oneclick™
accessing the unlimited

Information

Security-as-a-Service mit oneclick™

Stand: 01. November 2019

oneclick™ setzt als Komplettlösung für die Bereitstellung von Applikationen und Daten auf neueste Technologien und internationale Standards. Dabei funktioniert die oneclick™ Plattform als Trennschicht zwischen Remote-Usern und dem Unternehmensnetzwerk. Die Sicherheitsarchitektur schirmt kritische Systeme vor allen externen Angreifern ab.

1. Vorteile von oneclick™ als neues Bereitstellungs-modell

Eine wirkungsvolle Waffe gegen Schadsoftware

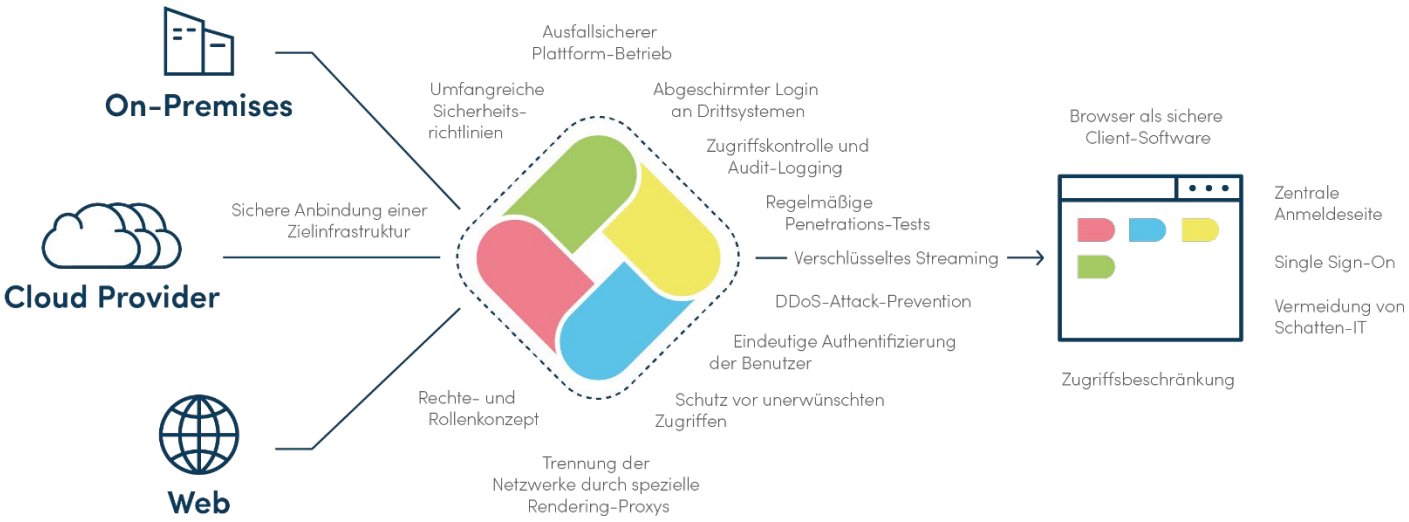
Verbindungen, wie offen am Internet hängende Microsoft-Exchange-, Terminal- bzw. RDS-Server oder besonders auch die oftmals im Homeoffice und Außendienst eingesetzten Client-to-Site-VPN Verbindungen zum Unternehmensnetzwerk, können Einfallstore für Schadsoftware-Angriffe sein. Weil mit oneclick™ keine Client-to-Site-VPN-Verbindungen mehr notwendig sind und die Plattform damit bekannte Einfallstore ad hoc schließt, gibt es schlichtweg keinen Angriffspunkt für Schadsoftware. Durch das von oneclick™ eingesetzte Streaming-Verfahren im Browser kann kein Endgerät einen Applikationsserver infizieren, denn eine direkte Kommunikation zwischen dem Anwender und dem Zielsystem kann vollständig ausgeschlossen werden. Es spielt keine Rolle, ob auf den Endgeräten alle Updates und Patches vorhanden sind.

