

WHITE PAPER

An Encrypted Client Hello Primer

What ECH Is, Why It's Important, and What Security
Leaders Can Do to Prepare

By John Grady, Principal Analyst
Enterprise Strategy Group

December 2023

Contents

Executive Summary	3
Encrypted Traffic and Its Impact on Cybersecurity	3
The Next Step for TLS: Encrypted Client Hello	5
Encrypted Client Hello	5
ECH Will Make It Harder for Security Teams to Maintain Visibility	6
Spotlight: Potential Impacts of ECH in Financial Services	7
Selective Decryption Becomes Impossible With ECH.....	8
What Security Leaders Can Do Right Now to Prepare for ECH	8
Conclusion	9

Executive Summary

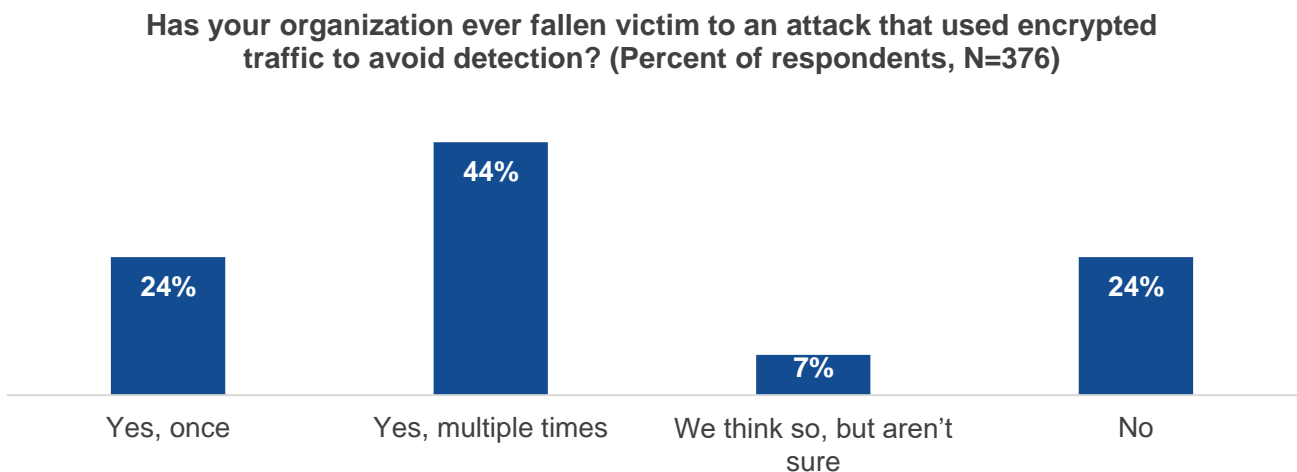
Encrypted traffic is certainly not new, but for many organizations it continues to be a significant threat vector. This is true even though a variety of avenues exist to detect threats within encrypted traffic. Yet even as many organizations work toward improving their encrypted traffic management and scanning, an important extension to the Transport Layer Security (TLS) 1.3 protocol promises to further complicate the issue. Encrypted Client Hello (ECH) will fundamentally change how the initial TLS handshake is initiated, making it more secure by encrypting all connection metadata fields used by network security solutions, in particular, to do selective decryption. While this is a positive for privacy, the change will have a major impact on how security teams maintain visibility into encrypted traffic, affecting not only network security but also information security and compliance. Today, there is no clear technological solution to this problem, but the ratification of the extension appears very likely. It is thus imperative that security leaders begin to educate themselves on ECH, work with their peers across the organization to analyze and plan for its impacts, implement a first set of mitigation measures, and engage with product vendors to assess who has a clear point of view and a potential solution for the ECH problem.

Encrypted Traffic and Its Impact on Cybersecurity

Encrypted traffic is now pervasive. While encryption was originally used to protect connections to sites where sensitive information such as credit card data was shared, nearly all web sessions are encrypted by default today. Yet while encryption can help ensure the security and privacy of users, it does pose a risk from an enterprise cybersecurity perspective. In fact, research from TechTarget’s Enterprise Strategy Group has found that scanning encrypted traffic for threats is a significant or notable concern for 83% of organizations.¹

This is likely due to the prevalence of attacks that use encryption to avoid detection. Among Enterprise Strategy Group research respondents, 24% indicated they had suffered an attack once that used encryption, while 44% said they had experienced such an attack multiple times (see Figure 1).

