

Member Lending Portal (front end)

Harbourline Credit Union (fictional)

Threat and Risk Assessment

RELEASED

Specimen. A released assessment of a fictional organisation, printed as the product produced it. The sign-in addresses of the people who accepted it are withheld; nothing else differs from the signed record.

Assessment	Member Lending Portal front end (run 12, engine 10.18, 10 Oct 2026) (tra_038b00493c384b42b97d)
Released	2026-10-11
Valid until	2027-10-11

Valid for at most one year from release, and to be reviewed earlier when any of these occur:

- A system, data or connection in scope changes
- A new known exploited vulnerability matches a named product
- A security incident touches an asset in scope
- A vendor or hosting arrangement changes
- Twelve months since release

Engine version at start	agents-2026.10.18
Risk table version	tra-risk-2026.09.1
Generated	10 October 2026, 9:23 pm Eastern

Rendered from the record as signed at release. SHA-256 79fb84e18236cc9e5dd12c9189ba4509bf194c6662d486b8344912139462eed, engine at release agents-2026.10.18.

This assessment is informed by the Harmonized Threat and Risk Assessment Methodology (TRA-1) and NIST SP 800-30. It is RiskWoven's own method and wording; it does not claim to be either. It is a point-in-time advisory assessment built from the statements, evidence and assurance inputs the organisation supplied. It is not an audit, a certification or a guarantee that the system is secure.

Executive summary

The assessment rated 49 risks across 4 subjects (3 assets and 1 connection). 20 are very high and 25 are high. By confidence, 3 ratings are verified, 14 rest on a safeguard that is described and not evidenced, and 32 are unknown. The organisation set its tolerance at medium; 45 risks sit above it and need a decision. 12 treatment plans address them. The highest classification is integrity at very high (5 of 5).

Classification

Dimension	Level	Meaning on the injury scale
Confidentiality	4 High	Serious harm. A reportable breach, material financial loss, or harm to individuals that needs remediation.
Integrity	5 Very high	Severe harm. Harm to health or safety, the loss of a licence to operate, or the end of the organisation.
Availability	4 High	Serious harm. A reportable breach, material financial loss, or harm to individuals that needs remediation.

Risks by band

Very high	20
High	25
Medium	4
Low	0
Very low	0

Risk appetite

Tolerance band	Medium
Rationale	The board accepts low and medium risks with owner approval on record because the credit union holds member financial data under provincial regulation; anything above medium must be treated.
Acceptance policy	Acceptance authority follows RiskWoven's default policy.
Risks above tolerance	45
Treatment plans	12

Scope and boundary

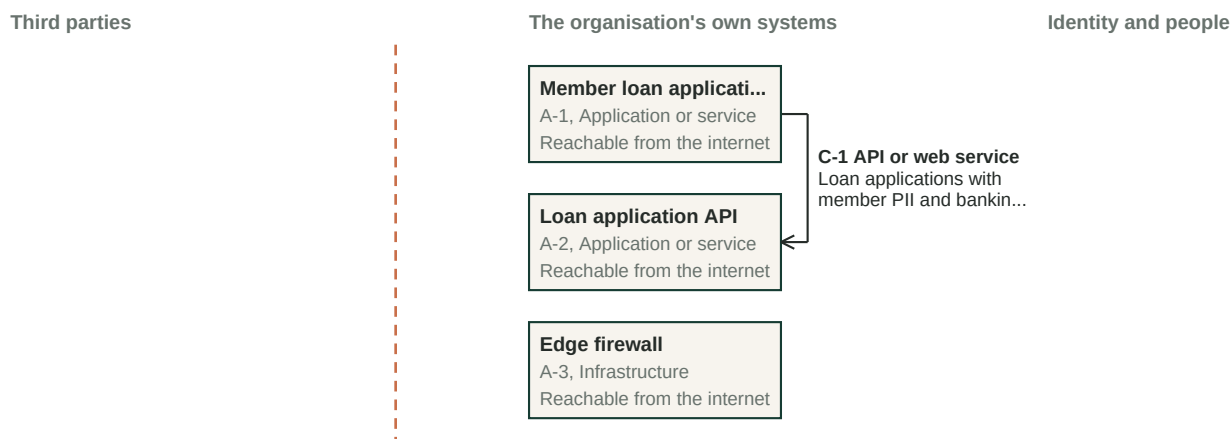
System	Member Lending Portal (front end)
Purpose	Public web application and API where Harbourline Credit Union members apply for personal and vehicle loans. About 900 applications a month.
Boundary	The public web app, its API, the link between them, and the edge firewall at head office.
Users	About 14,000 members can apply online. 3 IT administrators run the platform.
Hosting	The web app and API run in an AWS account in the ca-central-1 region. The edge firewall sits in the head office server room in Nova Scotia.
Data flows	Members submit name, address, date of birth, social insurance number, income and banking details through the web app, which sends them to the API over HTTPS.
Out of scope	The lending database, the staff console, the credit bureau link, the pre-screening model, the mail server and the backup appliance.

Out-of-scope items

Item	Reason	Reference
Lending database and staff systems	Covered by another assessment	Full portal assessment, October 2026

System as declared

Drawn from the assets and connections the organisation declared at intake. It is not a verified architecture.



Each box is an asset with its id, kind and stated exposure; each line is a declared connection with its channel and what crosses it, and the arrow shows the direction. The dashed vertical line is the boundary between third parties and the organisation's own systems.

Assets and connections

Assets

Id	Name	Kind	C	I	A	Exposure	Third party	Product and version
A-1	Member loan application web app	Application or service	4	4	4	Reachable from the internet	No	OpenJS Foundation Node.js 20.11.0
A-2	Loan application API	Application or service	4	5	4	Reachable from the internet	No	
A-3	Edge firewall	Infrastructure	3	4	4	Reachable from the internet	No	Fortinet FortiOS 7.0.12

Reason for the impact levels

Id	Name	Reason, as the owner stated it
A-1	Member loan application web app	This is the only way members apply online, about 900 applications a month. Every application passes through it with name, date of birth, SIN and banking details, so a leak or a tampered form is a reportable privacy breach. An outage stops new lending intake until it is back.
A-2	Loan application API	Every application record is written through this API, and it calls the credit bureau and the scoring model. A tampered request can change what is stored or what score comes back, which changes a lending decision. It carries the same member data as the web app, and intake stops if it is down.
A-3	Edge firewall	Guards the head office network where the mail server and backup appliance sit. Someone who controls it can redirect or watch office traffic and reach those systems. If it fails, the office loses the VPN and the nightly backup transfer, but the AWS portal keeps running.

Valuation step: proposed changes to the impact levels

Asset	Dim	From	To	Quote	Reason	Outcome
Edge firewall	C	3	4	The management interface is reachable from the internet over HTTPS from any source address, with no allowlist, VPN requirement or intrusion prevention rule in front of it.	The owner's rationale sets confidentiality at 3, noting that someone who controls the firewall can watch office traffic and reach the mail server and backup appliance.	Not accepted
Edge firewall	A	4	3	The lending database, the staff console, the credit bureau link, the pre-screening model, the mail server and the backup appliance.	The owner's rationale sets availability at 4, partly because a firewall failure stops the nightly backup transfer. The mail server and backup appliance are explicitly out of scope, so their loss cannot drive the injury level for this asset within this assessment boundary. The owner also notes that the AWS portal keeps running if the firewall fails.	Not accepted

Connections

Id	From	To	Direction	Channel	What crosses it
C-1	Member loan application web app	Loan application API	one-way	API or web service	Loan applications with member PII and banking details over HTTPS.

Safeguards as described and rated

Id	Statement	Status	Assets	Support	What would evidence it
SG-1	A managed web application firewall with rate limiting sits in front of the web app and the API.	In place	Member loan application web app; Loan application API	Unsupported	A dated WAF configuration export or managed-service portal screenshot naming both the Member loan application web app and the Loan application API as protected origins, together with the rate-limiting rule set in force, would evidence this claim.
SG-2	Every internet-facing system, including the edge firewall, is patched within 14 days of a vendor security release.	In place	Member loan application web app; Loan application API; Edge firewall	Unsupported	A dated patch log covering the Member loan application web app and the Loan application API, showing each vendor security release and the date the patch was applied, with all gaps within 14 days, would evidence this claim.
SG-3	The connection between the web app and the API uses TLS 1.2 or later.	In place	Member loan application web app -> Loan application API; Loan application API	Supported	Not recorded

Method

Scales. Each subject (an asset, or a connection between two assets) is rated against RiskWoven's closed catalog of 33 threats in three categories: deliberate, accidental and environmental. Three scales of 1 to 5 are used and printed below: injury (the harm done if the threat succeeds), likelihood (how probable the threat is, with a catalog anchor for each threat) and vulnerability (the strength of control, where 1 is well protected and 5 is exposed).

Impact. Impact is the subject's highest injury level on the dimensions the threat injures (confidentiality, integrity or availability), and the register names the dimension that set it. Impact levels are declared by the asset's owner with a stated reason and may be revised by the valuation step with a quoted reason. For an AI asset, the threats that apply depend on how it works as the organisation stated it (a language model used directly, one that acts through tools, classical machine learning, or rules); where that was not stated, every AI threat applies. A threat that applies to a subject's kind and was not rated is listed in Appendix D with the reason it was ruled out.

Likelihood. Likelihood starts from the catalog's anchor for the threat at the exposure the organisation stated for the subject, internet-facing or internal, and moves from the anchor only for a stated reason; a move of two or more steps needs a stated fact. Where the exposure was not stated, the higher of the two anchors is used. The register prints the anchor beside the rating.

Vulnerability. Vulnerability rates the strength of the safeguards as the organisation described them, not as tested. The two ratings combine as exposure = $\text{ceil}((\text{likelihood} + \text{vulnerability}) / 2)$, and the band is read from one fixed table of impact against exposure (version tra-risk-2026.09.1).

