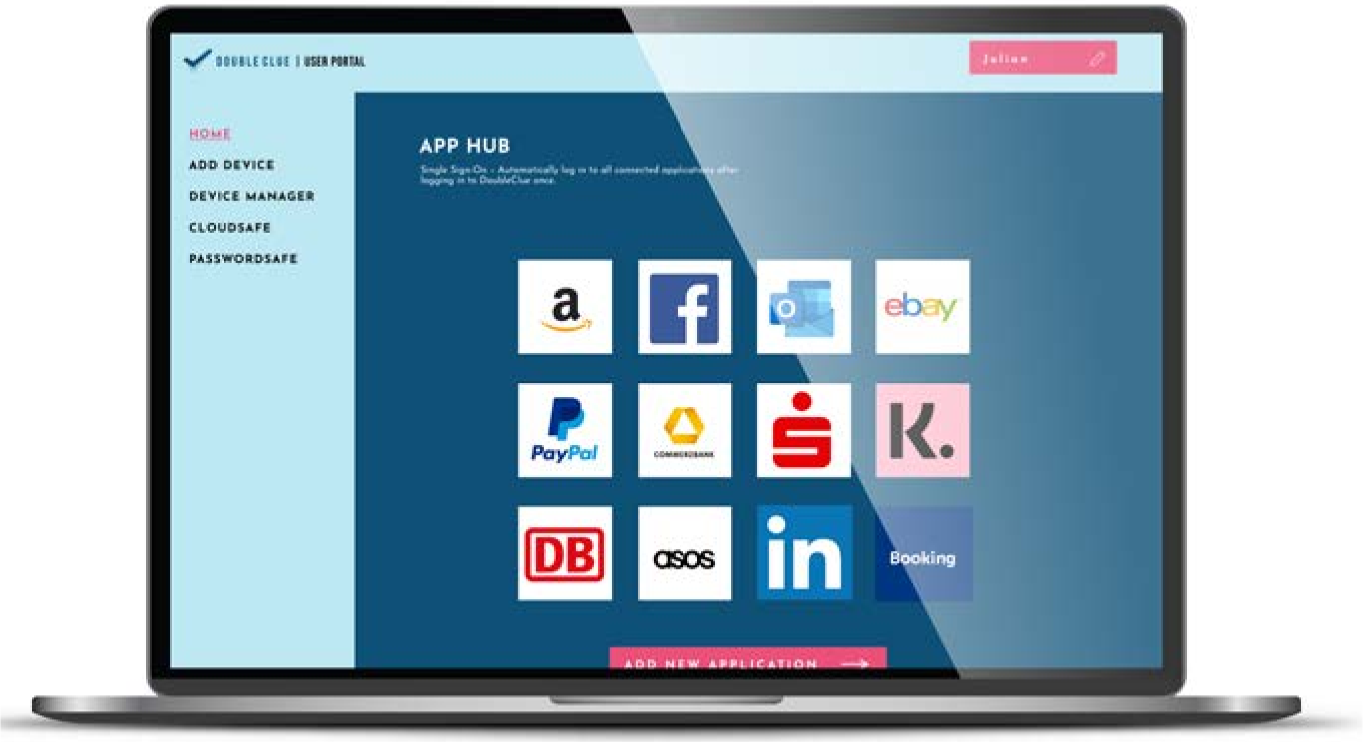
And thanks to Autofill, you will never have to enter a complex password in the browser again—just log in from anywhere in the DoubleClue app.

APPS FOR iOS & ANDROID

Users expect the same usability in corporate applications as they know from their free time. That's why DoubleClue offers you the possibility to manage passwords and approvals via an app on your mobile device.

DOUBLECLUE CLOUDSAFE

Important and confidential documents should never be sent via unencrypted emails. The DoubleClue CloudSafe therefore not only allows you to centrally store sensitive data in a protected, inaccessible area within your own IT infrastructure. It also opens up the possibility to securely share this access with your employees, partners, or service providers.



Single Sign-On – Automatically log in to all connected applications after logging in to DoubleClue once.

