GIRITECH®

G/On™ Virtual Access

Uneingeschränkter Zugriff auf Anwendungen & Ressourcen

kompatibel mit
Windows · Linux · Mac OS X · iOS · Android

G/On bietet in einer integrierten Lösung

- den richtigen Zugriff
- für die richtigen Personen
- auf die richtigen Applikationen
- unter den richtigen Bedingungen

G/On ist Access mit Rundumschutz

- Gegenseitige 2-Faktor-Authentifizierung
- Virtualisierte, hoch verschlüsselte Connectivity
- Netzwerk- und Applikationszugriffskontrolle
- Proxy und Firewall auf Applikationsebene

Giritech ist offizieller Partner von
T-City Friedrichshafen
Ein Gemeinschaftsprojekt der Deutschen Telekom und der Stadt Friedrichshafen

info@giritech.de • www.giritech.de

G/On ist, wenn es einfach überall funktioniert.

Mobilität in einer neuen Dimension: Schneller, vielseitiger und sicherer.

G/On ist die flexibelste, umfassendste Access-Lösung im Markt und eine zukunftsweisende Alternative zu den besten heute verfügbaren Connectivity- und Absicherungssystemen für den IT-Perimeter. Bei der Entwicklung war unser wichtigstes Ziel, dass Unternehmen signifikante Kosteneinsparungen realisieren, indem sie hochsicheren, einfach zu handhabenden Applikationszugriff für Mitarbeiter, externe Lieferanten und Geschäftspartner überall zur Verfügung stellen.

Universell und unkompliziert

Nutzer sind in Minuten mit G/On vertraut und müssen nicht über technische Vorkenntnisse verfügen. Das Design garantiert, dass sich der Remote Access auf jedem PC unabhängig von Sprache und Betriebssystem immer identisch darstellt. Programme und Ressourcen, wie zum Beispiel E-Mail, Citrix, Terminal Services, VMware, Intranetportale und sogar der eigene Büro-PC mit VoIP-Telefonie, stehen in kürzester Zeit produktiv und ortsunabhängig über Internet zur Verfügung. Mit einem Klick im selbsterklärenden G/On-Menü sind Sie absolut sicher verbunden.

> Dank G/On kann ich von zuhause auf alle für mich wichtigen Anwendungen zugreifen - und dies schnell und sicher.
>
> André Mebold, Director Corporate Services
> **World Vision Schweiz**

Mehr Freiheit durch VPN-Alternative

G/On arbeitet völlig installationsfrei und benötigt weder Treiber noch VPN-Verfahren oder unsichere Browser. Die von Giritech entwickelte, patentierte EMCADS®-Technologie sorgt dafür, dass unsichere Verbindungswege in höchster Qualität abgesichert und externe Computer vollständig vom Unternehmensnetzwerk isoliert sind, damit Sie sich um die Sicherheit keine Sorgen mehr machen müssen. Endlich sind Sie nicht mehr auf Computer angewiesen, die Ihr Unternehmen verwaltet und zur Verfügung stellt. Statt dessen können Sie genau den Computer nutzen, mit dem Sie schon immer arbeiten wollten oder irgendein Gerät, das gerade unterwegs zur Verfügung steht.

> Das Herausragende an der G/On Lösung ist, dass wir unsere sensiblen Informationen überall zuverlässig und sicher im Zugriff haben.
>
> Peter Sauter - Hauptamtsleiter
> **Landratsamt Bodenseekreis**

Multi-Faktor-Authentifizierung

Ein USB-, Software- oder mobiler Token bildet den 1. Authentifizierungsfaktor in G/On (auf dem USB-Token sind die Clients für alle unterstützten Betriebssysteme enthalten). Die Prüfung der eindeutigen Token findet online in Echtzeit bei jedem Verbindungsaufbau statt. Den 2. Authentifizierungsfaktor bilden Benutzername und Passwort.

Sobald der G/On-Server den Token akzeptiert hat, werden Benutzername plus Passwort abgefragt und gegenüber einem zentralen Verzeichnisdienst verifiziert (AD, LDAP, MS SQL oder G/On-eigene Datenbank). War die Prüfung erfolgreich, sendet der G/On-Server dem Nutzer eine Auswahl der für ihn zentral freigegebenen Applikationen und Ressourcen.

Bootfähiges G/On-Betriebssystem für absolute Kontrolle

Durch den Einsatz des optionalen G/On OS können Unternehmen auf gemanagte Computer verzichten, denn das für Malware nicht anfällige, vertrauenswürdige und zentral administrierte Betriebssystem macht jeden Rechner zum echten Zero-Client. Über G/On OS gebootet, stellt der PC ausschliesslich eine direkte Verbindung zum G/On Server des Unternehmens her.
G/On isoliert die Remote-Sitzungen eines Anwenders zu 100% von den Datenträgern und Kommunikationsschnittstellen des verwendeten Gast-PCs und macht damit jeden unbekannten Rechner zu einem vertrauenswürdigen, zentral verwalteten Device, das ohne Sicherheitsbedenken verwendet werden kann.

G/On im Unternehmen - Vorteile und Einsparpotenzial

Der Kostenaspekt

- Niedrige Gebühren pro Client (Mitarbeiter).
- Exakt budgetierbar und flexibel nach Bedarf erweiterbar.
- Reduzierter Personal-, Betriebs- und Administrationsaufwand.
- Minimale Hardwareanforderungen, dadurch hoher Investitionsschutz für Unternehmen jeder Grösse.
- Hohes Sparpotenzial durch volle Unterstützung virtualisierter Umgebungen und Thin Clients.
- Reduzierung von Wege- und Energiekosten sowie verbesserte CO_2-Bilanz.

