APERTURE RESEARCH
WORKS

INDEPENDENT PUBLIC-SOURCE CASE STUDY | NOT A CLIENT ENGAGEMENT

CrowdStrike: Did the Evidence Verify Both the Cause and the Fix?

Focused Evidence Review | Complete Case Pack

Evidence cut-off: 21 August 2026
Complete case-pack production: V1.0 | 23 August 2026

Package status: APPROVED FINAL PUBLIC EDITION
Human-approved for public release by Paul Hattingh on 23 August 2026. Evidence limitations and future review triggers remain controlling.

APPROVED FINAL PUBLIC EDITION

Aperture Research Works did not act for the subject or any other party in this public-source demonstration. The work is designed to show how evidence is tested before reliance. Proprietary internal prompts, scoring logic, QA architecture and protected working records are not published.

REALITY BEFORE RELIANCE.
VERIFICATION BEFORE INTERPRETATION.
EVIDENCE BEFORE NARRATIVE.

Document control and reliance boundary

Public brand	Aperture Research Works
Document	Complete Case Pack (CCP)
Product / capability	Focused Evidence Review
Operating mode	Independent Public-Source Case Study - Not a Client Engagement
Governing master	PHW Research AI v11.0
Evidence cut-off	21 August 2026
Research status	Research Complete / Approved
Public edition status	APPROVED FINAL PUBLIC EDITION
Professional boundary	Technical evidence review only; no software certification, cybersecurity audit or engineering sign-off.
Document version	1.0
PDF production date	23 August 2026
Human approval of exact PDF	Paul Hattingh | 23 August 2026 | Approved for public release
Release-date current-status check	Release-date current-status check completed 23 August 2026. The latest located issuer filings through 21 August 2026 were routine ownership filings and no material official development was identified that changes the incident-causation or remediation-evidence assessment.

PACKAGE CONTENTS

1. Document 1 - Principal Investigative Dossier
2. Document 2 - Claims-and-Evidence Matrix
3. Document 3 - Master Chronology
4. Document 4 - Source and Evidence Register
5. Document 5 - Public Portfolio Edition
6. Document 6 - Final Delivery Manifest

The combined case pack follows the controlled document sequence. A Specialist Appendix is omitted unless it adds a distinct professional function and the required competence boundary can be stated accurately.

DOCUMENT 1

PRINCIPAL INVESTIGATIVE DOSSIER

CrowdStrike: Did the Evidence Verify Both the Cause and the Fix? | Focused Evidence Review

Focused Evidence Review
Illustrative product level: US$1,500-$3,000
Matter reference: APERTURE-SAMPLE-2026-002
Evidence Cut-off: 21 August 2026
Source Freeze: SF2, 21 August 2026
Research status: Research Complete / Approved
Text version: 1.2

INDEPENDENT PUBLIC-SOURCE CASE STUDY - NOT A CLIENT ENGAGEMENT

Aperture Research Works did not represent CrowdStrike, Microsoft, any affected customer, regulator, litigant, insurer, investor or other party. Aperture did not have access to confidential source code, internal telemetry, privileged incident material, customer contracts or non-public third-party review reports. This assessment is limited to lawfully available public sources reviewed through the stated Evidence Cut-off.

Source IDs in square brackets refer to the Short Source Schedule.

MATTER OVERVIEW

On 19 July 2024, a CrowdStrike Falcon content configuration update caused Windows systems around the world to crash. Microsoft estimated that approximately 8.5 million Windows devices were affected, while the UK National Cyber Security Centre, the U.S. Cybersecurity and Infrastructure Security Agency, the Canadian Centre for Cyber Security and the U.S. Government Accountability Office separately identified a CrowdStrike update as the initiating event. The strongest official

evidence also supports that this was an operational software failure rather than a malicious cyberattack. [S03][S04][S11][S12][S13]

The important evidence question is narrower than the public controversy. It is not whether the outage happened or whether CrowdStrike was involved. Those propositions are well established. The useful decision question is whether the public record supports two more demanding conclusions: first, that CrowdStrike's technical root-cause account is sufficiently corroborated for responsible factual reliance; and second, that the principal controls introduced after the incident can be treated as materially implemented rather than merely promised.