Confidence. Whether a safeguard is evidenced is recorded apart from the rating, as confidence: verified when every safeguard the rating relies on is supported by attached evidence or the organisation stated that none is in place, claimed when a safeguard is described and not evidenced, and unknown when no safeguard was described, a claimed safeguard was contradicted, or no rating was given (a missing vulnerability reads as 5; a missing likelihood takes the catalog anchor and the row is marked provisional). A rating whose likelihood reason cites a known exploited entry with an unconfirmed version is held at claimed. Confidence is derived in code from the record, which includes the support rating the safeguard review gave each safeguard; confidence itself is never rated by a model. It gates acceptance: a risk whose confidence is below verified can be accepted only with a verification action and a date for it.

Exposures. Each risk is shown at three exposures: unmitigated (the same impact and likelihood with no safeguard, read as vulnerability 5), current (with the safeguards as described) and target (the band the organisation expects once its treatment is done).

Acceptance. A risk above the organisation's tolerance needs a decision. Who may accept a risk at each band follows the acceptance policy applied to this assessment, which is named under Risk appetite and printed with the table of bands.

Known exploited vulnerabilities. Where a product or a vendor was stated for an asset, it is matched in code against the CISA Known Exploited Vulnerabilities catalog, and each match is given to the likelihood rating as a fact. Each entry is in one of three states: version confirmed affected; product match, version unconfirmed; or ruled out by stated version, which is listed and not counted as a match.

Review. The assessment is valid for at most one year from release and is reviewed earlier when one of the review triggers listed with the validity date occurs.

Unknowns. Stated unknowns are recorded and listed with the claims, and a contradicted safeguard lowers confidence.

Scales

Level	Injury	Likelihood	Vulnerability
1	No lasting harm. An inconvenience that is absorbed inside a day.	Rare. No known interest or means, and no history of this happening to organisations like this one.	Well protected. Layered safeguards described and tested.
2	Minor harm. Some rework, a small cost, or embarrassment that stays internal.	Unlikely. Possible in principle; would need unusual effort or luck.	Protected. A safeguard in place that addresses this threat to this asset.
3	Moderate harm. A regulatory notice, a lost customer, or a public correction.	Possible. Happens to comparable organisations from time to time.	Partly protected. The safeguard is partial, or relies on one person or a manual step.
4	Serious harm. A reportable breach, material financial loss, or harm to individuals that needs remediation.	Likely. Routine for this kind of asset; expected within a year or two.	Weakly protected. A weak or informal measure.

Level	Injury	Likelihood	Vulnerability
5	Severe harm. Harm to health or safety, the loss of a licence to operate, or the end of the organisation.	Almost certain. Ongoing, automated, or already observed here.	Exposed. Nothing described stands between the threat and the asset.

Confidence

Confidence	Risks	Meaning
Verified	3	Every safeguard the rating relies on is supported by attached evidence, or the organisation stated that no safeguard is in place.
Claimed	14	The rating relies on a safeguard the organisation described and has not evidenced.
Unknown	32	No rating was given, no safeguard was described for the asset, a safeguard claimed for it was contradicted, or the safeguards listed for it were judged not to cover the pair.

Evidence state, beside confidence: Verified and Claimed as for confidence; Contradicted, a listed safeguard was contradicted for the asset; Assessed gap, rated and no listed safeguard addresses the pair; Not assessed, no vulnerability rating was given. A provisional row has no likelihood rating and carries the catalog anchor until rated.

Current band by impact and exposure

Impact	Exposure 1	Exposure 2	Exposure 3	Exposure 4	Exposure 5
5	Low	Medium	High	Very high	Very high
4	Low	Low	Medium	High	Very high
3	Very low	Low	Medium	Medium	High
2	Very low	Very low	Low	Low	Medium
1	Very low	Very low	Very low	Low	Low

Bands and what they commit the organisation to

Band	Meaning	Expectation
Very high	Severe. The organisation should not operate with this exposure.	Treated within 30 days. It cannot be accepted under this assessment's policy.
High	Serious. Harm is likely enough and large enough to need action soon.	Treated within 90 days, or accepted by an executive.
Medium	Material. The exposure could cause noticeable harm if left alone.	Treated within 12 months, or accepted with a written rationale.
Low	Minor. Some exposure remains, with limited consequence.	May be accepted once the risk owner signs off in the record.
Very low	Negligible. The safeguards in place leave little to act on.	Accepted by default. Reviewed once a year with the assessment.

Acceptance authority follows RiskWoven's default policy.

Assumptions, issues and limitations

Assumptions (3)

- Documents and records that were not supplied are treated as not existing for the purpose of this assessment, not as absent by oversight.
- Likelihood ratings drew on the CISA Known Exploited Vulnerabilities catalog as retrieved 2026-10-10 (4 matching entries). Matches are by product name and version as the organisation stated them; a product stated differently, or not stated, is not matched. A match means the organisation is potentially affected; it is not a confirmed vulnerability in this deployment. 11 further entries were ruled out by the stated version and are listed for the record.
- Likelihood ratings start from RiskWoven's anchor for each threat at the exposure the organisation stated for the subject (internet-facing or internal; not stated reads as the higher of the two). 1 rating moved two or more steps from the anchor, each on a stated fact.

Issues (5)

- 2 safeguards recorded as in place or partly in place carry no evidence and stand as stated only: SG-1, SG-2.
- 6 findings from the supplied assurance inputs are recorded as still open.
- 1 safeguard was contradicted in part by an assurance input the organisation supplied (penetration test, 2026-05-20) and is treated as partly in place for the assets named, and as stated for its other assets: SG-1 (A-2).
- 1 safeguard was contradicted in part by an assurance input the organisation supplied (vulnerability scan, 2026-08-12) and is treated as not in place for the assets named, and as stated for its other assets: SG-2 (A-3).
- 1 asset lacks a stated product or version, so a known exploited vulnerability match, or its version check, could not be made for it: A-2.

Limitations (2)

- This assessment is a point-in-time view built from the statements, evidence and assurance inputs the organisation supplied. Safeguards can change after the date of release. Valid for at most one year from release, and to be reviewed earlier when any of these occur: A system, data or connection in scope changes; A new known exploited vulnerability matches a named product; A security incident touches an asset in scope; A vendor or hosting arrangement changes; Twelve months since release.
- Out of scope: Lending database and staff systems (Covered by another assessment: Full portal assessment, October 2026).

Risk register

49 risks, most severe first, in two tables for each group of risks: the ratings, then the bands. Dim is the dimension that set the impact (C confidentiality, I integrity, A availability). I is impact, L likelihood, V vulnerability, E the exposure score. Anchor is the catalog's starting likelihood for the subject's exposure beside the rating given. Unmit. is the unmitigated band (no safeguard), Current the band with the safeguards as described, Target the band expected after treatment. Conf. is the confidence: how far the current band can be relied on. Evidence is the evidence state (see Method). "Needed" marks a risk above tolerance that has no decision yet. Appendix F gives the reason behind each vulnerability rating.

Risk	Subject	Threat	Dim	I	L	V	E	Anchor
R-A-1-T-A01	Member loan application web app	T-A01 Misconfiguration	C	4	4	5	5	anchor 4, rated 4
R-A-2-T-A01	Loan application API	T-A01 Misconfiguration	I	5	4	5	5	anchor 4, rated 4
R-A-2-T-A02	Loan application API	T-A02 Human error in operation	I	5	3	5	4	anchor 3, rated 3
R-A-2-T-A03	Loan application API	T-A03 Software defect	I	5	3	5	4	anchor 3, rated 3
R-A-2-T-D01	Loan application API	T-D01 Credential theft and account takeover	I	5	4	4	4	anchor 4, rated 4
R-A-2-T-D02	Loan application API	T-D02 Exploitation of a publicly known vulnerability in a named product	I	5	4	3	4	anchor 4, rated 4
R-A-2-T-D03	Loan application API	T-D03 Ransomware and destructive malware	I	5	3	4	4	anchor 3, rated 3
R-A-2-T-D05	Loan application API	T-D05 Insider misuse of access	I	5	2	5	4	anchor 2, rated 2
R-A-2-T-D14	Loan application API	T-D14 Abuse of exposed interface	I	5	5	4	5	anchor 4, rated 5
R-A-3-T-A01	Edge firewall	T-A01 Misconfiguration	I	4	4	5	5	anchor 4, rated 4
R-A-3-T-D01	Edge firewall	T-D01 Credential theft and account takeover	I	4	5	5	5	anchor 4, rated 5
R-A-3-T-D02	Edge firewall	T-D02 Exploitation of a publicly known vulnerability in a named product	I	4	5	5	5	anchor 4, rated 5

Risk	Unmit.	Current	Target	Conf.	Evidence	Decision
R-A-1-T-A01	Very high	Very high	Medium	Unknown	Assessed gap	treat, open
R-A-2-T-A01	Very high	Very high	High	Unknown	Assessed gap	treat, open
R-A-2-T-A02	Very high	Very high	Medium	Unknown	Assessed gap	treat, open
R-A-2-T-A03	Very high	Very high	Medium	Unknown	Assessed gap	treat, open
R-A-2-T-D01	Very high	Very high	High	Claimed	Claimed	treat, open
R-A-2-T-D02	Very high	Very high	High	Claimed	Claimed	treat, open
R-A-2-T-D03	Very high	Very high	Medium	Claimed	Claimed	treat, open
R-A-2-T-D05	Very high	Very high	Medium	Unknown	Assessed gap	treat, open
R-A-2-T-D14	Very high	Very high	Medium *	Claimed	Claimed	treat, open
R-A-3-T-A01	Very high	Very high	Medium	Unknown	Assessed gap	treat, open
R-A-3-T-D01	Very high	Very high	Medium	Unknown	Assessed gap	treat, open
R-A-3-T-D02	Very high	Very high	Medium	Unknown	Contradicted	treat, open

* The target is lower than safeguards alone can reach with the impact and likelihood unchanged (vulnerability at its floor of 1). The plan has to lower the likelihood or the impact as well.

