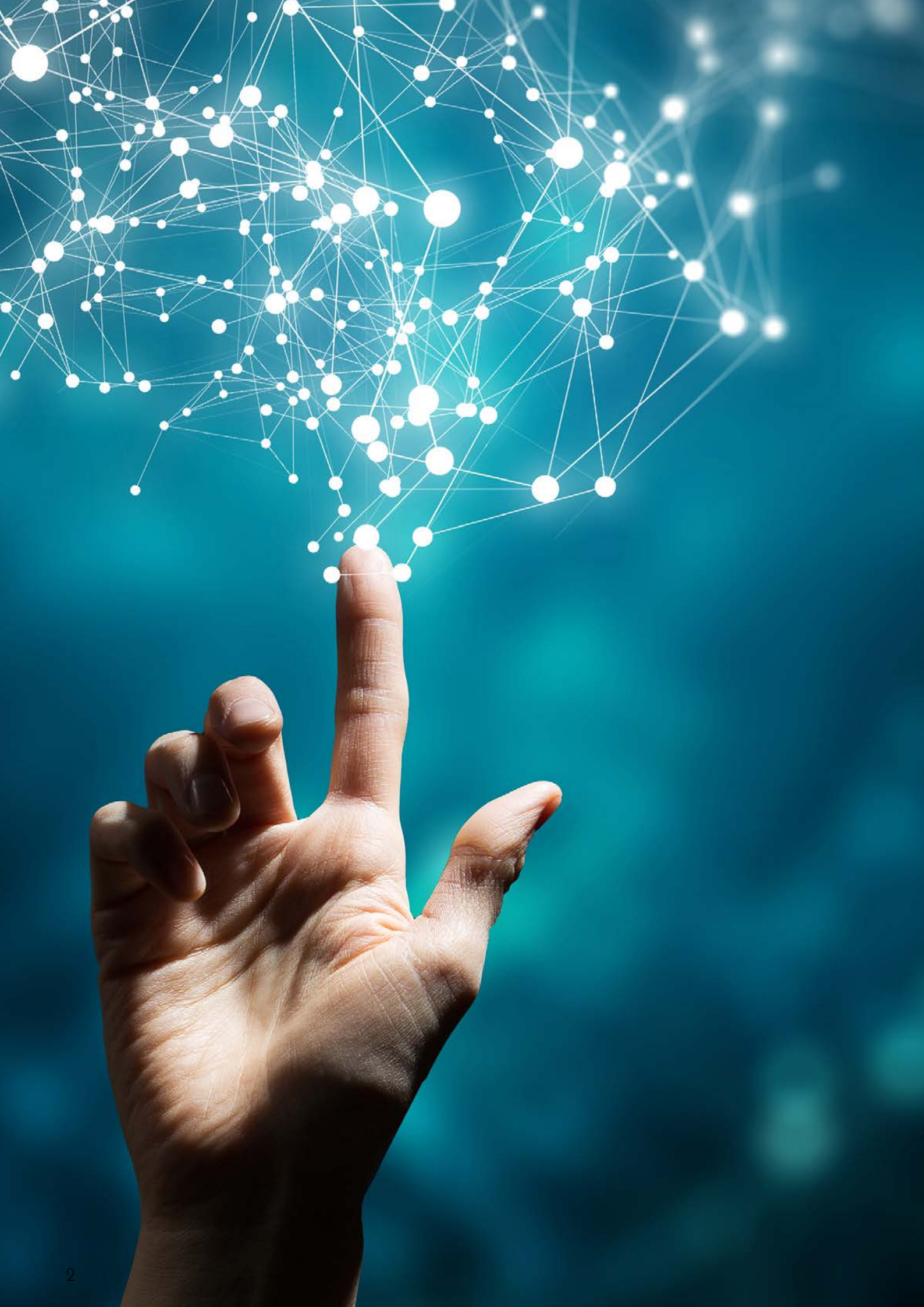




DOUBLECLUE

Cleverly Secures Identities





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

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

Such attacks were often due to the (unintentional) assistance of employees, for example, when they disclosed access data as a result of social engineering campaigns. But weak and reused passwords, unclear access policies, and a lack of security barriers also create vulnerabilities that make your systems attractive to cybercriminals.