Figure 1. Prevalence of Encrypted Attacks



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

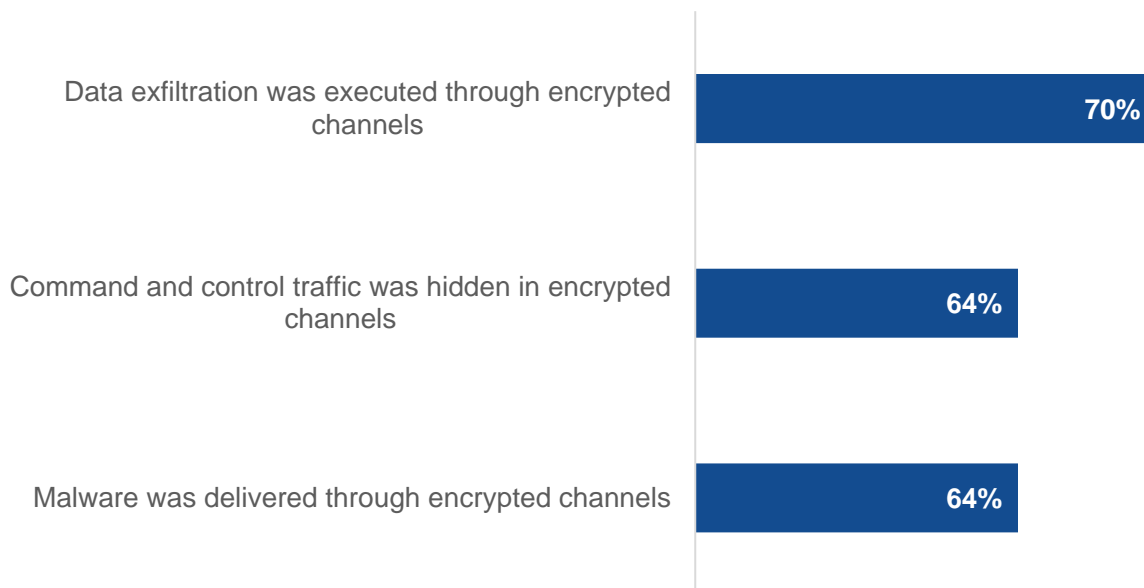
¹ Source: Enterprise Strategy Group Research Report, [The Evolving Role of Network Detection and Response](#), March 2023. All Enterprise Strategy Group research references are from this report and associated survey results set.

Further, attackers use encryption across a variety of attack stages, making the situation even more difficult to manage. Some of the most common attacks, shown in Figure 2, include:

- **Data exfiltration.** Once the attacker has access to sensitive business data, it is exfiltrated via encrypted channels, which makes data loss prevention solutions blind to such data leakage. Nearly three-quarters (70%) of respondents indicated this had occurred to their organization.
- **Command and control traffic.** Once a machine is compromised, the command-and-control traffic attackers rely on propagating the attack via privilege escalation and lateral movement across the network. This movement is typically encrypted to obscure the attackers' actions. Similar to malware delivery, 64% said they suffered attacks where command-and-control traffic was encrypted.
- **Malware delivery.** Attackers can compromise legitimate websites to serve malware and other exploits, using common business applications that use encryption, such as OneDrive or Box, to stealthily deliver malicious code. They can also procure secure socket layer (SSL) certificates for spoofed or fake sites to send malware via encrypted connections as part of phishing or other attacks. Nearly two-thirds (64%) of respondents said they had experienced an attack where malware was delivered via encrypted channels.

