WHITE PAPER

Securing Remote Connectivity

Solving the Five Challenges of Securing Remote Access

CONTENTS

EXECUTIVE SUMMARY

Making it easier for more people to access business applications “anywhere, anytime” is good for business. Employees appreciate the flexibility and convenience. It streamlines business processes by not restricting people to being in the office when they use applications. And enabling more people – both employees and external business partners - to use applications, effectively increases your return on investment.

The only factor preventing companies from taking full advantage of all these benefits is security.

Securing remote access requires addressing 5 major challenges:

- Authenticating users
- Securing the device
- Protecting the data
- Restricting network access
- Managing user’s rights and policies

On top of this is the need for accountability if things go wrong, as well as various legislative requirements for documenting that adequate security processes are in place.

There is a wide selection of solutions for each of these challenges. Implementing all of them is prohibitively expensive. This forces many companies to compromise – they only buy the solutions they feel protect them against the most obvious risks, and then they limit the number of users to minimize the risk if something does go wrong.

Giritech’s G/On solution provides a valuable alternative to this problem. G/On is the only solution on the market that effectively addresses all of the five challenges.

This reduces the cost and complexity of securing remote access. Now you can now easily afford to give both employees **and** external business partners quick, easy and secure access to business applications. This maximizes the value of these applications and helps you leverage the ubiquitous availability of the Internet.

Problem Analysis

What's the problem?

Today, the PC is the workplace of the world. For millions of people it is a "must-have" tool for getting their job done. The PC is also a prominent feature in many homes, a tool for storing our photos and our music, for playing games, for communicating via email, chat or VoIP. And, perhaps most importantly of all, the PC is our doorway to the Internet.

Via the PC at work and at home we can use the Internet to instantly interact with virtually every aspect of our professional and personal life "anywhere, anytime".

But do we? No, we don't. Either it's not allowed or we simply don't dare. And the reason is security. We've realized that locks and keys are necessary to prevent the wrong people accessing our corporate PC and the network it is connected to, as well as our home PC.

Is this a problem?

It depends on how many doors and locks you need. The IT industry has taken the threats of security very seriously. Scare tactics from vendors, government regulation and very real instances of cybercrime has left many companies weighed down by doors and locks and keys. Their infrastructure is a complex tangle of servers, firewalls and policies and their users are either burdened with an arsenal of hardware and software or only allowed to log in from a small subset of the devices that otherwise could satisfy their needs.

What's really at stake?

The problem IT managers face today is **not** whether or not they can protect their data and systems. The problem is we've developed an IT infrastructure that lets us do business everywhere all the time, but the cost of all the security measures means we just can't afford to do that.

Today it can be argued that a lot of expensive IT infrastructure is under-utilized simply because making it easy to access via the Internet is too risky. The solutions currently on the market are defensive measures – locks, bars and gates – that by their very nature are the antithesis of what business is all about: letting people work and trade when and where they want with the least amount of fuss.

The Holy Grail is a simple way to secure remote access – not just for your own employees but for everyone in your business ecosystem.

The source – and future – of the problem

To understand the size and shape of the problem today – and the implications for the future – let's take a quick step back and look at the evolution of information technology.

- ***Yesterday***
  The first computers were mainframes. These complex monolithic devices required a "protected" (air-conditioned etc.) environment to function properly. They could only be operated by highly skilled technicians – at a time when very few people in the world really understood how such devices worked. Access to them was limited and they offered limited connectivity with other devices. This made them easy to secure.

- ***Today***
  Then came the personal computer, networking technology and the Internet. The size of the devices decreased. Desktop PCs and laptops were easy to move from one location to another. And thanks to user-friendly graphical interfaces, even non-technical people could operate them. You could also connect them together to create a network so people could quickly and easily share information. And with the advent of the Internet, cheap global connectivity was achieved. The number of users skyrocketed to hundreds of millions of people - who could now also use PDAs and mobile phones in addition to their desktop and laptop PCs to access data using whole libraries of software developed by a vast industry of vendors.

  Suddenly the IT department found itself having to protect an ever-increasing amount of data that could be accessed by literally billions of devices. The fact that broadband "always-on" connections are now widely available is only escalating the size of the challenge. And the data protection legislation being enacted by governments around the world means businesses at all levels are being forced to take the challenge of securing remote access seriously.