Risk	Subject	Threat	Dim	I	L	V	E	Anchor
R-A-3-T-D03	Edge firewall	T-D03 Ransomware and destructive malware	A	4	5	5	5	anchor 3, rated 5
R-A-3-T-D14	Edge firewall	T-D14 Abuse of exposed interface	I	4	5	5	5	anchor 4, rated 5
R-C-1-T-A01	Member loan application web app -> Loan application API	T-A01 Misconfiguration	I	5	4	5	5	anchor 4, rated 4
R-C-1-T-A03	Member loan application web app -> Loan application API	T-A03 Software defect	I	5	3	5	4	anchor 3, rated 3
R-C-1-T-D02	Member loan application web app -> Loan application API	T-D02 Exploitation of a publicly known vulnerability in a named product	I	5	4	5	5	anchor 4, rated 4
R-C-1-T-D06	Member loan application web app -> Loan application API	T-D06 Supply chain compromise	I	5	2	5	4	anchor 2, rated 2
R-C-1-T-D07	Member loan application web app -> Loan application API	T-D07 Denial of service	A	4	4	5	5	anchor 3, rated 4
R-C-1-T-D14	Member loan application web app -> Loan application API	T-D14 Abuse of exposed interface	I	5	4	5	5	anchor 4, rated 4
R-A-1-T-A02	Member loan application web app	T-A02 Human error in operation	I	4	3	5	4	anchor 3, rated 3
R-A-1-T-A03	Member loan application web app	T-A03 Software defect	I	4	3	5	4	anchor 3, rated 3
R-A-1-T-D01	Member loan application web app	T-D01 Credential theft and account takeover	C	4	4	4	4	anchor 4, rated 4
R-A-1-T-D02	Member loan application web app	T-D02 Exploitation of a publicly known vulnerability in a named product	C	4	4	3	4	anchor 4, rated 4

Risk	Unmit.	Current	Target	Conf.	Evidence	Decision
R-A-3-T-D03	Very high	Very high	Medium	Unknown	Assessed gap	treat, open
R-A-3-T-D14	Very high	Very high	Medium	Unknown	Contradicted	treat, open
R-C-1-T-A01	Very high	Very high	High	Unknown	Assessed gap	treat, open
R-C-1-T-A03	Very high	Very high	Medium	Unknown	Assessed gap	treat, open
R-C-1-T-D02	Very high	Very high	High	Unknown	Assessed gap	treat, open
R-C-1-T-D06	Very high	Very high	Medium	Unknown	Assessed gap	treat, open
R-C-1-T-D07	Very high	Very high	Medium	Unknown	Assessed gap	treat, open
R-C-1-T-D14	Very high	Very high	Medium *	Unknown	Assessed gap	treat, open
R-A-1-T-A02	High	High	Medium	Unknown	Assessed gap	treat, open
R-A-1-T-A03	High	High	Medium	Unknown	Assessed gap	treat, open
R-A-1-T-D01	Very high	High	Medium	Claimed	Claimed	treat, open
R-A-1-T-D02	Very high	High	Medium	Claimed	Claimed	treat, open

* The target is lower than safeguards alone can reach with the impact and likelihood unchanged (vulnerability at its floor of 1). The plan has to lower the likelihood or the impact as well.

Risk	Subject	Threat	Dim	I	L	V	E	Anchor
R-A-1-T-D03	Member loan application web app	T-D03 Ransomware and destructive malware	A	4	3	4	4	anchor 3, rated 3
R-A-1-T-D04	Member loan application web app	T-D04 Data exfiltration	C	4	3	4	4	anchor 3, rated 3
R-A-1-T-D05	Member loan application web app	T-D05 Insider misuse of access	C	4	2	5	4	anchor 2, rated 2
R-A-1-T-D14	Member loan application web app	T-D14 Abuse of exposed interface	C	4	4	3	4	anchor 4, rated 4
R-A-1-T-E01	Member loan application web app	T-E01 Hosting region failure	A	4	2	5	4	anchor 2, rated 2
R-A-2-T-D04	Loan application API	T-D04 Data exfiltration	C	4	4	4	4	anchor 3, rated 4
R-A-2-T-D06	Loan application API	T-D06 Supply chain compromise	I	5	2	4	3	anchor 2, rated 2
R-A-2-T-D07	Loan application API	T-D07 Denial of service	A	4	4	4	4	anchor 3, rated 4
R-A-2-T-E01	Loan application API	T-E01 Hosting region failure	A	4	2	5	4	anchor 2, rated 2
R-A-3-T-A02	Edge firewall	T-A02 Human error in operation	I	4	3	5	4	anchor 3, rated 3
R-A-3-T-A04	Edge firewall	T-A04 Third-party outage	A	4	3	5	4	anchor 3, rated 3
R-A-3-T-A09	Edge firewall	T-A09 Backup or recovery failure	A	4	2	5	4	anchor 2, rated 2

Risk	Unmit.	Current	Target	Conf.	Evidence	Decision
R-A-1-T-D03	High	High	Medium	Claimed	Claimed	treat, open
R-A-1-T-D04	High	High	Medium	Claimed	Claimed	treat, open
R-A-1-T-D05	High	High	Medium	Unknown	Assessed gap	treat, open
R-A-1-T-D14	Very high	High	Medium	Claimed	Claimed	treat, open
R-A-1-T-E01	High	High	Medium	Unknown	Assessed gap	treat, open
R-A-2-T-D04	Very high	High	Medium	Claimed	Claimed	treat, open
R-A-2-T-D06	Very high	High	Medium	Claimed	Claimed	treat, open
R-A-2-T-D07	Very high	High	Medium	Claimed	Claimed	treat, open
R-A-2-T-E01	High	High	Medium	Unknown	Assessed gap	treat, open
R-A-3-T-A02	High	High	Medium	Unknown	Assessed gap	treat, open
R-A-3-T-A04	High	High	Medium	Unknown	Assessed gap	treat, open
R-A-3-T-A09	High	High	Medium	Unknown	Assessed gap	treat, open

Risk	Subject	Threat	Dim	I	L	V	E	Anchor
R-A-3-T-A10	Edge firewall	T-A10 Loss of access to keys or credentials	A	4	3	5	4	anchor 2, rated 3
R-A-3-T-D06	Edge firewall	T-D06 Supply chain compromise	I	4	2	5	4	anchor 2, rated 2
R-A-3-T-D07	Edge firewall	T-D07 Denial of service	A	4	3	5	4	anchor 3, rated 3
R-A-3-T-E01	Edge firewall	T-E01 Hosting region failure	A	4	2	5	4	anchor 2, rated 2
R-C-1-T-A04	Member loan application web app -> Loan application API	T-A04 Third-party outage	A	4	3	5	4	anchor 3, rated 3
R-C-1-T-A10	Member loan application web app -> Loan application API	T-A10 Loss of access to keys or credentials	A	4	2	5	4	anchor 2, rated 2
R-C-1-T-D04	Member loan application web app -> Loan application API	T-D04 Data exfiltration	C	4	4	3	4	anchor 3, rated 4
R-C-1-T-E01	Member loan application web app -> Loan application API	T-E01 Hosting region failure	A	4	2	5	4	anchor 2, rated 2
R-C-1-T-E03	Member loan application web app -> Loan application API	T-E03 Provider withdrawal or terms change	A	4	2	5	4	anchor 2, rated 2
R-A-1-T-D06	Member loan application web app	T-D06 Supply chain compromise	C	4	2	4	3	anchor 2, rated 2
R-A-1-T-D07	Member loan application web app	T-D07 Denial of service	A	4	3	3	3	anchor 3, rated 3
R-C-1-T-A11	Member loan application web app -> Loan application API	T-A11 Misdirected transmission	C	4	2	3	3	anchor 3, rated 2

Risk	Unmit.	Current	Target	Conf.	Evidence	Decision
R-A-3-T-A10	High	High	Medium	Unknown	Assessed gap	treat, open
R-A-3-T-D06	High	High	Medium	Unknown	Assessed gap	treat, open
R-A-3-T-D07	High	High	Medium	Unknown	Assessed gap	treat, open
R-A-3-T-E01	High	High	Medium	Unknown	Assessed gap	treat, open
R-C-1-T-A04	High	High	Medium	Unknown	Assessed gap	treat, open
R-C-1-T-A10	High	High	Medium	Unknown	Assessed gap	treat, open
R-C-1-T-D04	Very high	High	Medium	Verified	Verified	treat, open
R-C-1-T-E01	High	High	Medium	Unknown	Assessed gap	treat, open
R-C-1-T-E03	High	High	Medium	Unknown	Assessed gap	treat, open
R-A-1-T-D06	High	Medium	Not recorded	Claimed	Claimed	accept, open
R-A-1-T-D07	High	Medium	Not recorded	Claimed	Claimed	accept, open
R-C-1-T-A11	High	Medium	Not recorded	Verified	Verified	accept, open

Risk	Subject	Threat	Dim	I	L	V	E	Anchor
R-C-1-T-D15	Member loan application web app -> Loan application API	T-D15 Interception or tampering in transit	I	5	2	2	2	anchor 3, rated 2

Risk	Unmit.	Current	Target	Conf.	Evidence	Decision
R-C-1-T-D15	Very high	Medium	Not recorded	Verified	Verified	accept, open

How one risk was reached

The 3 highest-rated risks by current band, each followed from the asset to the decision. Every line is taken from the record; "Not recorded" marks a field the record does not hold.

