



**MEET  
SONAR**

# TABLE OF CONTENTS

About Us -----	4
Introduction -----	5
Billing -----	6
Financial Reporting -----	10
Customer Management and Support -----	12
Dispatch and Field Operations -----	14
Network Operations -----	19
Security and Compliance -----	23
-----	

At Sonar, we continuously seek new ways to offer our customers additional value and growth opportunities to expand their business,



Simon Westlake, CEO Sonar Software



2019 2020



The Startup 50 profiles the fastest-growing startups in the country. It is a companion list to the Growth 500 ranking of Canada's fastest growing companies which has, for over 30 years, been Canada's most respectable and influential ranking of entrepreneurial achievement.

2019 2020



Canada's Top Growing Companies is an annual program, produced by Report on Business, which ranks both public and private Canadian companies based on three-year revenue growth.

## ABOUT US

Sonar Software is a leading cloud-based provider of BSS & OSS solutions for Internet Service Providers. The platform offers a range of rich features that are mission-critical to the daily work of ISPs. Sonar is a scalable and fully integrated solution that helps service providers consolidate their data in one place for improved visibility, reduce dependency on multiple systems, and automate complex workflows for enhanced business efficiency and growth.

Sonar brings together some of the best minds and talents from across the industry. And we're far more than just software engineers. Our team also provides round-the-clock insight, guidance, and technical support for all our customers.

---

### Microsoft Airband Initiative

We believe that technology has the ability to empower and transform communities. To that end, Sonar has partnered with Microsoft to take part in its Airband Initiative. Together, we're helping to close the digital divide by bringing broadband access to millions of people in rural parts of the world.

# INTRODUCTION

As an organization operating in the time of Software-as-a-Service, you're presented with a plethora of customer management software and network management tools. Selecting the right tool, or combination of tools can frequently be frustrating and potentially overwhelming.

Sonar is designed to refine what might otherwise be multiple tools into a single, cloud-native, application. By combining billing automation, customer management, inventory lifecycle management, and networking overviews, Sonar is built to be a flexible, scalable, and robust one-stop software solution for your organization. Designed to make management easier across the board, Sonar provides a foundation for operational automation to help maximize profitability and growth in all of our partners. At Sonar, we take pride in being able to offer a solution built around the needs of our partners. We incorporate billing tools, financial tracking, Business Intelligence reporting, CRM tools, inventory tracking, and much more!

As services and applications continue to migrate to a cloud-based approach, you'll need a tool that keeps everything organized and can function as the center of your product suite through integrations, webhooks, and an advanced API powered by GraphQL.

## Flexible Billing **ENGINE**



No matter how many customers get added to your Sonar instance, and no matter how many different days need to be billed, Sonar is designed to automate customer invoicing, customer payments, and service charges in the background. By combining this automation with the flexibility to bill your way, Sonar offers a completely customizable and scalable solution for managing customer billing, invoices, and purchase orders.



# HOW SONAR MAKES IT **EASY**



Whether you're a large business with multiple Enterprise level customers or a mid-sized organization with thousands of relatively small customers, the billing process will typically follow a predictable pattern:

Establish a recurring or one-time service → Create an invoice → Receive payment for services rendered

While this flow is a simplification of what can traditionally expand into a much more complex system involving multiple payment methods and gateways, accounts receivable, tax reports, invoicing systems, and payment reminder notifications, it doesn't need to be a headache. Sonar is designed to automate billing in a scalable way, which means taking the complexity out of the equation. Sonar can also simplify invoice delivery with a native Print to Mail function built directly into your instance, which will automatically print customer invoices and send them as letter mail directly to their address.

Here are just some of the ways Sonar can make your life easier when it comes to managing billing and accounts.

# 1. SCALABLE BILLING PARAMETERS

A

Sonar lets you create default billing parameters that get applied to every account added to your instance as soon as they're created. This initial configuration needs to be performed once, and will automatically apply the parameters when a new account is created. Whether your customer signs up on the 1st of the month or the 11th, the default billing parameters will dynamically calculate the next bill date, next invoice date, and next payment date. In situations where the billing defaults don't apply, the billing settings can be overridden directly on the account on a case-by-case basis.

B

The same billing parameters that automatically apply on every account also have the flexibility to manage multi-month billing cycles or multi-month service plans on a monthly subscriber. Sonar gives your sales team the flexibility to build contracts that can expand upwards as far as you need them to. Not only can you see the flexibility with account configuration, but billing notifications are set up once and triggered automatically, with no manual involvement past the setup, no matter how long the billing cycle may be.

C

Sonar's default billing settings also control the addition of late fees - and the calculation that determines when an invoice becomes past due and when the late fees will apply to the customer's account. Account delinquency will then be handled automatically in Sonar, including service disconnections in the event of prolonged non-payment.

D

Beyond billing defaults, Sonar also provides flexible control over billing days, proration settings, and autopay settings. These billing settings even let you disable the automated daily billing in the event you use an external system to manage your organization's accounts. You can also define which days the system should check accounts for delinquency, minimum payment amounts, and autopay attempts.





## 2. Managing Payment Methods & Payment Processors

In addition to the flexibility provided by Sonar when it comes to your billing settings and defaults, we also allow you to fine-tune how you receive payments from your customers.

- A** By providing a large list of supported payment processors, Sonar provides the flexibility to integrate with the vendor that gives you the best odds of growing your business. Both bank account and credit card processors can be selected from a variety of payment gateways to make sure Sonar isn't restricting how you work.
- B** Along with the payment gateways, Sonar supports a number of payment methods. Whether your customers prefer to pay with their bank account, their credit card, cash, or check, Sonar allows you to record these payments directly on the customer account and apply them right to an invoice.
- C** As part of how Sonar integrates with the various payment gateways, customer payment information is never stored in your instance. Once the payment information is entered into the system, it becomes tokenized and encrypted with the payment gateway. Not only does this mean bad actors can't access your customer's payment information, but the information on the payment method can't be changed without removing and re-adding the payment method. When a transaction is sent from you to the payment gateway, all we receive is a confirmation code (or failure code).



3.

## FINANCIAL REPORTING

*Data is one of the most valuable resources on Earth. Understanding your data could be the key to unlocking potential growth, reducing areas of waste, and rapidly scaling your business*

With Sonar, you get built-in Financial reporting powered by Sonar's Business Intelligence. Sonar is packed to the brim with reports for you to use to keep your business on track, and a highly customizable view to make sure any report you need can be created to better serve your business.

Reports generated through Sonar's Business Intelligence can also be exported as a PDF or as CSV files for seamless integration into any accounting software used by your organization. This gives you more options, more accountability, and more resources to measure your financial success by any metric you choose. With Sonar, we even take it one step further – if you find that we're missing any reports we offer an extremely robust report generator built into your instance, and if that doesn't work, our support team can help you create custom ones to get you the information you're looking for.

