ShieldQ

ISO 27001 CERTIFICATION EUROPE™

PCI Security Standards Council™

Self-governing compliance doesn't work here anymore

GDPR READY

www.shieldq.com

Self-governing compliance doesn't work here anymore

Organizations handling sensitive data may be lulled into complacency, thinking that self assessment is enough to protect payment card numbers, health records, personally identifiable information *(PII)*, or legal and financial documents.

But such self governance can backfire, as threats such as cyber criminals find more inventive ways to invade your systems. Hotels, among the most highly targeted, have suffered very serious breaches in the past. It's no wonder: the hotels' point-of-sale *(POS)* system serves as its greatest vulnerability, while security weaknesses within ecommerce sites, and data being delivered via unprotected sources – such as front and back office operations via email, fax, telephone – pose significant risk.

Now, you'd think that financial institutions, surrounded by an army of regulations to ensure data security, would be immune. But they are among the top targets:

PricewaterhouseCoopers has found that cybercrime comprises a considerable 38% of threats – a statistic that can easily damage reputations.

Law firms, which store sensitive material like intellectual proprietary information and trade secrets, corporate financials for an upcoming IPO, or private details about clients, have not been ignored by cybercrime, either. Yet, in an American Bar Association Legal Technology survey, 47% of respondents admitted to having had no plan at all, much less a self-governing one – no surprise, since industry experts claim that security at legal organizations is known for being poor. Think how a resulting breach can bankrupt a firm.

"While the GDPR may be a European regulation, these new rules affect any organization worldwide that handles EU citizens' data...e.g., if a US financial institution takes on an EU client, then they fall under GDPR rulings."

Verizon's yearly Data Breach report summarizes confirmed data losses following a breach, according to industry.

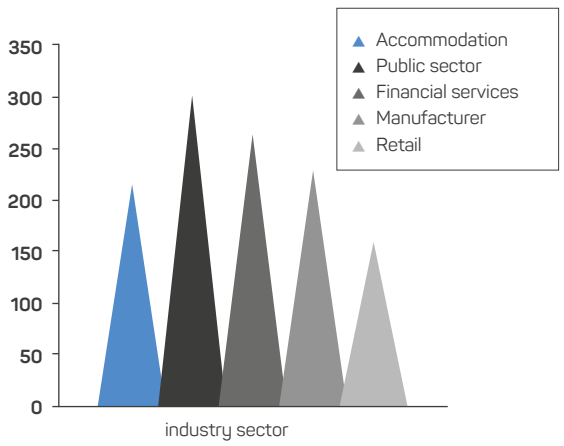
Rather sobering. But until now, there have not been too many consequences, or any substantial fines for non-compliant organizations suffering a data breach.

% Of Incidents With Confirmed Card Losses

Verizon Data Breach Investigations Report 2015

Confirmed Serious Incidents With Card Losses

Verizon Data Breach Investigations Report 2015



The GDPR: worldwide reach, worldwide fines

The European Parliament's General Data Protection Regulation *(GDPR)*, already in force, although officially effective as of 2018, will radically change the playing field for non-compliance, or self-governing compliance.

To be clear: while the GDPR may be a European regulation, these new rules affect any organization worldwide that handles EU citizens' data, from identity numbers to payment card data and financial/legal or health records. For example, if a US financial institution takes on an EU client, or if an Australian hotel accepts a booking from an EU guest, then they fall under GDPR rulings.

What does GDPR entail?

Key highlights include:

Sanctions. Using a tiered approach for penalties, data protection authorities propose fines of up to 4% of annual worldwide turnover. Other specified infringements can result in fines of up to 2% of annual worldwide turnover.

Compliance. The regulation places huge obligations on data controllers to maintain certain documentation and conduct data protection impact assessments.

Breach notifications. Such notices must be handled without undue delay, and where possible, within 72 hours.

Data processing responsibilities. Those handling data now have direct obligations, including implementing technical and organizational measures, notifying data controllers of breaches and appointing a data protection officer, if required.

International transfers. The rules require informed consent for where data will be stored. When "Safe Harbor rules" were abolished in 2015, organizations outside the EU were no longer allowed to self-assess their compliance. Organizations were anticipating the new European Data Laws would change this ruling and allow companies to return to self government. This hasn't happened. If data is being collected in the EU in relation to a client, but then is transferred to the US, for example, for any reason *(the customer has moved to the US and wants to work with a local branch of a bank, financial institution, etc.)*, the consent requirements have been made stricter.