This Focused Evidence Review tests both propositions, separates independently corroborated facts from vendor-dependent technical detail, tests alternative explanations, examines the post-incident control record through August 2026 and identifies the point at which public-source research reaches a genuine non-public evidence ceiling.

MATTER AT A GLANCE

Subject: CrowdStrike Falcon July 2024 Windows outage and post-incident remediation
Primary incident period: 19 July to September 2024
Remediation follow-through: August 2024 to July 2025
Current-status check: Through 21 August 2026
Primary evidence domains: Technical incident records, government and regulatory material, congressional testimony and written responses, current product-control documentation, independent implementation corroboration and SEC disclosures
Product: Focused Evidence Review
Governing master: PHW Research AI v11.0 Approved Governing Master, effective 20 August 2026
Client-facing finding: CAUSE CORROBORATED; REMEDIATION SUBSTANTIALLY SUPPORTED WITH A MATERIAL PUBLIC-VERIFICATION LIMITATION
Factual Status: CORROBORATED WITH MATERIAL QUALIFICATION
Evidential Confidence: HIGH on cause; MODERATE-HIGH on implementation; MODERATE on long-term operating effectiveness
Reliance Status: LIMITED RELIANCE ONLY
Overall conclusion classification: STRONGLY SUPPORTED as to cause; QUALIFIED as to remediation effectiveness

CENTRAL QUESTION

Did the public evidence sufficiently corroborate CrowdStrike's account that the 19 July 2024 global Windows outage resulted from a defective Falcon Rapid Response Content update, and does the available public record sufficiently support CrowdStrike's claim that the principal validation, testing, deployment and customer-control weaknesses identified after the incident were materially remediated?

DECISION OR RELIANCE QUESTION

Could an enterprise technology buyer, board, risk function, insurer, regulator or other decision-maker responsibly rely on CrowdStrike's public root-cause analysis and later resilience statements as sufficient evidence that the cause was understood and the principal control weaknesses were materially addressed, or would additional non-public assurance still be material for a high-consequence decision?

SCOPE

This review examined:

- the timing and affected-system profile of the 19 July 2024 incident;
- CrowdStrike's preliminary and final technical root-cause account;
- independent official corroboration of the CrowdStrike-update cause and non-malicious nature of the outage;
- the distinction between externally verifiable causation and vendor-dependent low-level technical detail;

- the validation, testing and rollout weaknesses CrowdStrike itself identified;
- remediation measures described in the technical RCA, congressional record and later follow-through material;
- the dates on which several key technical mitigations were reported as implemented;
- CrowdStrike's later claim that all RCA mitigations had been completed and independently validated;
- current customer content-update controls in CrowdStrike's public developer documentation;
- independent CIS documentation showing the practical availability of Early Access, General Availability and Pause update choices;
- CrowdStrike's July 2025 description of additional resilience engineering, ring-based deployment, recovery and testing capabilities;
- current SEC risk disclosures concerning the incident and the effectiveness of post-incident enhancements; and
- a final search for later official, regulatory or authoritative material that materially contradicted the established cause or changed the remediation picture.

This review did **not** examine:

- CrowdStrike source code, build systems or private engineering repositories;
- confidential test results, internal deployment telemetry, rollback metrics or exception logs;
- non-public third-party reviewer work product;
- endpoint forensic images from affected customers;
- penetration testing, code audit or exploitability testing by Aperture;
- the complete universe of July 19 litigation, damages or insurance claims;
- customer-specific contracts, service-level obligations, indemnities or recovery rights;
- securities valuation or investment merit;
- comparative procurement scoring against competing cybersecurity vendors;
- legal liability, regulatory compliance or professional-negligence conclusions; or
- a prediction that no similar incident can recur.