- ***Tomorrow***
  There are several key trends that seem destined to actually become part of our collective IT future. The first is a consolidation around the use of the Internet as a way of allocating access to software i.e. "software as a service". Salesforce.com and Microsoft's various rumblings on this front are prime examples. Service Oriented Architecture (SOA) and the much-hyped advent of Web 2.0 also confirm this trend. The second trend is that Internet capabilities seem likely to be added to all manner of devices that traditionally were "unwired", mainly to facilitate remote monitoring.

  The security implications of this are significant: as data access increases to being "everywhere, all the time" the need to protect sensitive personal and corporate data will increase. And the challenge of doing this - which is already gargantuan - will rise exponentially.

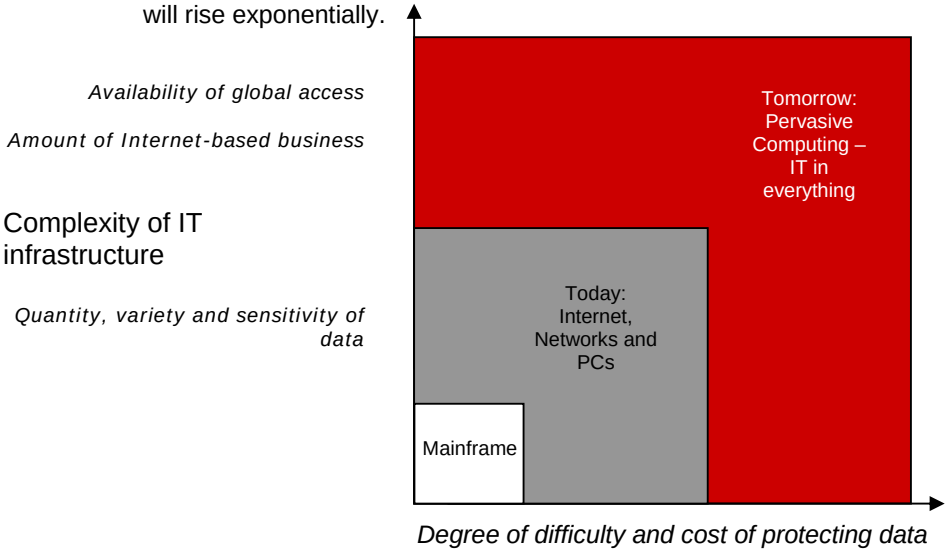

Figure 1: The need, size, complexity and expense of securing remote access will grow exponentially as the Internet becomes pervasive.

The Five Challenges of Securing Remote Access

As mentioned earlier, organizations around the world are spending billions of IT dollars on securing remote access. So what is all that money being spent on?

Giritech has identified five problems you need to address to secure any remote network connection:

1. Authenticate the user
2. Secure the device
3. Protect the data
4. Restrict network access
5. Manage rights and policies
6. Ensuring accountability