Der Sicherheitsaspekt

- Schutz vor Internetangriffen durch Viren, Spyware, Trojaner und Man-in-the Middle-Attacken.
- Patentierte, virtuelle Verbindung zwischen Client und G/On-Server im Unternehmen (”nodeless client”).
- Keine Nutzung von unsicheren Browsern, Plugins oder VPNs.
- Umsetzung aller relevanten Sicherheitsrichtlinien. Optional Vermeidung von Datenkopien, Cut & Paste usw.
- Schutz der Serverfarmen durch Trennung des Clientnetzwerks vom Servernetzwerk.
- Kontrolle der gesamten End-to-End-Kommunikation inkl. Authentifizierung, Autorisierung und Prozesskontrolle.

Der Nutzungsaspekt

- Einfachster Applikationszugriff auch auf komplexe Infrastrukturen. Auf jedem Computer identisch zu bedienen.
- Anbindung auf Wunsch an Citrix, VMware oder andere virtualisierte Umgebungen.
- Optimale Usability durch unkomplizierte Bedienung.
- Keine Einschränkung des Nutzers während des Remote-Access, z. B. weiterhin Zugriff auf Internet, Skype usw.

Bring Your Own Device - ohne Device-Management

Durch die verstärkte Nutzung privater Laptops, Smartphones und Tablet-PCs im Unternehmen (”Consumerization”) stehen IT-Abteilungen vor der Frage, wie ein effektives Management aller Zugriffe und Devices inklusive Sicherheitskontrolle umsetzbar ist. G/On löst diese Herausforderungen, ohne dass Sie zusätzliche Sicherheitstools oder Software für das Device-Management einsetzen müssen, denn G/On verwaltet zentral den Zugang - und nicht das mobile Gerät.

Browser und RDP absichern

Im Gegensatz zu einem VPN-basierten Browserzugriff auf Web-Apps, richtet G/On individuell gesicherte Browser-Sessions ein. Dieses Vorgehen isoliert jede einzelne Web-App wirkungsvoll gegenüber allen anderen und stellt sicher, dass parallel laufende Browser-Sitzungen weder Informationen auslesen, noch entwenden können.

Für den RDP-Zugang auf Arbeitsplatz-PCs im Büro, auf Terminal Server oder virtualisierte Umgebungen, richtet G/On entweder eine Port-Weiterleitung auf dem Mobilgerät ein, so dass jede RDP App verwendbar ist oder unterstützt optional einen rein Browser-basierten RDP-Zugriff. Die Anmeldedaten für die RDP-Session werden automatisch durch den G/On-Server per Single Sign-On übergeben.

Zentrales Management und einfachste Verteilung

Nach dem Download der G/On Client-App greifen Sie in wenigen Minuten von Ihrem Smartphone oder Tablet aus auf alle notwendigen Programme und Dateien zu. Intranet, CRM, Mail oder auch der eigene Arbeitsplatz können bereitgestellt werden. Das gesamte Access- und Device-Management erfolgt zentral über den firmeneigenen G/On-Server, ohne dass dafür Ihr Mobilgerät (extern) konfiguriert, verwaltet oder abgesichert werden muss.

Applikationszugriff für Windows, Linux, Mac und iOS.

Erstaunlich, wie viele Ideen in ein einziges Produkt passen.

G/On ist eine wegweisende Lösung zur Bereitstellung, Nutzung und Administration sicherer Remote Access Verbindungen in Unternehmen und Organisationen jeder Grössenordnung. Die beispiellose Kombination aus Sicherheit, Flexibilität, Bedienungskomfort, einfacher Bereitstellung und virtueller Connectivity macht G/On zur strategischen Access-Plattform auch in hoch sensiblen IT-Umgebungen.

» Funktioniert perfekt! Ich bin sehr beeindruckt von der Leistungsfähigkeit des G/On-Systems.

Ulf Lange - M.S.E.E.
RUAG Aerospace Sweden AB

Access auf Anwendungen und nicht auf das Netzwerk

Im Gegensatz zu konventionellen Zugriffsverfahren (LAN, Wi-Fi, WAN, VPN) verbindet G/On das Device des Nutzers nicht mit dem Servernetzwerk. Statt dessen wird eine virtuelle Verbindung zwischen der User-Session und den Applikationsservern und -diensten aufgebaut. Dies verhindert, dass die Kernsysteme und Dienste des Unternehmens gegenüber dem Internet offengelegt werden müssen und schützt vor einer Kompromittierung des Firmennetzwerks durch Hacking, Malware, Spyware, Man-in-the-Middle- oder Replay-Angriffe.

So einfach und so viele Möglichkeiten

Bei G/On dreht sich alles um Einfachheit. IT-Administratoren erledigen die Einrichtung und Verwaltung sicherer Remote-Access-Verbindungen im Handumdrehen und können sie in kürzester Zeit für alle Personen im Unternehmen freigeben. Und zwar auf jede Anwendung, Ressource oder Datei, die irgendwo benötigt wird. Nachfolgend einige typische Einsatzszenarien:

- **Integration von Citrix-Anwendungen**

Der optionale G/On Citrix-Connector unterstützt die nahtlose, hochperformante Einbindung von Citrix-Anwendungen inklusive Single Sign-On. Alle Änderungen, wie etwa das Freigeben oder Entfernen von Applikationen auf der Citrix-Seite, werden automatisch in das G/On User-Menü übertragen.

- **Terminal Services**

G/On bietet eine direkte end-to-end Verbindung mit Single Sign-On auf den Terminal Server Desktop und spezifische Anwendungen in geschlossenen Sessions. Da der Verbindungsclient auf dem USB-Token enthalten ist, lässt sich eine hochsichere Verbindung von praktisch jedem PC aus aufbauen. Funktionen des Terminal Servers, wie etwa die Freigabe von Laufwerken und Druckern oder die Übertragung der Zwischenablage, können optional aktiviert werden.

- **Web-Applikationen und Portale**

Webbasierte Lösungen, wie Intranets oder Portale, sind über G/On so angebunden, dass die Server nicht mehr gegenüber dem Internet offengelegt werden müssen. G/On schützt vor unberechtigten Zugriffen, Internetattacken oder Sicherheitslücken, die durch Browser bzw. Zertifikate verursacht werden.

