

GlobalSign Security Services for Hosting Companies

**Understanding the true opportunity for Hosting Companies & ISPs
to resell Online Security Services**

GLOBALSIGN WHITE PAPER

Steve Waite, Chief Marketing Officer
GMO GlobalSign, Inc



www.globalsign.com

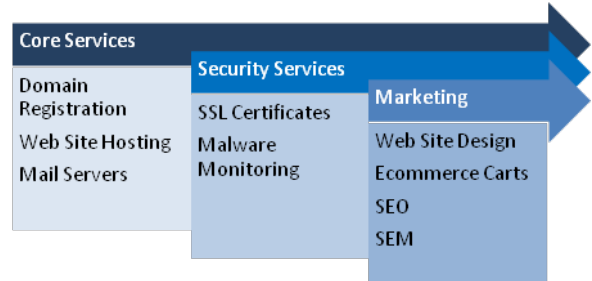
CONTENTS

- Introduction.....3
- How do the GlobalSign Security Services fit into hosting?3
 - SSL Certificates3
 - What is SSL?3
 - How should SSL be used?.....4
- Malware Monitoring4
 - What is Malware Monitoring.....4
 - Blacklisting5
 - Malware in Hosted Environments6
 - HackAlert - the GlobalSign Malware Monitoring Solution.....6
- Selling GlobalSign Security Services.....7
 - Selling / Bundling SSL Certificates7
 - Generate a new revenue stream / augment existing revenue stream.....7
 - Selling / bundling Malware Monitoring8
- Right product, right customer8
 - SSL Certificates8
 - Malware Monitoring9
- Getting a Fast Return on your investment9
 - SSL Reseller Models.....9
 - Pay As You Go (PAYG)9
 - Deposit9
 - Unlimited Issuance License.....9
 - Malware Monitoring Models9
- Deployment & Automation10
 - Hosting Companies10
 - Cloud Application/Service/Platform Providers10
 - Registrars11
- Partner Program Levels11
- Why Partner with GlobalSign?11
- About GlobalSign12

INTRODUCTION

The GlobalSign Partner Program is designed for ISP's, Web Hosts, Integrators, Domain Registrars and VARs who wish to integrate security services (SSL and Malware Monitoring) into their own product range, maximizing the SSL reseller opportunity and ensuring the highest levels of security within their networks.

This white paper explains GlobalSign's Internet security technology, its uses and necessity (and therefore the sales opportunity), advises on how to fit the services into existing hosting portfolios, and details how provisioning SSL can now be automated to degrees previously considered impossible.



HOW DO THE GLOBALSIGN SECURITY SERVICES FIT INTO HOSTING?

Many hosting companies that find they are already hosting hundreds of SSL Certificates and are recognizing the potential for revenue gains by increasing their average customer values through providing SSL Certificates as an authorized reseller. Hosting companies who offer SSL Certificates in their hosting packages or as a value-add option gain the immediate benefits of increased revenues and a more complete and "sticky" product portfolio.

Hosting customers need to protect the websites they host from distributing malware. Likewise they need to protect their own infrastructure. By protecting against malware distribution injection attacks, the host offers a significant value-add by protecting against the commercial ramifications of being blacklisted and excluded from the search engine results.

The below diagram shows a high level view of the value chain for hosting. Security services can easily be added as a value-add to all hosting bundles, or sold separately as an individual line item. As Security Services support the Core Services, the customer profile to Core Services is essentially identical.

SSL Certificates

What is SSL?

The Secure Sockets Layer (SSL) (and Transport Layer Security (TLS)) is the most widely deployed security protocol used today. It is essentially a protocol that provides a secure channel between two machines operating over the Internet or an internal network. In today's Internet focused world, we typically see SSL in use when a web browser needs to securely connect to a web server over the unsecure Internet.

Technically SSL is a transparent protocol, which requires little interaction from the end user when establishing a secure session. In the case of a browser, users are alerted to the presence of SSL when the browser displays a padlock, or in the case of Extended Validation SSL the browser address bar displays both a padlock and a green bar. This is the key to the success of SSL – it is incredibly simple experience for end users.

