

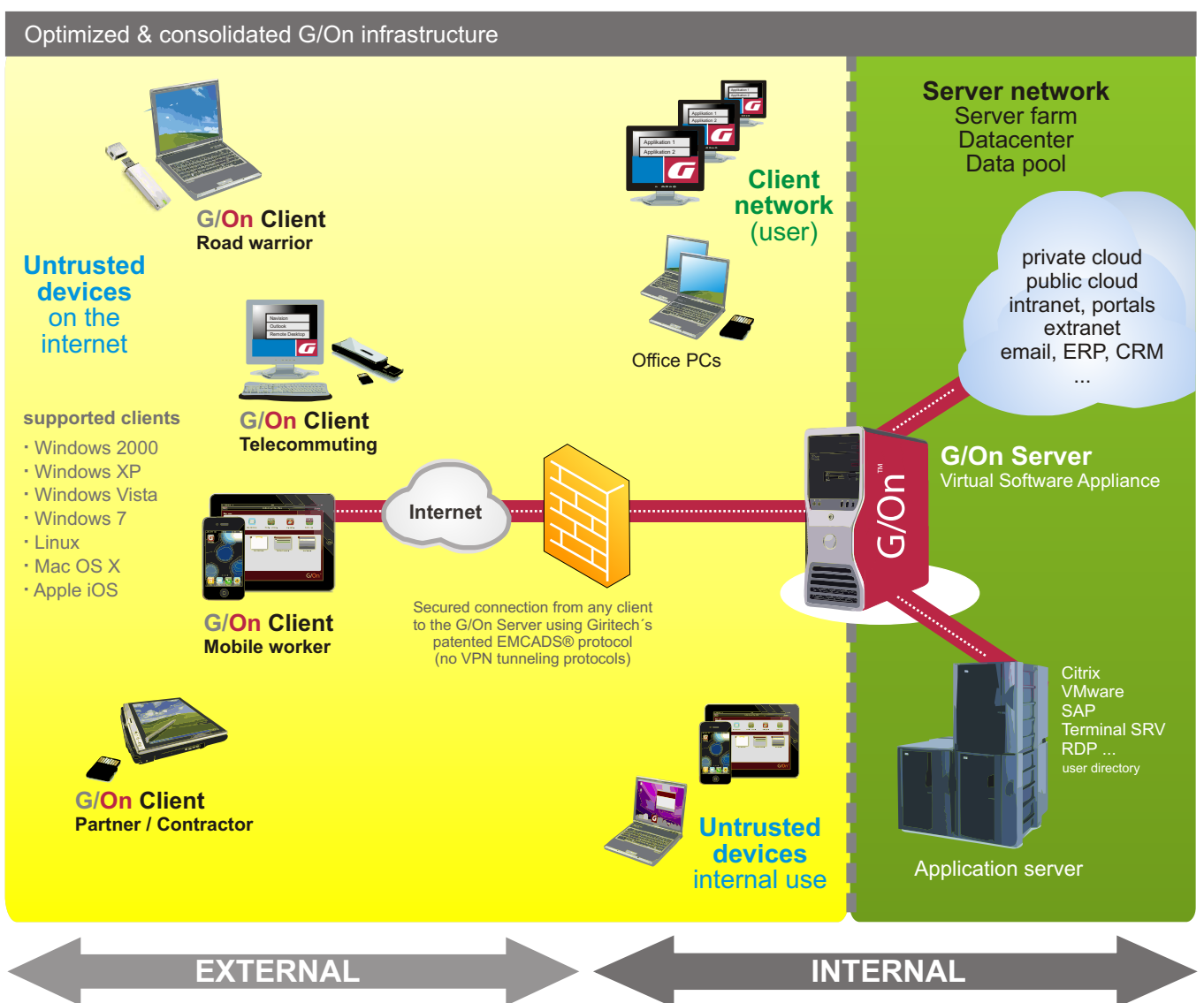


# G/On infrastructure and security

## Secure Virtual Access

G/On is client/server access technology, based on a virtual appliance which grants users connectivity to the required IT infrastructure following a centralised company policy management. G/On is built on a distributed port forwarding proxy technology that virtualizes the connections between user devices and the company's application servers and services.