FOCUSED-SCOPE CONTROL RECORD

Research period: 21 August 2026, including a second-pass source audit, current-status check, contrary-evidence search, independent-corroboration expansion and public-gap closure review on that date.
Restricted evidence set: S01-S17, selected because they directly address causation, technical mechanism, remediation, independent corroboration, implementation, present controls or current risk qualification.
Work not performed: No source-code examination, endpoint forensics, confidential third-party review, independent software test, customer interview, contract review, damages model or litigation merits analysis.
External specialist review: Not performed. A qualified software-security or reliability specialist would be required for high-reliance conclusions concerning code quality, control-design adequacy or operating effectiveness.
Registers not separately created: No separate entity-relationship, calculations, exhibits or right-of-reply register was created because none is material to this defined Focused Evidence Review at the present stage. Claims, sources, chronology, source dependence, contradictions, findings, evidence gaps and changes are controlled in the SF2 machine-readable research package.
Full-investigation recommendation: Not required for the present portfolio reliance question. A broader investigation and specialist review would be required if the intended use expands to high-consequence procurement, insurance, litigation, regulatory or technical-assurance reliance.
Permitted use: Public portfolio demonstration of a Focused Evidence Review and limited factual understanding of the defined incident and remediation record.
Reliance restriction: Limited Reliance Only, within the Central Question, Evidence Cut-off and exclusions stated above.
Escalation trigger: A high-consequence procurement, insurance, litigation, regulatory or technical-assurance decision would require additional non-public or independently testable evidence.

1. WHAT THE PUBLIC RECORD ESTABLISHES ABOUT THE OUTAGE

CrowdStrike's preliminary incident review states that at 04:09 UTC on 19 July 2024 it released a Rapid Response Content configuration update to Windows hosts running Falcon sensor version 7.11 and above. Systems online during the period before the defective content was reverted at 05:27 UTC could crash with a Windows blue screen. Mac and Linux hosts were not affected. [S01]

That account is independently corroborated at the level that matters for external causation. Microsoft described CrowdStrike's update as faulty, stated that the event was not a Microsoft incident and estimated approximately 8.5 million affected Windows devices. [S03] The UK NCSC described significant global disruption following a CrowdStrike security update and assessed that it was not malicious cyber activity. [S04] CISA stated that the widespread Windows outage was due to a CrowdStrike Falcon content update and not malicious cyber activity. [S12] Canada's Cyber Centre separately identified a faulty CrowdStrike Falcon channel-file update and published the affected C-00000291*.sys recovery path. [S11] GAO described a CrowdStrike software update as causing Windows operating systems to crash and disrupting critical infrastructure. [S13]

The public record therefore strongly supports the basic causal chain:

1. CrowdStrike distributed a Falcon content configuration update.
2. Affected Windows hosts processed that update.
3. The update triggered system crashes.
4. The impact was amplified by the deployment of CrowdStrike across enterprise and critical-service environments.
5. The incident was operational, not a malicious cyberattack.

No credible public evidence located in the two-pass review supports a competing theory that the initiating event was a Microsoft Windows update, an external attacker, customer-by-customer misconfiguration or an unrelated simultaneous infrastructure event. No later official source located through the Evidence Cut-off materially displaced this high-level causal account.

2. WHAT THE TECHNICAL ROOT-CAUSE ACCOUNT ADDS

CrowdStrike's External Technical Root Cause Analysis provides a substantially more granular mechanism than external sources can independently observe. It states that a new IPC Template Type defined 21 input parameter fields while the integration code supplied only 20 input values. Earlier Template Instances had used wildcard matching for the 21st field. On 19 July, a new non-wildcard criterion exercised the previously untested path, producing an out-of-bounds read and a system crash. [S02]

This mechanism is internally coherent and consistent with the known external symptoms. It is also supported by CrowdStrike's later congressional testimony and written responses, which repeated that a parameter mismatch escaped validation and testing and described the resulting failure path and mitigation work. [S05]

A material evidence distinction remains. Microsoft, NCSC, CISA, the Canadian Cyber Centre and GAO independently corroborate the **vendor-update cause**, Windows impact and operational nature of the event. They do not independently reproduce CrowdStrike's exact 21-versus-20 parameter mechanism, inspect the proprietary Content Interpreter, or audit the internal validator and build pipeline. [S03][S04][S11][S12][S13]

The low-level mechanism is therefore highly credible primary-party technical evidence, reinforced by consistency, public recovery evidence and later testimony, but it remains materially dependent on CrowdStrike-controlled evidence.