Extended Validation (EV) SSL Certificates (e.g. GlobalSign ExtendedSSL):



Standard SSL Certificates (e.g. GlobalSign DomainSSL and OrganizationSSL or entry level AlphaSSL):



SSL is a protocol, and in order to use the SSL protocol organizations need an SSL Certificate. An SSL Certificate is a small data file that digitally binds a cryptographic key to your organization’s details, typically:

- **Your domain name, server name or hostname**
- **Your company name and location**
- **In certain cases your organizational contact details**

An organization needs to install the SSL Certificate onto their web server to initiate SSL sessions with browsers. Depending on the type of SSL Certificate applied for, the organization will need to go through differing levels of vetting. Once installed, it is possible to connect to the website over <https://www.domain.com> as this tells the server to establish a secure connection with the browser. Once a secure connection is established all web traffic between the web server and the web browser will be secure.

How should SSL be used?

No matter what information is being submitted (i.e. via a form on your website to your server) you should be using SSL. SSL is not just for securing credit card transactions. All levels of personal information are sensitive and should be secured, from newsletter signups to account logins, SSL should be the minimum security standard when collecting and submitting data.

SSL should be used:

- **To secure online credit card transactions.**
- **To secure online system logins, sensitive information transmitted via web forms, or protected areas of websites.**

- **To secure webmail and applications like Outlook Web Access, Exchange and Office Communications Server.**
- **To secure workflow and virtualization applications like Citrix Delivery Platforms or cloud based computing platforms.**
- **To secure the connection between an email client such as Microsoft Outlook and an email server such as Microsoft Exchange.**
- **To secure the transfer of files over https and FTP(s) services such as website owners updating new pages to their websites or transferring large files.**
- **To secure hosting control panels logins and activity like Parallels, cPanel, and others.**
- **To secure intranet based traffic such as internal networks, file sharing, extranets, and database connections.**
- **To secure network logins and other network traffic with SSL VPNs such as VPN Access Servers or applications like the Citrix Access Gateway**

Malware Monitoring

What is Malware Monitoring

To understand the growing need for Malware Monitoring services it’s important to understand the growing threat of “drive-by-downloads”. Drive-by downloading is a hacker technique resulting in the unauthorized download and installation (Drive-by-Download) of unwanted malicious software (malware) onto the client PC of anyone visiting the website. It is designed to steal information from Internet users by forcing them to automatically download malicious software (malware) without their knowledge or consent. By using numerous techniques to:

- 1) **Add an invisible iFrame to a hosted web page, invisible to the human eye**
- 2) **Transparently direct the visitor’s browser to a server transmitting exploits designed to break the browser through known vulnerabilities**
- 3) **Use the now broken browser to download and install malware / viruses onto the victim’s machine**

Malware is often designed for criminal, political, and/or mischievous purposes. These purposes might include:

- **Stealing financial account numbers, passwords, corporate trade secrets, or other confidential information**
- **Tricking the user into buying something that she or he doesn't need**
- **Sending junk e-mail (spam)**
- **Attacking other computers or networks (zombie attacks)**
- **Distributing more malware**

Malware includes viruses, trojans, rootkits, spam bots, spyware and other varieties (source: stopbadware.org).

Most websites are vulnerable to malicious code injection. When they do fall victim to this kind of attack, the first impact is directly against the websites visitors, as the Malware installed on their PCs is designed to steal personal data, such as credit card and bank account information, or even provide the Hacker with complete control over the victim PC.

The website itself is quickly affected as angry customers begin to complain about personal data loss. The website often fairly quickly becomes flagged or blacklisted for hosting malicious content by organizations such as Google.

It is enough to simply visit an infected web; there is no requirement to click on any links. The malware may be designed to monitor keystrokes and steal passwords, listen for credit cards, steal personal information or lie dormant, waiting for the attacker to invisibly turn the infected machine into a "zombie". Co-ordinated attacks using infected zombie machines to overload specific servers or networks have become a significant problem throughout the last few years, with attacks such as Aurora (distributed denial of service attack against many major IT companies originating from China) and Operation Payback (distributed denial of service revenging against previous Wikileaks suppliers) making worldwide news.