Echtes Bring-your-own-Device (BYOD) ermöglichen

Mit oneclick™ lässt sich echtes BYOD umsetzen, indem Mitarbeiter ihre privaten Endgeräte umgehend für ihre Arbeit nutzen können, ohne Clients oder Plug-Ins zu installieren. Es werden keine zusätzlichen Lösungen, wie Network Access Control (NAC), Mobile Device Management (MDM) und Enterprise Mobility Management (EMM), benötigt. Diese stellen den Versuch dar, Benutzer und Geräte durch die Installation von Clients und Zertifikaten auf jedem Gerät zum Teil einer vertrauenswürdigen Zone zu machen. Allerdings sind diese Lösungen aufwändig zu implementieren und zu verwalten. Malware kann unbemerkt Geräte übernehmen, denen eigentlich vertraut wird. oneclick™ ist ein neues Modell, welches das Konzept der vertrauenswürdigen Geräte nicht mehr benötigt. Die sichere Barriere ist der Browser.

2. Enthaltene Sicherheits-Mechanismen

oneclick™ umfasst vielzählige Sicherheitsmechanismen, die „Out-of-the-Box“ als Service für Sie zur Verfügung stehen, um das Unternehmensnetzwerk, Ihre Infrastruktur, Applikationen und Daten bestmöglich vor Cyber-Angriffen zu schützen.



Ausfallsicherer Plattform-Betrieb

Für einen stabilen Dauerbetrieb wird die oneclick™ Plattform auf einem skalierenden Cluster, multi-redundant und an unterschiedlichen Standorten in der Google Cloud betrieben, mit Microsoft Azure als sofort verfügbarer Backup-Lösung. Durch die Konzeption von oneclick™ und die eingesetzte Kubernetes-Technologie sind alle angebundenen Kundennetzwerke strikt voneinander getrennt.

Schutz vor unerwünschten Zugriffen

oneclick™ ist durch einen intelligenten, vielschichtigen Verbund von Intrusion Detection und Prevention Systemen (IDS/IPS), Web Access Firewall (WAF) und servicedefinierten Netzwerkregeln effektiv gegen unerwünschte Zugriffe geschützt. Die Plattform hat darüber hinaus die SSL Cipher-Suite und Security Header nach OWASP implementiert.

DDoS-Attack-Prevention

Der Betrieb von oneclick™ in den Rechenzentren von Google Cloud und Microsoft Azure hat den Vorteil, dass Sie von den ausgereiften DDoS-Schutzmaßnahmen der großen Hyperscaler profitieren. Deren Systeme erkennen normale Datenverkehrsmuster durch Monitoring und maschinelles Lernen und wehren Angriffe zuverlässig ab. Die vorhandenen Kapazitäten der Backbone-Netze helfen beim Rausrouten von bösartigem Traffic.

Sichere Anbindung einer Zielinfrastruktur

Für eine sichere Verbindung zwischen der oneclick™ Plattform und einer Zielinfrastruktur wird über ein automatisiertes Verfahren ein permanenter VPN-Tunnel in einem isolierten Container nach dem IPSec-Standard aufgebaut. Die Kommunikation zwischen oneclick™ und den angebundenen Server-Standorten erfolgt über die gängigen Protokolle RDP, VNC, SSH und Telnet. Von oneclick™ muss keine Softwarekomponente auf den Servern installiert werden.

Verschlüsseltes Streaming

Aufgrund der selbstentwickelten Streaming-Technologie erreicht nur ein Bild des angebundenen Systems den Empfänger. Es besteht kein Risiko bei verlorenen, gestohlenen oder fehlerhaften Endgeräten, weil Applikationen und Daten niemals den sicheren Hosting-Standort verlassen. Kontrollsignale, wie z.B. von der Maus oder Tastatur, werden asynchron zurück übertragen. Die Verbindung zwischen den Streaming-Servern und dem Browser des Benutzers ist mit 256 Bit TLS 1.2 verschlüsselt (dem SSL-Nachfolger).

Trennung der Netzwerke durch spezielle Rendering-Proxys

Einen Kernpunkt der logischen Sicherheit nimmt die Trennung auf Protokollebene ein. Hierzu sichert ein Proxy die Kommunikation zum Zielsystem und übersetzt das ursprüngliche Remoteprotokoll in einen Bild- oder Videostream. Einem „Man-in-the-Middle"-Angreifer wird dadurch die Grundlage zur Einschleusung von Schadcode entzogen, ebenso wie der automatisierten Suche und Ausnutzung von Schwachpunkten im ursprünglichen Remoteprotokoll.