3. THE CONTROL FAILURE WAS BROADER THAN ONE BAD CONTENT FILE

The evidence does not support reducing the event to an isolated malformed content file with no wider process implication.

CrowdStrike's preliminary and final analyses state that the problematic content passed a Content Validator and that the mismatch escaped multiple layers of build validation and testing. [S01][S02] In the congressional record, CrowdStrike

acknowledged that the validation and testing processes then in use did not catch the discrepancy and that the relevant test scenarios had not exercised the condition that ultimately triggered the failure. [S05]

That matters because the decision-relevant failure chain had several layers:

- an input/schema mismatch existed;
- compile-time validation did not catch the mismatch;
- runtime bounds checking was insufficient for the exercised path;
- testing did not exercise the relevant non-wildcard scenario;
- the Content Validator did not prevent the problematic configuration from being distributed;
- the rapid content-distribution path exposed a broad installed base before the issue was detected and reverted; and
- customers initially had less control over Rapid Response Content delivery than CrowdStrike later introduced.

The root cause was technical, but the impact scale also exposed release-governance, testing and resilience weaknesses. The FCA's post-incident operational-resilience observations independently reinforce the importance of adequate update testing and phased releases in containing this class of failure. [S14]

4. ALTERNATIVE EXPLANATIONS TESTED

Alternative A: The outage was a cyberattack

Not supported. CrowdStrike stated that the incident was not a security incident or cyberattack. NCSC and CISA separately assessed or reported that the event was not malicious cyber activity. [S01][S04][S12]

Alternative B: Microsoft caused the outage through Windows

Not supported by the strongest evidence. Microsoft expressly described the event as resulting from CrowdStrike's update and said it was not a Microsoft incident. CrowdStrike's own technical record identifies its Falcon content path as the initiating mechanism. [S02][S03]

Alternative C: Customer configuration was the principal initiating cause

Not supported. The common failure mechanism was a centrally distributed CrowdStrike content update affecting eligible Windows sensors during a defined deployment window. Customer environments influenced exposure and recovery complexity, but the initiating defect was not shown to originate in independent customer changes. [S01][S03][S11]

Alternative D: A single malformed file was the entire problem, with no process failure

Incomplete. The public technical record identifies validation, testing, bounds-checking and rollout weaknesses that allowed the problematic content to produce system-wide crashes at scale. [S02][S05]

Alternative E: The absence of a publicly identified repeat event proves remediation effectiveness

Not established. A lack of an identical public recurrence is useful context but is not a substitute for control testing. CrowdStrike's fiscal 2026 SEC disclosure expressly states that it cannot guarantee the effectiveness of its software-resiliency, testing and customer-control enhancements. [S08][S09]

5. WHAT CROWDSTRIKE SAID IT CHANGED, AND WHEN

CrowdStrike's technical RCA and later congressional record identify a coherent remediation program. The measures included:

- compile-time validation of Template Type input counts;
- broader automated testing, including non-wildcard matching criteria for each field;
- additional Content Validator checks;
- runtime input-array bounds checks;

- staged or ring-based deployment of Rapid Response Content;
- increased customer control over where and when content updates are deployed;
- more granular release information and controls; and
- independent third-party review of Falcon sensor code and the end-to-end quality and release process. [S02][S05]

The implementation record includes specific dates. CrowdStrike's RCA states that a Sensor Content Compiler patch was developed on 19 July 2024 and entered production on 27 July; runtime bounds checking and an additional input-array-size check were added on 25 July; the relevant fixes were being backported to Windows sensor versions 7.11 and above with general availability expected by 9 August; and additional Content Validator checks were scheduled for production by 19 August. Later congressional responses stated that the mitigation actions had been implemented. [S02][S05]

By September 2024, CrowdStrike stated in an investor briefing that all RCA mitigations had been completed and independently validated. [S06]

The record did not stop there. CrowdStrike's July 2025 one-year follow-up described a new Content Distribution System using ring-based automated deployment, Sensor Self-Recovery for crash loops, a remediation toolkit, content pinning, a content quality dashboard, a Falcon Super Lab testing thousands of operating-system, kernel, hardware and third-party application combinations, and continuing outside expert code and process reviews. [S15] These remain company-originated implementation statements, but they provide later follow-through rather than a one-time 2024 promise.