Blacklisting

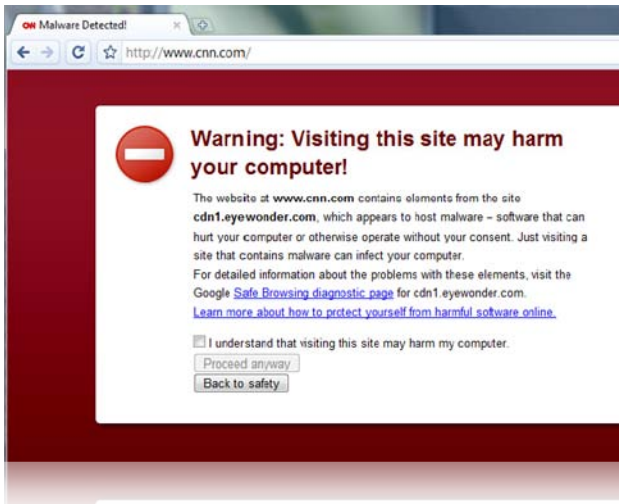
Due to the growing problem of malware distribution, Google in particular has taken a draconian view of any website distributing malware.

Google flagging has the greatest negative effect on websites as traffic is literally driven away from the site, due to Google posting warnings against visiting the site directly in their search results, or worse yet, removing the site from their search results altogether. This often has the effect of reducing a website's traffic from tens of thousands of visitors per day to almost zero.

Regardless of whether the site owners are knowingly distributing malware, a message will appear in the Google search results and also in browsers like Chrome and Firefox warning of the potential danger of visiting the website. For example:



"Remedial time, i.e. how long it takes to have Google remove you from blacklists, is undefined and frankly unknown. Reports in forums range from weeks to months..."



“Even major sites like cnn.com have been compromised and listed as distributing malware.”

Being blacklisted also means a website owner may find their domain listed on **stopbadware.org** – a central database of infected domains referenced by hundreds of applications and service providers. For website owners, blacklisting results in damage to business reputation, inevitable sharp drop in website traffic, and ultimately in revenues. The remedial actions needed to be removed are slow and expensive, with no guarantees of successfully regaining rankings.

Malware in Hosted Environments

Hosting companies need to be aware of the risk of compromise to their own infrastructure. As hackers typically seek the greatest economy of scale, attacking a hosting company’s infrastructure results in the highest return on effort. In August 2010, malware experts identified an infection in the Network Solutions infrastructure – a widget housed on Network Solution pages. The widget took advantage of an Internet Explorer vulnerability and resulted in the Koobface malware (a virus that “phones home” for further instructions) being widely distributed. The press identified the widget as being distributed via millions of landing pages reserved for parked domains.

Source:

<http://blogs.forbes.com/andygreenberg/2010/08/16/record-five-million-sites-were-likely-infected-by-hacked-web-widget/?partner=contextstory>

The Network Solutions explanation suggested the malware was actually only distributed via a NetSol blog:

“Our Security Team was alerted this past weekend to a malicious code that was added to a widget housed on our small business blog, growsmartbusiness.com. This widget was used to provide small business tips on Network Solutions’ under construction pages. We have removed the widget from those pages and continue to check and monitor to ensure security. The number of impacted pages that have reported publicly over the weekend are not accurate. We’re still investigating the number of web pages affected.

If you have downloaded the GrowSmartBusiness widget to your website, we recommend you delete that widget and scan your site for malware.”

Source: <http://blog.networksolutions.com/2010/security-alert-malware-found-on-widget/>

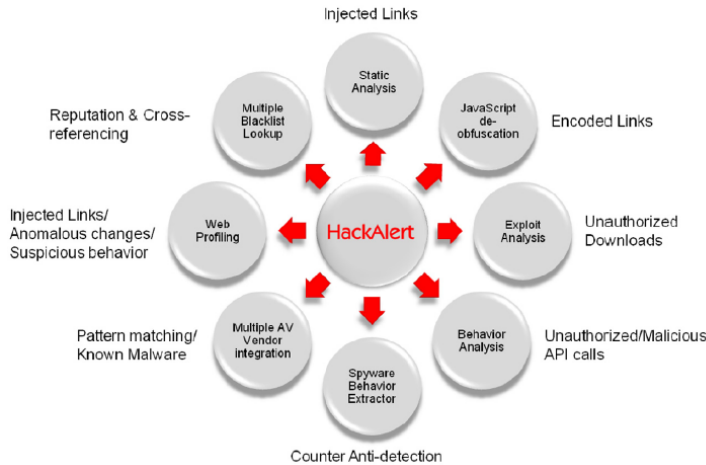
This kind of malware injection attack puts the reputation of the hosting company at risk, not just the hosted customer.