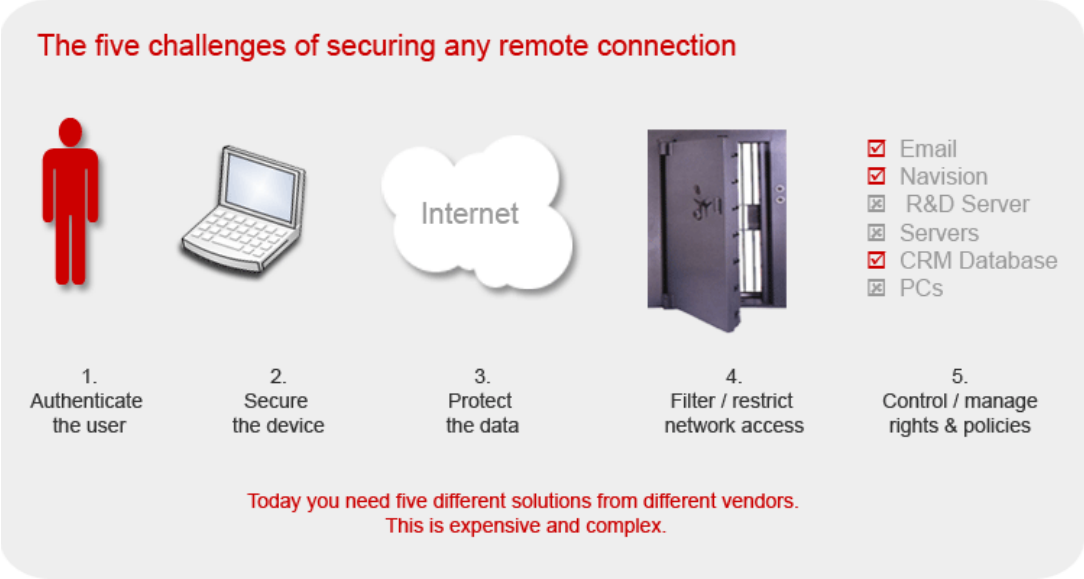

Figure 2: An overview of the five challenges involved in securing remote access.

1. Authentication

The most popular solution on the market is the secure token. Typically, this is a battery-driven device that generates a One-Time Password (OTP). Using tokens means you get two-factor authentication – your user name is something you know and the token is something you are supposed to have with you.

Installing a token solution means adding a server to your network, and connecting it to your infrastructure. Then you issue tokens to all your users. There is the cost of the licenses, plus the operating costs of keeping the servers and the tokens synchronized. You also need to remember that most tokens need to be renewed every few years – which means a large part of the cost is recurring.

While 2-factor user authentication is better than a single-factor password, for example, it doesn't protect users against "phishing" attacks where users are fooled into connecting to a fake website which attackers then use to gather confidential data such as bank account numbers, passwords and so on. This requires mutual client/server authentication i.e. a process for enabling the client to independently verify the identity of the server and vice-versa.

Here's a checklist of what you'll need

- √ Secure tokens
- √ Secure token server
- √ Secure token licenses
- √ IT resources

Note: The password is displayed on the token's screen, meaning anyone can read it. This is convenient if you've forgotten to take your token with you. Then you just can ring home or to your office, for example, and ask someone there to read out the password to you. But this, of course defeats the purpose of using tokens because it mean you don't have to have token with you to gain access.

2. End Point Security

The second risk point in securing any remote connection is the device you're connecting from. There are 2 things you need to guard against here.

First you want to make sure the device has not been compromised before you use it.

Secondly, you want to avoid leaving any data on the device that can be used to compromise your network later on.

The standard practice is to issue every user with a fully featured PC, set up, locked down and maintained by your IT department.

While this is expensive, it's much more secure than the alternative which means relying on ordinary users to ensure their own PC has all the latest security patches and is free of viruses or spyware.

It's also worth remembering that anti-virus and spyware scanners can only check for "known" risks. This means you might end up relying on a false sense of security.

To erase any sensitive data left behind when you make a connection, the standard solution is to download and run Active X or Java components that delete all trace of what you've been doing on the PC. This is a good solution but it's not always possible to use it due to local firewall policies.

Other solutions that you can use to make devices more secure are things like personal firewalls and encrypted hard drives. They work fine – but they also increase the cost and the complexity of the solution – both for users and your IT department.

Here's a checklist of available options:

- √ Anti-virus software
- √ Antispyware software
- √ Active X / Java component

- √ Personal firewall
- √ Encrypted hard drive
- √ IT administration costs
- √ User training

Nearly 90 percent of all personal computers could be infected with at least one form of spyware - National Cyber Security Alliance

Spyware on every 3rd PC analyzed. Each one had an average of 26 spyware programs – Earthlink & Webroot Software

There is currently over 10,000 PC viruses in circulation.

3. Protect the Data

Encrypting data as it travels over the public Internet is the next hurdle when securing any remote connection. The standard solution these days is the VPN.

There are two main types of VPNs – the IPSec VPN and the SSL VPN.

If you choose an IPSec VPN, you'll have to install a server on the network. You'll also need to install and configure a VPN client on every PC the user wants to connect from. And that's expensive. Plus they give you full network access which can be a serious security consideration. IPSec VPNs were designed to provide a secure tunnel between two secure environments. Breaking into that tunnel i.e. a “brute force” attack is not realistic given the standard of encryption being used today (e.g. AES and 3DES). It’s much easier to pry open the end of the tunnel. This places big demands on the physical security at each end plus the first 2 challenges of authenticating users and securing the device.

SSL VPNs is the mobile alternative to IPSec VPNs. SSL VPNs let users connect via a standard web browser. This lets you avoid the cost and hassle of installing a client on each PC. Most SSL VPNs also restrict users to accessing applications – not your entire network – which is a good security precaution. However they are also limited to applications that can run in a browser. This can require spending more money to "web enable" applications that are critical for your business.