6. WHAT IS PUBLICLY VERIFIABLE ABOUT THE REMEDIATION

The strongest publicly observable implementation evidence concerns customer control over content deployment.

Current CrowdStrike Developer Center documentation states that Content Update Policies control how and when content updates are deployed to hosts. The schema supports host-group attachment, Early Access and General Availability ring assignments, Pause for Rapid Response content, configurable delays and content-version pinning. [S07]

This is not only visible in CrowdStrike's own documentation. The Center for Internet Security published guidance describing the CrowdStrike update choices available to customers, including Early Access, General Availability and Pause Updates, and stated that CIS would use General Availability for its own monitored members. [S16] That provides independent implementation corroboration for a material customer-control component of the remediation program.

CrowdStrike's July 2025 follow-up also describes ring-based automated deployment, different schedules for test, workstation and mission-critical systems, content pinning and release-quality visibility. [S15]

The congressional record contains CrowdStrike's statement that staged deployment, additional runtime checks and enhanced validation/testing had been implemented. [S05] The September 2024 investor presentation goes further and states that all RCA mitigations were complete and independently validated. [S06]

These sources provide substantial support for **implementation**, but they do not all carry the same evidentiary weight:

- current developer documentation is directly observable and supports the existence of customer-facing controls;
- CIS independently corroborates practical customer update-ring choices;
- the one-year follow-up provides later operational detail, but remains a CrowdStrike statement;
- congressional testimony and written responses form an official public record, but the technical assertions remain CrowdStrike evidence; and
- the investor presentation is a formal company statement, but its "independently validated" conclusion is still reported by the company.

7. THE MATERIAL PUBLIC-VERIFICATION CEILING

The most important remaining limitation is not an unfinished desktop-research task. It is a public-source evidence ceiling.

CrowdStrike's August 2024 RCA said that two independent third-party software-security vendors had been engaged to review Falcon sensor code and the end-to-end quality process. [S02] The RCA also states that the out-of-bounds read issue had been independently reviewed. CrowdStrike's August 2024 technical response later described its exploitability analysis as peer

reviewed. [S17] Congressional material repeated that independent third-party vendors had been engaged. [S05] By September, CrowdStrike stated that all RCA mitigations had been independently validated. [S06]

A second, broader search was performed specifically for the reviewer identities, underlying validation reports, scopes, methodologies, exceptions and test results. No publicly inspectable underlying report or equivalent detailed assurance statement was located through the Evidence Cut-off.

That result must be characterized carefully. It does **not** prove that the independent work did not occur. It means the public record establishes the existence of review and a company-reported validation conclusion more strongly than it establishes the underlying basis of that conclusion.

For this defined public-source product, that issue is therefore **closed as a research search and retained as a structural non-public limitation**. It would become an evidence-request item in a commissioned high-reliance matter, not a reason to continue indefinite public web research.

8. CROWDSTRIKE'S OWN CURRENT RISK DISCLOSURES PRESERVE THE QUALIFICATION

CrowdStrike's fiscal 2026 Form 10-K acknowledges continuing business, customer, reputational, legal and financial consequences from the July 19 incident. More importantly for this review, it states that although the company is investing in enhancements to software resiliency, testing and customer controls, it cannot guarantee that those enhancements will be effective or that its products will not contain defects, errors or vulnerabilities. [S08]

The same material qualification remains present in current 2026 SEC reporting reviewed for this matter. [S09]

These disclosures do not contradict CrowdStrike's claim that remediation was implemented. They materially limit any stronger inference that implementation equals proven future effectiveness.

CrowdStrike's July 2025 resilience follow-up makes the same conceptual point from another direction by describing resilience as an ongoing discipline rather than a finished state. [S15]

A responsible evidence assessment should therefore distinguish three propositions:

1. **The root cause was understood:** strongly supported.
2. **Material mitigations were implemented:** substantially supported.
3. **Those mitigations are independently proven to prevent analogous failure over time:** not established to the same evidentiary standard in the public record.