Figure 2. How Attacks Use Encryption

**You indicated your organization suffered an attack that used encryption to avoid detection. Which best describes how the attack used encryption?
(Percent of respondents, N=284)**



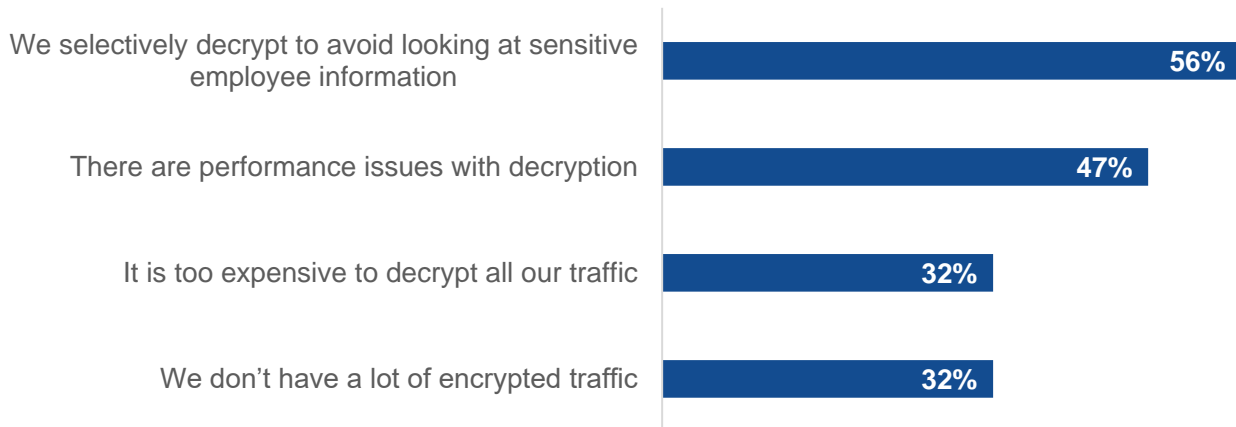
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

To gain visibility into encrypted sessions, security teams can decrypt and then inspect traffic either directly on the different tools used for scanning (such as firewalls, secure web gateways, etc.) or through a dedicated decryption tool that passes unencrypted traffic to scanning tools. This can improve performance and simplify policy management. Yet even with these options in place, many organizations do not decrypt and inspect all the traffic on their network. The most common reason organizations cite when forgoing decryption is to avoid looking at sensitive employee information, which was noted by 56% of respondents (see Figure 3). On the other hand, 47% pointed to performance issues and 32% cited cost as reasons they do not decrypt more. Nearly one-third (32%) believe their organization does not have a lot of encrypted traffic, which is unlikely and a concerning finding given that, in today's

web-centric environment, nearly all traffic is encrypted. In particular, it suggests that many might not understand the scope of encrypted traffic. So, while on the one hand managing encrypted traffic and scanning for threats is a key concern for many, there remain significant gaps in visibility even today.

Figure 3. Reasons for Not Decrypting All Traffic

You indicated your organization does not have visibility into all of its encrypted traffic. What are the reasons why? (Percent of respondents, N=247, multiple responses accepted)



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

The Next Step for TLS: Encrypted Client Hello

Issues with encrypted traffic become more problematic when evolving standards and their impact on the cybersecurity stack are not considered. The protocols used for encrypted web traffic are constantly changing, with each update to the protocol seeking to improve security, performance, and privacy. While often still referred to as *SSL encryption*, the SSL protocol has not been widely used in many years; TLS 1.0 was introduced in 1999.

Fast forward to today, and we are at the inflection point of the transition from TLS 1.2 to TLS 1.3, which provides a few key benefits, including:

- The removal of all nonsecure cipher suites from use, excluding any with known vulnerabilities and those that do not support perfect forward secrecy.
- Allowance for a simplified TLS handshake with fewer back-and-forth trips between the client and server.
- The adoption of server certificate encryption by default, further securing the initial handshake.

Many organizations are still in the process of adapting to TLS 1.3, and some security tools do not yet support the protocol. In these cases, sessions are downgraded to TLS 1.2 for decryption, which negates the security improvements in the upgraded protocol. Yet even before TLS 1.3 is broadly deployed, there is already a new extension to the protocol on the horizon that will add more complexity for security teams to navigate.