- **Zugriff auf den Office-PC**

Mit G/On greifen Sie per Remote Desktop auf Ihren Arbeitsplatz-PC zu und schalten ihn aus der Ferne sogar ein und aus (falls er Wake-On-LAN unterstützt). Das unsichere RDP-Protokoll wird über G/On vollständig abgesichert (keine IP-Verbindung zum Zielsystem), alle unternehmenswichtigen Applikationen stehen mit höchster Sicherheit überall und jederzeit zur Verfügung.

» Wir sind begeistert von der Flexibilität und dem hohen Grad an Sicherheit, die uns G/On bietet.

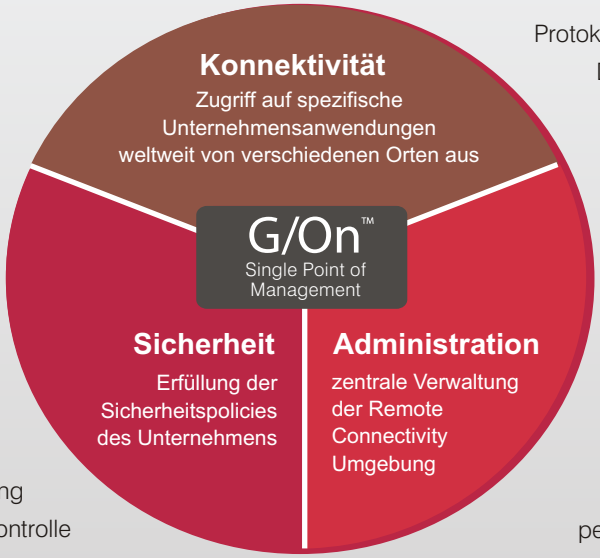
Frederik Gutzeit, Geräteteam Lagerkransystem
Service Center Burchardkai GmbH

- **Uploads/Downloads managen oder deaktivieren**

Die meisten Unternehmen benötigen eine effektive Kontrolle für Daten, die in das Netzwerk gelangen oder es verlassen. G/On stellt einen zentralen Zugangspunkt für alle Transfers bereit, der überwacht, auf Malware geprüft und protokolliert werden kann. Individuelle Zugriffe auf verschiedene Dateitypen oder öffentliche bzw. private Dateien lassen sich pro Benutzer im G/On Menü festlegen (freigeben oder vollständig verbieten).

So einfach ist “Alles-in-Einem”

Physische und virtuelle Desktops
Server-basierte Lösungen
Client/Server-Applikationen
Portale, Intranets, Webapps, FTP



Protokollierung & Einhaltung von Richtlinien
Dokumentierung der Security Policies
Definition von Zugriffsregeln

Authentifizierung
Geräteunabhängigkeit
Datenintegrität und Datenschutz
Identitätsmanagement & Autorisierung
Netzwerk- und Applikationszugriffskontrolle

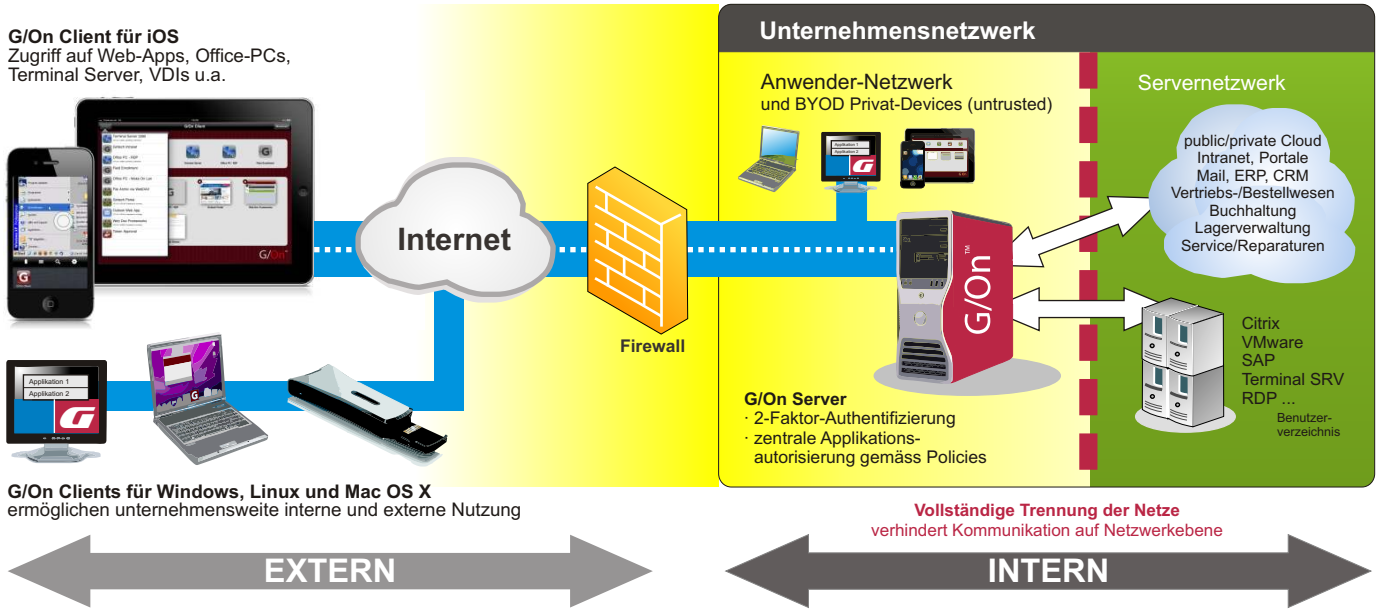
Token-Verwaltung / Device ID
Authentifizierungsregeln
Autorisierungsregeln
Definition von Anwendungsmenüs
performant, skalierbar & hochverfügbar

■ Hosting-Umgebungen / Software as a Service

Application Service Provider (ASPs) müssen ihren Kunden aus unterschiedlichsten Unternehmen einen einfachen, sicheren Zugriff auf gehostete Software und Daten gewähren. Mit G/On können sie einen sehr bediendungsfreundlichen 24/7 360° Zugang zu einem sehr günstigen Preis anbieten. Gleichzeitig entfallen Investitionen in Zugangstoken, VPNs, Endpunkt-Sicherheitssoftware, Packet Inspection Tools und zusätzlichen Security-Lösungen, was zu deutlichen Kosteneinsparungen führt.