Eindeutige Authentifizierung der Benutzer

Zur Authentifizierung der Benutzer unterstützt oneclick™ OpenID Connect (OIDC). OIDC verwendet das OAuth 2.0-Protokoll. Die Authentifizierung kann an sämtliche Drittdienste ausgelagert werden, die OIDC unterstützen, wie z.B. Azure AD, Okta, Ping Identity, Google, LinkedIn, Facebook etc. Alternativ ist auch ein Login mit klassischem Benutzername und Passwort sowie 2. Faktor möglich. Die Credentials werden dabei in einem Password Vault gespeichert, der entweder bei oneclick™ oder im lokalen Rechenzentrum des Kunden liegen kann. Der Vertrauensstatus wird fortlaufend während einer Session hinterfragt. Cookies werden alle 5 Sekunden neu überprüft.

Single Sign-On

Der oneclick™ Single Sign-On Service liefert einen Sicherheitsgewinn, da das Passwort nur einmal übertragen wird und sich der Benutzer anstelle einer Vielzahl meist unsicherer Passwörter nur noch eines merken muss. Dieses eine Passwort kann dafür komplex und sicher gewählt werden.

Abgeschirmter Login an Drittsystemen

Wenn oneclick™ als Authentifizierungsdienst genutzt wird, ist die Anmeldung des Benutzers bei oneclick™ der einzige Login, bei dem der Benutzername und das Passwort über den Browser als Client transportiert wird. Alle weiteren Authentifizierungsprozesse werden von Backend-Systemen durchgeführt. Für den Login werden dynamisch generierte, einmalige Passwörter und Tokens verwendet, die nicht von oneclick™ gespeichert werden. Die Anmeldeinformationen an Applikationen bleiben für die Benutzer verborgen.

Umfangreiche Sicherheitsrichtlinien

Für den Identitätsnachweis eines Benutzers kann ein zweiter Faktor hinzugefügt werden. oneclick™ nutzt dafür wahlweise einen Time-based One-time Password Algorithmus (TOTP-Verfahren) oder eine Textnachricht via Short Message Service (SMS). Ebenfalls kann der Zugriff (nur) von bestimmten IP-Adressen erlaubt oder verhindert werden. Sicherheitsrichtlinien sind individuell auf ganze Workspaces oder einzelne Applikationen anwendbar.

Zugriffsbeschränkung

oneclick™ gewährt nur den Zugriff auf freigegebene Applikationen und nicht auf das gesamte Unternehmensnetzwerk. Das oneclick™ Hybrid Drive bietet die Möglichkeit, den Zugriff auf Daten einzuschränken. Liegt keine Autorisierung vor, können keine Dateien vom Server auf das Endgerät heruntergeladen werden.

Rechte- und Rollenkonzept

Über ein Rollenkonzept können Sie für Ihre Administratoren detailliert festlegen, wer auf welche Bereiche innerhalb der Managementkonsole zugreifen kann und wer welche Komponenten, Ressourcen oder Benutzer neu anlegen, aktualisieren oder löschen darf.

Zentrale Anmeldeseite

Das zentrale Webportal für den Zugriff auf sämtliche Applikationen und Daten erschwert Phishing-Attacken, da Anwender ihren Benutzernamen und Passwort nur an einer einzigen Stelle eingeben müssen und nicht mehr an zahlreichen, verstreuten Stellen. Diese eine Stelle kann leichter auf Korrektheit (URL, SSL- Serverzertifikat, individuelles Design, etc.) überprüft werden.

Browser als sichere Client-Software

oneclick™ nutzt den Browser auf Endgeräten als Clientsoftware. Heutige Browser sind die sichersten und üblichsten Clients. Sie können auf allen Betriebssystemen und Endgerätetypen mit eingeschränkten Benutzerberechtigungen bereitgestellt werden. Wir empfehlen Google Chrome oder Mozilla Firefox. Die Sicherheitseinstellungen beider Browser werden in täglichen Abständen aktualisiert. Beide verwenden eine Sandboxing-

Technologie, d.h. sie werden nur in einem bestimmten Bereich des Betriebssystems ausgeführt, der von den restlichen Bereichen abgeschottet ist.

Zugriffskontrolle und Audit-Logging

Für besondere Sicherheitslagen und Auditzwecke ist es möglich, sämtliche Plattform- und Applikationszugriffe in Form von Protokolldateien nachzuvollziehen und revisionssicher aufzubewahren.

Vermeidung von Schatten-IT

Endnutzer sind nicht in der Lage, selbständig Software in ihrem Workspace zu installieren, wodurch Sie den Einsatz nicht autorisierter Software und die Vermischung mit der Unternehmenssphäre ausschließen können.