1. R-A-1-T-A01: Misconfiguration, on Member loan application web app

Asset	Member loan application web app (A-1), Application or service
Impact levels	C 4, I 4, A 4
Owner's reason	This is the only way members apply online, about 900 applications a month. Every application passes through it with name, date of birth, SIN and banking details, so a leak or a tampered form is a reportable privacy breach. An outage stops new lending intake until it is back.
Threat	T-A01 Misconfiguration (accidental)
Impact	4 High, set by confidentiality
Likelihood	Anchor 4 for this subject's exposure (Reachable from the internet); rated 4; deviation 0
Likelihood reason	The repository settings allow an administrator to merge and deploy their own pull request without a second reviewer enforcing the check, and the pipeline does not scan images before deployment; configuration controls are not fully enforced.
Safeguards relied on	None
Vulnerability	5 (Exposed)
Vulnerability reason	No safeguard listed for the Member loan application web app addresses misconfiguration; SG-1 and SG-2 as described operate at the perimeter and patching layer and have no bearing on configuration errors in the web app.
Safeguard bearing	No listed safeguard addresses this threat on this asset
Weakness described	None described
Unmitigated band	Very high
Current band	Very high (impact 4 against exposure 5)
Confidence	Unknown
Confidence reason	The safeguards listed for this asset were judged not to cover this pair; no evidence bears on the gap.
Evidence state	Assessed gap
Known exploited	None for this subject
Decision	Treat by Head of Lending (example), Business owner, on 2026-10-11
Target band	Medium
Plan	Introduce configuration baseline and change control across all assets. Action type: Remediation. Timeframe suggested: 30 days.

2. R-A-2-T-A01: Misconfiguration, on Loan application API

Asset	Loan application API (A-2), Application or service
Impact levels	C 4, I 5, A 4
Owner's reason	Every application record is written through this API, and it calls the credit bureau and the scoring model. A tampered request can change what is stored or what score comes back, which changes a lending decision. It carries the same member data as the web app, and intake stops if it is down.
Threat	T-A01 Misconfiguration (accidental)
Impact	5 Very high, set by integrity
Likelihood	Anchor 4 for this subject's exposure (Reachable from the internet); rated 4; deviation 0
Likelihood reason	An administrator can merge and deploy their own pull request without enforcement of peer review, and there is no specific check on fields sent to downstream services; the anchor applies and no mitigating controls beyond these are described.
Safeguards relied on	None
Vulnerability	5 (Exposed)
Vulnerability reason	No safeguard listed for the Loan application API addresses misconfiguration; SG-1, SG-2 and SG-3 as described have no bearing on configuration errors in the API.
Safeguard bearing	No listed safeguard addresses this threat on this asset
Weakness described	None described
Unmitigated band	Very high
Current band	Very high (impact 5 against exposure 5)
Confidence	Unknown
Confidence reason	The safeguards listed for this asset were judged not to cover this pair; no evidence bears on the gap.
Evidence state	Assessed gap
Known exploited	None for this subject
Decision	Treat by Head of Lending (example), Business owner, on 2026-10-11
Target band	High
Plan	Introduce configuration baseline and change control across all assets. Action type: Remediation. Timeframe suggested: 30 days.

3. R-A-2-T-D14: Abuse of exposed interface, on Loan application API

Asset	Loan application API (A-2), Application or service
Impact levels	C 4, I 5, A 4
Owner's reason	Every application record is written through this API, and it calls the credit bureau and the scoring model. A tampered request can change what is stored or what score comes back, which changes a lending decision. It carries the same member data as the web app, and intake stops if it is down.
Threat	T-D14 Abuse of exposed interface (deliberate)
Impact	5 Very high, set by integrity
Likelihood	Anchor 4 for this subject's exposure (Reachable from the internet); rated 5; deviation +1
Likelihood reason	The application status endpoint is reachable without authentication using only a guessable reference number, returns application status for any member, and on failed validation returns stack traces and internal table and service names; this is a confirmed open penetration test finding with no remediation date, no risk acceptance record, and no retest since May 2026, and Harbourline Credit Union has made no decision to restrict or authenticate the endpoint.
Relies on SG-1	A managed web application firewall with rate limiting sits in front of the web app and the API. Status: In place. Support: Unsupported. What would evidence it: A dated WAF configuration export or managed-service portal screenshot naming both the Member loan application web app and the Loan application API as protected origins, together with the rate-limiting rule set in force, would evidence this claim.
Vulnerability	4 (Weakly protected)
Vulnerability reason	SG-1 as described is only partly in place for the Loan application API, providing partial coverage against volumetric and pattern-based interface abuse, but the incomplete WAF coverage and absence of application-logic controls leave the API substantially exposed.
Safeguard bearing	A listed safeguard addresses this threat in part
Weakness described	SG-1 is only partly in place for the Loan application API, so WAF and rate-limiting coverage of exposed interface abuse is incomplete, and business-logic abuse is not addressed.
Unmitigated band	Very high
Current band	Very high (impact 5 against exposure 5)
Confidence	Claimed
Confidence reason	SG-1 is treated as partly in place for this asset: contradicted by an assurance input the organisation supplied (penetration test, 2026-05-20).
Evidence state	Claimed
Known exploited	None for this subject
Decision	Treat by Head of Lending (example), Business owner, on 2026-10-11
Target band	Medium
Plan	Enforce server-side authorisation on every API record request. Action type: Remediation. Timeframe suggested: 30 days.

Treatment plans

Each plan is one of two types. A remediation plan changes a control or the system. An assurance plan produces evidence, or verifies that a control already claimed operates as described; it raises confidence in a rating and does not by itself change the current band. The suggested owner is a role and the suggested timeframe follows the worst band the plan covers; the organisation assigns the owner and the target date in its decision.

1. [Remediation] Introduce configuration baseline and change control across all assets (suggested timeframe: 30 days)

6	3	9 risks: 6 very high, 3 high
Action	Define a documented security configuration baseline for each asset: the Member loan application web app (Node.js 20), the Loan application API, and the FortiGate 60F edge firewall. For the two applications, the baseline must cover HTTP security headers, disabled debug endpoints, dependency versions, environment variable handling and deployment pipeline settings. For the edge firewall, it must cover allowed management source addresses, VPN authentication settings and enabled services. Store each baseline in version control. Require that every change to a production configuration passes through a documented change record that names the change, the reviewer and the date before it is applied.	
Why	Misconfiguration and human error in operation are the primary vulnerability driver across the web app, the API and the edge firewall, all rated vulnerability 5. Neither the WAF (SG-1) nor the patch programme (SG-2) detects or prevents a misconfiguration introduced at deployment or through a manual change.	
Suggested owner	Platform engineering lead	
Treatment	treat	
Owner	Platform engineering lead	
Target date	2026-11-09	
Status	open	
Risks	R-A-1-T-A01, R-A-2-T-A01, R-A-2-T-A02, R-A-3-T-A01, R-C-1-T-A01, R-C-1-T-D02, R-A-1-T-A02, R-A-1-T-D02, R-A-3-T-A02	
Control ids	RW-TECH-021, RW-TECH-044, RW-CCM-085, RW-VM-030	

2. [Remediation] Implement redundancy, backup and recovery for all assets (suggested timeframe: 30 days)

3	8	11 risks: 3 very high, 8 high
Action	For the Loan application API and the Member loan application web app, deploy across at least two availability zones or regions so that a single hosting region failure does not take the service offline. Document the target recovery time and recovery point for each asset. For the FortiGate 60F edge firewall, document a failover procedure (secondary device or ISP failover) and test it at least once; retain the test record. For ransomware and destructive malware: deploy endpoint malware protection on the systems hosting the web app and the API; configure the edge firewall to block known malicious outbound destinations using Fortinet's threat intelligence feed.	
Why	Ransomware, denial of service, hosting region failure and third-party outage all affect availability across the edge firewall, the API and the web app. None of the current safeguards addresses availability or recovery. The edge firewall is a single point of failure for all internet traffic, and the API and web app have no documented failover.	
Suggested owner	Infrastructure and operations lead	

Treatment	treat
Owner	Infrastructure and operations lead
Target date	2026-11-09
Status	open
Risks	R-A-2-T-D03, R-A-3-T-D03, R-C-1-T-D07, R-A-1-T-D03, R-A-1-T-E01, R-A-2-T-E01, R-A-3-T-A04, R-A-3-T-D07, R-A-3-T-E01, R-C-1-T-A04, R-C-1-T-E01
Control ids	RW-TECH-026, RW-CP-037, RW-CP-038, RW-ORG-030, RW-TECH-019

3. [Remediation] Enforce MFA and least-privilege access across all systems (suggested timeframe: 30 days)

3	2	5 risks: 3 very high, 2 high
Action	Require multi-factor authentication for all administrative and privileged accounts on the Loan application API, the Member loan application web app and the FortiGate 60F edge firewall. For the edge firewall, disable password-only authentication for the management interface and VPN; enforce certificate or token-based MFA. For the two applications, enforce MFA for any account with deployment, database or configuration access. Conduct a role review for all accounts with access to loan application data: remove access that exceeds the role's stated need and document the resulting access matrix.	
Why	Credential theft and insider misuse carry very-high ratings on the Loan application API and the edge firewall. The WAF (SG-1) does not authenticate administrative users, and the patch programme (SG-2) does not limit what a compromised or malicious account can do once authenticated. MFA and least-privilege access are the direct controls for both threats.	
Suggested owner	Identity and access management lead	
Treatment	treat	
Owner	Identity and access management lead	
Target date	2026-11-09	
Status	open	
Risks	R-A-2-T-D01, R-A-2-T-D05, R-A-3-T-D01, R-A-1-T-D01, R-A-1-T-D05	
Control ids	RW-TECH-017, RW-TECH-014, RW-AC-129, RW-AC-128	