9. SOURCE-INDEPENDENCE ASSESSMENT

The evidentiary spine is not purely self-referential.

Independent or institutionally separate sources corroborate the high-level cause, affected platform and operational nature of the event. Microsoft, NCSC, CISA, the Canadian Cyber Centre and GAO all materially support the CrowdStrike-update causal account. [S03][S04][S11][S12][S13] The FCA independently identifies software-update testing and phased release as relevant resilience controls after examining firms' responses to the outage. [S14] CIS independently corroborates that CrowdStrike customer update-ring choices are operationally available. [S16]

The exact technical mechanism and most internal remediation detail remain more dependent on CrowdStrike's own evidence. Congressional testimony adds accountability and detail but does not transform company testimony into an independent technical audit. The reviewer reports themselves remain non-public in the source universe located.

The correct evidentiary treatment is therefore layered rather than binary.

APERTURE FINDING

CAUSE CORROBORATED; REMEDIATION SUBSTANTIALLY SUPPORTED WITH A MATERIAL PUBLIC-VERIFICATION LIMITATION

Factual Status: CORROBORATED WITH MATERIAL QUALIFICATION
Evidential Confidence: HIGH on cause; MODERATE-HIGH on implementation; MODERATE on long-term operating effectiveness
Reliance Status: LIMITED RELIANCE ONLY

The public record strongly corroborates CrowdStrike's central account that the 19 July 2024 outage was initiated by a defective Falcon content configuration update affecting Windows systems and was not a cyberattack. Multiple independent official and ecosystem sources materially support that high-level causal conclusion. [S03][S04][S11][S12][S13]

CrowdStrike's more granular technical explanation is credible and internally consistent, but the precise proprietary mechanism is principally supported by CrowdStrike's RCA and testimony. [S02][S05]

The remediation record is stronger than a set of unimplemented promises. It contains dated technical fixes, later congressional implementation statements, a company claim of completed independent validation, current customer-control documentation, independent CIS corroboration of customer update choices, and a one-year follow-up describing further ring-based deployment, recovery and testing controls. [S02][S05][S06][S07][S15][S16]

The material qualification is narrower after the SF2 review: the underlying third-party validation reports and internal operating evidence are not publicly inspectable. CrowdStrike's own current SEC disclosures also decline to guarantee the effectiveness of the post-incident enhancements. [S08][S09]

The evidence therefore supports reliance on the cause and on the existence of substantial remediation, but not an unqualified public-source conclusion that the entire remediation program has been independently demonstrated to operate effectively enough to prevent future analogous failure.

RELIANCE ASSESSMENT

Reliance Status: LIMITED RELIANCE ONLY.

Within the defined scope, the evidence supports limited factual reliance on the following propositions:

1. CrowdStrike's July 19 Rapid Response Content update initiated the affected Windows system crashes. [S01][S03][S04][S11][S12][S13]
2. The incident was operational rather than malicious cyber activity. [S04][S12]
3. CrowdStrike identified a validation/testing mismatch and related bounds-checking failure in its technical RCA. [S02]
4. CrowdStrike implemented or reported implementation of additional validation, testing, staged rollout, runtime safeguards and customer controls. [S02][S05][S15]
5. Current product documentation demonstrates that customer content-update policies, ring choices, delays and version-pinning controls exist. [S07]
6. CIS independently corroborates that Early Access, General Availability and Pause choices are available in practice. [S16]
7. CrowdStrike publicly claimed by September 2024 that all RCA mitigations had been completed and independently validated. [S06]
8. CrowdStrike continued adding resilience, recovery and testing controls during the following year. [S15]

This review does **not** support a conclusion that:

- the public record independently reproduces every low-level technical step in CrowdStrike's RCA;
- the underlying third-party reviewers' full methods and conclusions are publicly auditable;
- every remediation control has been independently tested by Aperture;
- the post-incident controls eliminate the possibility of a similar class of failure;
- Falcon is generally safe, unsafe, superior or inferior as a cybersecurity platform;

- CrowdStrike has no continuing legal or financial exposure; or
- a procurement, insurance, regulatory or litigation decision can rely on this portfolio review without matter-specific evidence.