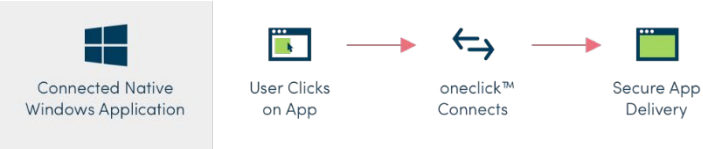
Regelmäßige Penetrations-Tests

Die oneclick™ Plattform wird regelmäßig Penetrations-Tests gemäß OWASP durch den TÜV unterzogen. Dabei wurden keine Sicherheitsprobleme bezüglich der Webapplikation identifiziert und keine Sicherheitslücken in Bezug auf die zugrunde liegenden Services gefunden.

3. Der Auslieferungsprozess

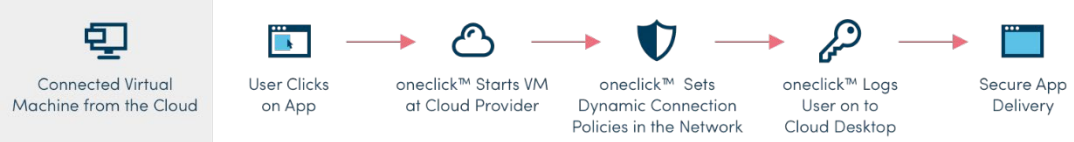
Die intelligente Sicherheit von oneclick™ schützt alle Arten von Applikationen, interne Webseiten, Desktops und Daten vor den Gefahren von Cyberattacken. Selbst Legacy-Anwendungen lassen sich durch die oneclick™ Plattform auf den aktuellen Stand der Technik bringen. Mit Hilfe von oneclick™ lassen sich problemlos sichere hybride Umgebungen aus On-Premises und Public oder Private Cloud umsetzen, die der Benutzer über den Workspace im Browser erreicht.

On-Premises



Wenn ein Benutzer in seinem Workspace auf eine App-Kachel klickt, überprüft oneclick™ die Berechtigungen des Nutzers. Sind die erforderlichen Rechte zugeteilt, stellt oneclick™ eine Verbindung zur Zielanwendung her, öffnet diese im Browser und loggt den Benutzer ein. Die App wird als verschlüsselter Stream an den Nutzer ausgeliefert.

Cloud



Beim Zugriff auf eine Virtuelle Maschine initiiert der Nutzer durch Klick auf die gewünschte Kachel im Workspace eine Aktion beim Cloud-Anbieter, z.B. den Start eines Desktops. oneclick™ startet anschließend die Virtuelle Maschine und setzt eine dynamische Netzwerk-Richtlinie, die nur Zugriffe aus oneclick™ zulässt. Nun loggt oneclick™ den Benutzer ein und die gewünschte Anwendung wird wiederum sicher als verschlüsselter Stream ausgeliefert.

Web

Ein analoger Prozess wird beim Zugriff auf firmeninterne Webanwendungen angestoßen. Der Benutzer wählt die gewünschte Anwendung aus, während oneclick™ die Berechtigung überprüft und einen sicheren Container startet. In dieser sicheren Container-Umgebung wird der Nutzer in die interne App eingeloggt und diese wird als verschlüsselter Stream ausgeliefert. Somit können über oneclick™ auch Legacy-Anwendungen sicher bereitgestellt werden. oneclick™ bietet dazu eine einmalige „Browser in Browser"-Technologie. Im Gegensatz zu anderen Lösungen werden keine zusätzlichen Terminal Server bzw. RDS-Lizenzen benötigt, um Webapplikationen zu schützen und den Zugang vom öffentlichen Internet zu verhindern.

4. oneclick™ und der Zero Trust Network Ansatz

Bei Zero Trust wird keinem Akteur, der Zugang zu Ressourcen oder Diensten im Netzwerk will, von vornherein vertraut. Jeder Zugriff wird individuell authentifiziert. **Forrester** prägte den Begriff bereits 2010 und stellte 2018 mit Zero Trust eXtended (ZTX) ein weiterentwickeltes Framework vor, anhand dessen IT-Verantwortliche ihre Sicherheitsarchitekturen gemäß Zero Trust aufbauen können. Das Konzept fußt auf zwei zentralen Säulen:

- sensible Daten identifizieren und ihren Fluss abbilden;
- klären, wer, wann, wo, warum und wie auf Daten zugreift und was mit ihnen gemacht wird.