HackAlert - the GlobalSign Malware Monitoring Solution

HackAlert helps website owners avoid a doomsday situation by providing monitoring for malicious code injection and drive-by-downloads by giving due warning of an infection and sufficient details to facilitate timely removal of the injected code - protecting both customers and corporate reputation.

The solution crawls a website and actively analyzes the content on each page for signs of compromise. HackAlert uses numerous unique techniques to ensure malicious code is identified quickly and even the most advanced malware distribution techniques are efficiently identified.

HackAlert's detection technologies include the following:



The cloud-based Malware Monitoring detection service immediately notifies website owners if their site is infected with malicious code being used to target end-user's Personal Computers with Drive-by Downloads. Delivered as a hosted Software Service (SaaS), HackAlert protects businesses and customers from the impacts of Malware Injection. Features include:

- **Identifies drive-by downloads and zero-day malware threats hidden in websites and online advertisements**
- **Optimizes multiple analysis techniques to detect malware drive-by downloads targeting end-users before the website is flagged by search engines as malicious**
- **Protects your clients and customers from malware injection and malicious advertising (malvertising)**
- **Deploys globally distributed crawler and analyzer agents for non-intrusive 24x7x365 drive-by download monitoring**
- **Identifies active malware downloads as well as links to dormant malware before the website is flagged by search engines such as Google**
- **Displays injected code snippets to facilitate immediate malware removal and code-level remediation**

- **Reports injected page, malware source, browser vulnerability being exploited and drive-by download destination**

RESELLING GLOBALSIGN SECURITY SERVICES

Selling / Bundling SSL Certificates

There are numerous additional benefits to be gained by joining GlobalSign's Partner Program over other SSL reseller programs. The partner account is quick and hassle free to set up, GlobalSign's web based Certificate Center (GCC), flexible API technology or direct Control Panel plugins are simple and easy to use. The system even offers the ability to manage sub-resellers and their own customers.

Generate a new revenue stream / augment existing revenue stream

SSL Certificates are now a key aspect of online security and are a requirement for any organization that has an online presence (to protect customers against phishing attacks, credit card fraud and identity theft, whilst protecting the organisation's brand and reputation against fraudulent websites). So why not take advantage of this opportunity and encourage clients to buy directly, rather than from a third party? Offer SSL as part of existing packages or as an additional value-add option to instantly generate a new source of revenue.

- **Offer SSL Certificates and prevent clients from purchasing elsewhere.**
- **Receive the industry's best margins with zero commitment**
- **Help to maximize the renewable revenue received from each customer**
- **Offer a 'one stop shop' hosting/VAR service with SSL readily available**

Being successful in a highly competitive market is extremely difficult, so differentiate from competitors by bundling SSL Certificates. SSL can be offered as part of an existing package, producing a comprehensive hosting product portfolio. GlobalSign's SSL is a superior product in the market place by means of feature set, compatibility

and account management / technical support. As well as expanding the organization’s product portfolio, the organization will be able to offer the most secure and advanced SSL products available.