4. [Remediation] Enforce server-side authorisation on every API record request (suggested timeframe: 30 days)

2	2	4 risks: 2 very high, 2 high
Action	For every endpoint on the Loan application API that returns or modifies a loan application record, add a server-side ownership check that confirms the authenticated caller is entitled to that specific record before returning any data. Use unpredictable, non-sequential record identifiers (for example UUIDs) so that enumeration does not yield valid targets. Return only the fields the calling role requires; strip internal identifiers, bureau responses and model outputs from responses to member-facing calls. After the change is deployed, retest access from a second authenticated account to confirm that account A cannot retrieve or modify account B's records.	
Why	Rate limiting and TLS (SG-1 and SG-3) slow enumeration but do not stop an authenticated caller from requesting records that belong to another member. Without a per-request ownership check, bulk exfiltration of member PII and banking details is possible through the API, which carries the highest impact rating in this assessment.	
Suggested owner	API development lead	
Treatment	treat	

Owner	API development lead
Target date	2026-11-09
Status	open
Risks	R-A-2-T-D14, R-C-1-T-D14, R-A-2-T-D04, R-C-1-T-D04
Control ids	RW-AC-129, RW-TECH-014, RW-TECH-024

5. [Remediation] Establish secure development and pre-release testing for software defects (suggested timeframe: 30 days)

2	1	3 risks: 2 very high, 1 high
Action	Define and document secure coding standards for the Loan application API and the Member loan application web app, covering input validation, output encoding, error handling, session management and data isolation between users. Integrate automated static analysis and dependency vulnerability scanning into the build pipeline for both applications so that every pull request is checked before merge. Add integration tests that assert one authenticated user cannot read another user's data (cross-account isolation). Require that a security test report covering these checks is produced and retained for every production release.	
Why	No safeguard currently addresses software defects on the Loan application API, the web app or the connection between them. A bug that leaks data between users or corrupts loan application records carries a very-high impact rating on the API. Pre-release testing is the primary control because defects must be caught before they reach production.	
Suggested owner	Software engineering lead	
Treatment	treat	
Owner	Software engineering lead	
Target date	2026-11-09	
Status	open	
Risks	R-A-2-T-A03, R-C-1-T-A03, R-A-1-T-A03	
Control ids	RW-TECH-040, RW-TECH-041, RW-TECH-037	

6. [Remediation] Restore 14-day patch cycle on edge firewall (suggested timeframe: 30 days)

2	2 risks: 2 very high	
Action	Apply all outstanding Fortinet FortiOS security updates to the FortiGate 60F immediately. The 'vulnerability scan dated 2026-08-12' found that the edge firewall is running FortiOS 7.0.12 and has not been updated since 2023, leaving it more than 12 months overdue; close those four open findings by bringing the device to the current supported release. Once current, set a documented 14-day maximum window between a Fortinet security advisory and patch application, enforced through a scheduled maintenance task.	
Why	SG-2 is recorded as absent for the edge firewall. The vulnerability scan confirms the device is critically out of date. An unpatched FortiOS at the network edge is directly exploitable via published CVEs and exposes the remote management and VPN interfaces to unauthorised access, driving both the exploitation and exposed-interface risks to very-high band.	
Suggested owner	Network infrastructure lead	
Treatment	treat	
Owner	Network infrastructure lead	
Target date	2026-11-09	
Status	open	
Risks	R-A-3-T-D02, R-A-3-T-D14	

Control ids

RW-TECH-020, RW-VM-030

7. [Remediation] Control and monitor third-party and supply chain dependencies (suggested timeframe: 30 days)

1	3	4 risks: 1 very high, 3 high
Action	Produce a dependency inventory for the Loan application API and the Member loan application web app listing every third-party library, build tool and external service they rely on, including the Node.js runtime and any npm packages. Subscribe to the relevant security advisory feeds (Node.js security releases, npm audit, Fortinet PSIRT) and assign a named role to act on each advisory within the 14-day window already stated in SG-2. For the FortiGate 60F, verify that firmware updates are sourced only from Fortinet's authenticated update channel and that the update integrity check is enabled.	
Why	Supply chain compromise carries a very-high rating on the connection and high ratings on the API and the edge firewall. No current safeguard addresses the integrity of third-party components or the continuity obligations of external providers. The Loan application API calls a credit bureau and a model endpoint, making third-party dependency a direct operational risk.	
Suggested owner	Technology risk lead	
Treatment	treat	
Owner	Technology risk lead	
Target date	2026-11-09	
Status	open	
Risks	R-C-1-T-D06, R-A-2-T-D06, R-A-3-T-D06, R-C-1-T-E03	
Control ids	RW-ORG-019, RW-ORG-022, RW-AIRMF-019, RW-RA-035	

8. [Remediation] Complete WAF coverage and rate limiting for the API (suggested timeframe: 30 days)

1	1	2 risks: 1 very high, 1 high
Action	Extend the managed WAF so that the Loan application API is a named protected origin with rate-limiting rules applied, closing the gap the customer's own answer identifies. The 'penetration test dated 2026-05-20' found a missing rate limit on the application status endpoint and verbose error messages as open findings; close both by configuring a per-IP and per-session request limit on that endpoint and suppressing stack traces and internal identifiers from all API error responses. Confirm that the WAF rule set covers the API's authenticated and unauthenticated routes, not only the web front end.	
Why	SG-1 is partly in place for the Loan application API: the WAF exists but the customer's answer records it does not fully cover the API, and the penetration test confirms the rate-limit gap.	
Suggested owner	Application security lead	
Treatment	treat	
Owner	Application security lead	
Target date	2026-11-09	
Status	open	
Risks	R-A-2-T-D02, R-A-2-T-D07	
Also acts on	R-A-2-T-D01, R-A-2-T-D03, R-A-2-T-D14, R-A-2-T-D04 (their own plan is another one)	
Control ids	RW-TECH-032, RW-TECH-033, RW-VM-030	

9. [Remediation] Manage and monitor TLS certificates and firewall credentials (suggested timeframe: 90 days)

2

2 risks: 2 high

Action	Produce an inventory of every certificate and credential used by the FortiGate 60F (VPN certificates, management interface certificate, pre-shared keys) and every TLS certificate used on the Member loan application web app to Loan application API connection. For each entry, record the expiry date, the renewal owner and the renewal lead time. Configure automated expiry alerts at least 30 days before each certificate or credential expires. For the edge firewall, store the VPN and management credentials in a secrets manager or password vault rather than in a shared document; rotate any credential that has not been rotated in the past 12 months.
Why	Loss of access to keys or credentials carries a high rating on both the edge firewall and the web app to API connection. The TLS certificate on the connection is the primary confidentiality and integrity control for member PII in transit; if it expires unnoticed the connection fails or falls back to an insecure state. No current safeguard tracks certificate or credential expiry on either asset.
Suggested owner	Platform engineering lead
Treatment	treat
Owner	Platform engineering lead
Target date	2027-01-08
Status	open
Risks	R-A-3-T-A10, R-C-1-T-A10
Control ids	RW-TECH-036, RW-AC-128

10. [Remediation] Schedule and test FortiGate configuration backups (suggested timeframe: 90 days)

1

1 risk: 1 high

Action	Configure the FortiGate 60F to export its full configuration automatically after every change and on a weekly schedule, storing the export in a location that is not on the device itself and is not reachable from the internet. Perform a restore test from the most recent backup to a test or staging device and record the outcome, the date and the role that conducted the test. Set a calendar reminder to repeat the restore test at least every six months. Retain the backup completion log and the restore test record as evidence.
Why	No safeguard covers backup or recovery failure for the edge firewall. The FortiGate 60F is a single managed appliance; if its configuration is lost through a destructive attack or hardware failure and no tested backup exists, recovery time is indeterminate. The vulnerability rating of 5 reflects the complete absence of this control.
Suggested owner	Network infrastructure lead
Treatment	treat
Owner	Network infrastructure lead
Target date	2027-01-08
Status	open
Risks	R-A-3-T-A09
Control ids	RW-TECH-025, RW-CP-037, RW-CP-038

11. [Remediation] Apply data leakage prevention to the web app (suggested timeframe: 90 days)

1

1 risk: 1 high

Action	Review every response the Member loan application web app sends to a browser and confirm that it returns only the fields the member's own session is entitled to see. Remove any endpoint or page that returns bulk record sets to an authenticated user beyond what their role requires. Add server-side controls that prevent a single session from downloading more than a defined number of records in a rolling time window, and log any breach of that threshold as a security event. Retain the review record and the logging configuration as evidence.
Why	SG-1 (the WAF) is in place for the Member loan application web app but rate limiting does not prevent a logged-in user from systematically copying records they are entitled to view one at a time. Data exfiltration by an insider or a compromised account requires a server-side volume control and audit trail that the WAF cannot provide.
Suggested owner	Application security lead
Treatment	treat
Owner	Application security lead
Target date	2027-01-08
Status	open
Risks	R-A-1-T-D04
Also acts on	R-A-2-T-D04, R-C-1-T-D04 (their own plan is another one)
Control ids	RW-TECH-024, RW-AC-129

12. [Remediation] Restrict and audit exposed endpoints on the web app (suggested timeframe: 90 days)

1

1 risk: 1 high

Action	Enumerate every route and endpoint served by the Member loan application web app that is reachable without authentication or with a low-privilege session. Disable or remove any admin panel, debug route, health endpoint or status page that does not need to be public. For endpoints that must remain accessible, confirm that authentication and authorisation checks are enforced at the server before any data is returned. Enable access logging on all routes and set up an alert for repeated requests to administrative or non-public paths from external addresses. Retain the endpoint inventory, the change record and the alert configuration as evidence.
Why	SG-1 is in place for the Member loan application web app but a WAF does not remove an endpoint from the application; it can only filter traffic in front of it. An exposed admin panel or debug route that exists in the application remains reachable if the WAF rule is misconfigured or bypassed. The direct control is to remove or gate the endpoint at the application layer.
Suggested owner	Application security lead
Treatment	treat
Owner	Application security lead
Target date	2027-01-08
Status	open
Risks	R-A-1-T-D14
Also acts on	R-C-1-T-D14 (their own plan is another one)
Control ids	RW-TECH-021, RW-VM-031

Acceptance and release

Role	Name	Title	Accepted	Signed in as	Note
Business owner	Head of Lending (example)	Business owner, Member Lending	2026-10-11	Withheld in this specimen	I accept the scope, the classification and the treatment plans. The five targets left at high need a further decision once their plans are done.
Business owner	Head of Lending (example)	Business owner, Member Lending	2026-10-11	Withheld in this specimen	
Security reviewer	IT Manager (example)	Security reviewer	2026-10-11	Withheld in this specimen	I agree with the scope and the risk ratings.