Binding corporate rules. These apply if an organization with many branches *(e.g., hotel chains, banks)* wants to make inter-group data transfers.

"One-stop shop." The laws represent one set of regulations for all, including a person's right to request that data to be deleted when no longer required.

Extensive audits. Every business process must be critically reviewed and changed when it does not comply with requirements. While this may seem harsh, it's in the organization's best interest, because among GDPR requirements is the right for individuals "to be forgotten": organizations must delete that data, especially when it's no longer necessary. This means that data must be stored according to rules that specify when and how it can be deleted.

Standards such as PCI DSS provide additional requirements on what type of cardholder data may or may not be stored and how it must be protected.

To avoid penalties, organizations must review all current business practices to ensure compliance with all relevant standards, at all times. Thus, the focus needs to be on all vulnerable aspects of an organization.

And size does not matter: Small- to medium-size organizations are not immune, either. While they, too, may have relied on self assessment in the past, they won't be able to, now: VISA has recently announced that acquiring banks must get proof that even very small, level-4 merchants are using PCI-accredited solutions.

It's clear that many organizations will need to find a sustainable solution appropriate to their business size, and one that can ensure complete, round-the-clock compliance.

Where are organizations falling short?

It's been established that security self assessment leaves much to be desired. See this list below; do any of them ring a warning bell?

- **Failure to invest in data security.** Many organizations have not been technology driven. Smaller entities may not have a dedicated IT team to ensure security, nor may they have the resources to invest in compliance and in security – both of which require ongoing investment, once in place.

- **Indefinite document storage.** Organizations tend to hoard, keeping outdated data long after they've outlived their need. This data may not necessarily be secured – and then what happens if there's a breach?

- **Unprotected, third-party providers.** Both hotels and organizations such as financial institutions receive sensitive information like payment card data, loan applications and financial portfolios from guests, staff, online affiliates and outsourced providers, including support teams. Do you know how – or even if – they protect this info?

- **Payment card data.** Industries like hotels process a very high volume of card transactions daily, storing store payment card data, often in several locations, and in several formats. Occasionally, this data is presented in "clear data format": it's not encrypted or tokenized – and rarely PCI compliant. This information is also often held for unnecessarily long periods of time, placing organizations at high risk.

Despite these risks, some entities are still not taking standards like PCI compliance and GDPR as seriously as they ought to – even when all the evidence suggests they should:

Reasons often given include:

- Very high cost expectations
- Lack of knowledge about available solutions
- Lack of IT expertise
- Fear of losing business from customers
- Confusion about various regulatory requirements
- False belief that self assessment will be sufficient
- Conscious decision that the risk of a breach is worth taking

Whatever the reason, there's a lot of misunderstanding surrounding PCI compliance and GDPR and possible solutions.

Common misconceptions include:

- **The extremely high cost of compliance.** The conventional road to accreditation is what deters organizations, because it requires:
  - Hiring a qualified security assessor *(QSA)*
  - Implementing the QSA's recommendations
  - Ensuring that compliance is maintained, year after year

While these activities can take a long time and require considerable investment, this approach is by no means the only one. Organizations don't realize that they can be fully compliant adopting cloud-based solutions, without investing in lengthy, costly processes. Such solutions typically cost less than 10% of conventional systems.

"Organizations don't realize that they can be fully compliant adopting cloud-based solutions, without investing in lengthy, costly processes. Such solutions typically cost less than 10% of conventional systems."

- **Disruptive to established workflows.** Often, organizations assume that, to become PCI compliant, entire workflows must change, causing massive disruptions to business continuity. In actuality, good, cloud-based solutions are sufficiently versatile and flexible, enabling PCI DSS level 1 compliance, with no change to legacy workflows, and minimal change to established procedures.

- **Long implementation times.** Like most systems, the process time varies, depending on how complex the organization is, and how long it takes to implement the tools they need to become PCI DSS compliant. Customized systems can take up to 18 months to implement, requiring significant resources and management time. With the right cloud-based service, however, organizations can become compliant in less than a month, provided that they plan sufficiently in advance.

