Security Architecture Guide

A holistic approach to service virtualisation

A Soonr White Paper

soonr

MANAGE™ PROTECT

Dedicated Geo-Redundant Data Centre Infrastructure

Soonr takes a holistic approach towards security, incorporating a variety of structures and mechanisms at various layers within the Soonr service architecture. The following descriptions convey the breadth and depth of security considerations that have become a cornerstone of the Soonr Workplace service.

As opposed to the common virtualised approach to cloud services, wherein cloud service providers lease processing and storage capacity from Internet infrastructure providers, all Soonr hardware and software in each data centre is 100% owned, operated, and managed by Soonr. In typical virtualised cloud environments, service applications and customer data actually share processing and storage platforms in a time-sliced manner, resulting in a minimum of separation between independent operating domains. With the dedicated data centre approach that Soonr has invested in, nothing operates on any Soonr hardware or software processing or storage platform except Soonr services.

True 100% isolation of the Soonr service eliminates the possibility of experiencing any service interruption, performance degradation or malware infection that might otherwise be caused by adjacent applications. Combined with multi-level regional and data centre redundancy, the Soonr infrastructure represents one of the most secure, reliable and available cloud service architectures available today.

Soonr uses a co-location model for deployment of Soonr owned and operated equipment and software, utilising the rack space, power, cooling and physical security of major world-class SSAE 16 audited data centres. These facilities are a classified as Tier 3 or better with N+1 fault tolerant systems guaranteeing 99.982% availability.

Soonr operates data centres in several different geographical regions, including Australia, the United States, Canada and Europe, and is planning further expansion into other regions. Within each region, two levels of redundancy are provided. First, within each data centre, redundant servers and file storage ensure that data centre level failures can be isolated and resolved quickly. Second, within each region, at least two independent data centres are physically distanced and isolated from each other, thus providing protection from higher-level data centre failures, or broader Internet related failures. This dual-level geo-redundancy ensures maximum availability and protection against data loss.

The physical presence of data centres in separate regions also means that data does not leave the region; it stays in Australia for Australian-based customers, the United States for U.S.-based customers, in the European Union for EU-based customers (in compliance with EU Safe Harbor and EU Country policies), and in Canada for C.A.-based customers (in compliance with PIPEDA and local regulations).

Summary

- Co-location model with HW and SW 100% owned, operated and managed by Soonr
- Geo-redundant, Tier 3, SSAE16 Audited data centres (two per region)
- Complete regional data set in each data centre
- Complete regional server setups in each data centre
- Data centre redundancy using RAID6 mirrored backup with replication
- Data stored redundantly within each data centre
- Modular clustered server farms for service scalability, redundancy and protection
- SLAs for availability (99.982%), response time, service restoral

SAS 70 / SSAE 16 Audits

In the rapidly changing landscape of cloud services, companies that handle sensitive information, such as in the finance and medical sector, find that they are under increasing scrutiny over their information processing controls. Soonr data centres are audited against SAS 70 / SSAE 16 criteria for system reliability and security, thus providing assurances regarding adequate oversight over the controls utilised in the processing of information. Similarly, Soonr's own internal security controls are audited against SSAE 16 criteria for employee policies, physical and logical access controls, intrusion detection and testing, service reporting, security incident procedures, training, change control and configuration management. In this manner, Soonr services can serve as a foundation upon which customers can build their SAS 70 / SSAE 16 compliant data processing and storage policies and practices.

Logical Access Security

All Soonr application servers are protected with OS security modules that apply Discretionary Access Control and Mandatory Access Control policies to all server processes, thus ensuring that no software process can be gainfully subverted.

All connection pathways within the Soonr infrastructure are highly regulated as to the kinds of traffic that are allowed between various internal server endpoints. Any network traffic that does not meet the expected data flow patterns is immediately interrupted and reported to monitoring personnel through alerts. All known attack vectors are specifically prohibited.

Comprehensive Monitoring

All of the Soonr regional data centres are monitored 24 hours a day, 365 days a year, by equipment service and operations staff, who also have immediate access to Soonr engineering personnel in the event that it becomes necessary. Co-location with major world-class data centre industry partners ensures that physical and environmental security is unsurpassed.

Soonr utilises dedicated software monitoring components that are designed to track and evaluate the operation of servers, networking equipment, applications and services within the Soonr service infrastructure. This also includes monitoring of resources such as processor load, memory usage and disk space usage.

Alerts regarding performance or potential security issues are automatically distributed to several on-call staff via SMS and email.

Testing, Risk Assessment and Compliance

Soonr makes use of independent 3rd-party testing, analysis and assessment services. Soonr's multi-faceted approach to testing and risk assessment incorporates the following elements; 3rd party penetration testing of Web, Agent, APIs, Periodic SAS/SSAE audits and Daily Hacker Safe® updates.

Soonr follows the Safe Harbor Principles published by the United States Department of Commerce with respect to the transfer of personal data from the European Union to the United States of America. Soonr's Privacy Policy, available at http://www.soonr.com/privacy, details certain policies implemented throughout Soonr to comply with Safe Harbor.