## 4. FLEXIBLE TAXATION AND TAXATION INTEGRATIONS

Sonar gives you the tools to completely customize your taxation in Sonar. Whether you're creating global taxes or restricting taxes to specific geographical areas of your service coverage, the taxes module of Sonar affords you the flexibility to create and limit the taxes as you see fit. Taxation in Sonar can be restricted to specific States, Counties, or any combination of ZIP/Postal Code, Cities, States, and Counties.

This flexibility also extends to tax exemption on your customer accounts. Each customer can be made exempt from portions or entire taxes depending on the specific scenario.

Finally, Sonar also provides the option of using Avalara for taxation purposes in order to automate the creation and management of your global and geographically restricted taxes.

# CUSTOMER MANAGEMENT & SUPPORT ADVANTAGES

The billing module is only one of the many ways Sonar makes it easy to scale the way you do business. In this section, the tools and features that will let your Customer Service Representatives create, modify, track, and troubleshoot your customer accounts will be highlighted in order to explore how Sonar's dedication to integration and flexibility make it the ideal one-stop software for controlling the customer experience from start to finish.

Whether you're managing accounts or responding to tickets, the various dashboards and advanced filtering features will ensure each customer request can be handled promptly and efficiently.

## ACCOUNT CREATION & ADDRESS QUALIFICATION

1.


The account creation process is robust, yet simple. When an account is being created, you supply a name, address, and contact information for your customer. Additionally, Sonar provides the option of supplying additional information in the form of custom fields, which are freeform, dropdown, or text limited fields where your organization provides the topic to be filled out.

Meanwhile, address qualification in Sonar simplifies the process of retaining serviceable addresses. Any time an address is added to your instance, it's stored in perpetuity as a known serviceable address. This means IP address assignments, inventory assignments, and account assignment history is all stored directly on the serviceable address and can be referred back to as needed by your support or sales team. Every serviceable address is verified by the Google Maps API, and the associated latitude and longitude coordinates are automatically stored with the address for precise geo-location, no matter where in the world your customer is located.

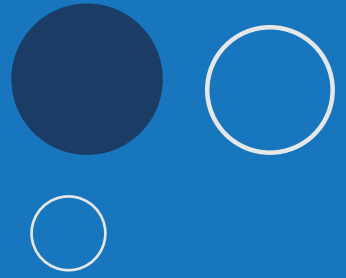
If you have any existing accounts from alternative sources, their information can be formatted to fit in Sonar and imported with all their history and information preserved. This means that for your customers, it'll be like nothing ever changed once their invoice is received.

## 2. ACCOUNT MANAGEMENT

Sonar brings the same simplicity to account management that was brought to account creation. Because Sonar is designed to be simple, we make it easy to manage services, packages, groups, and account relationships.

- 
- A** One of the key features of Sonar's account management is the ability to establish a parent account and a child account relationship between any two or more customer accounts in your Sonar instance. Any account can be either a Parent or a Child account and establishes a hierarchy of responsibility where the transactions of all linked child accounts will be combined into a single invoice on the parent account, simplifying both payment visibility and simplicity.
  - B** Service Management is made easy by providing you and your organization the ability to define every aspect of the service being added to the account. Each service is created by your team - from how often it bills, its price, and even the type of service. This means you can have recurring services, data services, expiring services, and pre-built packages, all on the same account. Discount services are just as easy to apply because Sonar gives you the option to select whether any created service should be applied as a debit, or as a credit. Services and packages added to accounts can also have their price, name, and description overridden on a case-by-case basis. This means that John Smith can have a tax-exempt \$100 service, while Jane Doe can have the same service set to bill \$5 a month.
  - C** Scheduled Events can also be used to manage account and service changes across your customer accounts. A few examples for scheduled events would be service plan changes, disconnections, holidays, or service upgrades. Setting these scheduled events is done from the account page, reducing the complexity and the number of clicks needed to set things up.
  - D** Account contacts can be removed and managed independently from the account itself. This means it's easy to update account ownership or primary contact changes. Customers can even make this change themselves by using the customer portal. With Sonar, you can even update mass email recipients fluidly by controlling the email types each contact should receive.

# 3. CALL LOGGING, TICKETING, AND TROUBLESHOOTING



With Sonar, the best elements of Customer Relationship Management software are brought together to create a unique, flexible experience for your organization. The CRM module in Sonar extends how you can communicate with your clients, how your clients communicate with you, and how all that information is stored within your instance and the customer account.

Tickets can be opened directly from an inbound email to any address configured within your Sonar instance, and through integration with Slack, notifications can be sent to the appropriate team as soon as a ticket comes in. Automatic replies can also be configured on a per email address basis, meaning that your replies from the sales address can be vastly different from the automatic reply sent when a ticket is received. Additionally, through the subscription system, multiple users can be notified any time a ticket reply comes in – especially useful for a new CSR coming in to learn the ropes. Another benefit of our ticketing system is mass notifications which can be customized to account groups, service plans, or even locations – useful for notifying your clients of upcoming maintenance or changes at an operational level. Or maybe you had an outage overnight which leads to numerous customer tickets the following morning, you can link all these customer tickets to a single internal ticket to track and document impact.

We also make basic troubleshooting easy with canned replies built right into our portal. Set variables, choose the groups, and enter in the message, canned replies give you the ability to address common questions when troubleshooting, provide accurate usage numbers to your clients, and make it easy to provide quotes and account information.

To round out the troubleshooting experience, each account can store call logs in addition to tickets. Each call log can then seamlessly be escalated into a ticket, and additional call logs can reference existing open tickets, and tying everything together is the ability to seamlessly link a job to an existing ticket, keeping the notes, truck roll, and customer interaction all in one place.

Troubleshooting can also make use of historical logging, as even if a call or ticket isn't logged upon an initial call, through the use of historical tracking the agent can see who last spoke with the customer (based on who opened the account) and gather details from them directly to ensure every customer interaction is as smooth and seamless as it can be.

# MANAGING YOUR INVENTORY CONSUMPTION & ORDERING

---

Managing Inventory items can be a tedious process as a result of the need to manage a wide selection of inventory models, items, and manufacturers. With Sonar, this process is simplified by letting your organization and warehouse teams control every aspect of inventory management. Whether you're adding new items or assigning them to your technicians, Sonar provides the ability to track not just hardware, but bulk equipment as well, with per-unit pricing and usability statuses. This means you can follow up on every piece of inventory in your system through every step of its lifecycle.