Dahinter steht die Überzeugung, dass Unternehmen ihren Kunden, Mitarbeitern und auch Anwendungen weder innerhalb noch außerhalb der Unternehmensgrenzen vertrauen

sollten. Stattdessen muss alles und jeder überprüft und kontrolliert werden, der versucht, auf Unternehmensdaten zuzugreifen.

2014 definierte **Google** seine eigene Zero-Trust-Variante mit Kontext-basiertem Zugangskonzept namens BeyonCorp. Vorerst wurde BeyonCorp nur intern eingesetzt, Google begann jedoch 2019 damit, die Technologie auch in seine Services für Kunden zu implementieren.

Die Marktforscher von **Gartner** sprangen mit ihrem CARTA-Ansatz 2017 auf den Zero-Trust-Trend auf. Die Abkürzung steht für "Continuous Adaptive Risk and Trust Assessment" und führt das ursprüngliche Prinzip weiter. Nach CARTA gilt es, Nutzer, Geräte und Apps nicht nur bei jeder Anmeldung zu prüfen, sondern deren Vertrauensstatus fortlaufend während der Session zu hinterfragen. Wird eine Veränderung festgestellt, die ein Risiko bedeutet, kann der gewährte Zugang zu einem Service eingeschränkt oder ganz unterbrochen werden. Kernkonzepte des CARTA-Ansatzes sind:

- durch adaptive, kontextabhängige Sicherheitsplattformen einmalige Sicherheitsschleusen einsetzen
- Risiken und Vertrauen kontinuierlich überwachen, bewerten und priorisieren - reaktiv und proaktiv
- mit Risiko- und Vertrauensbetrachtungen in digitalen Geschäftsinitiativen frühzeitig beginnen, schon im Entwicklungsprozess
- umfassende, vollständige Transparenz herstellen, einschließlich der Verarbeitung sensibler Daten
- Reaktionen mithilfe von Analytik, KI, Automatisierung und Orchestrierung schneller erkennen und mit Risikopriorisierung versehen

Auch Software Defined Perimeter (SDP) ist eine Möglichkeit, Zero Trust umzusetzen. Die Technologie basiert auf dem Black Cloud-Konzept, das die IT-Sicherheitsbehörde des US-Verteidigungsministeriums (DISA) entwickelt hat. Darin werden Netzwerkzugänge und Verbindungen nach dem Need-to-know-Prinzip aufgebaut. Die **Cloud Security Alliance (CSA)** beschreibt das Konzept als eine Kombination aus den drei Teilen:

- Geräte-Authentifikation
- identitätsbasierter Zugang
- dynamisch bereitgestellte Konnektivität

Will jemand auf eine App oder eine Ressource im Netzwerk zugreifen, wird er für genau diese authentifiziert und gelangt direkt dorthin. Die Zugriffsverwaltung wird vom Netzwerk-Perimeter an die Ressource oder App verlagert, so dass die Nutzer zu keinem Zeitpunkt wissen, wo sie sich im Netzwerk befinden.

Die unter Punkt 2 und 3 beschriebenen Sicherheits-Mechanismen von oneclick™ erfüllen vollständig die Anforderungen an einen ZTN-Ansatz. Die oneclick™ Plattform unterstützt Kunden ideal bei der Umsetzung des Konzepts.

Weiterführende 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

Haben Sie Fragen oder brauchen Sie weitere Informationen?

Wir helfen Ihnen gerne weiter!

Herr Dominik Birgelen
Customer Success Manager

Tel.: +41 44 578 88 93
E-Mail: dominik.birgelen@oneclick-cloud.com

oneclick™ - die Everything-as-a-Service-Plattform

Als zentrale Zugriffs- und Verteilplattform in der Cloud ermöglicht oneclick™ das Management des ganzen Technologie-Stacks für die Anwendungsbereitstellung. oneclick™ vereint Software-, Plattform- und Infrastruktur-as-a-Service aus beliebigen On-Premises und Cloud-Umgebungen hinter einem Webportal.
Everything-as-a-Service (XaaS) bedeutet, dass Sie all dies als Service konsumieren können.

oneclick™
accessing the unlimited

oneclick AG
Zollikerstraße 27
CH-8008 Zürich

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