Soonr complies with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Soonr's Privacy Policy (http://www.soonr.com/privacy/) details certain policies implemented throughout Soonr to comply with HIPAA.

Data Encryption and Authentication

All files handled by the Soonr service are secured, both in transit and in storage, using 256-bit AES-encryption. Furthermore, in order to maximise the separation between files, a different unique rotating encryption key is used for each file. None of the encryption keys are stored "in the clear" in any non-volatile storage, but rather are encrypted and stored under the protection of a master key. Authentication is ensured through the use of VeriSign certificate-based server authentication, which ensures that the user's agent will neither connect, nor cooperate with any server other than those that comprise the Soonr service. Even in the unlikely event of a successful attack on Internet DNS or routing infrastructure, which is quite outside the control of Soonr or any other SaaS provider, Soonr's certificate-based authentication.

Admin Policy & Account Management

Administrative Policy management and Account Management are particular strengths within the context of Soonr service administration and management, and provide for an extensive set of controls and processes that will ensure flexible and effective security policy enforcement. Admin-level account management and policy control includes mechanisms that allow Admins to:

- Create, edit, disable and delete Members, Connections, Groups and other Admins
- Convey to full Members the right to create Connections
- Control the ability of Members to create private Backups
- Review, assign and manage storage quota among Members
- Set and enforce Password Policies
- Establish Session Policies: Used to control the lifecycle of login sessions

In addition to these account-oriented policies and features, Soonr provides an additional set of powerful features that facilitate extensive Project control capabilities. Known as the "Manage Projects" feature, which is available as part of the Enterprise plan, this set of highly-privileged controls permits Team Admins to review and modify sharing and synchronisation rights, and also to view, download and delete any Project or document resources. Specifically, Admins can:

- Review and modify the sharing of Project resources that was established by other Members
- Review and modify the synchronisation status of any Member devices
- View, download and delete any shared Projects, Folders or Files owned by any Member

This set of Admin controls thus allows IT personnel to audit resource sharing and modify such Member sharing activities as necessary in order to enforce compliance with company guidelines.

Password and Two-Factor Authentication Policies

Soonr Workplace Team Members are authenticated into the Soonr service against databases in Soonr, Active Directory or a number of 3rd party systems that have been integrated with Soonr. When user authentication is performed against Soonr databases, Soonr Workplace Enterprise Team Admins can set global policies for password expiration (days), re-use cycle times, recent password interval (days), as well as password complexity and allowed failed login attempts.

Two-Factor Authentication, also known as 2FA, two-step verification or TFA, is an extra layer of security that is known as "multi-factor authentication" that requires not only a password and username, but also something that a Soonr Workplace Team Member has with them. This can be a physical "hard" token or a piece of information only they know or have immediately at hand, which may have been obtained through a "soft" token. Soonr Workplace Enterprise Team Admins can set policies to require 2FA as part of the web, agent or mobile device login flow into Soonr services for added layer of access control.

Content Policies

Access to content stored within Soonr is controlled and policed at different levels within the security architecture. Within the confines of overarching user policies that are established by Admins and enforced by the Soonr service, users are free to establish their own content access policies as they share Projects with others, effectively dictating the type and method of access afforded to others.

When Projects or sub-folders are shared with other Members or Connections, their access permissions can be specified at the appropriate level of granularity. In both the Soonr Workplace Pro and Enterprise Plans, access permissions to Projects or Sub-folders can be specified as Read-Only, Modify, Create & Modify and Full Access (including delete) based on the role of the Member. In addition, content owners can also control the ability for other Members to Reshare resources that they have shared.

Soonr Workplace Team Members can establish and manage URL-based Public Links to Project, Folder and File resources, thereby establishing a significant degree of granular control over content access. Public Links can be Member-specified with

expiration dates as well as access passwords, and can also be specified to either constrain or expand the access methodology as follows:

- View-only on web (Soonr Online)
- Download Enable / Disable
- Read-Only (no edit)
- Read-Only PDF Version (Source files converted to PDF by Soonr Workplace)
- Upload new or modified files

Additional protection of user content includes several cooperating mechanisms that defend against accidental deletion or overwriting of user files. While the File Lock mechanism enables users to voluntarily cooperate during the collaborative editing of documents, the file versioning and file branching mechanisms operate automatically to ensure that, even in the event of file conflicts or overwriting of files, no content is lost.

As Members edit and save subsequent versions of a file, the file versioning feature is a back-end Soonr Workplace service process that automatically retains the older over-written versions of all files for up to 180 days. At any point during that period, Members are able to access old versions through the web (Soonr Online).

File branching, a similar back-end automatic process, ensures that any attempt by two people to edit and save the same file at the same time will be captured as a file conflict, and will result in a branching of the file name at that point. One file will retain the original filename, while the second file will have the second Member's name appended to the file. This ensures that both sets of edits are retained.

Global Policies

Global Policies allow a Soonr Workplace Enterprise Admin to set global policies for allowing Public Links, restricting unlock over-ride to only the Project Owner and disabling Remote Access. Remote Access refers to the ability to remotely access a computer from any web browser, and requires the installation of the Soonr Workplace Desktop Agent onto the target computer. While this is an exceedingly useful feature, some Admins might feel that higher security and better control are achieved by disabling Remote Access.

