Security Culture at Silverfin

silverfin

Silverfin's purpose is to make accountants connected. To achieve this, Silverfin uses data and a variety of technology systems. The connection between accountants and their customers is trust-based, making it imperative that we build these systems on the fundamentals of this same principle to inspire trust.

We take this philosophy towards security with us throughout the entirety of Silverfin. Security is always on our mind, effortlessly. We are always critical and challenged to pause and think before acting. We like to call this our 'security reflex' which helps us make the right decisions at the right times.

As your trusted business partner, we act on a policy of transparency and responsible, timely communications. We also hold others in our ecosystem to these same high security standards; ensuring that working with Silverfin means working with a vetted, secure solution.

Compliance

Silverfin commits to compliance as a way of transparently communicating our security posture to our customers. We follow best practices in everything we do, and consult frameworks like ISO27001 and NIST for guidance.

Silverfin has the following certifications:
ISO27001

Our customers' & partners' personal data is safe with us! Silverfin is compliant with the GDPR and the UK Data Protection Act. Frequent legal & security audits ensure that our data protection practices continue to meet the appropriate standards.

People

Our people are what makes Silverfin, and the same goes for security. Security controls in general are always most effective when supported by a robust security culture. This is what we strive for at Silverfin. We engage our workforce across their entire lifecycle, from the time they apply and throughout their careers. This includes:

- Background checks (within legal boundaries)
- Training (starting day 1)
- Mobile device management
- Awareness campaigns
- Phishing exercises
- Security as a dedicated function
- Security newsletters

Access management

We follow the principle of least-privilege and implement zero trust wherever possible. This means we supply individuals with minimal access necessary to do their job ('least privilege & need to know'). The same ideology applies to our infrastructure and software. No component or system should have more access than it needs to perform its function.

Existing accesses are audited periodically to ensure accesses are minimal in practice.

Access to company resources is always piped through an authentication flow verifying the identity (using MFA & SSO) and the device initiating the connection.

For any other credentials, we utilise 1Password encrypted vaults.

Endpoint protection

Silverfin employs endpoint protection tools depending on the system type, and has specific measures to protect BYOD devices. We also follow the zero trust protocol here, and only permit access to company resources when we identify an individual over multi-factor authentication and verify the device initiating the connection. Endpoints are protected with disk encryption, strong authentication, anti malware and firewalls.

Product security

As Silverfin develops code to run its ever-evolving SaaS application, we utilise a secure development lifecycle (SSDLC) to minimise the chance of introducing vulnerabilities into our apps in Production.

This has become increasingly important in recent years as applications become more complex, and the impact of remediating a vulnerability after release is often magnitudes higher than if it had been detected during the early stages of development.

In short, our engineers always go through a process to handle, review and push code into production. This includes a variety of automated checks for vulnerabilities and dated dependencies. We also still do manual code reviews by someone who hasn't worked directly on a ticket to keep each other honest.

Risk management

Information security is sometimes difficult to grasp, and it can be hard to decide what to prioritise. For this reason, Silverfin uses risk management to estimate the threat landscape and its underlying risks. This allows us to make sensible choices and invest in the right areas to combat threat actors.

This approach is also apparent in how we deal with third parties internally. All vendors partnering with Silverfin undergo a risk assessment before they are allowed to become part of our ecosystem.

Cloud infrastructure

Our infrastructure is hosted with Google Cloud Platform (GCP), which is leading the way for modern cloud solutions. We operate in a few Google Cloud Regions (EUW & NA, depending on your preferred location) with fitting regional Kubernetes clusters to build our infrastructure stacks. Our entire infrastructure is code-based using Terraform, allowing for a significant amount of automation and ease of recovery. All of our stacks are entirely isolated, only sharing a common data layer.

For our databases, we also utilise AWS S3 for business continuity, as it would allow us to recover even if GCP would be completely unavailable.

Google Cloud is ISO27001, SOC1, 2 and 3 certified among others. Connections in our infrastructure are protected with firewalls, encryption and virtual networks. Our application is also protected by a WAF preventing and blocking OWASP top 10 vulnerabilities from harming us.

A diagram of our infrastructure can be shared after contacting our Sales team.

Security monitoring

Silverfin uses Datadog for its logging and monitoring purposes. We run agents on our applications and infrastructure, and keep our monitors in code in GitLab. If any parameters are out of bounds, we are automatically notified (even called) to take action.

Incident response

Silverfin's agile incident response process allows us to quickly assess a situation and escalate where necessary. We always build post-mortem reports so we can learn of each and every incident. If an incident occurs that impacts a customer, we will notify within the timeframe provided by our data processing addendum.

Vulnerability management

At an application level, Silverfin runs a variety of scans to identify vulnerabilities in libraries, code, docker images and dependencies. An automated bot performs updates automatically for vulnerable dependencies.

For our infrastructure, vulnerabilities are also patched automatically and code-based. We also have firefighters on duty each and every day to deal with any security issues immediately.

Additionally, we run a managed, private bug bounty program with Intigriti to continuously test our production environment for vulnerabilities. This is much more effective than a snapshot traditional, yearly penetration test.

Found a vulnerability? Get in touch with bugbounty@silverfin.com

Secrets management

Silverfin has a best of both worlds approach for encryption and key management with customer managed keys and KMS control.

Cloud Storage always encrypts our data on the server side before it is written to disk (Google-managed encryption keys). Besides that, there are other options available for KMS:

Customer-managed encryption keys
Customer-supplied encryption keys

For our Google Cloud Storage buckets, we use customer-managed keys.

Data encryption

All data in storage or travelling state is encrypted. Data that is being sent between you and us is always sent using HTTPS over TLS 1.2/1.3. Data at rest is encrypted over AES256.

Disaster recovery & availability

Our Disaster Recovery (DR) program ensures that our services remain available or are easily recoverable in the case of a disaster. Data is backed up over 2 redundant locations (geographically distant regions) with Google Cloud Platform to ensure data is available for recovery.

Our infrastructure setup and DR program allows us to quickly react to disasters and recover at a rapid pace:

- RTO -> 15m to 1hr
- RPO -> 10m

Silverfin maintains a publicly available system status webpage which includes real-time information on system performance, scheduled maintenance, service incidents history, and relevant security events.

Data protection

Data Protection matters to us!

Silverfin implements appropriate technical and organisational measures (as described above) to ensure, to the best of our abilities, the protection of (i) the personal data – including protection against careless, improper, unauthorised or unlawful use and/or processing and against accidental loss, destruction or damage; and (ii) the confidentiality and integrity of the personal data. When implementing these measures, Silverfin has taken into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

For more information on how Silverfin processes personal data:
See our privacy policy
See our data processing addendum

For a general overview, please consult our data protection page

Terms of use

www.silverfin.com