EFFECTIVELY SECURE YOUR EMPLOYEES' IDENTITIES

Consequently, the biggest vulnerability in your network is humans. The algorithms and AI that underpin virus scanners and threat protection today are so sophisticated that they are good at detecting malware and intercepting it before it can become a threat.

However, humans find this difficult: especially with 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 carelessness, (apparent) compulsions, or emotional influence. Research shows that data and personal (identification) information are often willingly disclosed if an emotional connection

can be established. This so-called social engineering can be found in phishing emails as well as in fraudulent phone calls or on fake websites.

By introducing a second factor to verify an employee's identity, they can reliably prevent identity fraud. Because only those who can identify themselves twice—with a second factor known only to them—are granted access to a file or system.

In addition, clear and goal-oriented access management ensures that only those employees who need access to sensitive areas of your corporate IT have it. This is especially relevant in finance, HR, and IT departments to minimize potential risks of misuse of data and systems.

DoubleClue is a comprehensive software for secure management of identities, accesses, and passwords as well as a central storage of sensitive data.



DOUBLECLUE - ALL FEATURES

DoubleClue reliably protects your company network from unauthorized and harmful third-party access. The software combines state-of-the-art Identity & Access Management (IAM) with state-of-the-art Multifactor Authentication (MFA) and comes standard with additional security functionalities that facilitate the daily work and collaboration of your employees.

IDENTITY & ACCESS MANAGEMENT

You can centrally manage accounts, identities, and accesses in the structured IAM platform. The core is the access management to systems and applications with automated authorization management and adaptive access guidelines for applications and user groups. This also allows the establishment of a so-called Privileged Access Management (PAM).

TWO-FACTOR AUTHENTICATION

Easy-to-implement two-factor authentication prevents intrusions into your network. DoubleClue offers you all the possibilities of a modern, password-free login: Choose the

DOUBLECLUE OFFERS YOU EIGHT OPTIONS FOR AUTHENTICATION

- Password (as the first factor)
- Push notification (passwordless login with DoubleClue app)
- QR code (passwordless login with DoubleClue in the DoubleClue app)
- OTP / One Time Passcode (also offline)
- OTP Hardware Token
- FIDO Token (biometric and others)
- Voice Message
- SMS passcode
- Desktop App with passcode (no smartphone required)

variant that best suits your company from various authentication options.

SINGLE SIGN-ON (SSO) DOUBLECLUE MYAPPLICATIONS

Your employees work simultaneously in different applications for which they need separate accounts with their access data. Thanks to Single Sign-On, a single login in DoubleClue MyApplications is sufficient to gain access to all required applications—with just one click.

PASSWORDSAFE WITH AUTOFILL FUNCTION

DoubleClue PasswordSafe greatly simplifies the management of many, even complex passwords. Easily store your passwords in one place and access them in bundles—directly from the web app or mobile app. MFA and encryption ensure that passwords are kept safe in your safe.

Autofill lets you conveniently log in anywhere from the DoubleClue app. This allows you to assign highly complex, secure passwords for each of your applications and accesses.