EFFECTIVELY SECURE THE IDENTITIES OF YOUR EMPLOYEES

The human factor is the biggest vulnerability for your corporate network. The algorithms and AI that underlie today's virus scanners and threat protection are so good and sophisticated that they detect malware well and intercept it before it can become a threat.

However, humans find this difficult: especially under performance and time pressure, your employees are inclined to open an attachment or follow a link without closer inspection. Cybercrime, therefore, relies on human interaction—be it due to negligence, due to (apparent) constraints, or due to emotional influence.

Data and personal (identification) information are often willingly disclosed if an emotional relationship can be established—this so-called social engineering can be found in phishing e-mails as well as in fraudulent telephone calls or on fake websites.

The establishment of a second factor prevents identity theft. After all, only those who can identify themselves twice—with a second factor known only to them—will ultimately gain access to a file or system. Access management also ensures that only those employees who really need access to sensitive areas of your corporate IT have it.

70% OF GERMAN COMPANIES WERE AFFECTED BY CYBERSEC ATTACKS IN 2019.*

*Source: https://www.bitkom.org/sites/default/files/2019-11/bitkom_wirtschaftsschutz_2019_0.pdf

INCREASE IN EMPLOYEE SATISFACTION THANKS TO STRONG USABILITY

Passwordless login increases productivity and acceptance: your employees don't need to remember multiple complex passwords and can log in to their PC and applications with one click. Thanks to SSO, they can switch between their applications within the DoubleClue UserPortal without interruption.

At the same time, your admins do not need complex password policies any further. Even a simple, insecure password has been turned into a secure login with the highest security requirements through MFA. Besides, it is also possible to generate long, secure passwords for frequently used applications, which employees can automatically save in the PasswordSafe.

With DoubleClue you get a multitool for secure password management, secure data exchange, and central storage for passwords and sensitive documents.

PRIVATE CLOUD CAPABILITY TO CONNECT ALSO REMOTE OR EXTERNAL RESOURCES

The future will be passwordless. And characterized by remote work. Increasing digitization offers more and more opportunities for location-independent working. Companies must be prepared for the fact that their IT is located in various private and public networks over which they have no control. However, these represent a potential gateway for viruses and other malicious applications.

DoubleClue enables you to secure these networks thanks to MFA and IAM.

In particular, cloud tools connected to the Internet, such as those used for collaboration or communication, are a risk to your IT. Especially if they were introduced at short notice and without sufficient security standards or are even used on private devices.

In the remote work environment, data transfer of important and especially confidential documents is also at risk. With DoubleClue Cloudsafe, these documents are stored in a central location secured by MFA in your private or the German DoubleClue Cloud. You can share access to them with employees, partners, and customers without having to transport them via unencrypted and insecure email communication.

SECURE COMMUNICATION– WITH INTERNAL & EXTERNAL STAKEHOLDERS

It's not just your employees who pose a potential security threat to your IT or confidential documents: equally—and perhaps to an even greater extent—it's external stakeholders who pose a potential risk. After all, how do you guarantee that the same high-security standards apply there as in your company?

The DoubleClue CloudSafe allows you to give external partners, suppliers or freelancers access to confidential files stored there. Without having to send them or even have them leave your servers. Grant access, write, or read-only rights to external as well as internal stakeholders, so you can be sure that your data remains confidential.

CLOSE YOUR WINDOWS BACKDOOR FROM THE HARMFUL ACCESS OF THIRD PARTIES

Many companies use Microsoft Windows as their operating system. However, every system has so-called backdoors that allow third parties to gain access to your system and, for example, leak data.

DoubleClue can close these backdoors and thus not only secure your user identities but also generally prevent access to your system. Especially if you have no access restrictions to your premises, you should secure local access with MFA.

DEPLOYMENT AND IMPLEMENTATION

Stay agile and choose the licensing and hosting model that best suits your business—on-premises, or in the cloud on servers in Germany.

No matter which hosting model you choose, the functionality of DoubleClue and its apps remain unaffected. The DoubleClue app enables your employees to access your data at any time—no matter where they are.

We also offer our customers a full range of services related to the implementation and support of their DoubleClue applications. You can flexibly adapt the level of support to your business model: From an all-round carefree package of implementation, roll-out, and support to individually tailored services—we will be happy to advise you on the best implementation for your needs.