Encrypted Client Hello

While TLS 1.3 did adopt server certificate encryption by default, the “Client Hello” message still sends many fields in the clear. Specifically, the server name indication (SNI) field and application layer protocol negotiation (ALPN) are sent in clear text. These fields include important information, as SNI indicates what host the client is attempting to

connect to, which assists the server in presenting one of many certificates that may be available. ALPN assists in indicating which application layer protocol is supported by the client (i.e., HTTP/2 or HTTPv1.1, DoT, IMAP, FTP, SMB2, SIP, etc.). If an entity—be it a middlebox or attacker—were positioned in the middle of a conversation between a user and application, they could easily glean session details because these values are passed in the clear. In the case of attackers, this could help them to impersonate one of the parties because they understand the expected activity of the connection.

ECH is a proposed extension to TLS 1.3 that would close these gaps and hide TLS metadata from any devices or entities intercepting the traffic. To accomplish this, a colossal set of innovations and creative design had to be thought through and organized. The ECH extension introduces a Client Hello Outer (CHo) that contains “dummy” information as well as a Client Hello Inner (CHi) that contains the real Client Hello message and is encrypted. Architecturally, a client-facing server would sit in front of multiple content servers to help maintain anonymity of those servers. Every 48 hours, the client-facing server would set up the ECH configuration and, in particular, the public keys of a new cryptography called *Hybrid Public Key Encryption (HPKE)*. The distribution mechanism of the ECH configuration necessitated extending the DNS protocol with service bindings, allowing each DNS entry to contain a new entry called *resource records*. The web browser requesting a resource would first reach out to the DNS resolver and be provided with the HTTPS resource record for the site in question, which includes the HPKE public key for the ECH server. This allows the browser to securely encrypt the Client Hello message and access the client-facing server through an encrypted connection from the start. In effect, this model would have the client-facing server acting as a TCP forwarder, receiving and decrypting the ECH.

ECH is a proposed extension to TLS 1.3 that would close [privacy] gaps and hide TLS metadata from any devices or entities intercepting the traffic.

In addition to improving the protection of user traffic from potential attackers, there are privacy benefits ECH will provide as well. With ECH implemented, it will be harder for device providers and governments to track and control activity. Further, with no access to the metadata from users’ activity on the web, the ability for content providers to serve targeted adware will be curtailed. Finally, the use of ECH servers in front of application servers will provide additional protection and anonymity by shielding them from direct access.

Currently, ECH is an Internet-Draft (I-D) at the Internet Engineering Task Force (IETF), with it likely to enter “last call” very soon. As there is a chain of dependencies with other I-Ds, it is expected that editorial reviews will require five to six months of elapsed time for a final ratification that may happen by summer 2024. Yet the importance of and agreement around ECH at the IETF is such that some vendors, including Google, Mozilla, and Cloudflare, have begun to announce early support for the extension. With these implementations already available and more likely to follow prior to the ratification, the need for security and IT teams to quickly develop a plan for their organization is clear.

ECH Will Make It Harder for Security Teams to Maintain Visibility

While the benefits of ECH are clear, a range of potential impacts stemming from its introduction must be considered. From an infrastructure perspective, content providers will have to stand up ECH servers that are powerful enough to manage the connections to multiple content servers. DNS will also be affected as records become larger due to the added role of managing public ECH keys. Keys are rotated often, and it takes time for changes to propagate. So while there is a grace period written into the protocol, it will be a notable adjustment for many organizations.

Yet the most significant impact from the introduction of ECH will arguably be on the security team. To alleviate some of the challenges with decryption and further preserve user privacy, some vendors have introduced tools that

organizations are using to detect anomalies in encrypted traffic without decrypting. These tools analyze traffic metadata, the TLS handshake, and other pieces of information to infer whether a connection is malicious. Enterprise Strategy Group research has found that 45% of organizations say they use these types of capabilities today, which—while likely high—points to significant interest in this type of approach. Unfortunately, this type of approach relies on the very information that ECH will encrypt, making it difficult if not impossible for them to detect threats in encrypted traffic. This will leave decryption as the only effective means of detecting threats in encrypted traffic. Yet when ECH is utilized in the handshake, decryption will only be able to occur if the middlebox handling decryption is ECH-aware.