One of the main advantages offered by Sonar, and in turn an inventory system built by your organization, is the flexibility to enter data however it fits your mold. For example, adding a router designed for installation at the customer premises has you adding the manufacturer, creating the models, setting the various fields used for inventory tracking, the price of all items of the same inventory model (in the case of direct customer purchase), and its description. From there, it's a matter of creating assignees and locations for the organization, and your basic inventory sheet is ready to use. Assignees are also completely customizable, whether they're a warehouse, a field technician, or a specific shared vehicle, you can create assignees to suit any situation.

Beyond managing how inventory is created, Sonar offers an incredibly versatile inventory module, allowing you to search through your inventory in real-time with a set of simple filters and optional advanced filtering. The filters can also be combined to refine your results to make sure you're getting the details that you specifically want. No more frustrating inventory spreadsheets or audits - Sonar lets you find any inventory item with ease. And because every change is tracked in Sonar, your warehouse team will always know where each inventory item moved to, when it was moved down to the minute, and who moved it. This applies to your in-warehouse equipment and to equipment deployed to the customer premises (or in the process of being RMA'd), as every step of the process can be tracked within the inventory module.

Sonar also provides the ability to order more inventory from directly within your instance. Instead of needing to tie together multiple disparate systems, you can easily take a request for new inventory items from your warehouse team and send it to your preferred vendor through the Purchase Order module in Sonar. The entire purchase order process is customizable, you add the vendors, the vendor models, and even the vendor items. The prices can be based on existing wholesale rates you have with the vendor, and the purchase orders will automatically be emailed to the vendor's email address that you provide.

# DISPATCHERS & FIELD TECHNICIANS

Sonar is designed with internet service providers in mind, which means our software is designed to be seamlessly incorporated into your existing dispatcher workflow. Schedule availability, drive times, and vacation time can all be entered into the system and will be used to display which field technicians are available for which jobs. Add in geofencing, an expansive mapping module, and various views and filters for the scheduling module, and you might start to see how Sonar can make it easy for your dispatchers. But it doesn't stop there - Sonar also has a free mobile app, available on Android and iOS, which links back to your instance and allows your field technicians to submit account changes - even when they're offline.

## MAPPING MODULE & GEOFENCING

1.

The mapping module in Sonar provides an overview of your serviceable area by displaying your network sites and customer accounts in a visual interface. The map allows you to filter what you see on a variety of levels. Whether you're looking for accounts within a specific location with the lasso tool or wanting to exclude specific results, such as inventory locations or network sites, the mapping module facilitates that.

Similarly, part of the robust mapping module is the ability to create a Geofence for your field technicians. This allows you to restrict your field operations to specific geographical service areas. Each geofence can be created to span any desired area, and multiple geofences can be nested within existing zones. With geofences, you can ensure that service zones requiring certain training or certifications can only be serviced by technicians that meet those requirements. Additionally, if you service multiple counties or states and have technicians residing within a short distance of each of those locations, geofences let you strategically dispatch technicians by creating geofences that determine a maximum service range.



## 2. JOB SCHEDULING & TRUCK ROLLS

On the topic of field technicians, the scheduling module in Sonar combines numerous features to simplify the truck roll experience for your organization and your customers.

A

**Job Types** - In Sonar, every dispatch job is made as a specific type of job, and the creation of each type is made to be as flexible as possible for your organization. Each job type is named, given a default length, and what actions should be automated upon completion of the job, whether the job was failed or completed successfully.

Task templates can also be assigned to any job type, which will be a list of actions that the field technician will need to complete before the job can be considered complete.

B

**The Scheduling Module** - The scheduling module presents two functionally similar views for scheduling your technicians. The first is the job list, which displays every job in your instance through the use of filters. This view provides some unique information, such as how long a technician has been active on a job, or the current job status.

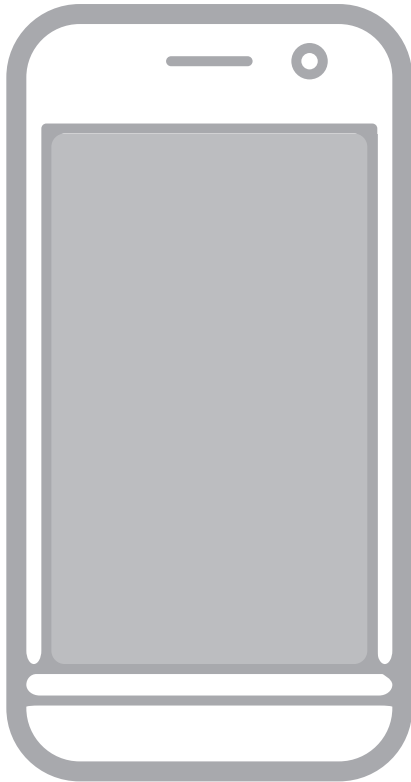
The second view is the dispatcher view. While there are several ways to schedule a job using Sonar, the dispatcher view provides a visual interface for scheduling jobs, meaning a simpler, more accessible interaction with the software. All technicians will be listed initially, and when a job is selected and brought onto the calendar, unavailable or invalid field technicians will be grayed out. The dispatcher view will also dynamically display the calculated drive time between each job to better inform the day's job schedule.

Further, multiple technicians can be scheduled on the same job as required. Each job booking gives you the option to select multiple technicians and only show times where both technicians are available. This allows you the flexibility to dispatch as many or as few technicians as needed and make sure that the correct technicians are going out.

C

**Schedule Availability & Pre-Set Scheduling** - With a basic understanding of the scheduling module, the next step is understanding how your field technicians fit into the schedule. This is done in two stages. The first is setting the overall availability for your field technicians through the use of Schedule Availability in Sonar. This setting module allows you to define which technicians are available in certain time frames, and what jobs those technicians can be dispatched to.

# 3. SONAR FIELD TECH MOBILE APP



## No Service. No problem!

Use the app in online or offline mode; account changes automatically sync when the connection is restored. Access critical information and tools when offline to avoid any delays in successful job completion.

## On the go data capture

Upload documents, photos and quickly add notes to the account, complete the job with e signatures using built-in digital contracts.

## Eliminate human error & callbacks

Customizable task lists ensure that your field techs get the job done, whether it's a residential or business service call. Improve the customer experience and say goodbye to unnecessary paperwork and duplicate data entry.

## Arrive on time, Every time!

See a complete overview of your jobs scheduled for the day and use the GPS route guidance to arrive on time and make a great first impression. Save time and avoid unnecessary setbacks with our built-in navigation.



A well-documented install leads to fewer callbacks and simple troubleshooting if issues arise in the future.

## EMPOWER YOUR FIELD TECHNICIANS

The Field Tech Mobile App was designed with mobile devices in mind rather than simply providing a mobile interface for the web UI, simplifies the field technician's communication back to your Sonar instance while they're out in the field. Whether they're simply replacing equipment, troubleshooting network issues, or taking payments from the customer, the mobile app will facilitate that.