» Einfacher geht's nicht. Man kann G/On nutzen, ohne zu wissen wie es funktioniert, oder was dahinter steckt. Echtes Plug and Play eben.

Dr. Uwe Metzinger
Gemeinschaftspraxis Ailingen



Keine Entscheidungen bezüglich des Zugriffs werden auf dem Client getroffen. Der Client erstellt eine virtuelle und auf den Prozess gelockte Verbindung (nodeless client). Client und Server authentifizieren sich gegenseitig live und online.

Der G/On-Server prüft multiple Authentifizierungsfaktoren, um den User zu validieren. Danach autorisiert er einen Satz von Anwendungen pro Nutzer. Der G/On-Server leitet den Datenverkehr des Nutzers an die richtigen Applikationsservices über eine Single-Port TCP-Verbindung weiter.

Der Nutzer hat das Gefühl eines direkten Zugriffs auf Anwendungen und Ressourcen. Tatsächlich besteht nur eine virtuelle Verbindung zum G/On-Server und nicht ins Netzwerk (das Endgerät wird nicht mit dem Servernetzwerk verbunden). G/On verwaltet sämtliche Sicherheitsrichtlinien bezüglich des Zugriffs auf Applikationsservices (Single Point of Management).

Layered Security mit 360° Rundumschutz.

Kein Browser, kein SSL, kein IPSec, kein Tunnel. Einfach von Haus aus sicher.

Bei klassischen VPNs für Remote Access stellt sich schnell die Frage, welche Sicherheit tatsächlich vorhanden ist? Um alle neuralgischen Punkte zu adressieren, werden spezialisierte Produkte wie Token- und Zertifikatserver, IDS, IPS, DMZ, Identity-Management, Firewalls und vieles mehr integriert. Das Ergebnis ist eine komplexe Infrastruktur, in der mögliche sicherheitsrelevante Fehler, sowie der damit verbundene Überprüfungsaufwand überproportional ansteigen. G/On vermeidet derartige Probleme, durch eine innovative, nicht VPN basierte Technologie.

Nachteil: VPN

Ein VPN ist vergleichbar mit einem "Tunnelsystem", das technisch nach aussen abgedichtet ist. Die einzelne “Röhre” (Verbindung) kann nicht durchlöchert werden, so dass Inhalte weder ab- noch hinzufliessen können (dies entspricht einer fehlerfreien VPN-Konfiguration mit maximaler Sicherheit). Denken wir uns ein solches Tunnelsystem mit Wasser gefüllt, dann “fliessen” die Daten, Ressourcen und Applikationen auf den freigegebenen Ports zwischen den Netzen. Alle Anwender können diese Datenverbindungen transparent nutzen.

> G/On steht für maximale Sicherheit und einfachste Nutzung. Eine Access-Lösung, die uns rundum überzeugt.
>
> Marcel Jost - Leiter Informatik
> **Gemeinde Ittigen**

Was aber, wenn irgendein Segment in diesem Verbund "verschmutzt" (infiziert) wird? Giessen wir in das mit Wasser gefüllte Tunnelsystem durch einen Trichter an einer einzigen Stelle “Schmutzwasser” (Malware) hinein, dann fliesst dieses ungehindert durch das gesamte System und infiltriert sämtliche Netze. Jedes Segment ist betroffen, oftmals ohne dass eine Abschottung technisch möglich ist. Die Bereinigung ist in solchen Fällen ausgesprochen aufwendig, weil immer alle Bereiche gesäubert oder zumindest untersucht werden müssen.

Vorteil: G/On

G/On implementiert ein abgestuftes Sicherheitsmodell, das unabhängig von der Endpunktsicherheit einen applikationsbasierten Zugriff auf zentral freigegebene Anwendungen bietet. Wird die G/On Infrastruktur an einer Stelle “verunreinigt”, dann ist ausschliesslich dieser Bereich betroffen - eine Ausbreitung in andere Segmente oder auf den G/On Server ist durch die physische Trennung der Netze ausgeschlossen.

Im Falle eines Angriffs muss lediglich exakt der beeinträchtigte Bereich gereinigt werden, die restliche Infrastruktur kann wie gewohnt arbeiten und spürt keinerlei Auswirkungen. Bei korrekter Konfiguration kann sogar ein infizierter Arbeitsplatz-PC weiterhin benutzt werden und der Administrator verwendet die G/On-Verbindung, um sich auf diesen Arbeitsplatz zu verbinden und die Malware zu eliminieren.

Netzwerk konsolidieren - Access absichern

In einer optimierten und konsolidierten G/On-Infrastruktur folgen alle Clients den zentral vorgegebenen Unternehmenspolicies. Sämtliche Endgeräte können exakt in der selben Weise und mit dem selben Bedienungskomfort genutzt werden. Das Betriebssystem muss nicht „personalisiert“ werden, denn G/On managt nicht das Endgerät, sondern verwaltet und sichert die Verbindung in das Servernetzwerk.

Natürlich kann G/On auch in vorhandene Infrastrukturen integriert werden, ohne dass Änderungen notwendig sind. Die Lösung liefert dann neue Strategien zur IT-Konsolidierung, Senkung der Kosten und Vereinfachung des Managements.