Cybercriminals do not play by the rules and use whatever means they can to compromise target organizations. As a result, it is expected that they will continue to hide within encrypted traffic and exploit the current lack of awareness around ECH to their advantage. For example, they may create new forms of command-and-control communications hiding within an ECH enabled TLS1.3 session or use GREASE ECH, or dummy ECH. Because middleboxes will be unable to see the destination of the traffic and therefore perform interception, security teams will be very hard-pressed to detect this traffic.

Spotlight: Potential Impacts of ECH in Financial Services

The adoption of ECH and its impact on network visibility could introduce certain challenges and potential negative impacts, particularly relative to compliance in the financial services industry (FSI). Some of the key considerations include the following:

- **Compliance monitoring.** Network visibility plays a crucial role in compliance monitoring within the FSI vertical. Regulatory requirements often mandate the monitoring and inspection of network traffic for various purposes, including detecting and preventing unauthorized access, ensuring data integrity, and detecting suspicious activities or compliance violations. With ECH encrypting the “Client Hello” message, traditional network-monitoring tools might struggle to fully inspect the encrypted traffic, potentially hindering compliance-monitoring efforts.
- **Risk mitigation and incident response.** Network visibility is also essential for promptly detecting and responding to security incidents and data breaches. ECH could limit visibility into specific websites or services being accessed, making it more challenging to identify potential security threats or anomalous behavior. This could affect incident response capabilities, potentially delaying detection and response times, which would be detrimental to compliance requirements and risk-mitigation efforts.
- **Compliance reporting and auditing.** Compliance regulations often require organizations in the FSI vertical to provide detailed reports and audit trails of their security measures and activities. Reduced visibility due to ECH could affect the accuracy and completeness of such reports. Compliance teams might need to find alternative means or solutions to ensure the necessary visibility and evidence collection, possibly requiring additional investment in endpoint security tools or alternative monitoring techniques.
- **Legal and regulatory considerations.** Financial institutions operate in a highly regulated environment, and compliance with laws and regulations is of the utmost importance. The use of ECH should be assessed in light of specific legal and regulatory requirements applicable to the FSI sector. Compliance teams should evaluate the potential implications of reduced visibility on compliance with specific regulations, such as data protection, privacy, or sector-specific requirements.
- **Collaboration with regulators.** Financial institutions often work closely with regulatory bodies to ensure compliance and address any concerns or inquiries. The reduced visibility introduced by ECH may require institutions to engage in proactive discussions with regulators to address the impact on compliance-monitoring capabilities and determine acceptable alternatives or compensating controls. Open communication and collaboration can help bridge the gap between security needs and compliance requirements.

Selective Decryption Becomes Impossible With ECH

Currently, organizations can selectively decrypt a web session based on the destination. For example, if a user is accessing their personal bank account, the middlebox is aware of this and would keep the connection encrypted. While an ECH-aware middlebox can decrypt ECH-enabled TLS 1.3 traffic, it cannot do so selectively because the information about destination that would be used to decide whether or not to decrypt is hidden. So, without knowing what the destination is, the decision would have to be made whether to decrypt or not, effectively negating selectivity.

With currently available technology, security teams do not have a lot of good options. That said, options that do exist include the following:

- **Ignore the extension.** In this case, the decryption policy would be based on the client-facing ECH server. However, because this sits in front of the actual destination content server and anonymizes it the policy would be negated. Further, the disconnect between the client browser setup for ECH and the middlebox not acknowledging the ECH extension may result in an error.
- **Downgrade to TLS 1.2.** As some do now, security teams could downgrade TLS 1.3 connections using ECH to TLS 1.2 (where ECH is not available). However, this negates the privacy and security improvements of TLS 1.3 and ultimately would lead to the same error as ignoring the extension because the ECH client-facing server is configured for the protocol. Additionally, with TLS 1.3 servers becoming more prevalent than TLS 1.2 servers, degrading could keep the client from connecting if the server only supports TLS 1.3.
- **Block sessions using ECH.** As ECH becomes more widely adopted, this option will become untenable. As noted, vendors including Google, Mozilla, and Cloudflare have already released at least limited support for this extension. With this early adoption already in place, it is likely that within a few years organizations blocking sessions using ECH would be blocking a majority of their traffic.
- **Disable the option within browsers.** This option will likely exist in most browsers but will face a number of limits. Because it requires that the organization control its clients, it will be difficult to enforce on BYOD devices. Over time, as ECH becomes more prevalent, browsers may also remove this option and revert to a mandatory ECH mode.
- **Strip the new DNS resource records.** This option will disable ECH from any client requesting it through that DNS over HTTPS service because the client will not access its ECH parameters stored in the DNS new resource records. It will likely only remain an option early in the adoption cycle and will phase out when browsers remove the ability to keep ECH as optional.