Session Policies

Session Policies allow a Soonr Workplace Enterprise Admin to specify global session timeout, remember-me and IP address display policies for added control of user sessions into Soonr services.

IP Address White List Policies

The IP Address White List is also commonly referred to as an Access Control List (ACL) in computer networking security terminology. This feature enables the Soonr Workplace Enterprise Admin to place restrictions on service login. Specifically, service login can be restricted based upon a combination of the mode of access (browser, mobile app, desktop agent) and the source IP address.

General Device Policies

Device policies supported by Soonr Workplace enable Admins to ensure that lost or stolen computers or mobile devices can be removed from backup and sync plans (if supported) eliminating the possibly of data leakage to unintended recipients. Soonr Workplace's remote data wipe capability allows Admins to specifically target individual user accounts, Projects,

folders, files or devices/computers, maintaining a wall of access security around corporate data. Soonr Workplace's Device Policies specifically address:

- Lost device protection (no credential/id persistence)
- Encryption of all session related information on local device
- Role-based User Policies

Mobile Device Policies

Mobile Device Policies allow the Soonr Enterprise Admin to set global policies on allowing/disallowing the ability to create content, edit content, and export content to secondary or third party applications on mobile devices. Similarly the Team Admin can configure a policy to require a PIN passcode on mobile devices each time the Soonr Workplace mobile app is accessed by the user. Furthermore, an option is provided to set a failed passcode threshold, and to erase mobile device data upon passing that threshold, also known as a "poison pill".

Mobile Device Policies are designed to improve common device management tasks such as deleting all of the Soonr content on a stolen or lost smartphone or tablet. As an example of a remote-wipe policy, a Soonr Admin can check the Require Passcode policy, Enable Erase Data policy, and set the Failed Passcode Threshold value to 5. In this example, if a device is stolen and the Soonr Mobile app is launched, it will block access to any Soonr data unless the correct pin code is entered. After 5 incorrect pin code entries, the Soonr Mobile app will clear all user data out of its cache and remain locked.

Active Directory Integration for User Deployment

Enterprise-class account management and authentication for users and groups is supported within Soonr Workplace through the Active Directory Integration feature, which is available as part of the Enterprise plan. This feature enables IT personnel to import user and group account metadata from Active Directory into Soonr Workplace, and to force all Soonr Workplace user authentication through Active Directory. Soonr does not maintain any log-in information during user authentication, but acts as a proxy between the user and Active Directory servers.

Application Management Authentication

Mobile device data is encapsulated within the mobile app for greater content control. One of the more unique aspects of the Soonr Workplace service offering includes integrated Office-style viewing, creation and editing tools for mobile devices. Currently supported on iOS and Android platforms, these integrated apps ensure that mobile viewing, creation and editing by users is done within the confines of the Soonr Workplace Mobile App. This effectively ensures that mobile-accessible data remains within an envelope of privacy, minimising exposure of company data to 3rd-party applications.

Reporting

Beyond privacy-oriented security features such as encryption, access policies and account management, Soonr Workplace implements a set of advanced reporting capabilities that are specifically designed to support auditing for compliance with company

policies. These advanced reporting features, which are available as part of the Enterprise plan, enable Admins to generate and export custom reports in order to establish audit trails and analytics on the following types of events:

- Team Events: Account management events for all users and groups
- User Access Events: Device access, PC access, User logins, IP address mapping
- Project Events: All changes to any Projects, folders, or files
- User Report: List of all Team Members, their roles, storage quota, creation timestamp and last login
- Computer Report: List all desktop agents by Member, computer type, OS and Agent versions, installation timestamp and last connect timestamp
- Mobile Device Report: List of all mobile clients by Member, mobile device type, OS, and App versions, number of logins and last login timestamp

Reports can be customised and filtered to include or exclude a variety of events based upon various criteria, such as date range, user ID, file name, IP address, method of access and more. Reports can be either viewed on-screen or exported to either PDF or XLS formats. When reporting on user accesses, any user access event can be mapped to specific source IP addresses, and can be viewed on a geographical map.

About Soonr

Embraced by users and endorsed by IT, more than 150,000 businesses trust Soonr for their secure file sharing and collaboration needs. Soonr Workplace empowers mobile teams and organisations to do business faster from any device anywhere. We deliver our services through a worldwide network of cloud service providers, VARs, solution providers, and system integrators. Founded in 2005 and headquartered in Silicon Valley, we are privately-held and backed by major investors.

About Manage Protect

Manage Protect is an Australian award-winning Cloud Technology specialist. We deliver a best-of-breed integrated security platform of cloud-based services through local provisioning, help desk, presales support, training and certification.

Manage Protect is an Australian business committed to making email and the Internet a secure, safe, compliant and productive environment for businesses. We achieve this through our network of trained and certified partners across Australia & New Zealand.

Our suite of cloud-based managed services delivers true business grade, best-of-breed solutions focused on making business use of the Internet simple, secure and reliable.