Contrary to conventional access methods (LAN, Wi-Fi, WAN, VPN), G/On does NEVER connect the user's device to the server network. Instead, it creates virtual connections between the user session and the application servers and services, thus protecting the company's core systems and services from being exposed towards the internet and safeguarding them from outside or inside attacks.



In an optimized and consolidated G/On infrastructure (see above), all clients follow the centrally defined company policies. In consequence, all devices can be used in the same way, with equal ease-of-use. The operating system must not be personalized, because G/On does never manage the device but manages and secures the connection to the server network.

However, G/On can also be fully integrated into existing IT infrastructures without the need for any changes - but it delivers new strategies which allow consolidation, simplified management and significant cost-savings.

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. July 2011 Giritech GmbH.



# G/On versus VPN - Fact Sheet

## Advantages of Gritech's access and security platform G/On 5

### Why is G/On better suited for Remote Access than other products?

- G/On is a true technology platform for any kind of access: network access, access to services, to the cloud (private or public), to TS farms, virtualized desktops (VDI)...
- Device independency (Windows, Linux, Mac OS X, iOS ...)
- no installation and no administration on client
- no browser required (browsers are a security risk)
- not limited in possible uses (all applications which communicate through TCP)
- extremely high scalability (1 to several 10.000 users)
- huge cost advantages (up to 84% savings in two years source: project work by TU Darmstadt, M. Axtmann, 2011)
- ease of use
- access centrally managed (devices, users, policies, zones)
- "Bring Your Own Device" offerings can be implemented on the fly without changing the IT infrastructure, without reducing security, without adding device-management-software, without administrative access to the devices etc.
- secures business continuity, e.g. in case of illness, on the road, in case of pandemia ...
- supports implementation of worldwide service- and support-conceptions (e.g. mechanical engineering and construction)
- basic installation takes less than half a day

### How does the on-board VPN solution of Microsoft for Windows 7 / Server 2008 R2 compare?

- similar price structure - Microsofts solution is cheaper if there are dedicated volume/licensing agreements in place (source: TU Darmstadt)
- OS support extremely limited: only Windows 7 and Server 2008R2 - no Windows XP, Vista, Mac OS X, iOS etc.
- based on IPv6: requires additional gateways for conversion of IPv4 to v6 and vice versa
- authentication solely based on certificates is not sufficient, requires integration of 3rd party products (token...)
- no integrated 2-factor-authentication
- local setup requires installation rights /administrative rights (expenditure, data traces, access to PCs required)
- high complexity
- substantially lower security: no process control, no nodeless connection, no software on token to be brought along
- no equal encryption
- endpoint administration and -security required
- no centralised administration and software deployment
- client PC must meet high requirements (hardware/software)
- lower performance, higher latency
- ease of use very limited: no automatic G/On-menu but instead manual creation of e.g. startup icons required
- BranchCache(tm): Caching of file- and webserver-content on various computers may be a potential security risk
- must not be used on uncontrolled / unmanaged / unknown computers by definition - which contradicts flexible "everywhere-use"