SSL Certificate Features:

- **AlphaSSL, DomainSSL, OrganizationSSL and ExtendedSSL (EV SSL) all from the same account**
- **Trusted by all browsers, applications and mobile devices**
- **Unlimited server licensing**
- **Strong security – SGC included in all GlobalSign Certificates free of charge**
- **Issued from a 2048 bit root (globally embedded since 1998)**
- **Secures both www and non-www with single certificate**
- **\$1k-\$250k warranty**
- **Clickable Site Seal**
- **Installation health check**
- **Worry free refund policy**

SSL options include:

- **Wildcard SSL – secure unlimited subdomains with a single Certificate**
- **Multi-domain SSL – secure up to 40 different domains in a single Certificate**
- **IP Address and intranet name inclusion**
- **Multi-year discounts**

Selling / bundling Malware Monitoring

Malware Monitoring for hosting companies is a relatively new offering, nevertheless, it is proving to be a critical component of the hosting provider’s value chain. Websites can choose their level of preferred protection by choosing a plan which suits their risk management policies and cost sensitivity:

- **Basic & Basic Plus plan** – a limited number of pages of the website are scanned once a day. Infection alerts are sent by email only.
- **Premium & Premium Plus plan** –scanning is deeper and the frequency of scanning is increased. The website owner has a management portal to monitor site scanning activity and gain direct access to remedial advice.
- **Custom plan** – the website owner can customize the number of pages scanned, and the frequency at which they are scanned.

RIGHT PRODUCT, RIGHT CUSTOMER

SSL Certificates

GlobalSign offers a full range of SSL Certificates designed to meet the requirements of each customer profile – from entry level to high end enterprise:

SSL Product	Customer Profile
AlphaSSL	Entry level, price-sensitive customers needing an instant issuance Certificate. Highest success is found when bundling AlphaSSL in price-competitive hosting packages. Can also be added to the value-add products at low cost, ensuring entry-level virtual hosting customers are not forced to shop around for SSL “deals”.
GlobalSign DomainSSL	Ideal for brand savvy and security conscious customers. Instant issuance is combined with an extended feature set including SGC security, Subject Alternative Names (multi-domain) support and significant warranties. Highest success is found when adding to higher end virtual hosting packages and entry level dedicated hosting packages.
GlobalSign OrganizationSSL	Necessary for brand savvy and security conscious customers. Traditionally vetted organization validated SSL is combined with an extended feature set including SGC security, Subject Alternative Names (multi-domain) support and significant warranties. Highest success is found when adding to

dedicated hosting packages where identity assurance is necessary for customers to maximise sales / conversions.

GlobalSign ExtendedSSL Ideal for brand savvy and security conscious customers. Extended validation policies activate the green address bar and the Certificate offers a further extended feature set including SANs - Subject Alternative Names - (multi-domain) support for applications such as Unified Communications for Microsoft Exchange 2007 / Office Communications Server and a \$250k warranty. Highest success is found when offering as a high value upsell across all hosting packages and where the green bar is needed to maximize sales and conversions.

Custom The Custom Plan is a customized version of the Premium plan available to larger hosting companies wishing to specify the scan frequency and the number of pages scanned.

Malware Monitoring

GlobalSign Malware Monitoring plans are designed to provide varying levels of alert protection based on website size, scan frequency and management tools needed:

Malware Monitoring Plan	Customer Profile
Basic	Entry level, low risk websites. A daily scan of the first pages of a single site alerts the website owner by email if malware is identified.
Basic Plus	As per the Basic plan, but with the number of pages scanned increased to expand Malware Monitoring coverage.
Premium	Aimed at higher risk websites. The number of pages scanned daily is further increased and additional patent pending malware identification technologies such as behaviour analysis and exploit analysis are introduced. Customers are given access to a web portal to monitor reports and gain insight into risks and remedial actions.
Premium plus	Ideal for higher risk, larger websites. As per the Premium Plan but with the pages scanned further increased.

GETTING A FAST RETURN ON YOUR INVESTMENT

With all new ventures the return on investment must outweigh the associated costs. With GlobalSign's Reseller Program there are very few, if any costs involved, with many benefits to take advantage of. Partners are assigned a dedicated account manager, marketing support manager and technical support services are readily available from local presence in the US, UK, Belgium, France and Germany.

SSL Reseller Models

Pay As You Go (PAYG)

Partners simply use a credit card to purchase each Certificate that is resold. Discounts are immediate – ensuring that even without commitment, the best SSL reseller margins in the industry are achieved.

Deposit

Partners place a deposit, with the amount placed linked to the discount rate made available. The deepest per Certificate discounts are available via the deposit method. Unlike other SSL Providers, deposits with GlobalSign do not expire and can be rolled over, year on year.