G/On 5 - Die wichtigsten Sicherheitsfeatures auf einen Blick

G/On Gateway Server

- Firewall auf Applikationsebene.
- Proxy-Funktionalität separiert Clients von Applikationsservern.
- Keine Tunnelingprotokolle wie IPSec, SSL, L2TP oder PTPP.
- Network Access Control auf Anwendungsebene.
- Zentrale Authentifizierung und Autorisierung der Nutzer.
- Implementierung und Durchsetzung von Sicherheitsrichtlinien.
- Lautlos: Antwortet nur authentifizierten G/On-Clients.

G/On Client (Windows, Linux und Mac OS X)

- Port-Weiterleitungs-Proxy: Daten des Applikationsclients auf dem Remote-PC werden abgefangen und verschlüsselt an den korrespondierenden G/On Gateway Server weiterleitet.
- Implementierung und Durchsetzung aller Entscheidungen des G/On-Servers auf der Clientseite.
- Automatische Trennung nach definierter Inaktivität.
- Prozesskontrolle (lock to process) erlaubt auf der Clientseite nur gültigen, bekannten Anwendungen die Kommunikation (White-List Firewall).
- Verbindungen und Programme werden automatisch beim Entfernen des Tokens bzw. Beenden des Clients geschlossen.

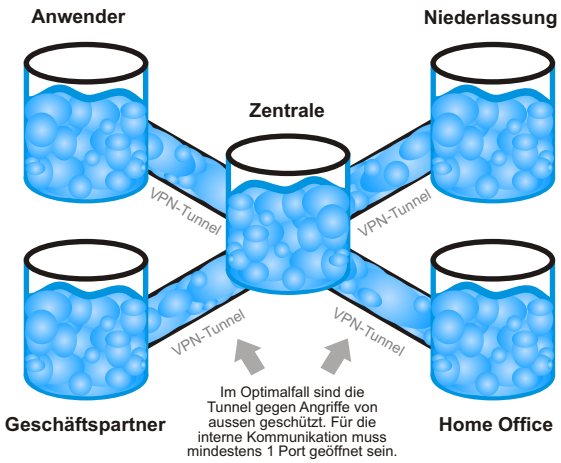
Verschlüsselung

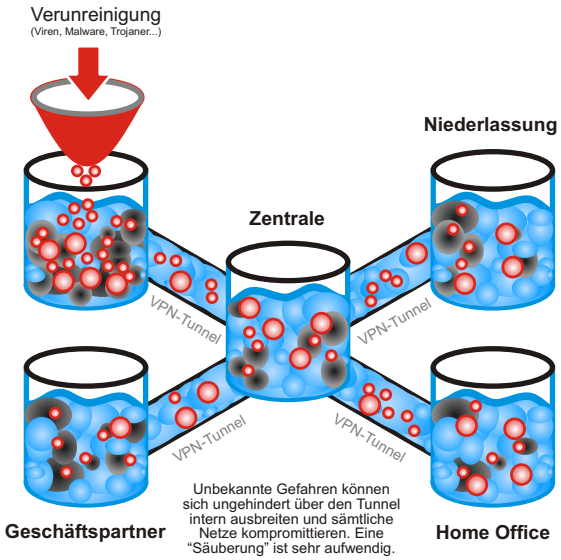
- Wechselnde 256-bit AES Schlüssel, getrennt für Up- und Downstream. 163-bit ECC für das zeichnende Schlüsselpaar (Client/Server) und den sicheren Schlüsselaustausch.
- Prüfsummen (SHA-1 Hashing) verhindern Man-in-the-Middle Angriffe, Replay- und Spoofing-Attacken.

2-Faktor Authentifizierung

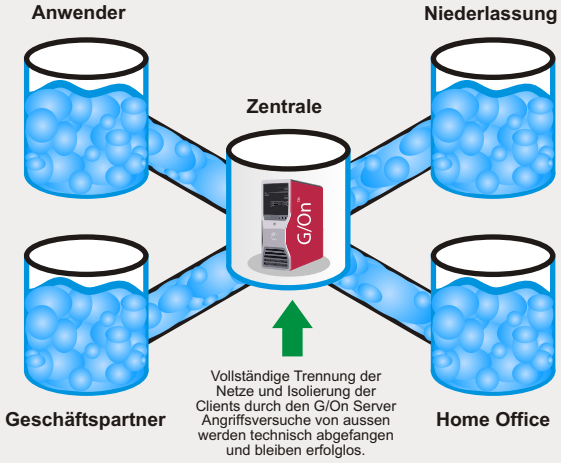
- Kryptografisch gesicherte, am Server akzeptierte Token sorgen in Verbindung mit Username/Passwort für optimalen Schutz.

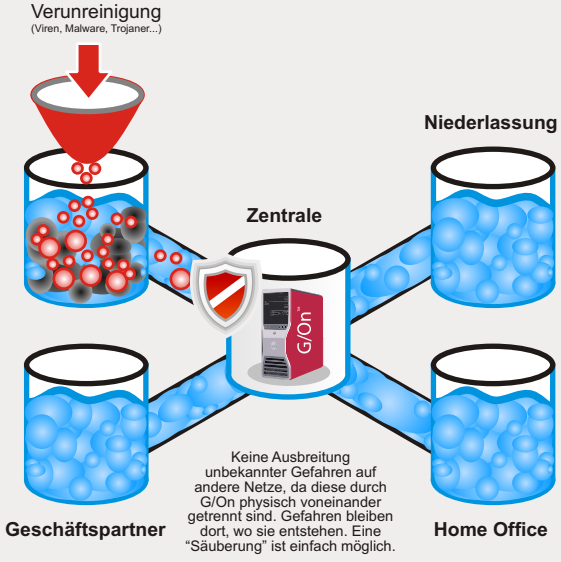
VPN





G/On Virtual Access





Weil Sie mehr brauchen als nur ein VPN.

Die Vorteile der Sicherheits- und Access-Plattform G/On 5.

Warum ist G/On für Remote Access besser geeignet als andere Produkte?