- **Huge ongoing IT overhead to remain compliant.** While compliance is a continual process, it does not necessarily require a team of IT experts. With cloud-based services, there's no need to integrate anything into the organization's existing infrastructure. Thus, there's no IT overhead and no need to hire an in-house security specialist to support the system.

- **Conflicting QSA opinions and interpretations of PCI DSS requirements.** Like any other industry, not every expert will agree on how to interpret a standard or a law. Any cloud solution accredited by a QSA ensures there is no misunderstanding about its acceptability, and that such a solution is being constantly being updated.

- **Uncertainty concerning the security of cloud solutions.** Cloud solutions are no riskier, and are no less secure than physical solutions. Indeed, they may be more secure, since it's a function of the security you build into your organization. As Information Age mentions, perimeter protection solutions are similar. And when it comes to the risk of employees who want to steal data, the cloud makes it more difficult to locate it, for a simple reason: there's no person to befriend as an accomplice in the deed. The cloud is an entity.

Cloud solutions also must comply with tougher standards, and must build secure data centers.

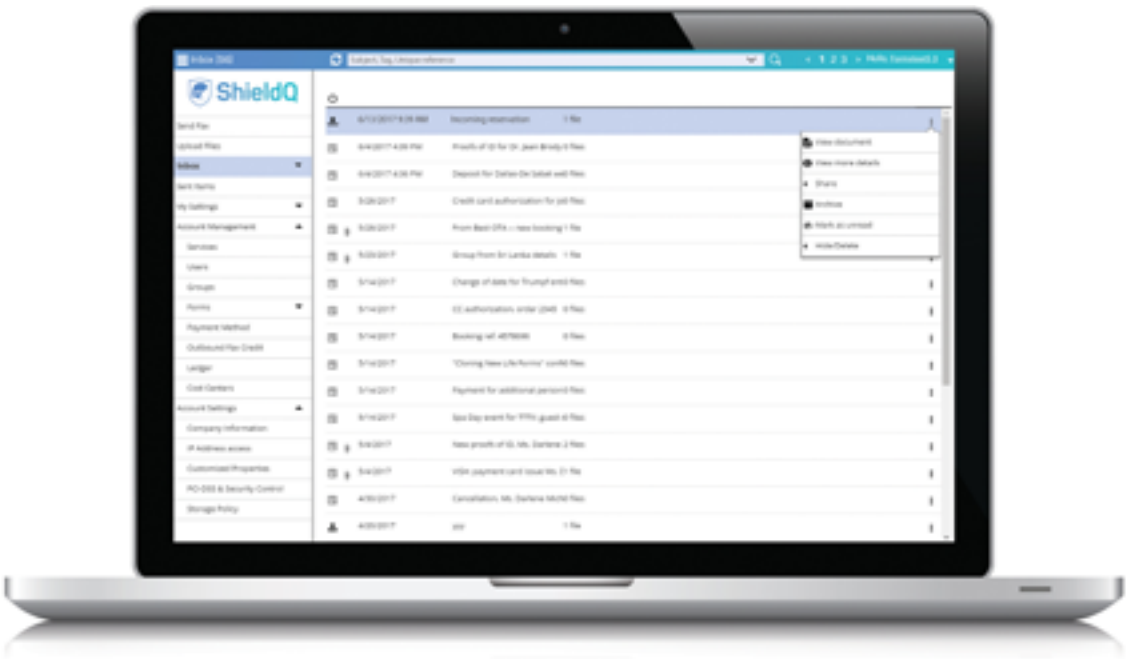
Third-party providers need to be compliant, too

Third-party service providers offer many, many services, such as orders and bookings to many organizations the world over. The question is, are organizations aware if these providers protect credit card or PII data? In the hotel industry, at least, it seems that there was no awareness till now.

Several hoteliers have discovered that most of their providers are non-compliant, and have for years been relying solely on self assessment – with no true understanding of what PCI DSS accreditation actually entails. Belatedly, many hotels are finally making sure that something's being done to correct the situation.

The reasons for this proactive approach is most likely a consequence of the latest version of the PCI-DSS standard, which delves into the relationship between service providers and their clients, demanding documentation that proves compliance. Drilling deeper, hotels have required that third-party providers sign a "Supplier Responsibility Matrix," where the two parties agree who takes responsibility for each element of PCI compliance, and whether their QSA's Attestation of Compliance *(AOC)* covers those areas of responsibility.