Unlimited Issuance License

GlobalSign has pioneered the Unlimited Issuance License. This enables hosting companies to issue an unlimited number of Certificates for a yearly flat fee. This model has been very successful with companies mass issuing SSL Certificates such as LiquidWeb, 123-Reg, Webfusion & Singlehop.

Malware Monitoring Models

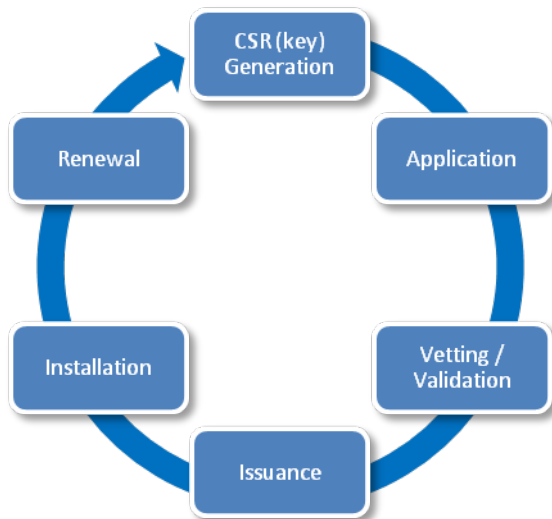
GlobalSign works with hosting companies on a per case basis to advise and implement appropriate Malware Monitoring models. Typically we advise that hosting companies adopt across all customers the basic scanning service, with upsell paths to higher value / higher risk sites.

This may be added as part of the hosting bundle, or even as a value-add service to protect the hosting company's good name in the industry.

Deployment & Automation

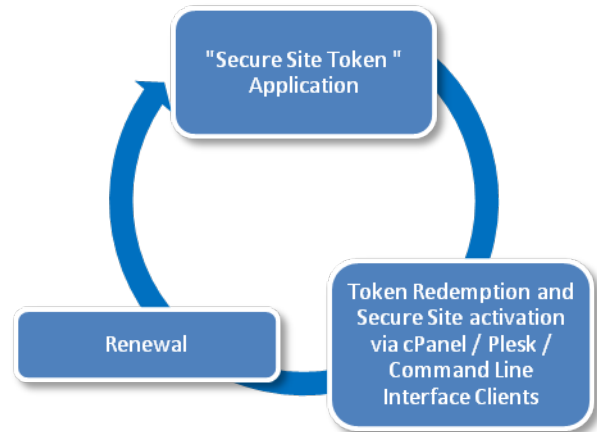
SSL Certificates follow a lifecycle model that can be segmented into 6 stages. When selecting an SSL Provider, it is important to understand which stages of the lifecycle have been automated or optimized. A poorly optimized lifecycle will put undue pressure on your support staff through customer phone calls and technical issues.

Traditional Certificate provisioning:



For example, GlobalSign offers AutoCSR to automate the CSR (key) generation. The various APIs allow for automated application submission. Our patent pending validation methods speed up the vetting component. Further API calls allow for the automated retrieval of issued Certificates. Our unique OneClickSSL technology offers integration into IIS, Apache and various Control Panels to automatically install issued Certificates and activate secure sites.

Certificate provisioning via OneClickSSL:



For more details on OneClickSSL automation technology please visit our website at www.globalsign.com/partners or contact us.

Finally our QuickRenew technology ensures that renewal steps are minimized to reduce the risk of expired Certificates. GlobalSign is pioneering automation like no other Certificate Authority.

Hosting Companies

Hosting companies can use the GlobalSign Certificate Center (GCC) to manage the full lifecycle of their SSL Certificates. Alternatively, GlobalSign offers a number of APIs (XML and AJAX) to automate the inclusion of SSL into existing workflows.

GlobalSign's HackAlert Malware Monitoring service is configured via API and web based management portal. Advanced JSON responders ensure the latest domains can be registered instantly.

Cloud Application/Service/Platform Providers

GlobalSign is pioneering SSL based security in the cloud. Via GCC and the Cloud API service (launched Q1 2011) GlobalSign Partners can create on-demand Certificates with up to 40 SANs (multi-domain) in each Certificate, and automatically add/remove SANs as needed by their cloud application. Talk to our Cloud Specialist team for more details.