- G/On ist eine echte Technologieplattform für Access in jeder Form: Netzwerk-Access, Zugriff auf Services, Cloud-Access (private/public), TS-Farmen, virtualisierte Desktops (VDIs)...
- Device-Unabhängigkeit (Windows, Linux, Mac OS X, iOS usw.)
- keine Installation und keine Administration auf dem Client
- kein Browser erforderlich (Stichwort: “Sicherheitsrisiko”)
- nicht limitiert hinsichtlich der Nutzungsmöglichkeiten (alle Anwendungen, die über TCP kommunizieren)
- sehr hohe Skalierbarkeit (1 bis mehrere 10.000 User)
- enorme Kostenvorteile (bis zu 84% Einsparung in 2 Jahren, Quelle: Projektarbeit der TU Darmstadt, M. Axtmann, 2011)
- einfachste Bedienung
- zentral verwalteter Access (Devices, User, Policies, Zones)
- "Bring Your Own Device" Angebote können unmittelbar umgesetzt werden, ohne Infrastrukturänderung, ohne Einschränkung der Sicherheit, ohne Device-Management-Software, ohne administrativen Zugriff auf die Devices usw.
- sichert Business Continuity, z. B. im Krankheitsfall, auf Reisen, bei Pandemien ...
- ermöglicht die Realisierung weltweiter Service- und Supportkonzepte (z. B. im Anlagenbau)
- Grundinstallation in weniger als einem halben Tag realisiert

Was sind die Vorteile gegenüber anderen Produkten?

- Whitelist-Firewall, Proxy, Authentication und Authorization
- Nodeless-Connection
- Kommunikation über TCP und HTTP 1.1 (Proxy-Support)
- 2-Faktor-Authentifizierung mit Challenge-Response-Prüfung der Token
- FIPS 140-2 zertifizierte AES-256 bit Verschlüsselung
- drastische Reduzierung der Komplexität (1 einzelnes Produkt für alle Anforderungen, Single-Point of Service, Single-Point of Management)
- keine Einschränkung der Nutzer und Devices (kein Lockdown des Internets oder bestimmter Programme/Dienste, das System kann exakt wie zuvor weiter verwendet werden, ohne dadurch die Sicherheit zu kompromittieren)
- Transparenter Netzwerkzugriff optional für Trusted Devices oder vertrauenswürdige Benutzergruppen (z. B. Admins).
- gegenseitige Authentifizierung (Client-Server)
- optional mehrere Zugangspunkte (Gateways)
- integriertes Load-Balancing
- Prozesskontrolle und Lock to process, nur Daten autorisierter Anwendungen werden transportiert
- aufgrund der Architektur sicher gegenüber Man-in-the-Middle Angriffen, DOS-Attacken, Session Overflow usw.
- keinerlei Modifikation der IT-Infrastruktur erforderlich, G/On kann mit bestehenden IT-Strukturen 1:1 arbeiten
- Potential zur IT-Konsolidierung: keine Zertifikatserver, keine Token-Server, keine Sicherheitstoken oder SMS-Dienste ...
- virtuelle Appliance, keine Hardware erforderlich (G/On-Server auf physikalischer oder virtueller Maschine einsetzbar)
- Cold-Standby: G/On-Software auf neuen Windows-Server kopieren (physikalisch / virtuell), Dienst starten, läuft!
- integrierte Anbindung an Citrix XenApp
- Connectoren für HTTP, Socks und RDP - inkl. Single Sign-On
- Token-Devices mit Speicher (nach Common Criteria zertifiziert bis EAL 5+), sodass der G/On-Client und Anwendungsclients direkt "mitgebracht" werden können
- Token-Devices unterliegen keiner Zwangserneuerung
- Token enthalten keine Authentifizierungsdaten des Benutzers
- keine Anwendungsmenüs auf den Token
  Menü-Deployment erfolgt durch den G/On Server nach erfolgreicher Authentifizierung und Autorisierung
- abhängig von der Konfiguration: Keine Daten, kein Caching, keine Cookies usw. auf dem Client-Computer
- zentrales Software-, Policy- und Identitätsmanagement
- Prüfung des Windows-Security-Centers auf dem Client: OS-Version, Service Packs, Firewall, Antivirus und Updates
- Zeitzonen für den Anwendungszugriff
- erlaubte Client- und Server-IP-Ranges für den Access
- erlaubte Zugriffszeit mit Datumsbereich und Uhrzeit
  (z. B. Zugriff von Mittwoch ab 8 Uhr bis Donnerstag 14 Uhr)
- Field Enrollment: Tokenverteilung und "Betanken" der Token mit Software im Betrieb
- Softwarepaketmanagement: Hinzufügen, Aktualisieren und Austauschen von Software
- G/On OS Betriebssystem
  Vom G/On-Token bootfähiges, gehärtetes Linux-Betriebs-system mit ausschliesslicher Connectivity zum G/On Server für Hochsicherheitsumgebungen, das aus einem unsicheren, unkontrollierten PC einen voll durch G/On gemanagten und zentral verwalteten PC macht.

Success Story

World Vision Schweiz: VPN erfolgreich abgelöst.

Unterwegs oder von zu Hause arbeiten – ohne Einbusse der Sicherheit.

In einem Katastrophenfall sind alle Kräfte bei World Vision Schweiz gefordert. Die Verantwortlichen in Dübendorf sind darauf angewiesen, dass innerhalb von kurzer Zeit Spenden und weitere Hilfestellungen organisiert werden können. Oftmals wird für die Sachbearbeitung auf ehemalige Mitarbeitende zurückgegriffen. Da ist der G/On Access und Security Token ein überaus nützliches Arbeitsgerät und hat schnell das traditionelle VPN abgelöst.

World Vision Schweiz ist ein christlich-humanitäres Hilfswerk. Im Mittelpunkt der Arbeit steht die Unterstützung von Kindern, Familien und ihrem Umfeld im Kampf gegen die Armut und Ungerechtigkeit. World Vision leistet mit regionalen Entwicklungsprojekten, die mit Patenschaften finanziert werden, langfristige Entwicklungszusammenarbeit und ist auch in der Not- und Katastrophenhilfe tätig.

