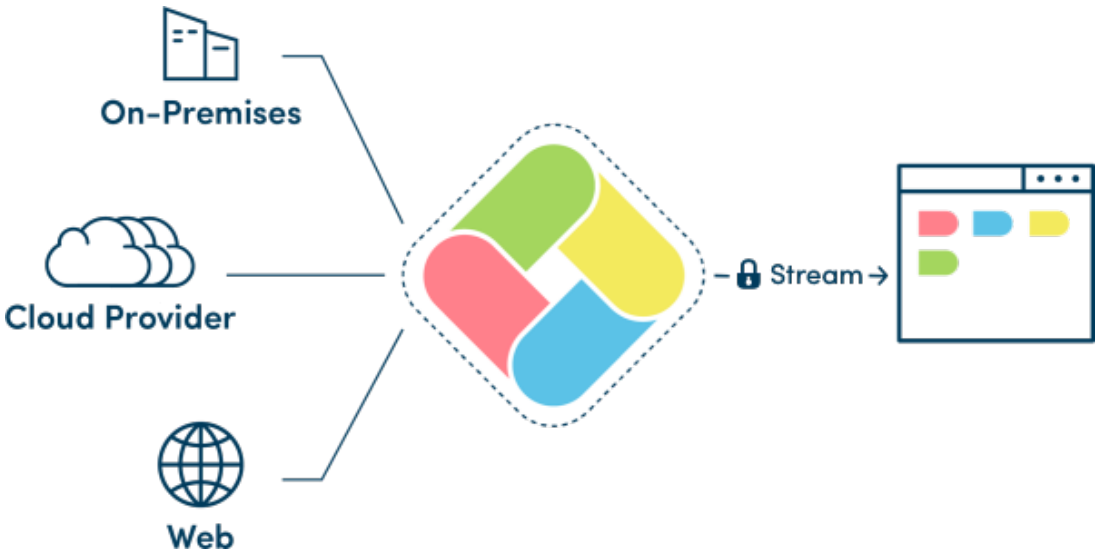
oneclick™
accessing the unlimited

Information

Security-as-a-Service with oneclick™

Status: April 20, 2020

oneclick™ is a turnkey cloud service with integrated security for the provisioning and delivery of applications and data. The platform acts as an intermediary and at the same time as a separation layer between all users and enterprise resources, no matter where they are located and who is providing them. The security architecture reliably shields critical systems from external attackers. oneclick™ works with any server location and any type of deployment: Native Windows, Linux and MacOS applications hosted on-premises or in the cloud, as well as internal and external web applications.



1. Advantages of oneclick™ as a new delivery model

Implement a Zero Trust Architecture

The oneclick™ platform is based on best practices in IT security, namely the principles of a Zero Trust Architecture (ZTA). In this approach, no actor who wants access to resources or services in the network is trusted from the outset. Every access, whether from outside or inside, is individually authenticated. Users are not only checked each time they log in, but their trust status is continuously queried during the sessions. If a change is detected that poses a risk, the granted access to a service is interrupted. Zero Trust focuses on the protection of defined company resources instead of individual network segments. oneclick™ supports customers in the consistent implementation of the concept.

An effective weapon against malware

Connections that remain open on the internet can be entry points for malware attacks. These include, for example, Microsoft Exchange, terminal or RDS servers, or client-to-site VPN connections to the corporate network. They are often used in the home office and in field service, and are especially vulnerable. Because no client-to-site VPN connections are required with oneclick™, the platform closes known entry gates by design. There is simply

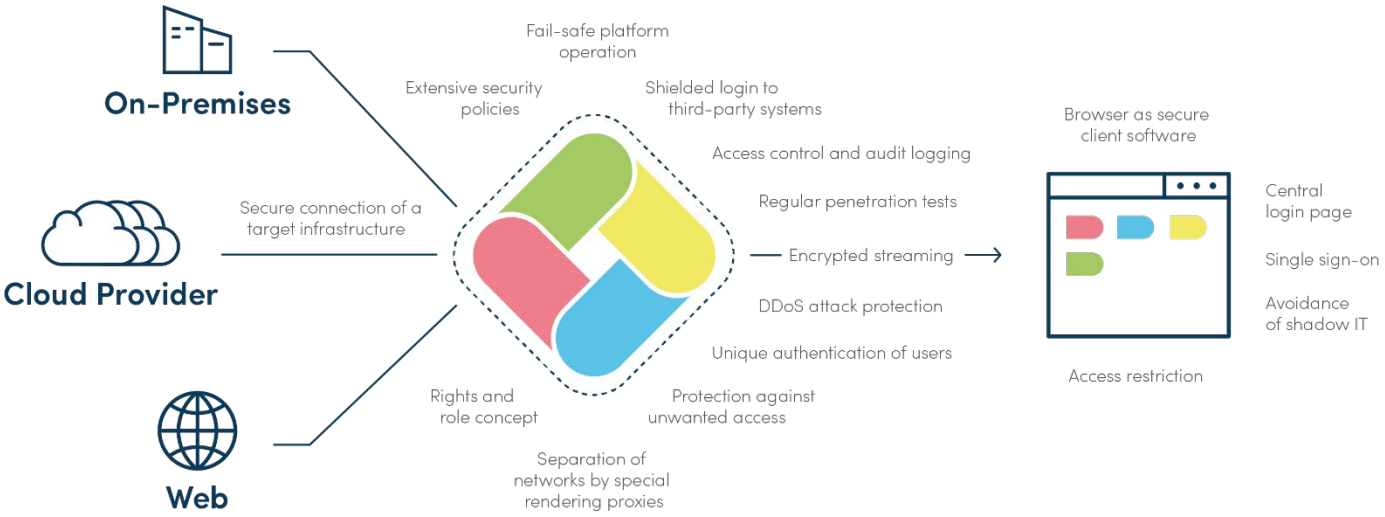
no point of attack for malware anymore. The streaming method used by oneclick™ ensures that no end device can infect an application server because direct communication between the user and the target system is entirely ruled out. It also does not matter anymore whether all updates and patches are available on the end devices.