Registrars

GlobalSign offers a unique service to Domain Registrars – the ability via API to create an SSL Certificate for each domain as it is registered. This gives Domain Registrars the ability to bundle SSL Certificates with every domain sales. Talk to our Registrar Specialist team by contacting us at www.globalsign.com/partners for more details.

PARTNER PROGRAM LEVELS

GlobalSign offers 4 levels of Partnership – Authorized, Silver, Gold and Platinum.

Authorized Partners receive instant discounts, a reseller partner portal (GlobalSign Certificate Center), canned sales and marketing resources and instant access to technical support.

Silver, Gold and Platinum Partners receive accelerated discounts, access to the advanced APIs, control panel plugins, dedicated marketing assistance, varying levels of co-marketing / co-branding opportunities & feature prioritisation.



WHY PARTNER WITH GLOBALSIGN?

With fantastic margins and increased revenue potential, this is a simple, but sophisticated reseller program enabling you to generate new revenue streams, expand your product portfolio and provide the best SSL and Malware Monitoring there is available. The program is built around the needs of hosting companies, fulfilling both technical and marketing requirements:



The program has an extremely fast return on investment with the option of no commitment. It also involves minimal time, effort and resources. But don't just take our word for it, ask any of our thousands of hosting partners...

"We chose GlobalSign based on reliability, cost and overall ROI. Our customers have increasing security concerns which prompted us to find a provider who could offer the most reliable and cost effective SSL security solution."



Travis Stoliker, Marketing Director

"It is vitally important to us that we partner with the most credible and forward thinking vendors for every third party service we offer. Since the start of our relationship we've been able to pass on the value of the GlobalSign brand as well as the strong security its products offer. Our partnership has many co-marketing initiatives and development plans in place, with on-going industry leading improvements in certificate issuance workflows, as well as continued education to our customers about online security threats - leading to a customer experience both our companies can be proud of."



Thomas Vollrath, CEO, Webfusion

INQUIRE ABOUT THE PARTNER PROGRAM

To join now, or for further information about becoming a GlobalSign SSL & Malware Monitoring Partner visit our website at www.globalsign.com/partners.

ABOUT GLOBALSIGN

GlobalSign was one of the first Certification Authorities and has been providing digital credentialing services since 1996. It operates multi-lingual sales and technical support offices in London, Brussels, Boston, Tokyo and Shanghai.

GlobalSign has a rich history of investors, including ING Bank and Vodafone. Now part of a GMO Internet Inc group company - a public company quoted on the prestigious Tokyo Stock Exchange (TSE: 9449) whose shareholders include Yahoo! Japan, Morgan Stanley and Credit Suisse First Boston.

As a leader in public trust services, GlobalSign Certificates are trusted by all popular Browsers, Operating Systems, Devices and Applications and include SSL, Code Signing, Adobe CDS Digital IDs, Email & Authentication, Enterprise Digital Solutions, internal PKI & Microsoft Certificate Service root signing. It's trusted root CA Certificates are recognized by all operating systems, all major web browsers, web servers, email clients and Internet applications; as well as all mobile devices.

Accredited to the highest standards

As a WebTrust accredited public Certificate Authority, our core solutions allow our thousands of enterprise customers to conduct secure online transactions and data submission, and provide tamper-proof distributable code as well as being able to bind identities to Digital Certificates for S/MIME email encryption and remote two factor authentication, such as SSL VPNs.

GlobalSign US & Canada

Tel: 1-877-775-4562

www.globalsign.com

sales-us@globalsign.com

GlobalSign EU

Tel: +32 16 891900

www.globalsign.eu

sales@globalsign.com

GlobalSign UK

Tel: +44 1622 766766

www.globalsign.co.uk

sales@globalsign.com

GlobalSign FR

Tel: +33 1 82 88 01 24

www.globalsign.fr

ventes@globalsign.com

GlobalSign DE

Tel: +49 30 8878 9310

www.globalsign.de

verkauf@globalsign.com

GlobalSign NL

Tel: +31 20 8908021

www.globalsign.nl

verkoop@globalsign.com