These requirements are certainly very demanding. But if you think about it logically, it all boils down to applying the same fundamental security principles to other sensitive data as well, like PII records, which have 10 times the value of a payment card record.



What needs securing

Faxes: alive and kicking

It may come as a surprise even to users, but ask a financial organization or a hotel how many faxes they receive daily, and the answer will largely be – very few, or even none at all. But that's not really true. Most grossly underestimate the number of faxes they receive. Financial and legal organizations need signed materials, and still insist on faxing, since these documents are recognized as legally binding, with their proofs of receipt. With hotels, people send in faxes for specific requests, like conference facilities or spa bookings, which cannot be made online, or send payment card authorization forms.

Thus, faxes seem here to stay for awhile. But handling them is a very manual process, requiring printing the fax, punching or masking the CVV number, filing in a binder, and storing it in a locked cabinet for long periods. Some organizations have a locked room dedicated exclusively to the fax machine and the storage cabinets.

Unsurprisingly, many faxes simply get lost, wasting hours of staff time to find them or recover data sent on them.

With so many data breach risks, both internal and external, it makes sense to make faxes PCI compliant also. One solution enables staff to capture and store the fax image in a centralized, PCI DSS level 1 queue. Employees access faxes using two-factor authentication. The solution also provides a full audit trail of who views a fax, and when. To further comply with PCI-DSS standards, the fax image is displayed in a browser, with no print or download allowed.

"Most grossly underestimate the number of faxes they receive. Financial and legal organizations need signed materials, and still insist on faxing, since these documents are recognized as legally binding, with their proofs of receipt."

Other PCI-inbound fax solutions functions are available, much like a PCI DSS document management system in the cloud, where one can share, forward, and tag documents.

Faxes can be renamed, assigned unique reference details *(date of client intake; check-in date),* then subsequently archived and easily retrieved. Such solutions – costing no more than a regular fax machine to maintain – are simple and fast to deploy.

"While some organizations set up email servers to filter inbound emails...in almost all cases, emails still remain in PCI scope."

Inbound payment card data in emails

Even though organizations warn clients not to send sensitive personal data via email, they still do. To prevent any data leakage issues, some have set up their email servers to filter inbound emails, so that they are quarantined or rejected outright.

While this measure does limit risk, in almost all cases emails still remain in PCI scope: the emails remain "at rest" within the system.

There are several network architectures that you can adopt to solve this issue:

1. Use your existing domain with content filtering: Apply legacy email filtering tools *(e.g., Symantec, Microsoft, Barracuda)* with existing email servers to automatically identify and route emails with sensitive data *(either in body copy or in attachments)* while still in motion, to a secure, accredited queue. This solution is simple and inexpensive to deploy. Upon arrival, they can be manually or automatically distributed to users.

2. Use a dedicated mailbox from an accredited inbound document service, which treats all incoming messages as secure, delivered to a unified queue over the TLS channel.

3. Use a new, branded domain for secure communication, which treats all incoming messages, as secure, delivered to an accredited, unified queue over the TLS channel. This option, however, incurs higher setup and account administration fees.

Similar to fax management, the authorized user would be required to login to view the email before being able to assign a unique ID, tag, rename, share, forward and archive the document.

Handwritten notes

Handwritten notes are standardly used at reception desks, jotting down missing information from forms *(payment card numbers, personal identity card numbers)*.

This data is held in binders, stored in back offices, where they can usually be accessed by many non-authorized staff. Clearly, this is not PCI-compliant, and should have been stopped long ago. Yet, this practice remains commonplace.

An effective, inexpensive solution lets forms, payment card authorization forms and even scraps of paper with sensitive data be stored permanently in a PCI-DSS level 1 environment. With such a secure inbound document management and storage service, organizations can scan or *(more conveniently)* photograph the document using a smartphone. The image is immediately uploaded through a secure, online document-capture form on the organization's webpage. The document is then forwarded instantly into a compliant, document management queue. Once safely in the queue, users can rename, share, tag and archive documents in exactly the same way as fax and email, described previously. Original documents can then be shredded, while the image is permanently deleted.