Release check

The release check passed and the assessment was released on 2026-10-11.

Appendix A. Known exploited vulnerabilities

Version confirmed affected: the stated version is inside a published affected range. Product match, version unconfirmed: the product matches and the version was not stated or could not be checked, so the organisation is potentially affected. Ruled out by stated version: the stated version is outside every affected range; listed for the record and not counted as a match.

CISA Known Exploited Vulnerabilities catalog, retrieved 2026-10-10; matched 2026-10-10; 4 matching entries; 11 ruled out by the stated version.

Source: CISA Known Exploited Vulnerabilities catalog, retrieved 2026-10-10T06:01:55.835Z

Asset	CVE	Product	Name	Added	EPSS	Ransomware	Verdict
Edge firewall	CVE-2025-68686	Fortinet FortiOS	Fortinet FortiOS Exposure of Sensitive Information to an Unauthorized Actor Vulnerability	2026-07-27	Not scored	Not known	Version confirmed affected
Edge firewall	CVE-2019-6693	Fortinet FortiOS	Fortinet FortiOS Use of Hard-Coded Credentials Vulnerability	2025-06-25	Not scored	Known	Ruled out by stated version
Edge firewall	CVE-2025-24472	Fortinet FortiOS and FortiProxy	Fortinet FortiOS and FortiProxy Authentication Bypass Vulnerability	2025-03-18	Not scored	Known	Version confirmed affected
Edge firewall	CVE-2024-55591	Fortinet FortiOS and FortiProxy	Fortinet FortiOS and FortiProxy Authentication Bypass Vulnerability	2025-01-14	Not scored	Known	Version confirmed affected
Edge firewall	CVE-2024-21762	Fortinet FortiOS	Fortinet FortiOS Out-of-Bound Write Vulnerability	2024-02-09	Not scored	Known	Version confirmed affected
Edge firewall	CVE-2023-27997	Fortinet FortiOS and FortiProxy SSL-VPN	Fortinet FortiOS and FortiProxy SSL-VPN Heap-Based Buffer Overflow Vulnerability	2023-06-13	Not scored	Known	Ruled out by stated version
Edge firewall	CVE-2022-41328	Fortinet FortiOS	Fortinet FortiOS Path Traversal Vulnerability	2023-03-14	Not scored	Not known	Ruled out by stated version
Edge firewall	CVE-2022-42475	Fortinet FortiOS	Fortinet FortiOS Heap-Based Buffer Overflow Vulnerability	2022-12-13	Not scored	Known	Ruled out by stated version
Edge firewall	CVE-2018-13374	Fortinet FortiOS and FortiADC	Fortinet FortiOS and FortiADC Improper Access Control Vulnerability	2022-09-08	Not scored	Known	Ruled out by stated version
Edge firewall	CVE-2018-13382	Fortinet FortiOS and FortiProxy	Fortinet FortiOS and FortiProxy Improper Authorization	2022-01-10	Not scored	Known	Ruled out by stated version
Edge firewall	CVE-2018-13383	Fortinet FortiOS and FortiProxy	Fortinet FortiOS and FortiProxy Out-of-bounds Write	2022-01-10	Not scored	Known	Ruled out by stated version
Edge firewall	CVE-2021-44168	Fortinet FortiOS	Fortinet FortiOS Arbitrary File Download	2021-12-10	Not scored	Not known	Ruled out by stated version

Asset	CVE	Product	Name	Added	EPSS	Ransomware	Verdict
Edge firewall	CVE-2018-13379	Fortinet FortiOS	Fortinet FortiOS SSL VPN Path Traversal Vulnerability	2021-11-03	Not scored	Known	Ruled out by stated version
Edge firewall	CVE-2019-5591	Fortinet FortiOS	Fortinet FortiOS Default Configuration Vulnerability	2021-11-03	Not scored	Known	Ruled out by stated version
Edge firewall	CVE-2020-12812	Fortinet FortiOS	Fortinet FortiOS SSL VPN Improper Authentication Vulnerability	2021-11-03	Not scored	Known	Ruled out by stated version

Appendix B. Claims and stated unknowns

Claims ledger

Claim	Status	Statement	Round	Note
SG-2 holds for the web app and the API only; the edge firewall has not been patched since 2023 and remains outside the 14-day policy in practice.	clear	Your answer to question 8 (round 1)		Confirms and extends the contradiction already recorded for SG-2 against A-3. The customer's own words confirm the firewall is excluded from the 14-day patching policy in practice.
AWS WAF is attached to the application load balancer in front of the web app and the API, managed day to day by Harbourline's internal IT team.	clear	Your answer to question 2 (round 1)		Specific product, attachment point and managing team are all named.
Neither open penetration test finding has been remediated, tracked, risk-accepted or retested since May 2026.	clear	Your answer to question 3 (round 1)	3	Unambiguous statement covering both findings.
The Loan application API runs Node.js 20.11.0 in a container on Amazon ECS with Fargate in ca-central-1; the Node.js version has been pinned since January 2024 and release advisories have not been reviewed since then.	clear	Your answer to question 4 (round 1)	3	Runtime, version, hosting platform, region and advisory review gap are all stated specifically.
The FortiGate management interface is reachable from the internet over HTTPS from any source address, with no allowlist, VPN requirement or intrusion prevention rule in front of it.	clear	Your answer to question 6 (round 1)	3	Exposure is stated precisely and completely.
Two of the three FortiGate administrator accounts use FortiToken MFA; the third is a shared local emergency account with no MFA and a password unchanged since before 2024.	clear	Your answer to question 7 (round 1)	3	Account count, MFA status and credential age are all stated specifically.
The FortiGate keeps its default local event log; there is no alerting on authentication attempts and no one reviews the log on a schedule.	clear	Your answer to question 10 (round 2)		Logging capability and review absence are stated without ambiguity.
There is no plan to disable or rotate the shared FortiGate emergency account.	clear	Your answer to question 11 (round 2)		Unambiguous statement. Whether the former provider still holds the password is recorded as unknown per partlyNotKnown.
None of the four firewall scan findings has been formally risk-accepted; they are simply unaddressed with no risk acceptance record.	clear	Your answer to question 12 (round 2)		Unambiguous statement covering all four findings.

Claim	Status	Statement	Round	Note
The application status endpoint is the only API path not covered by the rate-based rule; it can be called without sign-in using only a guessable reference number, and on failed validation it returns stack traces and internal table and service names.	clear	Your answer to question 13 (round 2)	3	Endpoint exposure, authentication requirement, reference format and error disclosure are all stated specifically.
Only the three IT administrators have standing access to the AWS account; on the FortiGate, only the three administrator accounts exist, one of which is the shared emergency account.	clear	Your answer to question 14 (round 2)		Access scope for both platforms is stated without ambiguity.
Changes to the API go through pull requests reviewed by one of the other two administrators, but there is no specific check on the fields sent to the credit bureau or the pre-screening model.	clear	Your answer to question 15 (round 2)	3	Change-control process and its gap are both stated specifically.
The AWS account holds only the web app, the API, their load balancer and WAF; no other Harbourline systems share it.	clear	Your answer to question 16 (round 2)		Account scope is stated specifically. The account ID was withheld, which is not required for the assessment.
There is no remediation plan for the edge firewall; none of its four scan findings has an owner or a target date.	clear	Your answer to question 1 (round 1)	3	Absence of plan, ownership and scheduling is stated without ambiguity.
The outbound API connections to the credit bureau and the pre-screening model are outside this assessment boundary; the fields sent are controlled only by the API code with no separate written interface specification inside the boundary.	clear	Your answer to question 5 (round 1)		Boundary position and control mechanism are both stated specifically.
No one has checked Node.js 20 security advisories issued since January 2024 against the web app or the API.	clear	Your answer to question 9 (round 2)		Advisory review gap is stated unambiguously. Whether any advisories are unaddressed is recorded as unknown per partlyNotKnown.
A managed web application firewall with rate limiting sits in front of the web app and the API.	contradicted	Safeguard SG-1	1	Contradicted by an assurance input the organisation supplied (penetration test, 2026-05-20); treated as partly in place for A-2, and as stated for the other assets it names. The customer's answer (question 2) names no evidence item against that: "AWS WAF, attached to the application load balancer in front of the web app and the API. Our internal IT team manages the rules day to day. The rate-based rule covers the web app paths; the API's application status endpoint is not covered..."
Every internet-facing system, including the edge firewall, is patched within 14 days of a vendor security release.	contradicted	Safeguard SG-2	1	Contradicted by an assurance input the organisation supplied (vulnerability scan, 2026-08-12); treated as not in place for A-3, and as stated for the other assets it names. The customer's answer (question 1) names no evidence item against that: "There is no remediation plan for the edge firewall. None of its four scan findings has an owner or a target date; all four are unscheduled. The 14-day policy applies to the web app and the API, which are rebuilt monthly; it has not been..."