Ultimately, all these solutions are partial and short term in nature. In many cases, they would be ineffective against malicious attack.

What Security Leaders Can Do Right Now to Prepare for ECH

While there are no immediate technical or architectural changes security leaders need to make at the moment, there are some steps that can be taken to get ready for this change over the next few years. First, an ad-hoc community including prominent financial institutions, the author of DNS, and others, are developing an I-D about ECH deployment considerations that offers a comprehensive approach to the problem with some mitigations proposals. This is being developed as an opened public [GitHub](#) should security leaders need advice, be willing to provide feedback, or be interested in participating in this community work. From an internal perspective, security leaders should raise awareness around ECH so employees can familiarize themselves with it.

Because of the potential regulatory and legal questions that will arise from maintaining effective control over ECH traffic, security leaders should also interface with a variety of other roles within the organization.

Ideally, this would expand outside of the security organization to IT as well. As noted, the infrastructure requirement to support ECH will necessitate changes, so network and applications teams may or may not be unaware that this change is on the horizon. Speaking to IT counterparts about how they might handle these changes for a public resource that external users will access could provide helpful information in developing a strategy for internal users.

Because of the potential regulatory and legal questions that will arise from maintaining effective control over ECH traffic, security leaders should also interface with a variety of other roles within the organization. Compliance and legal teams can begin to investigate the impact of ECH on maintaining compliance with regulations such as the GDPR, DORA, NIS2, CCPA, HIPAA, and PCI DSS. Data protection officers must weigh in on the impact on data processing activities, providing data privacy impact assessments relevant to local regulations and guidance on the balance of organizational risk and employee privacy. Risk teams can provide input into possible outcomes of losing visibility into encrypted traffic.

Security leaders should begin to reach out to their vendor contacts to understand their plans and roadmap around ECH. Understanding whether ECH is on their radar, their initial plans to address the change, and whether they are providing guidance to customers are all good starting points for a discussion. Additionally, this situation provides an opportunity to speak to alternative vendors to understand their point of view on and plans for ECH. With the impact of this change as significant as it is, ultimately organizations may need to add or replace vendors to have effective control over ECH traffic.

Conclusion

Overall, there is little doubt that ECH is a good step forward to advance the security and privacy of web use. With such a significant portion of peoples' lives now centering around the web, it is critical to provide as many protections as possible. But security teams have a clear responsibility to protect their organization as well, and this requires maintaining visibility across as much of the environment as possible. Unfortunately, ECH will significantly change this calculus.

As always, proper planning and early action can make a difference and help ensure security teams remain on track and do not become blind to ECH-enabled traffic. When the extension is ratified, cross-functional collaboration and in-depth technology assessments will be critical. But in the short term, security leaders should focus on educating themselves and their organizations, as well as having initial conversations with all relevant stakeholders on the ECH extension.

©TechTarget, Inc. or its subsidiaries. All rights reserved. TechTarget, and the TechTarget logo, are trademarks or registered trademarks of TechTarget, Inc. and are registered in jurisdictions worldwide. Other product and service names and logos, including for BrightTALK, Xtelligent, and the Enterprise Strategy Group might be trademarks of TechTarget or its subsidiaries. All other trademarks, logos and brand names are the property of their respective owners.


Information contained in this publication has been obtained by sources TechTarget considers to be reliable but is not warranted by TechTarget. This publication may contain opinions of TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget's assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at cr@esg-global.com.

About Enterprise Strategy Group

TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

 contact@esg-global.com

 www.esg-global.com