PUBLIC-SOURCE GAP CLOSURE AND STRUCTURAL LIMITATIONS

The second-pass SF2 review distinguishes between a **research gap that can still reasonably be filled from public sources** and a **structural limitation that requires non-public evidence or a different engagement**.

G01 - Independent validation work product: CLOSED AS PUBLIC-SOURCE SEARCH / STRUCTURAL LIMITATION. CrowdStrike's public record establishes engagement of independent reviewers, describes at least one independently reviewed technical issue and later claims independent validation of all RCA mitigations. A targeted second search did not locate the underlying reviewer identities, reports, methodology, exceptions or detailed test results. Further ordinary public-source searching is not reasonably expected to convert that non-public assurance layer into auditable evidence. [S02][S05][S06][S17]

G02 - Source code, build artifacts, telemetry and control logs: OUTSIDE DEFINED PUBLIC-SOURCE SCOPE. These are not missing public sources. They are internal technical evidence that would require lawful access in a commissioned matter. Their absence prevents independent reproduction of the proprietary RCA and full operating-effectiveness testing, but does not defeat the high-level cause finding.

G03 - Current existence of customer rollout controls: CLOSED FOR THIS PRODUCT. CrowdStrike's current developer material documents the controls, CIS independently corroborates the practical Early Access, General Availability and Pause choices, and CrowdStrike's one-year follow-up records additional ring, pinning and resilience capabilities. [S07][S15][S16]

G04 - Long-term operating effectiveness: QUALIFICATION RETAINED, NOT AN OPEN DESKTOP-RESEARCH GAP. Public evidence can show implementation indicators and current controls, but cannot provide audit-level proof that all internal controls operate effectively over time. CrowdStrike's SEC disclosure itself preserves this qualification. [S08][S09]

G05 - Alternative official root cause or later material contradiction: CLOSED THROUGH THE EVIDENCE CUT-OFF. The final current-status search located no later official or regulatory finding that materially displaced the established CrowdStrike-update cause. This is negative-evidence context, not proof that no future evidence can emerge.

G06 - Litigation, contractual liability and damages: SCOPE EXCLUSION. Those questions are separate from the Central Question and would require a separate legal/evidence engagement.

Research-closure assessment: No unresolved public-source research gap remains that reasonably requires further desktop research before substantive human approval of this defined Focused Evidence Review. The remaining limitations are expressly identified, non-public, specialist-dependent or outside scope.

WHAT COULD CHANGE THE CONCLUSION

The conclusion should be reassessed if any of the following becomes available or occurs:

- publication of the underlying independent third-party review or a sufficiently detailed independent assurance statement;
- credible technical evidence materially contradicting the 21-versus-20 parameter mismatch or other core RCA findings;
- a later official investigation establishing a materially different root cause;
- evidence that a stated mitigation was not implemented or was subsequently withdrawn;
- a material recurrence involving the same or a closely analogous validation and rapid-content deployment failure;
- independent operating-effectiveness evidence materially strengthening or weakening the remediation conclusion; or
- a new SEC, regulatory or judicial finding materially changing the incident or remediation record.

RECOMMENDED NEXT STEP

For this defined public portfolio product, **no further public-source research is required before human approval**. SF2 closes the reasonable public research cycle while preserving the material non-public assurance limitation.

For a high-consequence vendor-selection, insurance, regulatory, litigation or enterprise-resilience decision, the next step would be a separate matter-specific technical assurance review. That review should seek the underlying third-party validation reports, current control-design documentation, rollout and rollback evidence, representative test artifacts, control-exception history and, where appropriate, review by a qualified software-security or reliability specialist.

PROFESSIONAL BOUNDARY

This product is an evidence-assurance assessment. It is not a penetration test, source-code audit, digital-forensic investigation, cybersecurity certification, legal opinion, regulatory audit, expert-witness report, insurance opinion, procurement recommendation or investment recommendation. No conclusion is expressed on CrowdStrike's legal liability or on the security efficacy of Falcon generally.