While the mobile app does provide a more limited set of actions when compared to the full web interface, there are several advantages. The first is a more focused view for your field technicians - they'll see the day's schedule, have access to the customer's account, seamlessly access driving directions, and be able to queue offline actions when the technician has no service.

# USING SONAR TO MANAGE & PROVISION YOUR NETWORK

Because Sonar was and is designed by a development team filled with experience in the Internet Service Provider business space, it can do a lot more than just billing. One of the ways Sonar makes it easy for you is by including several tools and features to make your job easier when it comes to managing your organization's internal and customer-facing network infrastructure. From incorporating billing for data and voice services in a flexible way to providing a dynamic network map, Sonar provides tools to control your network – your way.

# 1.

## NETWORK TOOLS

### NETWORK SITES

A

Network sites are a way to monitor and track the originating point for your services in Sonar. Whether you're a Wireless Internet Service Provider or a more traditional ISP, a network site will always be useful.

Network sites have inventory linked to them, IP address pools assigned to them, and customer provisioning can be traced back to the equipment on the network site. Additionally, network sites are used to establish a network map based on connected devices and backhauls, which in turn is used to create a network map in Pulse.

### PULSE MAPPING

B

Using the connected devices linked to each of your network sites and the IP addresses assigned to them, Sonar creates a dynamically generated, constantly updating network map right in your instance. It can be viewed from any network site, exported as an image, and filtered for a more precise view of your network. This map will show connected devices, the backhauls connecting each network site, and connection endpoints, all in a single view.

While Pulse may not be as detailed or as expansive as a true network map you might create, it nonetheless provides a valuable tool in your arsenal while troubleshooting network issues in your instance.

### DYNAMIC NETWORK MONITORING

C

One of the additional advantages of mapping your network with Pulse is Sonar's ability to then continuously monitor the devices added to your network sites for any issues. Using a tool built by Sonar called a "Poller", each of your devices will be contacted through SNMP and ICMP to confirm their status and uptime. Any issues found with your devices will then be displayed on the network dashboard, and further details can be gathered by reviewing the monitoring history of each device.

# 2.

## PROVISIONING TOOLS

### A

#### INLINE DEVICES, RADIUS, DHCP, & INCOGNITO

Sonar is designed around simplicity, and to make things easier for your network team and your organization, we offer a variety of methods to provision your customers with data services and IP addresses.

Whether you prefer to use all MikroTiks on your network or have a mix of devices, Sonar's robust provisioning integrations will help automate getting your customers online. Each integration has a similar setup process, each as straightforward as the other. Your organization can even mix and match different provisioning technologies to make sure you're delivering the best possible service to your customers no matter what they subscribe to. The array of built-in methods mean that wireless customers, cable customers, and fiber customers can all be connected and monitored using Sonar alone.

### B

#### WEBHOOKS & API

While Sonar strives to provide a native integration experience that meets all your networking needs, the GraphQL API in combination with a very long list of webhook endpoints means that nearly any networking tool, provisioning tool, or 3rd-party integration can be connected to your Sonar instance.

With the GraphQL API, your instance becomes completely transparent. There are very few limits on what can be accessed, and the same is true for the webhook endpoints. If you can modify it using the API, there will likely be an endpoint to trigger action on the same item.

This means device provisioning and IP address assignments aren't limited to the native integrations but can be automated outside Sonar, while the actions take place in Sonar without your intervention.

# 3.

## DATA & VOICE SERVICES

For Data billing, the data service is created with the download and upload speed, limits, and overage charges in the event of a bandwidth limit. The data itself is tracked through your own network devices and sent through to Sonar for easy viewing by your team and by your end-user.

Voice billing is flexible as well, allowing you to determine the number of minutes, local or long-distance, allowed to each service bracket, as well as define the classification of local numbers for that service. Additionally, the DID assigned to the customer is shown on the invoice, and if multiple DIDs are assigned then each DID will appear on the invoice as a unique line item.

# SECURITY & COMPLIANCE

## SONAR AND GENERAL DATA PROTECTION REGULATION

---

### **Security in the Cloud**

Sonar has implemented technical security and privacy protection solutions offered by Microsoft Azure to maintain the confidentiality, integrity, availability, and privacy of client data stored in the cloud.

Our Cloud Service Provider (Microsoft Azure) platforms meet a broad set of international and industry-specific compliance standards, such as the General Data Protection Regulation (GDPR), ISO 27001, HIPAA, FedRAMP, SOC 1, and SOC 2. Rigorous third-party audits verify their adherence to the strict security controls these standards mandate. Refer to Microsoft Service Trust Portal which has a listing of all their Audit Certifications.

### **Data Security - Industry Standard Encryption and Secure Connections**

Sonar's data is transmitted to and from our servers over HTTPS and is encrypted in transit (TLS 1.2 and above for data in transmission) and using AES 256-bit encryption for protecting data at rest. All communications use SSL encryption, and our data is stored in SOC 1 Type II, SOC 2 Type I, and ISO 27001 certified Cloud Data Centers.

### **Network Security - Intrusion Detection and Prevention**

Our networks are protected by Microsoft Azure firewalls configured to follow industry best practices for network ingress/egress security. The firewall is configured for Extended Detection and Response (XDR) monitoring of security vulnerabilities and threats to protect against malware, brute-force attacks, SQL injections, Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, worms, and botnets.

Azure Network Security Groups (NSGs) are used to control both inbound and outbound traffic to our cloud Virtual Network. NSG's are used to filter traffic at the network layer by using security rules to allow or deny traffic based on 5-tuple information: protocol (TCP, UDP, ICMP), source (IP address), source port, destination, and destination port.

Sonar has established detailed operating procedures, security policies, processes and security tools designed to: ensure the safety of all Sonar employees, suppliers, partners and customers; control the quality of, and maintain the integrity of, all Sonar information systems and services; and provide continuous availability and optimized performance.

# SECURITY & COMPLIANCE SONAR AND GENERAL DATA PROTECTION REGULATION

---

## Data Governance

Sonar understands the Cloud Shared Responsibility Model and its ownership of data as it relates to Cloud Services subscribed to using Microsoft Azure. Sonar has achieved CyberSecure Canada certification, and is actively working towards ISO 27001 certification. Our commitment to data privacy and security are centered around protecting the confidentiality, integrity, privacy, availability and security of data, to prevent and detect external threats by disclosing our rights and obligations in our Privacy Policy which is aligned with GDPR (General Data Protection Regulation) requirements.

## European Data Transfer

The European Commission has the power to determine, on the basis of article 45 of Regulation (EU) 2016/679 whether a country outside the EU offers an adequate level of data protection.