Regardless of which one VPN you choose, you'll have pay for the hardware and the software licenses. And if you need to support large groups of users, you'll probably also want to buy extra hardware to boost performance.

Here’s a checklist of available options:

IPSec VPN?

- √ Install a VPN server on the network
- √ Install IPSec VPN clients on every PC that employees want to use
- √ Set up certificate server
- √ Pay for software licenses
- √ Add manpower to keep them running

SSL VPN?

- √ Install SSL VPN appliance on your network
- √ Tell users which URL to connect from
- √ Webify non-browser based applications
- √ Pay for software license.
- √ Add SSL acceleration hardware to improve performance

4. Control Network Access

The fourth problem is limiting network access. Today, a firewall is essential. But firewalls need to be set up and managed correctly. And you also need some way of checking who goes in and out of the ports that you do open up. The more ports you open and the more people who can open those ports, the bigger the risk that people can sneak in undetected.

There are various ways of strengthening your network perimeter. You can buy an Intrusion Detection or Prevention system. You can also hire external consultants to test and monitor your network defense systems. Unfortunately, neither of these options is cheap or simple.

Here's a checklist of available options:

- √ Intrusion Detection / Prevention Systems
- √ Rigid policies that limit business flexibility
- √ External consultants

5. Managing Resource Usage

The fifth problem is limiting what people can do once they are connected. This is important because it addresses the fact that a large percentage of exploits are perpetrated by legitimate network users – i.e. your own employees.

This problem is solved by defining rights and policies for each user. SSL VPNs are actually better here because they limit users to an application they can see in a web browser. IPSec VPNs on the other hand become another node on the network – something an intruder can easily exploit.

You can also tighten security by adding extra passwords for specific applications and databases. But this makes life more difficult – both for users and your IT Help desk.

To make things easier you might also invest in a single-sign on solution. This means users only have to sign in once to access everything they're authorized to use. But it's also an extra expense.

Here's a checklist of available options:

- √ Network monitoring applications
- √ Manpower
- √ Employee training
- √ Extra passwords
- √ Single-sign on solution

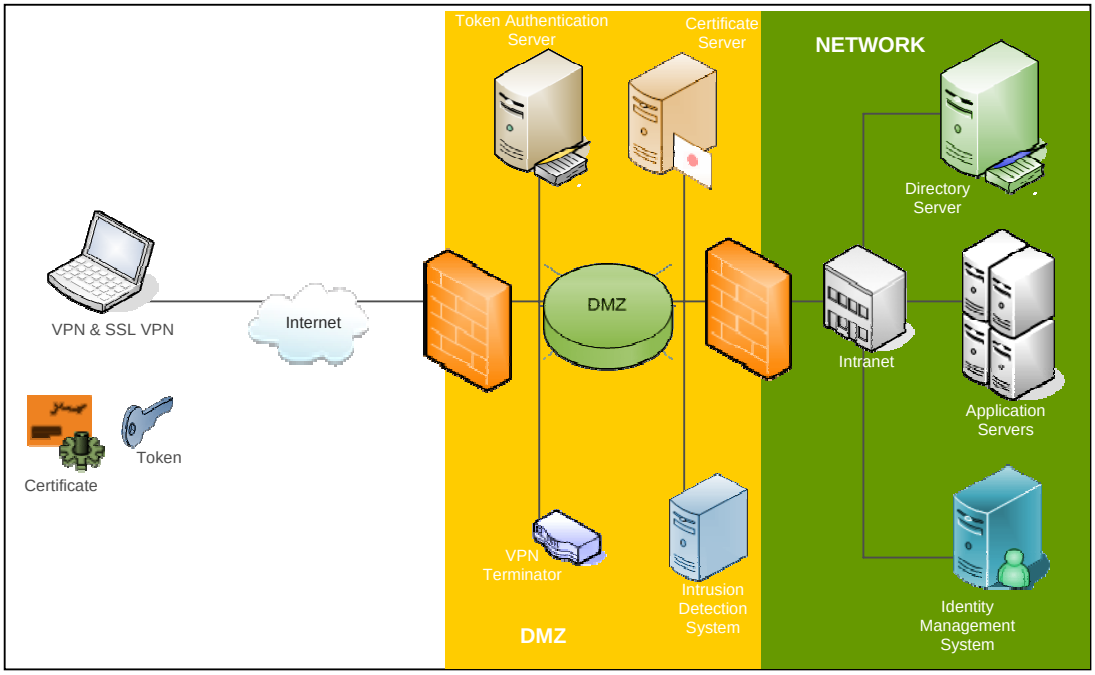

Figure 3: Solving the 5 challenges adds complexity to the network architecture.