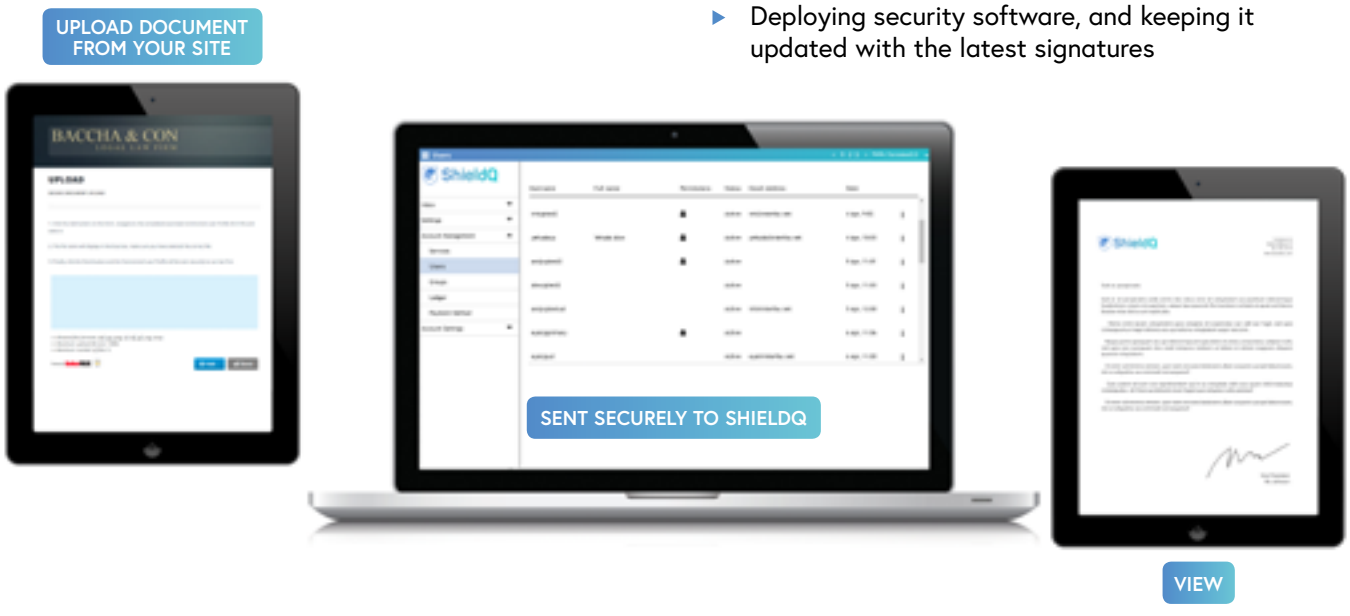
Organizations can also create multiple URLs using the online form. The service provides CSS capabilities, to enable you to custom-design and integrate each URL into the organization's website.