In 2001, the EU recognized Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) as providing adequate protection.

Canada's adequacy status ensures that personal data can flow from the EU to Canada without any further safeguard being necessary.

Microsoft has long used the Standard Contractual Clauses as a basis for transfer of data for its enterprise online services. The Standard Contractual Clauses are standard terms provided by the European Commission that can be used to transfer data outside the European Economic Area in a compliant manner. Microsoft has incorporated the Standard Contractual Clauses into all of their Volume Licensing agreements. For personal data from the European Economic Area, Switzerland, and the United Kingdom, Microsoft ensures that transfers of personal data to a third country or an international organization are subject to appropriate safeguards as described in Article 46 of the GDPR.

Canada's adequacy determination in Commission Decision 2002/2/EC has been attached for reference.



# CANADA'S ADEQUACY DETERMINATION IN COMMISSION DECISION 2002/2/EC

4.1.2002

EN

Official Journal of the European Communities

L 2/13

## COMMISSION DECISION

of 20 December 2001

**pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act**

(notified under document number C(2001) 4539)

(2002/2/EC)

THE COMMISSION OF THE EUROPEAN COMMUNITIES,

Having regard to the Treaty establishing the European Community,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data <sup>(1)</sup>, and in particular Article 25(6) thereof,

Whereas:

- (1) Pursuant to Directive 95/46/EC Member States are required to provide that the transfer of personal data to a third country may take place only if the third country in question ensures an adequate level of protection and if the Member States' laws implementing other provisions of the Directive are complied with prior to the transfer.
- (2) The Commission may find that a third country ensures an adequate level of protection. In that case, personal data may be transferred from the Member States without additional guarantees being necessary.
- (3) Pursuant to Directive 95/46/EC the level of data protection should be assessed in the light of all the circumstances surrounding a data transfer operation or a set of data transfer operations, and in respect of given conditions. The Working Party on Protection of Individuals with regard to the processing of Personal Data established under Article 29 of Directive 95/46/EC has issued guidance on the making of such assessments <sup>(2)</sup>.
- (4) Given the different approaches to data protection in third countries, the adequacy assessment should be carried out and any decision based on Article 25(6) of Directive 95/46/EC should be made and enforced in a way that does not arbitrarily or unjustifiably discriminate against or between third countries where like conditions prevail nor constitute a disguised barrier to trade, regard being had to the Community's present international commitments.
- (5) The Canadian Personal Information Protection and Electronic Documents Act ('the Canadian Act') of 13 April 2000 <sup>(3)</sup> applies to private sector organisations that collect, use or disclose personal information in the course of commercial activities. It enters into force in three stages:

As from 1 January 2001, the Canadian Act applies to the personal information, other than personal health information, that an organisation, which is a federal work, undertaking or business, collects, uses or discloses in the course of commercial activity. These organisations are found in sectors such as airlines, banking, broadcasting, inter-provincial transportation and telecommunication. The Canadian Act also applies to all organisations that disclose personal information for consideration outside a province or outside Canada and to employee data relating to an employee in a federal work, undertaking or business.

<sup>(1)</sup> OJ L 281, 23.11.1995, p. 31.

<sup>(2)</sup> WP 12 : Transfers of personal data to third countries : applying Articles 25 and 26 of the EU data protection directive, adopted by the Working Party on 24 July 1998, available at [http://europa.eu.int/comm/internal\\_market/en/media/dataprot/wpdocs/wpdocs\\_98.htm](http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wpdocs_98.htm)

<sup>(3)</sup> Electronically published (paper and web) versions of the Act are available at [http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6\\_4/C-6\\_cover-E.html](http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/C-6_cover-E.html) and [http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6\\_4/C-6\\_cover-F.html](http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/C-6_cover-F.html). Printed versions are available at Public Works and Government Services Canada — Publishing, Ottawa, Canada K1A 0S9.

# CANADA'S ADEQUACY DETERMINATION IN COMMISSION DECISION 2002/2/EC

From 1 January 2002, the Canadian Act will apply to personal health information for the organisations and activities already covered in the first stage.

As from 1 January 2004, the Canadian Act will extend to every organisation that collects, uses or discloses personal information in the course of a commercial activity, whether or not the organisation is a federally regulated business. The Canadian Act does not apply to organisations to which the Federal Privacy Act applies or that are regulated by the public sector at a provincial level, nor to non-profit organisations and charitable activities unless they are of a commercial nature. Similarly it does not cover employment data used for non-commercial purposes other than that relating to employees in the federally regulated private sector. The Canadian Federal Privacy Commissioner may provide further information on such cases.

- (6) To respect the right of the provinces to legislate in their fields of jurisdiction, the Act provides that upon the passage of substantially similar provincial laws, an exemption may be granted to organisations or activities that will then be covered by the provincial privacy legislation. Section 26(2) of the Personal Information Protection and Electronic Documents Act gives the federal cabinet the power, 'if satisfied that legislation of a province that is substantially similar to this Part applies to an organisation, a class of organisations, an activity or a class of activities, to exempt the organisation, activity or class from the application of this Part in respect of the collection, use or disclosure of personal information that occurs within that province'. The Governor in Council (Canadian federal cabinet) makes exemptions for substantially similar legislation by way of Order-in-Council.
- (7) Where and whenever a province adopts legislation that is substantially similar, the organisations, classes of organisations or activities covered will be exempted from the application of the federal law for intra-provincial transactions; the federal law will continue to apply to all interprovincial and international collections, uses and disclosures of personal information as well as in all instances where provinces have not created substantially similar legislation in whole or in part.
- (8) Canada formally adhered to the 1980 OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data on June 29, 1984. Canada was among the countries that supported the United Nations Guidelines Concerning Computerized Personal Data Files which were adopted by the General Assembly on 14 December 1990.
- (9) The Canadian Act covers all the basic principles necessary for an adequate level of protection for natural persons, even if exceptions and limitations are also provided for in order to safeguard important public interests and to recognise certain information which exists in the public domain. The application of these standards is guaranteed by judicial remedy and by independent supervision carried out by the authorities, such as the Federal Privacy Commissioner invested with powers of investigation and intervention. Furthermore, the provisions of Canadian law regarding civil liability apply in the event of unlawful processing which is prejudicial to the persons concerned.
- (10) In the interest of transparency and in order to safeguard the ability of the competent authorities in the Member States to ensure the protection of individuals as regards the processing of their personal data, it is necessary to specify in this Decision the exceptional circumstances in which the suspension of specific data flows may be justified, notwithstanding the finding of adequate protection.
- (11) The Working Party on Protection of Individuals with regard to the processing of Personal Data established under Article 29 of Directive 95/46/EC has delivered an opinion on the level of protection provided by the Canadian Act, which have been taken into account in the preparation of this Decision <sup>(1)</sup>.