Claim	Status	Statement	Round	Note
The scan covered connections to the Credit bureau API and the Lendwise AI pre-screening model, which are declared out of scope.	clear	The attached evidence "TLS and network path scan of the Member Lending Portal components, 2 September 2026"	1	Your answer to question 5 confirms those outbound connections are outside this boundary: 'No. The outbound connections from the API to the credit bureau and the pre-screening model are outside this boundary and are covered by the full portal assessment.'
The Loan application API calls the bureau and the model.	clear	Loan application API	1	Your answer to question 5 confirms the API makes those calls but they are out of scope. Your answer to question 4 clarifies the runtime: 'The API is a Node.js 20.11.0 service in a container on Amazon ECS with Fargate in ca-central-1.'
The lending database, the staff console, the credit bureau link, the pre-screening model, the mail server and the backup appliance are deliberately out of scope.	clear	The scope answer "What is deliberately out of scope"		Your answer to question 5 confirms the credit bureau and pre-screening model connections are outside this boundary. The remaining items are not contradicted by any supplied statement.
The edge firewall has not been patched since 2023 and patching is more than 12 months overdue.	open finding	The vulnerability scan, 2026-08-12	1	The finding stands and stays open until it is fixed; a contradiction withdraws the safeguard it disproves, not the finding. It is what contradicts SG-2: Contradicted by an assurance input the organisation supplied (vulnerability scan, 2026-08-12); treated as not in place for A-3, and as stated for the other assets it names. The statement was contradicted and the customer's answer (question 8) names no evidence item against that: "The scan is correct. The firewall still runs FortiOS 7.0.12, has not been updated since 2023, and is outside the 14-day patching in practice. SG-2 holds for the web app and the API only."
A rate limit is missing on the application status endpoint.	open finding	The penetration test, 2026-05-20	1	The finding stands and stays open until it is fixed; a contradiction withdraws the safeguard it disproves, not the finding. It is what contradicts SG-1: Contradicted by an assurance input the organisation supplied (penetration test, 2026-05-20); treated as partly in place for A-2, and as stated for the other assets it names. The statement was contradicted and the customer's answer (question 3) names no evidence item against that: "Neither finding has been remediated and neither is tracked. There is no remediation date, no risk acceptance record, and no retest since May 2026."

Claim	Status	Statement	Round	Note
The connection between the web app and the API uses TLS 1.2 or later.	clear	Safeguard SG-3		The TLS scan (the attached evidence "TLS and network path scan of the Member Lending Portal components, 2 September 2026") confirms: 'The Member loan application web app and the Loan application API accept TLS 1.2 and TLS 1.3 only; TLS 1.0 and 1.1 handshakes were refused.'
The assessment boundary includes the link between the web app and the API.	clear	The scope answer "What is inside the assessment boundary"		The boundary is specific: four named components. The TLS scan confirms the link exists and is tested.
The web app and API run in an AWS account in the ca-central-1 region.	clear	The scope answer "Where it runs and who hosts it"		Region and provider are named. AWS is listed as a required inventory topic (R-inventory) because it is not in the asset list.
The FortiGate 60F has remote management and VPN enabled.	clear	Edge firewall	1	Product model, location and two enabled services are named. AI-1 corroborates the version (FortiOS 7.0.12) and the scan evidence notes the management interface accepts TLS 1.1.
Members submit social insurance numbers and banking details through the web app.	clear	The scope answer "What data moves in, through and out"		Data categories, direction and transport are all named. This is specific and checkable.

Stated unknowns

None recorded.

Safeguards contradicted by the organisation's own inputs; confidence is lowered for the assets named

Safeguard as claimed	Statement
A managed web application firewall with rate limiting sits in front of the web app and the API.	Safeguard SG-1
Every internet-facing system, including the edge firewall, is patched within 14 days of a vendor security release.	Safeguard SG-2

Appendix C. Category waivers

None recorded.

Appendix D. Threats ruled out

Threats that apply to a subject's kind and were not rated. "AI architecture" means code ruled the threat out from how the organisation said the AI works; "Threat assessment" means the assessment ruled it out and gave the reason shown.

No threat was ruled out for a subject.

Appendix E. Examiner questions

Round	Questions asked	Answered
1		8
2		8
3		7
Total	23	23

Appendix F. Why each vulnerability and confidence

Risk	V	Why this vulnerability	Confidence	Why this confidence
R-A-1-T-A01	5	No safeguard listed for the Member loan application web app addresses misconfiguration; SG-1 and SG-2 as described operate at the perimeter and patching layer and have no bearing on configuration errors in the web app.	Unknown	The safeguards listed for this asset were judged not to cover this pair; no evidence bears on the gap.
R-A-2-T-A01	5	No safeguard listed for the Loan application API addresses misconfiguration; SG-1, SG-2 and SG-3 as described have no bearing on configuration errors in the API.	Unknown	The safeguards listed for this asset were judged not to cover this pair; no evidence bears on the gap.
R-A-2-T-A02	5	No safeguard listed for the Loan application API addresses human error in operation; SG-1, SG-2 and SG-3 as described have no bearing on mistakes made by staff managing or operating the API.	Unknown	The safeguards listed for this asset were judged not to cover this pair; no evidence bears on the gap.
R-A-2-T-A03	5	No safeguard listed for the Loan application API addresses software defects in its own codebase; SG-1, SG-2 and SG-3 as described have no bearing on internally introduced bugs.	Unknown	The safeguards listed for this asset were judged not to cover this pair; no evidence bears on the gap.
R-A-2-T-D01	4	SG-1 as described is only partly in place for the Loan application API, providing some rate-limiting coverage against credential-stuffing, but authentication controls on the API itself are not addressed by any listed safeguard.	Claimed	SG-1 is treated as partly in place for this asset: contradicted by an assurance input the organisation supplied (penetration test, 2026-05-20).
R-A-2-T-D02	3	SG-2 as described patches the Loan application API within 14 days of a vendor release, and SG-1 as described provides partial WAF coverage, together reducing exposure to known vulnerabilities, though the partial WAF and patching window leave some residual risk.	Claimed	No evidence was attached for SG-2, which the rating relies on. SG-1 is treated as partly in place for this asset: contradicted by an assurance input the organisation supplied (penetration test, 2026-05-20).
R-A-2-T-D03	4	SG-1 as described is only partly in place for the Loan application API and may block some web-delivered malware, but ransomware reaching the API host through other vectors is not addressed by any listed safeguard.	Claimed	SG-1 is treated as partly in place for this asset: contradicted by an assurance input the organisation supplied (penetration test, 2026-05-20).
R-A-2-T-D05	5	No safeguard listed for the Loan application API addresses insider misuse of access; SG-1, SG-2 and SG-3 as described operate at the perimeter, patching and transport layers and have no bearing on what an authorised user does once they have access.	Unknown	The safeguards listed for this asset were judged not to cover this pair; no evidence bears on the gap.

Risk	V	Why this vulnerability	Confidence	Why this confidence
R-A-2-T-D14	4	SG-1 as described is only partly in place for the Loan application API, providing partial coverage against volumetric and pattern-based interface abuse, but the incomplete WAF coverage and absence of application-logic controls leave the API substantially exposed.	Claimed	SG-1 is treated as partly in place for this asset: contradicted by an assurance input the organisation supplied (penetration test, 2026-05-20).
R-A-3-T-A01	5	No safeguard is counted for the Edge firewall against misconfiguration; SG-2 is not in place for this asset and patching does not address configuration errors.	Unknown	SG-2 was claimed for this asset and contradicted by an assurance input the organisation supplied (vulnerability scan, 2026-08-12), so what protects the asset is not established.
R-A-3-T-D01	5	No safeguard is counted for the Edge firewall against credential theft and account takeover; SG-2 is not in place for this asset.	Unknown	SG-2 was claimed for this asset and contradicted by an assurance input the organisation supplied (vulnerability scan, 2026-08-12), so what protects the asset is not established.
R-A-3-T-D02	5	No safeguard is counted for the Edge firewall against exploitation of a publicly known vulnerability; SG-2, which would directly address this threat by patching the firewall, is not in place for this asset.	Unknown	SG-2 was claimed for this asset and contradicted by an assurance input the organisation supplied (vulnerability scan, 2026-08-12), so what protects the asset is not established.
R-A-3-T-D03	5	No safeguard is counted for the Edge firewall against ransomware and destructive malware; SG-2 is not in place for this asset and would not directly address ransomware execution in any case.	Unknown	SG-2 was claimed for this asset and contradicted by an assurance input the organisation supplied (vulnerability scan, 2026-08-12), so what protects the asset is not established.
R-A-3-T-D14	5	No safeguard is counted for the Edge firewall against abuse of an exposed interface; SG-2 is not in place for this asset, and keeping the firewall patched would reduce the attack surface on its management interface.	Unknown	SG-2 was claimed for this asset and contradicted by an assurance input the organisation supplied (vulnerability scan, 2026-08-12), so what protects the asset is not established.
R-C-1-T-A01	5	TLS configuration on the connection between the web app and the API does not prevent misconfiguration of either component or of the connection itself, so no safeguard is counted for this threat.	Unknown	The safeguards listed for this asset were judged not to cover this pair; no evidence bears on the gap.
R-C-1-T-A03	5	TLS secures the transport layer but does not detect or prevent software defects in the web app or the API, so no safeguard is counted for this threat.	Unknown	The safeguards listed for this asset were judged not to cover this pair; no evidence bears on the gap.
R-C-1-T-D02	5	TLS on the connection between the web app and the API encrypts traffic in transit but does not patch or mitigate publicly known vulnerabilities in either component, so no safeguard is counted for this threat on this connection.	Unknown	The safeguards listed for this asset were judged not to cover this pair; no evidence bears on the gap.
R-C-1-T-D06	5	TLS secures the transport layer between the two components but does not detect or prevent a supply chain compromise affecting either the web app or the API, so no safeguard is counted for this threat.	Unknown	The safeguards listed for this asset were judged not to cover this pair; no evidence bears on the gap.
R-C-1-T-D07	5	TLS on the connection between the web app and the API does not limit request volume or protect availability, so no safeguard is counted against denial of service on this connection.	Unknown	The safeguards listed for this asset were judged not to cover this pair; no evidence bears on the gap.
R-C-1-T-D14	5	TLS encrypts the channel but does not restrict or validate how the API interface is used, so no safeguard is counted against abuse of the exposed interface.	Unknown	The safeguards listed for this asset were judged not to cover this pair; no evidence bears on the gap.