Elimination of solutions for Endpoint and Mobile Device Management

With oneclick™, real BYOD can be implemented by allowing employees to immediately use their private end devices for their work without installing clients or plug-ins. No additional solutions for Endpoint and Mobile Device Management (MDM) are required. These attempt to make users and devices part of a trusted zone by installing clients and certificates. However, these solutions are complex to implement and manage. Malware can take over unnoticed devices that are actually trusted. oneclick™ is a new model that no longer requires the concept of trusted devices. The safe barrier is the browser.

2. Included safety mechanisms

oneclick™ includes numerous security mechanisms that are available "out-of-the-box" as a service to protect your corporate network, infrastructure, applications and data against cyber attacks.



Fail-safe platform operation

To ensure a stable and continuous service, the oneclick™ platform is operated on a scalable cluster, multi-redundant and at different locations in the Google Cloud, with Microsoft Azure as an immediately available backup solution.

Dedicated environment for each customer

Through the design of oneclick™ and the Kubernetes technology applied, each customer gets his own isolated environment. Only the oneclick™ orchestration platform and the streaming pods are operated in the public cloud, while applications and data in connected data centres are safe from foreign authorities due to the connection and encryption mechanisms described below.

Protection against unwanted access

oneclick™ is effectively protected against unwanted access through an intelligent, multi-layered combination of intrusion detection and prevention systems (IDS/IPS), web access firewall (WAF) and service defined network rules. The platform has also implemented the SSL Cipher Suite and Security Header according to OWASP.

DDoS attack prevention

Operating oneclick™ in the Google Cloud and Microsoft Azure data centres has the advantage that you benefit from the mature DDoS protection measures of the large hyperscalers. Their systems detect normal traffic patterns through monitoring and machine learning and reliably block attacks. The existing capacities of the backbone networks help to route out malicious traffic.

Secure connection of a target infrastructure

For a secure connection between the oneclick™ platform and a target infrastructure, an automated process is used to set up a permanent VPN tunnel in an isolated container according to the IPSec standard. The communication between oneclick™ and the connected server locations takes place via the common protocols RDP, VNC, SSH and Telnet. From oneclick™ no software component has to be installed on the servers.

Encrypted streaming

Due to the self-developed streaming technology, only an image of the connected system reaches the receiver. There is no risk of lost, stolen or defective end devices because applications and data never leave the secure hosting location. Control signals, e.g. from the mouse or keyboard, are transmitted back asynchronously. The connection between the streaming servers and the user's browser is encrypted with 256 bit TLS 1.2 (the successor of SSL).

Separation of networks by special rendering proxies

A key aspect of logical security is separation at the protocol level. A proxy secures the communication with the target system and translates the original remote protocol into an image or video stream. This deprives a man-in-the-middle attacker of the basis for introducing malicious code, and of automated scanning and exploitation of vulnerabilities in the original remote protocol.

Unique authentication of users

To authenticate users, oneclick™ supports OpenID Connect (OIDC). OIDC uses the OAuth 2.0 protocol. Authentication can be outsourced to any third-party services that support OIDC, such as Azure AD, Okta, Ping Identity, Google, LinkedIn, Facebook, etc. Alternatively, a login with classic username and password combined with a second factor is possible. Such credentials are stored in a password vault, which can be located either at oneclick™ or in the customer's local data centre. The trust status is continuously checked during a session. Cookies are re-validated every 5 seconds.

Single Sign-On

The oneclick™ Single Sign-On Service improves security because the password is only transmitted once and the user only has to remember one password instead of a large number of mostly insecure passwords. This one password can be complex and secure.

Shielded login to third-party systems

If oneclick™ is used as an authentication service, the user's login to oneclick™ is the only login where the username and password are transported via the browser as a client. All other authentication processes are performed by backend systems. For the login, dynamically generated, unique passwords and tokens are used, which are not stored by oneclick™. The login information to applications remains hidden for the users.