Control and Accountability

Now there's only one problem left to solve. It's not a security problem as such but it is closely related – the need to control everything (preferably in real time) while maintaining a complete record of what people do while they're connected.

Right now, there's no easy way to make the whole process totally transparent. If you find something has gone wrong, you have to gather information from different systems to build up a complete picture of who might have been involved. This takes time and there's no certainty you'll get conclusive results.

Here's what you'll need to solve this problem:

√ Extra IT resources for examining different system logs

So now we've seen all the standard options for securing remote access to your network, let's take a look at G/On.

How do IT managers handle this problem today?

Most companies use various combinations of the solutions mentioned above. Typically they will offer different sets of solutions to different users.

For example, an employee who wants to work from home will be given a corporate PC protected by an IPSec VPN and a secure token. The PC will be locked down to ensure no unauthorized software can be installed and antivirus and antispyware software will be pushed out to the PC automatically.

Mobile employees who travel regularly might be given access to an SSL VPN system so they can quickly and conveniently check their email from any airport lounge, hotel lobby or Internet café. They are likely to be equipped with a secure token to boost the

level of user authentication, and if the IT manager likes to sleep well at night, he will also invest in regular training to remind users to log out of the secure session once they are finished.

But what about people outside your own organization? How do you quickly and easily give them secure access to your applications?

The simple answer is that most people don't. Doing it properly is too expensive. And doing it cheaply is too risky as there is simply no easy way of enforcing accountability if anything goes wrong.

Introducing G/On

G/On is a product based on Giritech's patented EMCADS technology. Unlike traditional security solutions, G/On is able to address all of the challenges involved with securing remote access.

G/On is a client/server platform and installation is a simple four step process:

1. The G/On Server is installed on a separate server just inside the main perimeter firewall.

2. Groups and users can be added to G/On's own database. Alternatively, G/On can be connected to synchronize with Microsoft's Active Directory.

3. The G/On Server is then configured to connect to the applications that people will be accessing. There are various ways of doing this depending on the applications and how they are to be used. (Consult a Giritech Certified Partners for more information.)

4. Finally, the G/On clients for that specific server are created by the server and can be distributed either on G/On USB keys or as a G/On Desktop version.

Managing G/On is made easy via the administration toolkit. Adding or deleting users, changing their menus takes only minutes.

For users, the experience is even easier. They simply launch the G/On client – this is done automatically when they plug in the G/On USB key or double-click the G/On Desktop icon. Then they enter their standard username and password and choose which application they want from the menu that is pushed out to them by the G/On Server once they've been authenticated.

G/On and the five challenges

This is how G/On solves the five challenges discussed earlier.

1. Authentication.

Each G/On client is unique and contains a secret it shares with the G/On Server it is made to connect to. Together with your username and password, this means real 2-factor authentication. The G/On USB is something that has to be physically present to make the connection, while your password is something you have to know to enter the system.

G/On's authentication process is further strengthened by its use of mutual client/server authentication. This means the G/On Server is able to confirm the authenticity of the G/On client that is connecting to it, and the G/On client is also able to confirm the identity of the G/On Server. This effectively eliminates the risk of "phishing".

Finally, the authentication process is object-based. All the information exchanged between the client and server is packaged as a "process", which means (a) no is ever transmitted in unencrypted, and (b) the encrypted data is wrapped up into an object that any attacker would need to first crack open before they can start breaking the encryption key which has been chosen randomly for that session.

2. Securing the device

The G/On client doesn't use the host PC's operating system and it doesn't make the PC part of the network it's connecting to. Instead it creates a nodeless connection that is independent of the host PC. This significantly minimizes any risk of spyware or viruses on the PC being able to subsequently create a connection that can gain access to your applications.