DOUBLECLUE KEEPASS PLUGIN

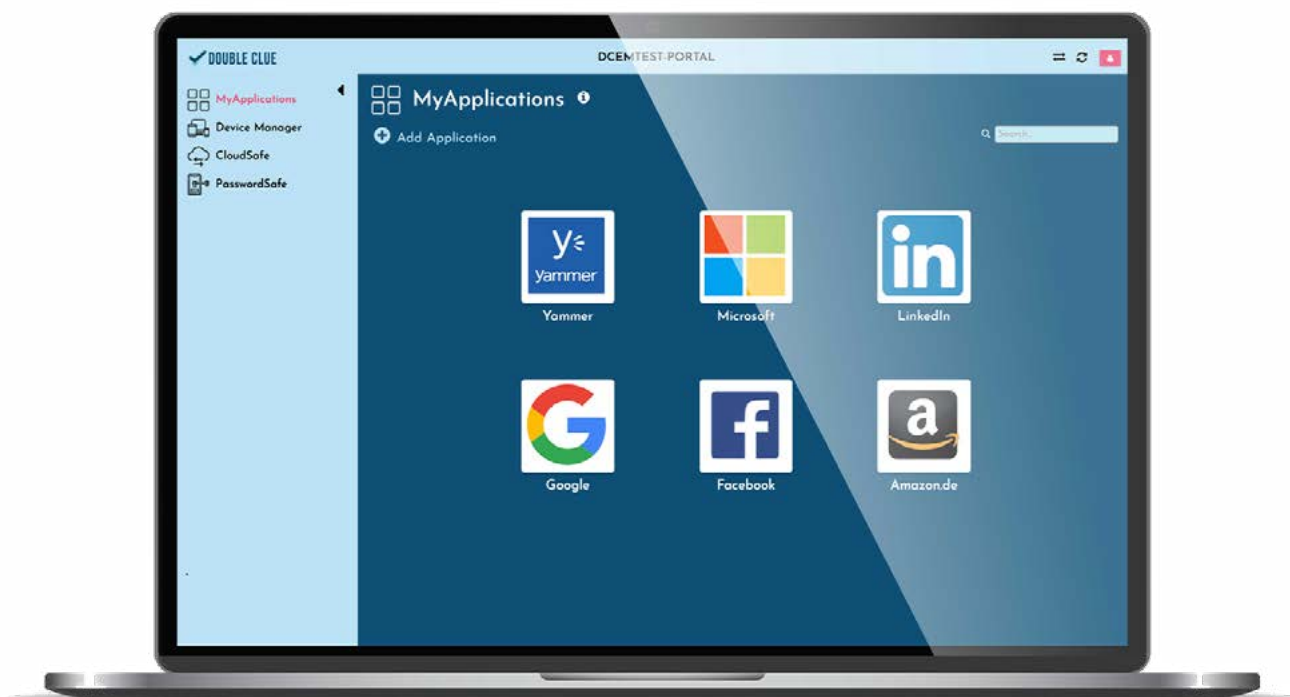
The globally popular open-source password manager KeePass lacks two things by default for use in an enterprise environment: multifactor authentication and the ability to share passwords with colleagues, partners, and service providers. The DoubleClue KeePass plugin allows easy import and export of password (kdbx) files between the two systems.

DOUBLECLUE APP FOR IOS & ANDROID

Users today expect high usability. Therefore, DoubleClue offers you the possibility to manage passwords and approvals via a modern and clear app on your mobile device.

DOUBLECLUE CLOUDSAFE

Important and confidential documents should never be sent via unencrypted emails. DoubleClue CloudSafe therefore not only allows you to centrally store sensitive data in an MFA-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—without your data leaving the server.



HIGH INTEROPERABILITY

DoubleClue can be fully and easily integrated into your infrastructure. The solution supports all common protocols and integrates on-premises and cloud ("as a service") services via common standards. The solution is therefore also ideally suited for hybrid environments.