Our services for consulting, implementation, roll-out, and ongoing support

- From the standalone license to the HWS all-round carefree package: Choose the license model that best suits your business and resources, e.g.
  - lifetime Managed MFA
  - lifetime Managed Software Support
- Consulting on implementation strategy before software rollout
- Training of administrators and user communication
- 30-day free trial with support
- Full implementation and roll-out support

SAMPLE IMPLEMENTATION GUIDE FOR AN ON-PREMISES LICENSE

We estimate a maximum of two months for implementation and roll-out when using an On-Premises license (incl. test phase).

The effective working time without the test phase is about 1–2 weeks, depending on the size of the company.

0.5-2 DAYS
After your request, we will send you your installation data for installing your DoubleClue application on your servers. The time required for the technical implementation depends on the complexity of your IT landscape.

1 MONTH
We estimate one month for the test phase. Depending on your choice of support scope, we already offer you training of your admins as well as the supervised implementation of your entire environment here.

2 WEEKS
Roll-out after successful implementation; within these 2 weeks your employees will receive information on how to use the software. The actual registration takes place in two steps for the user:

- Receipt of an email with the documentation and subsequent installation of the DoubleClue App (desktop or mobile).
- Registration in the app via QR code or data entry

2 WEEKS
Hyper care support by HWS to ensure a smooth roll-out and high user adoption.

SAMPLE IMPLEMENTATION GUIDE FOR A SaaS LICENSE

We estimate a maximum of two months for implementation and roll-out when using a SaaS license (incl. test phase).

The effective working time without the test phase is about 1–2 weeks, depending on the size of the company.

ZERO-TIME
After your request, you will receive an email from us with the URL and your dial-in details to your DoubleClue tenant in our German high-security cloud. You can now fully use DoubleClue.

1 MONTH
We estimate one month for the test phase. Depending on your choice of support scope, we already offer you training of your admins as well as the supervised implementation of your entire environment here.

0.5 –2 DAYS
Technical implementation; time required depending on the complexity of your IT landscape

2 WEEKS
Roll-out after successful implementation; within these 2 weeks your employees will receive information on how to use the software. The actual registration takes place in two steps for the user:

- Receipt of an email with the documentation and subsequent installation of the DoubleClue App (desktop or mobile).
- Registration in the app via QR code or data entry

2 WEEKS
Hyper care support by HWS to ensure a smooth roll-out and high user adoption.

TECHNICAL FUNCTIONALITIES

DoubleClue supports all common protocols such as SAML, OpenID, or RADIUS. With just a few clicks, you can set up 2-factor authentication for remote access, so your employees can work from anywhere–and still have the best possible security.

VPN SECURING VIA RADIUS PROTOCOL

The RADIUS (Remote Authentication Dial-In User Service) protocol can be used to secure user identities and access rights via VPN. Service providers (VPN) and identity providers (DoubleClue) exchange IP addresses and a shared secret key to identify users. The link is quick and easy to implement, so securing VPN does not require significant effort.

EXCHANGE OF METADATA VIA SAML OR OPENID

SAML (Security Assertion Markup Language) is used to exchange metadata to link the service provider and DoubleClue in a trustworthy manner. Depending on the provider, the necessary metadata includes certificates and web addresses, as well as a few other attributes required by the service provider. The setup is also quick and straightforward.

DoubleClue integrates on premise and cloud („as a service") services via all kinds of common standards:

- RADIUS: well-known network protocol especially for VPN and firewall solutions
- SAML 2.0 and OpenID / Oauth 2.0: Web-based SSO protocols, especially web services such as AWS, Dropbox, ...
- APIs / REST interfaces: Open programming interfaces for web applications.
- Active Directory Federation Services (ADFS) plugin: Authentication of .NET platforms and all web-based MS products such as Office 365 or OWA
- Remote Gateway WebAccess Plugin: Securing Microsoft Remote Desktop connections
- ADFS Windows and Linux OS Login: Securing the workstation and access to the operating system

Your benefits with DoubleClue:

- Easy protection of cloud-based MS products like O365
- Support for all user directories
  - Active Directory
  - Azure AD
  - LDAP Directories
- Automatic import of users and groups from the domain
- Automatic synchronization in real time: added and deleted users as well as domain settings

ACCESS TO EXISTING ACTIVE DIRECTORY

DoubleClue accesses your existing Active Directory. You don't need to create your user directories from scratch but can easily access the existing data. With DoubleClue, you can create or deny access to groups of users and create policies. For example, timeouts, restrictions on authentication methods, and the classification of secure networks that do not require multiple multifactor authentications.