<sup>(1)</sup> Opinion 2/2001 on the adequacy of the Canadian Personal Information and Electronic Documents Act — WP 39 of 26 January 2001 available at [http://europa.eu.int/comm/internal\\_market/en/media/dataprot/wpdocs/index.htm](http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm)

# CANADA'S ADEQUACY DETERMINATION IN COMMISSION DECISION 2002/2/EC

4.1.2002

EN

Official Journal of the European Communities

L 2/15

- (12) The measures provided for in this Decision are in accordance with the opinion of the Committee established under Article 31 of Directive 95/46/EC,

HAS ADOPTED THIS DECISION:

## Article 1

For the purposes of Article 25(2) of Directive 95/46/EC, Canada is considered as providing an adequate level of protection for personal data transferred from the Community to recipients subject to the Personal Information Protection and Electronic Documents Act (the Canadian Act).

## Article 2

This Decision concerns only the adequacy of protection provided in Canada by the Canadian Act with a view to meeting the requirements of Article 25(1) of Directive 95/46/EC and does not affect other conditions or restrictions implementing other provisions of that Directive that pertain to the processing of personal data within the Member States.

## Article 3

1. Without prejudice to their powers to take action to ensure compliance with national provisions adopted pursuant to provisions other than Article 25 of Directive 95/46/EC, the competent authorities in Member States may exercise their existing powers to suspend data flows to a recipient in Canada whose activities fall under the scope of the Canadian Act in order to protect individuals with regard to the processing of their personal data in cases where:

- (a) a competent Canadian authority has determined that the recipient is in breach of the applicable standards of protection; or
- (b) there is a substantial likelihood that the standards of protection are being infringed; there are reasonable grounds for believing that the competent Canadian authority is not taking or will not take adequate and timely steps to settle the case at issue; the continuing transfer would create an imminent risk of grave harm to data subjects and the competent authorities in the Member State have made reasonable efforts in the circumstances to provide the party responsible for processing established in Canada with notice and an opportunity to respond.

The suspension shall cease as soon as the standards of protection are assured and the competent authority concerned in the Community is notified thereof.

2. Member States shall inform the Commission without delay when measures are adopted on the basis of paragraph 1.

3. The Member States and the Commission shall also inform each other of cases where the action of bodies responsible for ensuring compliance with the standards of protection in Canada fails to secure such compliance.

4. If the information collected under paragraphs 1, 2 and 3 provides evidence that any body responsible for ensuring compliance with the standards of protection in Canada is not effectively fulfilling its role, the Commission shall inform the competent Canadian authority and, if necessary, present draft measures in accordance with the procedure referred to in Article 31(2) of Directive 95/46/EC with a view to repealing or suspending this Decision or limiting its scope.

# CANADA'S ADEQUACY DETERMINATION IN COMMISSION DECISION 2002/2/EC

---

## *Article 4*

1. This Decision may be amended at any time in the light of experience with its functioning or of changes in Canadian legislation, including measures recognising that a Canadian province has substantially similar legislation. The Commission shall evaluate the functioning of this Decision on the basis of available information, three years after its notification to the Member States and report any pertinent findings to the Committee established under Article 31 of Directive 95/46/EC, including any evidence that could affect the finding in Article 1 of this Decision that protection in Canada is adequate within the meaning of Article 25 of Directive 95/46/EC and any evidence that this Decision is being implemented in a discriminatory way.
2. The Commission shall, if necessary, present draft measures in accordance with the procedure referred to in Article 31(2) of Directive 95/46/EC.

## *Article 5*

Member States shall take all the measures necessary to comply with this Decision at the latest at the end of a period of 90 days from the date of its notification to the Member States.

## *Article 6*

This Decision is addressed to the Member States.

Done at Brussels, 20 December 2001.

*For the Commission*  
Frederik BOLKESTEIN  
*Member of the Commission*

# SONAR'S TECHNICAL SECURITY OVERVIEW

---

## 1.0 Purpose

This document has been compiled to provide clients and partners with an overview of Sonar Software's security-related technologies, policies, and best practices by addressing many of the most common questions and areas of importance to our valued business partners.

The information in this document is to be considered highly confidential and may only be distributed with permissions within the implementing organization.

If you require any additional information please reach out to your Sonar contact and they will initiate the internal request immediately.

## 2.0 Information Security

### 2.1 Cloud Security

Sonar leverages the power and security of Microsoft Azure, DigitalOcean, and Amazon Web Services (AWS) to keep client data secure, confidential, and private in the cloud.

Microsoft Azure Cloud Infrastructure Certifications: ISO 9001, ISO 27001, ISO 27017, ISO 27018, ISO 20000-1, ISO 22301, SOC 1-3, CSA STAR.

DigitalOcean Cloud Infrastructure Certifications: ISO 9001, ISO 27001, ISO 14001, ISO 50001, ISO 22301, SOC 1-3, CSA STAR, PCI-DSS.

AWS Cloud Infrastructure Certifications: ISO 9001, ISO 27001, ISO 27017, ISO 27018, SOC 1-3, FedRAMP & FIPS.

Laws, Regulations & Privacy: PIPEDA, CISPE, FERPA, HIPAA, ITAR & EU DPD.

Alignments/Frameworks: CIS, CJIS, CSA, FISC, FISMA, ICREA, NIST & EU-US Privacy Shield.

All Data Centers maintain SSAE-16 attestation in conjunction with their auditor. SSAE-16 attestation is based on an in-depth series of documented controls covering the operational management of the Data Center Hosting infrastructure.

For more details, visit:

**Microsoft Azure** <https://servicetrust.microsoft.com>

**DigitalOcean** <https://www.digitalocean.com/trust/certification-reports/>

**Amazon Web Services (AWS)** <https://aws.amazon.com/artifact/>

# SONAR'S TECHNICAL SECURITY OVERVIEW

---

## 2.2 Network Security

1. Network Security Group controlled access to our private VNets.
2. Extended Detection and Response (XDR) monitoring of security vulnerabilities and threats.
3. Intrusion detection and prevention systems to protect against malware threats, brute-force attacks, SQL injections, Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, worms, and botnets.
4. Operating procedures, security policies, and processes ensuring the safety of all Sonar employees, suppliers, partners and customers.
5. Operating procedures, security policies, and processes controlling the quality of, and maintaining the integrity of, all Sonar information systems and services.
6. Monitoring systems providing continuous availability and optimized performance.
7. VPN Administration of all servers.
8. Centralized logs for all services.
9. Audit logs of all environmental changes.