«Im Katastrophenfall ist es unabdingbar, dass man sofort reagieren und ein gut funktionierendes Netzwerk zur Verfügung stellen kann», so André Mebold, Mitglied der Geschäftsleitung von World Vision Schweiz. «Einerseits braucht es Leute vor Ort. Andererseits sind auch die Mitarbeitenden in der Schweiz, welche Spenden entgegennehmen und Koordinationsarbeiten leisten, unerlässlich.»

Gegenwärtig unterstützt World Vision Schweiz über 100 Projekte in 30 Ländern. Damit eine unmittelbare Reaktion sichergestellt werden kann, müssen unter Umständen zusätzliche Leute rekrutiert werden. «Diesbezüglich nutzen wir die vielen Vorteile des G/On Access und Security Token», sagt Daniel Kast, Leiter der Informatik-Abteilung. So könne auf ehemalige Mitarbeitende zurückgegriffen werden, ohne dass diese einen Arbeitsplatz in Dübendorf benötigen würden.

«Vielmehr stellen wir zum Beispiel einer Mitarbeiterin, welche durch ihre Mutterrolle nicht mehr voll arbeiten möchte, sich aber für solche Notfalleinsätze zur Verfügung stellt, einen G/On Stick zu. Sie kann uns so von ihrem Heimcomputer aus unterstützen.»

Strategischer Wechsel von VPN zu G/On

Doch nicht nur im Katastrophenfall ist G/On zum wichtigen Arbeitsgerät geworden: World Vision Schweiz möchte seinen Mitarbeitenden die Möglichkeit bieten, tageweise von zuhause aus zu arbeiten. Entsprechend muss eine reibungslose Anbindung an die verschiedenen Server sichergestellt sein.

Vor dem Wechsel zu G/On hat World Vision Schweiz mit dem klassischen VPN gearbeitet. Diese Netzwerk-Lösung habe sich aber nicht bewährt und eine flexible Einrichtung von Home-Offices bislang verhindert.

Die Unterschiede sind markant. So bestätigt IT-Chef Daniel Kast, dass die VPN-Einzelbetreuung für seine Abteilung einen grossen Aufwand bedeutet habe. «Die Implementierung von G/On hingegen ging innerhalb weniger Tage von statten, denn PC-spezifische Software-Installationen entfallen. Auch der User-Support ist unkompliziert, da - im Gegensatz zu VPN - keine speziellen Kenntnisse erforderlich sind und mehrfaches Einloggen entfällt.»

Hat sich der User also via G/On erfolgreich beim Terminal-Server angemeldet, stehen ihm sämtliche individuell freigegebenen Ressourcen und Programme zur Verfügung.

Fakten: World Vision Schweiz

Herausforderung

- Integration einer sicheren Remote-Access-Lösung für unterwegs und im Homeoffice.

Vorteile

- Einfache Einrichtung eines Homeoffice Arbeitsplatzes, geringe Anforderungen an die Infrastruktur.
- Ideal für temporär eingesetzte Arbeitskräfte, die lediglich den G/On Token benötigen, um zuhause einsatzbereit zu sein.
- Mit G/On kann zuhause gleichzeitig das Web benutzt werden.
- G/On ist die ideale Lösung in Notfällen bei Ausfall von Arbeitsplätzen, z.B. Brand, Diebstahl, Zerstörung.
- Bei Verlust oder Defekt eines Notebooks auf Reisen kann mit G/On irgendein PC verwendet werden.
- Die Anzahl benötigter Notebooks konnte reduziert werden (Kosteneinsparung).
- G/On benötigt minimale Anwender-Instruktion. Einstecken – einloggen – fertig!

Internet:	www.worldvision.ch
Lösung:	G/On USB und G/On MicroSD
aktueller Ausbau:	Einbindung von iPads und Android Tablets über G/On

André Mebold spricht userseitig einige weitere positiven Aspekte von G/On an: «Internet oder Skype kann ich jederzeit nutzen, auch wenn ich über G/On mit dem Server verbunden bin. Zudem kann ich Dokumente auf meinem Drucker zuhause ausdrucken. Das war mit VPN alles deutlich komplizierter und aufwendiger.»

Die Einführung von G/On war aber noch von weiteren strategischen Überlegungen begleitet: So ist zum Beispiel die Einsparung von fixen Arbeitsplätzen ein Thema. World Vision Schweiz hat seit der Einführung von G/On bereits PC Hardware einsparen können. Verschiedene Mitarbeiter schätzen es zudem, dass sie den Laptop nicht immer mit nach Hause nehmen müssen, sondern mit G/On problemlos vom Heimcomputer aus auf den Server zugreifen können. «Ich kann beispielsweise eine Update abends um zehn Uhr, wenn niemand mehr arbeitet, von zuhause aus durchführen», sagt der IT-Verantwortliche.

Sicherheit von Experten bestätigt

Häufig werden bei externen Access-Tools Sicherheitsmängel entdeckt. Da Datensicherheit bei World Vision Schweiz eine übergeordnete Rolle spielt, haben die Verantwortlichen G/On von einem neutralen Sicherheitsexperten prüfen lassen. Das Gutachten hat gezeigt, dass der Access Token keine Sicherheitslücken aufweist. Denn die Applikation, welche für ein sicheres Login und eine abhörsichere Kommunikation nötig ist, befindet sich direkt auf dem Stick. Der Einführung stand also nichts mehr im Wege. «Dank der kompetenten Unterstützung von Avatech konnten wir G/On bereits nach kurzer Zeit nutzen.», bestätigen Daniel Kast und Raphael Kranzkowski, der massgeblich an der Einführung von G/On beteiligt war.

Angesprochen aufs Thema Sicherheit, führt Raphael Kranzkowski einen weiteren Vorteil aus: «Bei einem Ausfall von Arbeitsplätzen, zum Beispiel durch Brand oder Diebstahl, können wir dank G/On und unseren Back-Up-Tapes den Normalbetrieb innert nützlicher Frist wieder herstellen.»