- VPN and firewall security via **RADIUS** (Remote Authentication Dial-In User Service) protocol
- Integration of web-based single sign-on protocols such as **SAML 2.0** (Security Assertion Markup Language) and **OpenID/ OAuth 2.0**
- Connection to open programming interfaces for web applications via **APIs** (Ap-

plication Programming Interface) or **RESTful APIs**

- Authentication of .NET platforms and web-based MS products using **Directory Federation Services (ADFS) plugin**
- Securing Microsoft Remote Desktop connections via **Remote Gateway Web-Access plugin**
- Access to existing **Active Directory**, e.g. Azure AD, LDAP Directories to automatically import users and groups from the domain, including real-time synchronization



REMOTE SPARK



Meraki

SONICWALL™



OS LOG-IN SECURE (WINDOWS/ MAC/ LINUX)

Every machine needs an operating system to become accessible to users. Hardly any user is aware of the fact that there is a serious security gap even before the actual log-in: This is because it is possible to bypass the log-in process.

DoubleClue can close this gap for Microsoft, Mac, and Linux-based systems and thus not only secure your user identities but also prevent access to your system in general. Especially if you have no access restrictions to your premises, you should secure local access with MFA.

SECURING 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 client to switch between cloud and on-premises environments.

LEVERAGE EXISTING ACTIVE DIRECTORY (AD) TO CREATE ADAPTIVE POLICIES

DoubleClue accesses your existing Active Directory. You don't need to create your

user directories from scratch, you can conveniently use your existing data. Policies allow you to create user groups and associated access rights in DoubleClue, as well as create advanced rules. These include timeouts, restrictions on authentication methods, and classification of secure networks that do not require repeated multifactor authentication.

MULTI-TENANT CAPABILITY ENABLES PRIVILEGED ACCESS MANAGEMENT

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

Because of this multi-client capability, DoubleClue also allows deep Privileged Access Management (PAM) to separate areas that require special protection. You can define the policies for this individually, depending on your company's data protection and compliance policies.

YOUR BENEFITS WITH DOUBLECLUE

INCREASE EMPLOYEE SATISFACTION

A simplified login process increases your employees' productivity and acceptance. Thanks to centrally stored passwords, they no longer have to actively remember a large number of complex passwords. In addition, thanks to single sign-on, employees can log on to their PC and thus to their applications with a single click. The DoubleClue UserPortal allows uninterrupted switching within applications.

At the same time, your admins can do away with complex password policies for logging on to the PC. Even a simple password becomes a secure log-in with the highest security requirements thanks to the additional MFA.

SECURELY CONNECT EXTERNAL NETWORKS

Modern work also means remote work. Increasing digitization offers more and more opportunities for location-independent work. 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 technically secure these networks thanks to MFA and IAM.

Especially cloud tools connected to the Internet, e.g. for collaboration or communica-

tion, are an additional risk in these networks. Especially if they were introduced at short notice and without sufficient security standards or are even used on private devices.

SHARING DATA ACCESS WITH INTERNAL & EXTERNAL CONTACTS

In the remote work environment, data transfer of important and especially confidential documents is also at risk. But it's not just your employees distributed in virtual teams that are a potential security vulnerability for your IT or confidential documents here: equally—and perhaps to an even greater extent—it's external stakeholders that pose a potential risk. After all, how do you guarantee that the same high-security standards apply there as in your company?

The integrated DoubleClue CloudSafe stores confidential documents in a centralized location secured by MFA in your private or the German DoubleClue Cloud. This centralized encrypted storage allows you to give employees, external partners, suppliers or freelancers access to the 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 and internal stakeholders alike, so you can be sure your data remains confidential.





STAY AGILE

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 allows your employees to access your data even when they are hosted in-house—no matter where they are.

We also offer our customers full-service support in connection with the implementation and support of their DoubleClue applications. You can flexibly adapt the level of support to your business model: From the HWS all-around carefree package of implementation, roll-out, and support to individually tailored services—we will be happy to advise you on the best implementation for you.

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

- From the stand-alone license to the HWS all-around 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
- 90-day free trial with support
- Full support of implementation and roll-out

DO NOT ADAPT YOURSELF
TO THE SOLUTION, THE
SOLUTION ADAPTS TO YOU.