## 2.3 Data Security

1. Data is transmitted to and from our servers over HTTPS and is encrypted in transit (TLS) using 256 bit AES (or higher) encryption.
2. Data is stored and encrypted at rest using AES 256-bit encryption.
3. All communications use SSL (Secure Sockets Layer) encryption and all data is stored in SOC 1 Type II, SOC 2 Type I, and ISO 27001 certified data centers.
4. Tokenization of sensitive client payment data.
5. Geographic Data residency options are available.

## 2.4 Physical Security

Sonar applications are hosted on Microsoft Azure, DigitalOcean, and Amazon Web Services, in state-of-the-art regional data centers, designed to protect mission-critical systems with fully redundant subsystems and compartmentalized security zones. Our cloud data centers adhere to the strictest physical security measures including, but not limited to, the following:

1. Multiple layers of authentication for server area access
2. Two-factor biometric authentication for critical areas
3. Camera surveillance systems at key internal and external entry points
4. 24/7 monitoring by security personnel
5. All physical access to the data centers is highly restricted and stringently regulated

## 2.5 User Controls

Access to Sonar sessions is under the control of Super Administrators. Sonar Super Administrators are assigned by the customer for each Sonar instance with module-based user roles, and granular-access permissions.

# SONAR'S TECHNICAL SECURITY OVERVIEW

---

## 3.0 Application Security

### 3.1 Application Environment

Code check-ins that are peer reviewed

Enforced password complexity rules and restrictions on re-use

Session access control to restrict access to session data

Session timeout policy in place and enforced

Server OS Hardening and Configuration Management

HTTP Security Headers

XSS-Protection

X-Frame-Options

HTTP Strict Transport Security

Cache-Control

X-Content-Type

Content-Security-Policy

### 3.2 Penetration Testing

Sonar completes penetration testing every 4 months to check for exploitable vulnerabilities, to ensure the integrity of our online defences.

## 4.0 Technology Governance

### 4.1 Compliance

Sonar is actively working towards both ISO 27001 and ISO 27003 certification. The assessment phase has been completed, and we expect to have ISO 27001 and ISO 27003 certification in 2022. Sonar's commitment to privacy and security are centered around protecting your data, preventing external threats, empowering your individual rights, and the transparency enumerated by the GDPR (General Data Protection Regulation). Sonar's cloud service platforms meet a broad set of international and industry-specific compliance standards, such as the General Data Protection Regulation (GDPR), ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2. Rigorous third-party audits verify their adherence to the strict security controls these standards mandate.

# SONAR'S TECHNICAL SECURITY OVERVIEW

---

## 4.2 Privacy Practices

Sonar has implemented a Privacy Management Program aligned with global privacy requirements, including Canada's Personal Information Privacy and Electronic Documents Act (PIPEDA), the California Consumer Privacy Act (CCPA), the California Privacy Rights Act (CPRA), the General Data Protection Regulation (GDPR) in the UK and Europe, and PCI DSS in the United States. As a certified organization, we have also covered all of the Canada Cyber Secure Requirements pertaining to privacy in our Privacy Management Program.

We utilize leading-edge tokenization as our encryption method to ensure the highest level of security in transferring sensitive data. We have stringent requirements and processes to follow when choosing our data-storage providers, listed above, who must maintain the highest level of compliance with privacy legislation. We do not collaborate with third-party payment-process providers who are not PCI-DSS compliant.

## 4.3 Operational Management & Access

Sonar may require access to customer data when dealing with support requests. When this is required, the Sonar customer support agent will request access from the customer Administrator, who will then grant the access and be responsible for removing it when the support request is completed.

Like most online services, we have a small number of employees who must be able to access user data for the reasons stated in our privacy policy. We have strict policy and technical access controls that prohibit employee access except in these circumstances.



# SONAR'S SECURITY STRATEGIES

---

## Security is a Top Priority

At Sonar, trust is woven into the fabric of everything we do. We're driven to build and provide a platform for our ISPs that also keeps their data safe and private. We deploy industry-leading safeguards, and continuously monitor our systems, so our customers can rest easy knowing their data is protected 24/7 in the cloud.

## Security in the Cloud

Sonar leverages the power and security of Microsoft Azure, DigitalOcean, and Amazon Web Services to keep client data secure, confidential, and private in the cloud.

Our cloud service platforms meet a broad set of international and industry-specific compliance standards, such as the General Data Protection Regulation (GDPR), ISO 27001, HIPAA, FedRAMP, SOC 1, and SOC 2. Rigorous third-party audits verify their adherence to the strict security controls these standards mandate.

Data is stored in state-of-the-art regional data centers, designed to protect mission-critical systems with fully redundant subsystems and compartmentalized security zones. Our cloud data centers adhere to the strictest physical security measures including multiple layers of authentication for server area access, two-factor biometric authentication for critical areas, camera surveillance systems at key internal and external entry points, and 24/7 monitoring by dedicated security personnel.

## Data Security - Industry Standard Encryption and Secure Connections

Sonar's data is transmitted to and from our servers over HTTPS and is encrypted in transit (TLS) using AES 256-bit encryption. At rest, our data is stored and encrypted using AES 256-bit encryption. All communications use SSL encryption, and our data is stored in SOC 1 Type II, SOC 2 Type I, and ISO 27001 certified data centers.

## Network Security - Intrusion Detection and Prevention

Our networks are protected by firewalls configured to follow industry best practices for network ingress/egress security. Extended Detection and Response (XDR) monitoring of security vulnerabilities and threats protects against malware, brute-force attacks, SQL injections, Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, worms, and botnets.

Sonar has established detailed operating procedures, security policies, and processes designed to: ensure the safety of all Sonar employees, suppliers, partners, and customers; control the quality of, and maintain the integrity of, all Sonar information systems and services; and provide continuous availability and optimized performance.

# SONAR'S SECURITY STRATEGIES

---

## **Our Shared Security Partnership**

Because Sonar connects to technology that you are responsible for maintaining, security becomes a shared responsibility between Sonar and you.

## **Application Data Shared by Looker**

Sonar utilizes a number of first and third-party tools in order to provide and improve the service.

**Product usage** - A third-party service (Pendo) that gathers data to help us understand customer usage, where our customers perceive the most value, and what areas drive the most impact. This data is analyzed and used to improve the Sonar product.

**Configuration backups** - A Sonar service that encrypts backups of system configurations, encrypted user and database credentials, and Sonar user settings. For redundancy, configuration backups are stored in multiple cloud providers.

**System error reports** - A Sonar service that transmits runtime exceptions to Sonar internal systems in order for our technicians to diagnose issues with the product.

**Support access** - A Sonar service that allows Sonar technicians to troubleshoot problems by permitting authentication into a customer's Sonar instance.

**Email notifications** - A Sonar service that transmits emails in order to provide new account welcome emails, forgotten password reset links, etc.