SUPPORT FOR HYBRID ENVIRONMENTS

Often companies use some older applications on-premises and newer ones already in the cloud. DoubleClue connects both worlds so you can secure your hybrid environment with just one tool. All you need to do is create an agent for your tenant to switch between cloud and on-premise environments.

MULTI-TENANT

Complex enterprises with a highly differentiated business structure require the greatest possible flexibility in installation. That's why DoubleClue allows you to install multiple, separate, and completely segregated tenants for clear access management. This allows you to include strategic partners or suppliers as well as customers or freelancers in addition to internal resources.

CUSTOMER REFERENCES

SECURING REMOTE WORK

Our customer from the field of politics/public institutions needed to secure its employees while working from home using multifactor authentication. In this sensitive area, the protection of speakers during digital conferences on explosive political topics is particularly relevant to exclude eavesdropping.

The actual company network had already been equipped with a VPN beforehand. Due to the existing IT infrastructure, we were able to complete the implementation, test phase, review phase, and go-live in about two hours each.

SECURING CRITICAL INFRASTRUCTURE

Our customer from the energy supply sector needed stronger protection for its control network in the area of water, electricity, and gas supply using MFA and IAM. Both remote workstations and on-site PCs needed to be secured, as the lack of access controls meant that stronger authentication methods were also required for PCs in the field.

In addition to standard security for normal users, users requiring special protection (PAM) were also defined.

By using DoubleClue, we were able to create individual policies for the three identified user groups. Using a so-called PAM (Privileged Access Management), we were able to introduce stricter access and authentication solutions for the, particularly critical systems. The customer uses a Windows operating system on its computers. DoubleClue secures the existing Windows logins with a second factor, making it impossible to log in only by using the Windows password.

SECURE DIGITIZATION

Our customer from the steel industry needed help securing its digitization strategy, especially cloud-based collaboration tools.

Also, they needed special protection for the personnel server on which all employee data is stored. We were able to separate this from the rest of the IT using a separate tenant so that only the HR manager now has access to it via MFA.

HWS INFORMATIONSSYSTEME GMBH

The HWS Group offers its customers comprehensive IT services, especially in the areas of operations and software development. With our more than 180 employees from Neustadt an der Aisch and the near-shore delivery center on Malta, we support and accompany well-known customers within the scope of long-term projects.

The focus is on international companies from the insurance, automotive, and healthcare industries, fashion/lifestyle as well as the bigger medium-sized companies of all sectors. We offer a wide range of highly qualified IT services in the B2B sector such as infrastructure management, IT operations, IT service desks, software development for complex applications including DevOps for the maintenance and further development of software solutions. Our IT security solution "DoubleClue" is accompanied by our German development team as well as German and English speaking support to provide companies worldwide with secure identity and access management as well as a strong multifactor authentication solution.

IT Security made in Germany!

As a medium-sized company with a long company history, we are a reliable and close partner; we value personal relationships, which is why we respond individually and directly to each customer and their wishes and requests. We see ourselves as a direct partner and do not communicate via automated tools or through outsourced support. You always have direct and close contact with us!

Learn more about us and our services and software products here.

hws-gruppe.de // doubleclue.com

HWS GRUPPE

DOUBLE CLUE

YOUR CONTACT

Marc Pantalone, Business Development Manager

HWS INFORMATIONSSYSTEME GMBH
Wilhelmstr. 16 | 91413 Neustadt a. d. Aisch

+49 (0) 151 6733 5945

marc.pantalone@hws-gruppe.de

We are partners

Allianz für Cyber-Sicherheit
Partner