Extensive security policies

A second factor can be added to validate a user's identity. oneclick™ uses either a time-based one-time password algorithm (TOTP method) or a text message via Short Message Service (SMS). Also, the access (only) from certain IP addresses can be allowed or disallowed. Security policies may be applied to entire workspaces or single applications.

Access restriction

oneclick™ only grants access to shared applications and not to the entire corporate network. The oneclick™ Hybrid Drive allows you to restrict access to data. This ensures that files may only be downloaded from the server to the end device with authorisation.

Rights and role concept

Using the concept of roles, you can define in detail for your administrators who can access which areas within the management console and who can create, update, or delete which components, resources, or users.

Central login page

The central web portal for access to all applications and data makes phishing attacks more difficult because users only have to enter their username and password once, rather

than in numerous, scattered locations. This simplifies the verification procedures (URL, SSL server certificate, individual design, etc.).

Browser as secure client software

oneclick™ uses the browser on end devices as client software. Today's browsers are the most secure and most common clients. They can be deployed on all operating systems and end device types with restricted user authorisations. We recommend Google Chrome or Mozilla Firefox. The security settings of both browsers are updated daily. Both use sandboxing technology, i.e. they are only executed in a specific area of the operating system that is isolated from the rest.

Access control and audit logging

For special security situations and audit purposes, it is possible to trace all platform and application accesses in the form of log files and store them in a revision-proof manner.

Avoidance of shadow IT

End users are unable to independently install software in their workspace, which allows you to prevent the use of unauthorised software and interference with the corporate sphere.

Regular penetration tests

The oneclick™ platform is regularly subjected to penetration tests according to OWASP by the TÜV. No security problems were identified with regard to the web application, nor have any security gaps been found in the underlying services.

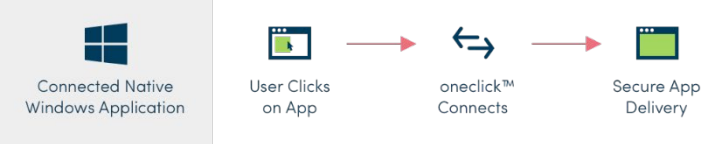
Security Operations Centre

The Security Operations Center (SOC) of the oneclick™ platform is operated by professional cyber security experts. The team works according to recognised standards and frameworks, such as MITRE ATT&CK, to reliably keep cyber risks in check.

3. The delivery process

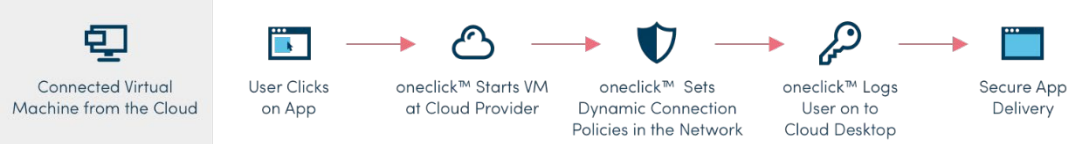
The intelligent security of oneclick™ protects all types of applications, internal websites, desktops and data from the dangers of cyber attacks. Even legacy applications can be brought up to the state-of-the-art through the oneclick™ platform. With the help of oneclick™, secure hybrid environments of on-premises and public or private cloud can be easily implemented, which the user can reach via the workspace in the browser.

On-premises



When a user clicks on an app title from his workspace, oneclick™ checks the user's permissions. If the required rights are assigned, oneclick™ establishes a connection to the target application, opens it in the browser and logs the user in. The app is delivered to the user as an encrypted stream.

Cloud



When accessing a virtual machine, the user initiates an action at the cloud provider by clicking on the desired tile in the workspace, e.g. the start of a desktop. Then, oneclick™ starts the virtual machine and sets a dynamic network policy which only allows access from oneclick™. Now oneclick™ logs in the user and the desired application is securely delivered as an encrypted stream.

Web

An analogous process is triggered when accessing company internal web applications. The user selects the desired application while oneclick™ checks the authorisation and starts a secure container. In this secure container environment, the user is logged into the internal app and this is delivered as an encrypted stream. Therefore, even legacy applications can be securely deployed via oneclick™. For this purpose, oneclick™ offers a unique "Browser in Browser" technology. Unlike other solutions, no additional terminal servers or RDS licenses are required to protect web applications and prevent access from the public internet.

Do you have any questions or would you like further information?

We would be delighted to help you further!

Mr. Dominik Birgelen
Customer Success Manager

Phone: +41 44 578 88 93
Email: dominik.birgelen@oneclick-cloud.com

oneclick™ - the Everything-as-a-Service Platform

As a central access and distribution platform in the cloud, oneclick™ enables the management of the entire technology stack for application provisioning. oneclick™ combines software, platform and infrastructure as a service from any on-premises and cloud environment behind one web portal.
Everything-as-a-Service (XaaS) means that you can consume all of this as a service.

oneclick™
accessing the unlimited

oneclick AG
Zollikerstraße 27
CH-8008 Zurich

T (+41) 44 578 88 93
info@oneclick-cloud.com
https://oneclick-cloud.com