### Which are the advantages of G/On over other products?

- whitelist firewall, proxy, authentication and authorization
- nodeless connection
- communication through TCP and HTTP 1.1 (proxy support)
- 2-factor-authentication with challenge-response verification of tokens
- FIPS 140-2 certified AES-256 bit encryption
- drastically reduces complexity (1 single product for all access requirements, single point of service, single point of management)
- no user- or device-restrictions (e.g. no lockdown of internet connectivity or certain apps / services, each system can be used exactly as before without compromising security)
- mutual authentication (client-server)
- multiple access points optional (gateways)
- integrated load balancing
- process control and lock to process: only data of authorized applications are forwarded
- "secure by design" protects against man-in-the-middle attacks, DOS attacks, session overflow etc.
- no modification of IT infrastructure required, G/On works 1:1 in existing IT structures
- potential for IT consolidation: no certificate servers, no token server, no security tokens or SMS services ...
- virtual appliance, no hardware required (G/On Server can be deployed on physical or virtual machines)
- cold standby: just copy the G/On software onto a new Windows server (physical/virtual), launch the service, done!
- integrated connectivity to Citrix XenApp
- specialized connectors for HTTP, socks and RDP - including Single Sign-On
- token devices with memory (Common Criteria EAL 5+ certified) allow to carry the G/On-Client and additional application clients
- token devices must not be force-renewed
- depending on configuration: no data, no caching, no cookies etc. on the client computer
- centralized software-, policy- and identity-management
- validation of Windows Security Center on client: service packs, OS version, firewall, antivirus and (important) updates
- time zones for user access
- allowed client- and server-IP ranges for access
- allowed access time with specified date and time (e.g. access wednesday 8:00 to thursday 14:00 o'clock).
- field enrollment: token distribution and adding software to tokens in the field
- software package management: add, update or replace software
- G/On OS: Secured Linux operating system bootable from G/On token with exclusive connectivity to the G/On server, ideally suited for maximum security environments - turns any unsecured, uncontrolled PC into a fully controlled and centrally managed PC



# Why VPN tunneling should be avoided

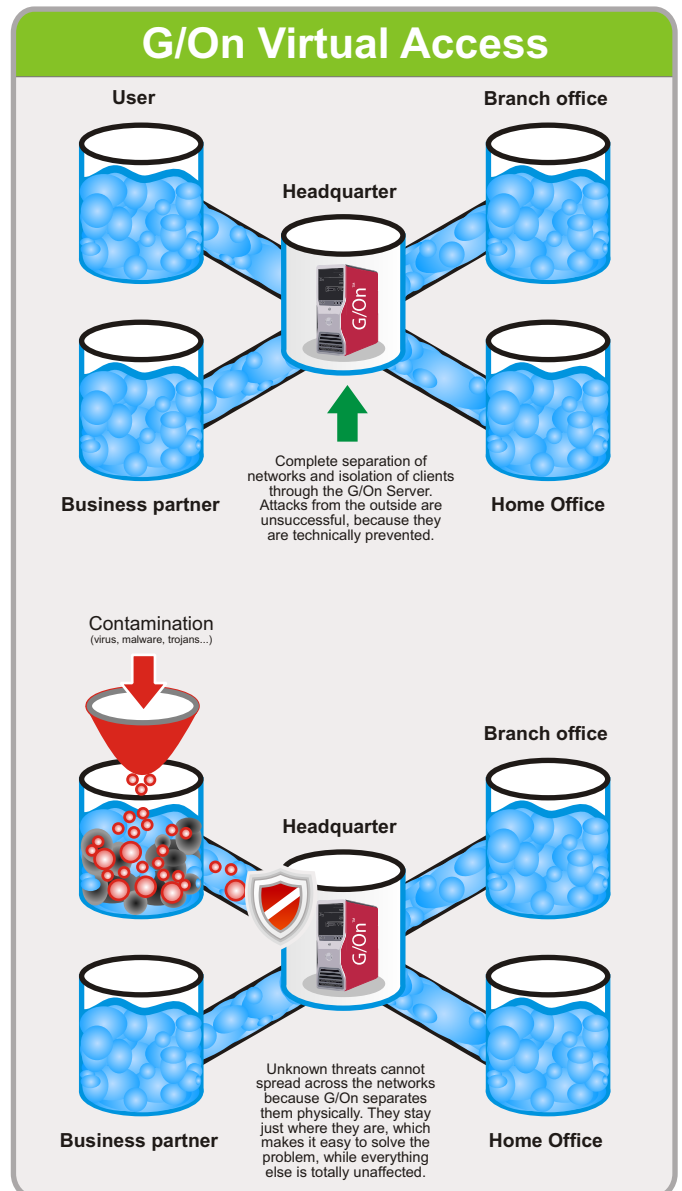
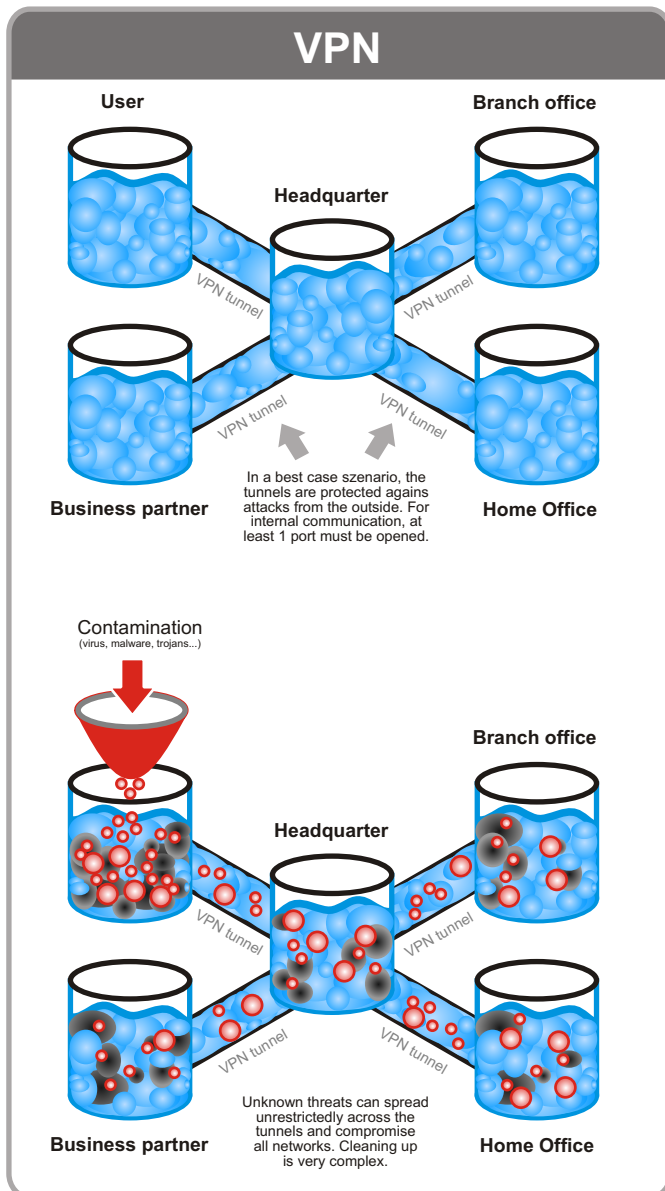
## Prevent your networks from being compromised