Once launched, the G/On client automatically connects to the G/On Server. This means users don't have to remember special URLs or download or install anything to make it work. Furthermore, it doesn't leave any trail that can be used later to compromise your network. This means there's no need to download and run any Active X or Java components.

3. Data protection

G/On encrypts all traffic using 256-bit AES. Checksums are used to prevent spoofing and man-in-the-middle attacks. It also features mutual client/server authentication which eliminates the risk of phishing and pharming attacks.

Unlike VPNs, G/On does not use tunneling protocols. The encrypted data is simply sent across the Internet based on the concept that if an attacker is watching the stream or does steal some of the packets, they won't be able to do anything with it because of the level of encryption used while the checksum feature will alert the G/On Server and cause it to resend the packets via another route.

The benefits of this is that G/On connections are not only secure, they are also very stable.

4. Controlling network access

The G/On Server only responds to request for a connection initiated by G/On clients that it recognizes. (And because each client is made unique because it is tied to either the USB key or PC it is deployed on, the G/On Server is able to unambiguously verify its authenticity.)

G/On only connects through one port in the firewall. This can be Port 3945, the port specifically assigned by the Internet Assigned Numbers Authority (IANA) to the EMCADS Server. Other ports including Port 80 and 443 can also be used.

These factors prevent unauthorized users gaining access to the applications on a network.

5. Restricting application access

G/On users can only see the applications they are authorized to use when they log on. The rest of the network is invisible to them, unless of course they are using an application like Microsoft Terminal Services or Citrix which lets them access other resources on the network.

Depending on how it is configured, G/On can also function as a single sign on platform to a range of different applications. This eliminates the need for extra passwords.

You can also use G/On to define different security "zones" depending on which IP address people log on from, and which PC they are using. Application access policies

can then be defined for each zone. For example, you can enter IP address of, say, a local office in another country which you judge to be a secure environment. You can then set the system up so that any user connecting from this IP address, will be given access to the full range of applications. If they later connect from an unknown IP address, then you might configure the system to only let them connect to their email application via a terminal services session.

This features makes it easy to regulate levels of security an automatically enforce these levels without any further intervention from administrators.

Accountability and tracking

G/On handles every aspect of every connection. This makes it easy to log what the system is used for to ensure improved accountability.

G/On

- √ G/On Server license
- √ G/On clients (free)
- √ G/On USB keys (optional)

FACT BOX

GOn and the Five Challenges

1. **Authentication**
   Strong 2-factor authentication ✓
   Mutual client/server authentication ✓
   The token must be physically present ✓

2. **Endpoint Security**
   Nodeless connection reduced risk of viruses entering the network via the connection or spyware subsequently being used to reopen the connection after a user has logged off ✓
   Nothing to download, install or configure ✓
   No URLs to remember ✓
   No virtual shredder needed ✓

3. **Data Encryption**
   256-bit AES using EEC (+ support for at least 40 other encryption schemes)
   Immune to spoofing and man-in-the-middle attacks
   No PPTP or L2TP means better stability

4. **Network Perimeter**
   The G/On Server doesn't broadcast – it only responds to authentic G/On clients via a single port.

5. **Application Connectivity**
   Virtual connection to applications – not the entire network ✓
   Single-sign on eliminates need for multiple passwords ✓
   Zones let IT Admins regulate level of access based on IP address and device used to host connection ✓

Summary of Benefits

G/On is a cost-efficient alternative compared to investing in the different solutions that together can provide the same level of security for remote access.

IT Administrator

G/On gives IT managers an easy way of securing remote access and a simple tool for administering users.

They can streamline their IT infrastructure by replacing several different solutions including secure tokens and VPNs with just one solution. It also reduces the need for DMZs and replication servers and corporate laptops.

End Users

The benefits for users are simplicity and mobility. The G/On client launches automatically, so they don't have to download, configure or install anything, or memorize special URLs or extra passwords. All they need is their G/On client on either a USB key or a PC, plus their user name and password.

Business Managers

G/On makes sense for managers because it gives them a way of increasing the value of their other business applications. Now they can afford to give access to more people in both their own organization as well as external business partners – regardless of where the person is connecting from.

About Giritech

Giritech® was founded in Denmark in 2003. Today it has offices in seven European countries and markets G/On worldwide through a network of over 130 partners. G/On™ is the first product based on Giritech's patented EMCADS® technology.

For more information, please visit www.giritech.com