oneclick™
accessing the unlimited

Information

Security-as-a-Service with oneclick™

Status: November 01, 2019

As a complete solution for the provision of applications and data, oneclick™ relies on the latest technologies and international standards. The oneclick™ platform functions as a separation layer between remote users and the corporate network. The security architecture shields critical systems from all external attackers.

1. Advantages of oneclick™ as a new delivery model

An effective weapon against malware

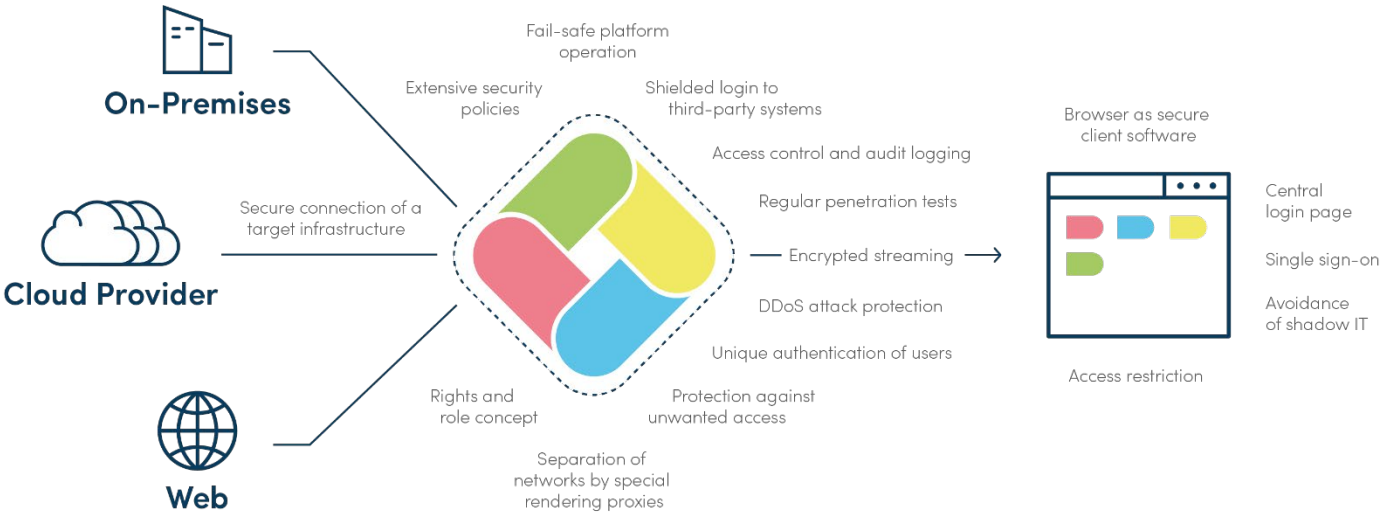
Connections, such as Microsoft Exchange, terminal or RDS servers hanging openly on the internet, or especially the client-to-site VPN connections to the corporate network often used in the home office and field service, can be open entry points for malware attacks. Because no client-to-site VPN connections are necessary with oneclick™ and the platform thus closes known entry points ad hoc, there is simply no point of attack for malware. Due to the streaming method used by oneclick™ in the browser, no end device can infect an application server because direct communication between the user and the target system can be completely ruled out. It does not matter whether all updates and patches are available on the end devices.

Enable real Bring Your Own Device (BYOD)

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 such as Network Access Control (NAC), Mobile Device Management (MDM) and Enterprise Mobility Management (EMM) are required. These represent an attempt to make users and devices part of a trusted zone by installing clients and certificates on each device. 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 needs 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

For a stable continuous operation, 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. Due to the conception of oneclick™ and the used Kubernetes technology, all connected customer networks are strictly separated from each other.

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 to 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 as well as second factor is possible. The credentials are then 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 provides a gain in 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 prove 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 prevented. Security policies are individually applicable 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 offers the possibility to restrict access to data. If there is no authorisation, no files can be downloaded from the server to the end device.

Rights and role concept

Using a role concept, 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 in one place and no longer in numerous, scattered places. This one place can be more easily checked for correctness (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.