Risk	V	Why this vulnerability	Confidence	Why this confidence
R-A-1-T-A02	5	No safeguard listed for the Member loan application web app addresses human error in operation; SG-1 and SG-2 as described have no bearing on mistakes made by staff managing or operating the web app.	Unknown	The safeguards listed for this asset were judged not to cover this pair; no evidence bears on the gap.
R-A-1-T-A03	5	No safeguard listed for the Member loan application web app addresses software defects in its own codebase; SG-1 and SG-2 as described have no bearing on internally introduced bugs.	Unknown	The safeguards listed for this asset were judged not to cover this pair; no evidence bears on the gap.
R-A-1-T-D01	4	SG-1 as described places rate limiting in front of the Member loan application web app, which reduces the volume of credential-stuffing attempts, but the WAF does not govern authentication strength or session controls, leaving the web app substantially exposed to account takeover.	Claimed	No evidence was attached for SG-1, which the rating relies on.
R-A-1-T-D02	3	SG-2 as described closes known vulnerabilities within 14 days of a vendor release, and SG-1 as described provides a WAF layer that can block known exploit patterns, together giving partial layered protection, though a window remains between disclosure and patching.	Claimed	No evidence was attached for SG-1, SG-2, which the rating relies on.
R-A-1-T-D03	4	SG-1 as described provides a WAF in front of the Member loan application web app that may block some web-delivered malware, but ransomware reaching the host through other means is not addressed by either listed safeguard.	Claimed	No evidence was attached for SG-1, which the rating relies on.
R-A-1-T-D04	4	SG-1 as described sits in front of the web app and may block some injection-based exfiltration paths, but outbound exfiltration channels are not addressed by either listed safeguard.	Claimed	No evidence was attached for SG-1, which the rating relies on.
R-A-1-T-D05	5	No safeguard listed for the Member loan application web app addresses insider misuse of access; SG-1 and SG-2 as described operate at the network and patching layer and have no bearing on what an authorised user does once signed in.	Unknown	The safeguards listed for this asset were judged not to cover this pair; no evidence bears on the gap.
R-A-1-T-D14	3	SG-1 as described places a WAF with rate limiting in front of the Member loan application web app, which addresses volumetric and pattern-based abuse of exposed interfaces, though application-logic abuse is not covered.	Claimed	No evidence was attached for SG-1, which the rating relies on.
R-A-1-T-E01	5	No safeguard listed for the Member loan application web app addresses a hosting region failure; SG-1 and SG-2 as described have no bearing on availability when the underlying hosting infrastructure is unavailable.	Unknown	The safeguards listed for this asset were judged not to cover this pair; no evidence bears on the gap.
R-A-2-T-D04	4	SG-3 as described encrypts the connection between the web app and the Loan application API, reducing interception risk, and SG-1 as described provides partial inbound filtering, but outbound exfiltration from the API is not addressed.	Claimed	SG-1 is treated as partly in place for this asset: contradicted by an assurance input the organisation supplied (penetration test, 2026-05-20).

Risk	V	Why this vulnerability	Confidence	Why this confidence
R-A-2-T-D06	4	SG-2 as described reduces the window during which a known-compromised component remains unpatched on the Loan application API, but upstream supply chain compromise through a dependency or build process is not otherwise addressed.	Claimed	No evidence was attached for SG-2, which the rating relies on.
R-A-2-T-D07	4	SG-1 as described is only partly in place for the Loan application API, providing partial rate-limiting coverage against application-layer denial of service, but the incomplete coverage and absence of network-layer protection leave significant residual exposure.	Claimed	SG-1 is treated as partly in place for this asset: contradicted by an assurance input the organisation supplied (penetration test, 2026-05-20).
R-A-2-T-E01	5	No safeguard listed for the Loan application API addresses a hosting region failure; SG-1, SG-2 and SG-3 as described have no bearing on availability when the underlying hosting infrastructure is unavailable.	Unknown	The safeguards listed for this asset were judged not to cover this pair; no evidence bears on the gap.
R-A-3-T-A02	5	No safeguard is counted for the Edge firewall against human error in operation; SG-2 is not in place for this asset and patching does not address operator mistakes.	Unknown	SG-2 was claimed for this asset and contradicted by an assurance input the organisation supplied (vulnerability scan, 2026-08-12), so what protects the asset is not established.
R-A-3-T-A04	5	No safeguard is counted for the Edge firewall against a third-party outage; SG-2 is not in place for this asset and patching has no bearing on third-party availability.	Unknown	SG-2 was claimed for this asset and contradicted by an assurance input the organisation supplied (vulnerability scan, 2026-08-12), so what protects the asset is not established.
R-A-3-T-A09	5	No safeguard is counted for the Edge firewall against backup or recovery failure; SG-2 is not in place for this asset and patching has no bearing on backup integrity or recoverability.	Unknown	SG-2 was claimed for this asset and contradicted by an assurance input the organisation supplied (vulnerability scan, 2026-08-12), so what protects the asset is not established.
R-A-3-T-A10	5	No safeguard is counted for the Edge firewall against loss of access to keys or credentials; SG-2 is not in place for this asset and patching has no bearing on key or credential management.	Unknown	SG-2 was claimed for this asset and contradicted by an assurance input the organisation supplied (vulnerability scan, 2026-08-12), so what protects the asset is not established.
R-A-3-T-D06	5	No safeguard is counted for the Edge firewall against supply chain compromise; SG-2 is not in place for this asset and would only partially address this threat.	Unknown	SG-2 was claimed for this asset and contradicted by an assurance input the organisation supplied (vulnerability scan, 2026-08-12), so what protects the asset is not established.
R-A-3-T-D07	5	No safeguard is counted for the Edge firewall against denial of service; SG-2 is not in place for this asset and patching does not address volumetric or protocol-level denial of service.	Unknown	SG-2 was claimed for this asset and contradicted by an assurance input the organisation supplied (vulnerability scan, 2026-08-12), so what protects the asset is not established.
R-A-3-T-E01	5	No safeguard is counted for the Edge firewall against a hosting region failure; SG-2 is not in place for this asset and patching has no bearing on availability when the hosting infrastructure fails.	Unknown	SG-2 was claimed for this asset and contradicted by an assurance input the organisation supplied (vulnerability scan, 2026-08-12), so what protects the asset is not established.
R-C-1-T-A04	5	TLS on the connection between the web app and the API does not maintain availability when a third-party provider experiences an outage, so no safeguard is counted for this threat.	Unknown	The safeguards listed for this asset were judged not to cover this pair; no evidence bears on the gap.

Risk	V	Why this vulnerability	Confidence	Why this confidence
R-C-1-T-A10	5	TLS secures data in transit but does not manage, rotate or recover keys or credentials used by the web app or the API, so no safeguard is counted for this threat.	Unknown	The safeguards listed for this asset were judged not to cover this pair; no evidence bears on the gap.
R-C-1-T-D04	3	TLS 1.2 or later as described encrypts the connection, making passive interception of data in transit harder, but it does not address exfiltration that originates from within either endpoint or that uses an alternative path.	Verified	Every safeguard the rating relies on is supported by attached evidence: SG-3.
R-C-1-T-E01	5	TLS on the connection between the web app and the API does not provide redundancy or failover if the hosting region fails, so no safeguard is counted for this threat.	Unknown	The safeguards listed for this asset were judged not to cover this pair; no evidence bears on the gap.
R-C-1-T-E03	5	TLS on the connection between the web app and the API does not protect against a provider withdrawing service or changing terms, so no safeguard is counted for this threat.	Unknown	The safeguards listed for this asset were judged not to cover this pair; no evidence bears on the gap.
R-A-1-T-D06	4	SG-2 as described reduces the window during which a known-compromised component remains unpatched on the Member loan application web app, but supply chain compromise through an upstream dependency or build process is not otherwise addressed.	Claimed	No evidence was attached for SG-2, which the rating relies on. To be verified by 2026-12-31: Attach the build log showing the last two monthly image builds of the web app and its dependency versions.
R-A-1-T-D07	3	SG-1 as described places a managed WAF with rate limiting in front of the Member loan application web app, which directly addresses application-layer denial of service, though network-layer volumetric attacks upstream of the WAF remain outside its scope.	Claimed	No evidence was attached for SG-1, which the rating relies on. To be verified by 2026-12-31: Export the AWS WAF rate-based rule configuration showing the web app paths it covers.
R-C-1-T-A11	3	TLS as described provides server authentication on the connection between the web app and the API, which reduces the risk of transmission to an unintended host, but it does not control where the application directs requests at the application layer.	Verified	Every safeguard the rating relies on is supported by attached evidence: SG-3.
R-C-1-T-D15	2	TLS 1.2 or later as described directly addresses interception and tampering in transit on the connection between the web app and the API, providing encryption and integrity protection for data on that path.	Verified	Every safeguard the rating relies on is supported by attached evidence: SG-3.