Dasselbe gilt, wenn auf Auslandreisen das Notebook ausfällt: Mit dem Stick und einem Internet-Café oder Computer im Hotel kann sofort wieder auf die Daten zugegriffen werden. Einstecken, einloggen und es kann gearbeitet werden.

Weitere G/On Success Stories, Referenzen und Videoclips finden Sie online auf: www.giritech.de.

Mit G/On sind Sie in bester Gesellschaft.

Referenzanwender (Auszug).

- Artemis Control AG
- AIS Consulting Group GmbH
- Atlific Hotels & Resorts
- APA Austria Presse Agentur
- Ausgleichskasse des Kantons Bern
- Caritas Passau
- Cimber Aviation Group
- Danish Cancer Society
- Diakonisches Werk Kassel
- Die Johanniter
- Dunkermotoren
- Ev.-ref. Kirchgemeinde Fällanden
- Gemeinde Horw
- Gemeinde Ittigen
- Gemeindeverwaltung Volketswil
- Gemeinde Wallisellen
- GVZ Gebäudeversicherung Kanton Zürich
- Heinemann Verlag
- Heron Aviation
- Hessisches Ministerium für Wissenschaft und Kunst
- HHLA Hamburger Hafen und Logistik AG
- IG ICT Interessengemeinschaft Zürcher Gemeinden
- Integic
- Intertec Tegro AG
- J. Poulsen Shipping A/S
- Kirchgemeinden des Kanton Bern
- Landratsamt Biberach
- Landratsamt Bodenseekreis
- Liebenau Beratung und Unternehmensdienste GmbH
- Mariaberg e.V.
- Migros-Verteilbetrieb Neuendorf AG
- miromatic
- MTU Tognum
- NEF Fonden
- Notariatsinspectorat des Kantons Zürich
- Ökodata
- RIZ AG Regionales Informatikzentrum
- satorius stedim biotech
- Siemens Schweiz AG
- Spielhofer Treuhand AG
- Staatliche Fraunhofer Berufsschule 1
- Stadt Bad Saulgau
- Stadt Bremgarten
- Stadt Kempten (Allgäu)
- Stadt Sigmaringen
- Stadt Opfikon
- Stadtverwaltung Dübendorf
- Stadtverwaltung Schlieren
- Stadtverwaltung Uster
- Stadtwerke Borkum
- Storebaelt (Grosse Belt Brücke)
- Swiss Mains
- Telekom Deutschland
- TCA Thomann Computer Assembly AG
- T-City Friedrichshafen
- Thüringer Miniterstium für Bildung, Wissenschaft und Kultur
- Texpa
- Universitätsklinikum Essen
- Universitätsklinikum Mannheim
- Vaekstfonden
- Wasserversorgung Birmensdorf
- WAZ Mediengruppe
- World Vision Schweiz
- Zeppelin Systems

» Die Einfachheit der Nutzung ist unübertroffen. G/On wird von unseren Mitarbeitern sehr geschätzt.

Dieter Laube, IT Betreuer
Mariaberg e.V.

Setzen Sie auf Wachstum

G/On macht Sie fit für die Arbeitswelt von morgen.

Kosten

Mit G/On senken Sie Ihre Kosten

- Verringern Sie die Zeit für die Administration einer Accesslösung.
- Konsolidieren Sie Ihre IT-Infrastruktur.
- Verlängern Sie die Nutzungsdauer vorhandener Hardware bzw. setzen Sie kostengünstige Hardware ein (z. B. Thin Clients).
- Vermeiden Sie teure Device- und Hardware-Wartungszyklen.
- Reduzieren Sie den Aufwand des Konfigurations-Managements.

Flexibilität

G/On gibt Ihnen mehr Flexibilität

- Ermöglichen Sie minutenschnell mobiles und dezentrales Arbeiten.
- Geben Sie Partnern Zugriff auf präzise spezifizierte Applikationen.
- Nutzen Sie G/On zur gesicherten Datenübertragung via Web.
- Konnektieren Sie einfach auf Ihre virtualisierten Desktops.
- Etablieren Sie Supportlösungen für Ihre Industrieanlagen.
- Realisieren Sie Telearbeitsplätze im Handumdrehen.

Sicherheit

G/On sorgt für höchste Sicherheit

- Entscheiden Sie, wer welche Applikationen nutzen darf, aber gewähren Sie niemandem einen direkten Zugang in Ihr Intranet.
- Vermeiden Sie das Risiko von Datenverlust durch den Einsatz datenloser Systeme.
- Sichern Sie die Aufrechthaltung Ihrer Betriebsbereitschaft in Krisensituationen.
- Schützen Sie den Zugang auf Anwendungen in der Cloud.
- Vertrauen Sie auf transparente Sicherheit.

Giritech GmbH
Deutschland · Österreich · Schweiz
Mariabrunnstrasse 123
88097 Eriskirch (Germany)

Tel. +49 7541 9710990
Fax +49 7541 97109999

Mail: info@giritech.de
Web: www.giritech.de

Ihr Giritech Partner

Giritech reserves the right to change the information contained in this document without prior notice. Giritech®, EMCADS™ and G/On™ are trademarks and registered trademark of Giritech A/S. Giritech A/S is a privately held company registered in Denmark. Giritech's core intellectual property currently includes the patented systems and methods known as EMCADS™. Other product names and brands used herein are the sole property of their owners. Informations published in this document are provided according to present knowledge and based on publicly available sources. Although they have been carefully selected and researched, we explicitly indicate, that some informations may not be current due to irregular changes or updates of this document. Giritech does not guarantee its accuracy or completeness and nothing in this document shall be construed to be a representation of such a guarantee. Giritech accepts no responsibility for any liability arising from use of this document or its contents. All rights reserved. Unauthorized copying, editing, and distribution of this document is prohibited. © 2011 Giritech GmbH.