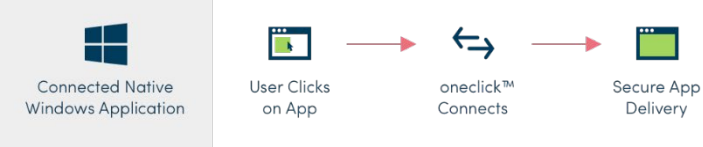
Regular penetration tests

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 and no security gaps were found with regard to the underlying services.

3. The delivery process

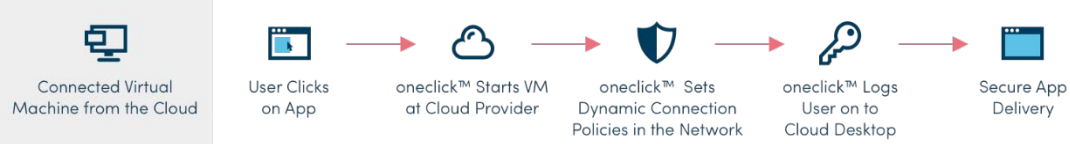
The intelligent security of oneclick™ protects all types of applications, internal websites, desktops and data from the dangers of cyber attacks. Even legacy applications can be brought up to the state-of-the-art through the oneclick™ platform. With the help of oneclick™, secure hybrid environments of 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, 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.

4. oneclick™ and the Zero Trust Network Approach

With Zero Trust, no actor who wants access to resources or services on the network is trusted from the outset. Each access is individually authenticated. **Forrester** already coined the term in 2010 and in 2018 presented Zero Trust eXtended (ZTX), a further developed framework that IT managers can use to build their security architectures according to Zero Trust. The concept is based on two central pillars:

- identify sensitive data and map their flow;
- clarify who, when, where, why and how accesses data and what is done with it.

This is based on the conviction that companies should neither trust their customers, employees nor applications within nor outside the company boundaries. Instead, everything that attempts to access corporate data must be reviewed and controlled.

In 2014, **Google** defined its own Zero Trust variant with a context-based access concept called BeyonCorp. Initially, BeyonCorp was only used internally, but in 2019 Google began implementing the technology in its customer services.

Gartner's market researchers jumped on the Zero Trust trend with their CARTA approach in 2017. The abbreviation stands for "Continuous Adaptive Risk and Trust Assessment" and continues the original principle. According to CARTA, users, devices and apps must not only be checked each time they log on, but their trust status must also be continuously questioned during the session. If a change is detected that represents a risk, the access granted to a service can be restricted or completely interrupted.

Core concepts of the CARTA approach are:

- use unique security gateways through adaptive, context-dependent security platforms
- Continuous monitoring, evaluation and prioritization of risks and trust - reactive and proactive
- start early with risk and confidence considerations in digital business initiatives, already in the development process
- provide full, complete transparency, including the processing of sensitive data
- Identify responses faster with analytics, AI, automation, and orchestration and prioritize risk

Software Defined Perimeter (SDP) is another way to implement Zero Trust. The technology is based on the Black Cloud concept developed by the IT Security Authority of the US Department of Defense (DISA). It establishes network access and connections according to the need-to-know principle. The **Cloud Security Alliance (CSA)** describes the concept as a combination of the three parts:

- device authentication
- identity-based access
- dynamically provided connectivity

If someone wants to access an app or a resource in the network, he is authenticated for exactly this and gets there directly. Access management is moved from the network perimeter to the resource or app, so users never know where they are on the network.

The safety mechanisms of oneclick™ described under point 2 and 3 fully meet the requirements of a ZTN approach. The oneclick™ platform ideally supports customers in implementing the concept.

Further links:

- https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html
- https://cheatsheetseries.owasp.org/cheatsheets/REST_Security_Cheat_Sheet.html
- https://en.wikipedia.org/wiki/IPsec
- https://techcrunch.com/2019/04/10/google-extends-its-beyondcorp-security-model-to-g-suite/
- https://www.gartner.com/smarterwithgartner/the-gartner-it-security-approach-for-the-digital-age/
- https://en.wikipedia.org/wiki/Software_Defined_Perimeter
- https://cloudsecurityalliance.org/research/working-groups/software-defined-perimeter/#_overview
- https://en.wikipedia.org/wiki/Five_Ws

https://en.wikipedia.org/wiki/Transport_Layer_Security

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