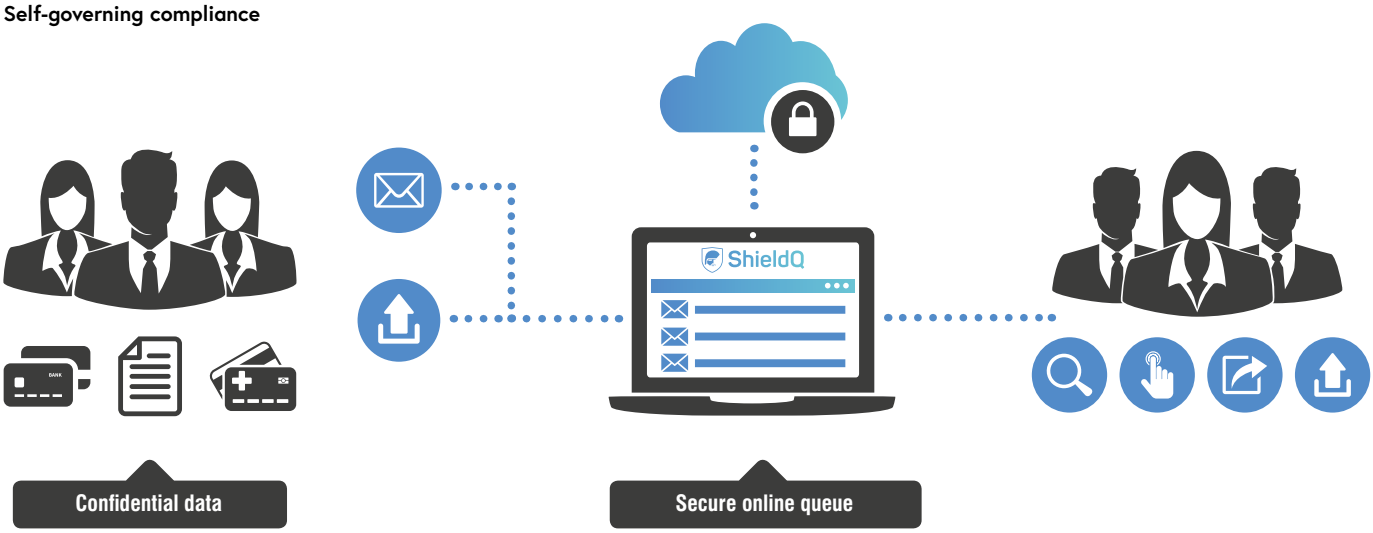
Last, but not least: POS

The primary cause of POS breaches appears very simple to fix, but is actually difficult: Many POS systems operate using unsupported Windows versions, which are easy, lucrative targets for cybercriminals. Malicious software like ALINA, vSkimmer, Dexter and FYSNA
target POS devices and are widely available in the cybercrime community.

For optimum PoS security, prevention should include *(but should not be limited to)* the following:

- Deploying the latest operating system on all PoS devices, with the latest patches
- Limiting access to the Internet
- Implementing hardware-based, point-to-point encryption
- Instituting an IP lockdown on POS terminals
- Auto-deleting payment cardholder data from terminals
- Employing PCI access control procedures to restrict PoS systems only to their intended uses
- Limiting internal access to physical POS devices
- Enforcing policies regarding POS physical repair and/or upgrade
- Deploying security software, and keeping it updated with the latest signatures





Network security measures should include:

- Maintaining regular checks to identify if devices have been tampered with or have been replaced with bogus devices
- Patching vulnerabilities, and monitor for changes in system components
- Ensuring that your organization is constantly protected against vulnerabilities in both systems and applications, even in-between patch cycles
- Protecting against malware and malicious URLs
- Encrypting communication between applications and data
- Restricting two-way communication to only what is required

What your compliance solution should do for you

In the absence of a specific technical standard for GDPR, PCI DSS requirements provide the ideal technical framework to meet the new European regulation's challenging demands. While lacking some of the procedural processes often found in such standards as ISO 27001, there is no question that from a technical standpoint, information security specialists say that there is no better commercial security standard to protect PII and payment data, than PCI DSS Level 1.

The tools used by any system will vary according to the organization workflow and size, but the endgame's the same: most leading commentators in this field agree that a PCI-compliant or GDPR-ready solution ought to offer:

- **A safe, secure environment:** Ensure that all payment data is stored in one, secure place for easy management and retrieval
- **Affordability:** The service needs to be cost-effective and scalable
- **Flexible, simple, quick deployment:** There should be minimal to no changes necessary to existing business processes, workflows and systems; deployment should be quick, minimizing internal resource requirements
- **Flexible storage policies:** Users ought to be able to define common storage and deletion policies, based on significant document attributes, such as dates.
- **Auditing:** The service should be fully compliant with the latest version of PCI DSS standards, with documented and contractual agreements clearly defining areas of responsibility between the organization and the provider.
- **Secure uploads:** Organizations like hotels or legal and financial institutions take payment data as security for advance reservations, or for forms, via their websites. Other organizations regularly request highly sensitive documents, such as passports, as proof of ID. All these organizations can provide a safe and secure method of delivering this data through an upload page on their own website.

Conclusion

It may seem daunting to overcome self-assessment complacency, to become 100% PCI compliant. But, now more than ever before, it is achievable, more easily than you can imagine. All the required tools are readily available at low cost, and are simple to implement – if you know where to look.

Yet, you still may have many questions. Contact us about any of the topics discussed in this document, and we'll do our best to answer as fully as possible.

ShieldQ

Global offices:

Interfax Communications Limited,
Unit 7, Coolport Coolmine Business Park,
Blanchardstown, Dublin 15, Ireland, D15 HC91

Phone: +353 1 905 8968
Email: sales@shieldq.com

US offices:

Interfax Communications US
7915 Westglen, Houston,
TX 77063, USA

Phone: 1 (713) 429 1217
Email: salesus@shieldq.com

www.shieldq.com