**In-app guides and in-product messaging** - A third-party service (Pendo) that delivers personalized messages to users to help them more easily use the Sonar product. This service collects basic pseudonymized usage data in order to personalize messages and guides.

# SONAR'S SECURITY STRATEGIES

---

## Sonar's Responsibilities

Cloud security - Sonar uses major, well-established, cloud hosting providers to reinforce our security program with additional security and availability operational controls.

Product security - Sonar is responsible for ensuring that the code quality for our application is developed according to industry-wide best practices for software development, and is regularly tested for vulnerabilities.

Corporate security - Sonar is responsible for educating and disseminating security best practices throughout the organization, and ensuring that our applications, systems, and networks are securely configured and monitored.

## Your Responsibilities

### Cloud Security

You are responsible for configuring secure access between the Sonar application and your database. Sonar can provide recommendations on how to:

- Enabling secure database access using tools like IP whitelisting, SSL/TLS encryption, and SSH tunneling

- Setting up the most locked-down database account permissions for your instance

### Product security

You are also responsible for controlling access and permissions for users of your Sonar instance within your company. Sonar recommends:

- Setting up user authentication using either a native username/password option

- Setting up the most restrictive user permissions and content access that still allow people to carry out their work, paying special attention to who has admin privileges

- Setting up any API usage in a secure way

# SONAR'S SECURITY STRATEGIES

---

## Cloud Security Architecture

Sonar leverages the power and security of Microsoft Azure, DigitalOcean, and Amazon Web Services to keep client data secure, confidential, and private in the cloud. Sonar customers also have the added advantage of Sonar's own security best practices. In addition, Sonar also uses industry best practices for the development and testing of our application, ensuring that our code quality meets our standards before becoming part of a Sonar release.

## Cloud Infrastructure

Public cloud facilities - Sonar is managed in public cloud data centers. These facilities implement numerous physical and environmental controls to ensure that our customer data is well protected from possible theft or loss.

Data security architecture - Sonar follows best practices for security architecture. Proxy servers secure access to the Sonar application by providing a single point to filter attacks through IP blacklisting and connection rate limiting.

Redundancy - Sonar employs a cloud-based distributed backup framework for Sonar-hosted customer servers.

Availability and durability - The Looker application can be hosted in a variety of different public cloud data centers worldwide.

## Monitoring & Authentication

Access to a customer's back-end servers - Access to a Sonar-hosted back-end environment requires approval and multiple layers of authentication.

Access to a customer's Sonar application - Employee access to customer Sonar instances is provided in order to support a customer's needs. Access requires approval and multiple layers of authentication.

Monitored user access - Access to your Sonar environment is uniquely identified, logged, and monitored.

Network and application vulnerability scanning - Sonar's front-end application and back-end infrastructure are scanned for known security vulnerabilities.

Centralized logging - Logs across the Sonar production environment are collected and stored centrally for monitoring and alerting on possible security events.

Reputation monitoring/threat intelligence - Collected logs and network activity are checked against commercial threat intelligence feeds for potential risks.

Anomaly detection - Anomalous activity, like unexpected authentication activity, triggers alarms.

# SONAR'S SECURITY STRATEGIES

---

## Data Security Encryption

AES encryption - Locally-stored sensitive application data is encrypted and secured using AES 256-bit encryption.

TLS encryption - Data in transit is encrypted and secured from the user's browser to the application via TLS 1.2.

## Product security

Code development - Our code is developed using a documented system development lifecycle process

Peer review and unit testing of code - Our code is peer-reviewed before being committed to the master code branch of the Sonar application. Sonar also performs automated functional and unit tests.

Code quality tests - Sonar utilizes automated tests specifically targeting injection flaws, input validation, and proper CSRF token usage.

Penetration testing - Sonar completes regular penetration testing to check for exploitable vulnerabilities, to ensure the integrity of our online defenses.

## Corporate Security

### Personnel & Third Parties

Security organization - Led by our Cybersecurity Engineer, Sonar has established a dedicated information security function responsible for security and data compliance across the organization.

Policies and procedures - Sonar has implemented a wide range of security policies that are maintained, communicated, and approved by Leadership to ensure everyone clearly knows their security responsibilities.

Background checks - All new Sonar employees are required to pass a background check.

Security awareness education - All Sonar new hires complete security training as part of their onboarding with the company. Employees receive routine security awareness training and confirm adherence to Sonar security policies. Employees are reminded of security best practices through informal and formal communications.

# SONAR'S SECURITY STRATEGIES

## Incident response

On-call - Sonar's Security and DevOps team is available 24/7 to respond to security alerts and events.

Policies and procedures - Sonar maintains a comprehensive and documented Incident Response Plan.

Incident response training - Sonar employees are trained on security incident response processes, including communication channels and escalation paths.



# CERTIFICATE

Bulletproof Solutions ULC  
hereby certifies that the Management System of  
**Sonar Software Inc.**  
PO Box 540 DeBolt, Alberta, T0H 1B0

has been assessed and found to be in accordance with the management system requirements in  
**Baseline Cyber Security Controls for Small and Medium Organizations V1.2**  
for the following scope of activities:

**Infrastructure and software systems providing hosting services (SaaS)**

Certificate No.	C002-CSC103-07-21
Certified since	2021-07-07
Valid from	2021-07-07 (decision date)
until	2023-07-06 (expiry date)



**BULLETPROOF**  
a GLI company

*\*Subject to annual surveillance audits*

This certificate can be validated by email request at: [certifications@bulletproofsi.com](mailto:certifications@bulletproofsi.com)  
[www.bulletproofsi.com](http://www.bulletproofsi.com)



**Brian Ronan**  
Certification Manager

Bulletproof Solutions  
25 Alison Blvd  
Fredericton, NB, E3C 2N5

# CLOSING REMARKS

Over the course of this document, a number of features were highlighted in order to help demonstrate the variety of ways Sonar can help your organization grow by simplifying day-to-day operations, automating repetitive tasks performed by numerous departments, and how it's been designed to place the needs of your organization first.

Before directing you to our knowledge base and video resources for more information, there are a few extra features that deserve your attention in addition to those already mentioned. The first is the extensive documentation and functionality provided by the GraphQL API. With GraphQL, you can access and modify the data in your Sonar instance in new ways, and for custom or complicated queries, our support team is available for guidance. Additionally, Sonar provides a Customer Portal, built using Laravel and accessible through GitHub, that your organization can download to provide a layer of access and control to your customers.

Building on these concepts, Sonar also offers assistance with creating custom reports with Sonar's Business Intelligence, in-app documentation in addition to an external knowledge base, and easy-to-use feature request forms for any functionality you find missing that you believe would help your organization grow.