A VPN is comparable to a system of „tunnels“, which is technically sealed up towards the outside. Each individual pipe (connection) cannot be perforated, so that content cannot flow to or drain off (conforms to an error-free VPN configuration with maximum security).

If we imagine such a tunnel system being filled with water, then all data, resources and applications float on the enabled ports between the networks. Each user can transparently utilise these data links.

But what if any segment of this compound structure is being “polluted” (infected)? Once we start pouring “dirty water” (malware) into the liquid filled tunnels at just one point, the pollutant floats unrestrictedly through the whole system and infiltrates all the networks. Each segment is affected, often without a lockdown being technically possible. As a result, the cleanup process is very complex, because all areas must be decontaminated or at least being investigated.

Due to the complete network isolation, such attacks are not possible when using G/On. If the infrastructure is “polluted” at one point, then solely this area is affected – a spreading into other segments (or the G/On server) is impossible thanks to the physical separation of the networks. In case of an attack, only exactly the affected segment needs to be decontaminated, while the remaining infrastructure stays intact and online without any impact. If configured correctly, even an infected computer can still be used and the administrator is capable of connecting to this computer, eliminating the malware by making use of the G/On connectivity.



Girtech reserves the right to change the information contained in this document without prior notice. Girtech®, EMCADS™ and G/On™ are trademarks and registered trademark of Girtech A/S. Girtech A/S is a privately held company registered in Denmark. Girtech'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. Girtech does not guarantee its accuracy or completeness and nothing in this document shall be construed to be a representation of such a guarantee. Girtech 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. July 2011 Girtech GmbH.