EXEMPLARY IMPLEMENTATION OF AN ON-PREMISES LICENSE

We estimate a maximum of two months for implementation and roll-out when using an on-premises license (including the 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 to install 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 trial period. Depending on your choice of support scope, we already offer training of your admins here as well as the supervised implementation of your overall environment.

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 process 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 acceptance.

EXEMPLARY IMPLEMENTATION OF AN SaaS LICENSE

We estimate a maximum of two months for implementation and roll-out when using a SaaS license (including the 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, we will send you an email with the URL and your dial-in data to your DoubleClue client in our German high-security cloud. You can now fully use DoubleClue.

1 MONTH

We estimate one month for the trial period. Depending on your choice of support scope, we already offer training of your admins here as well as the supervised implementation of your overall environment.

0.5–2 Days

Technical implementation; time required depending on the complexity of your IT environment

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 process 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 acceptance.



USE CASES

VPN SECURITY FOR REMOTE WORK IN PUBLIC INSTITUTIONS

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

The actual company network was already equipped with a VPN beforehand. Thanks to the RADIUS protocol integrated into the solution, DoubleClue enables deep technical protection of VPNs with multifactor authentication set up. This ensures that an unauthorized person cannot access the secure VPN network—including the provider and operator of the VPN client.

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 CONTROL NETWORK

Our customer from the energy supply sector needed strong protection for its control network in the area of water, electricity, and gas supply, separated from the rest of the infrastructure by means of MFA and IAM. This includes remote workstations as well as PCs in the field, as the latter were potentially accessible due to weak access controls.

Based on our client's requirements, we were able to identify three user groups, each of which required individual access policies. In addition to the standard protection of normal users, we used DoubleClue to define users requiring special protection and assigned them stricter access and authentication solutions for the, particularly critical systems by means of a so-called PAM (Privileged Access Management).

Furthermore, the customer uses a Windows operating system on its computers. DoubleClue secures the Windows log-ins so that it is not possible to bypass the login process. In addition, strong multifactor authentication was made mandatory for all users.



SECURE DIGITIZATION IN MEDIUM-SIZED BUSINESSES

Our mid-market customer in the steel industry needed help securing its digitization strategy. The expansion of remote work introduced cloud-based communication and collaboration tools, as well as a new VPN tool.

DoubleClue now protects VPN connection technically while unifying the login process with MFA on the network and connected machines.

In addition, the customer needed special protection for the personnel server where all employee data is stored. The high-security requirements for data protection in the personnel area made it necessary to technically separate the personnel department from the rest of the idea. By means of a separate client, the HR department was separated from the rest of the IT. Strict access restrictions mean that only the HR manager can access this client after verifying his own identity.

DIGITIZATION OF MEDICAL FACILITIES

Our medical facility clients need comprehensive software to accompany their digitization. This is because improved networking, especially with cloud or software-as-a-service applications, increases the potential for danger many times over due to their openness to the Internet. At the same time, patient and health data are documents that require special protection.

Collaborative use of machines and applications is also mapped by the DoubleClue solution. In the area of access and identity management, DoubleClue offers comprehensive solutions for authentication on shared devices. DoubleClue guarantees the highest security standards while ensuring the usual uninterrupted login and workflows.

DoubleClue is the comprehensive hospital identity management software that combines the highest IT security standards with the first-class usability.

HWS INFORMATIONSSYSTEME GMBH

HWS Gruppe offers its customers comprehensive IT services, software development, and consulting, especially in the areas of IT infrastructure, cloud operations, and identity protection. More than 150 employees from Neustadt an der Aisch (Middle Franconia) and the near-shore delivery center in Malta support both DAX corporations and upper mid-sized companies in holistic IT projects. Thanks to a progressive and demanding service approach, we have been convincing customers as a reliable and close partner for more than 20 years.

IT Security made in Germany!

Our comprehensive IT security solution "DoubleClue" provides companies worldwide with secure identity and access management as well as a strong multifactor authentication solution..

Learn more about us and our services and software products at hws-gruppe.de & doubleclue.com.