SHORT SOURCE SCHEDULE

S01. CrowdStrike, 24 July 2024.
Preliminary Post Incident Review: Content Configuration Update Impacting the Falcon Sensor and the Windows Operating System (BSOD).
Primary-party incident source. Used for deployment timing, affected sensor scope, reversion timing, initial validator explanation and early mitigation plan. Limitation: CrowdStrike-authored.

S02. CrowdStrike, 6 August 2024.
External Technical Root Cause Analysis: Channel File 291.
Primary-party technical source. Used for the parameter mismatch, out-of-bounds read, test and validation findings, dated technical mitigations, staged deployment, customer control and independent third-party review engagement. Limitation: detailed proprietary mechanism is not independently reproducible from public evidence alone.

S03. Microsoft, 20 July 2024.
Helping our customers through the CrowdStrike outage.
Independent ecosystem corroboration. Used for Microsoft's statement that this was not a Microsoft incident, its description of CrowdStrike's faulty update and its estimate of approximately 8.5 million affected Windows devices. Limitation: Microsoft is part of the affected ecosystem, not an incident auditor.

S04. UK National Cyber Security Centre, 19 July 2024.
Statement on major IT outage.
Independent government cyber-authority source. Used for the assessment that the global disruption followed a CrowdStrike security update and was not malicious cyber activity.

S05. U.S. House Committee on Homeland Security, 24 September 2024.
An Outage Strikes: Assessing the Global Impact of CrowdStrike's Faulty Software Update.
Official congressional hearing record containing CrowdStrike testimony and written responses. Used for validation and testing admissions, mitigation implementation, staged deployment, customer control, runtime safeguards and third-party review engagement. Limitation: technical assertions are still CrowdStrike statements within an official forum.

S06. CrowdStrike Investor Briefing, September 2024.
Investor presentation stating that all RCA mitigations were completed and independently validated. Used as a material primary-party completion claim. Limitation: the presentation does not provide the underlying independent reviewer reports, methods or detailed results.

S07. CrowdStrike Developer Center, current through 21 August 2026.
Content Update Policies documentation.
Current primary-party product documentation. Used as an observable implementation indicator showing control over when content deploys, host-group application, Early Access and General Availability rings, Pause for Rapid Response, delays and version pinning. Limitation: existence of a control interface is not proof of full internal operating effectiveness.

S08. CrowdStrike Holdings, Inc., Form 10-K for fiscal year ended 31 January 2026.
SEC-filed regulated disclosure. Used for current incident consequences and the express qualification that the company cannot guarantee the effectiveness of post-incident resiliency, testing and customer-control enhancements. Limitation: issuer disclosure, not an independent technical audit.

S09. CrowdStrike Holdings, Inc., 2026 Form 10-Q current-status disclosure reviewed through the Evidence Cut-off.
SEC-filed regulated disclosure. Used for continuing incident-related risk, cost and effectiveness context. Limitation: issuer disclosure, not an independent technical audit.

S10. European Banking Authority, operational-risk publication discussing the July 2024 event.
Independent institutional source. Used as additional corroboration that a CrowdStrike configuration update caused a widespread Windows outage and demonstrated material operational-resilience and concentration risk.

S11. Canadian Centre for Cyber Security, 19 July 2024.
Alert AL24-010: Issue impacting CrowdStrike Falcon EDR.
Independent government cyber-authority evidence. Used for the faulty CrowdStrike Falcon update, Windows crash behavior and the C-00000291*.sys remediation path.

S12. U.S. Cybersecurity and Infrastructure Security Agency, 19 July 2024.
Widespread IT Outage Due to CrowdStrike Update.
Independent government source. Used for Windows impact and the statement that the outage was due to a CrowdStrike Falcon content update rather than malicious cyber activity.

S13. U.S. Government Accountability Office, 23 September 2024.
Cyber Resiliency: CrowdStrike Outage Highlights Challenges, GAO-24-107733.
Independent government source. Used for high-level causal corroboration and critical-infrastructure resilience context.

S14. UK Financial Conduct Authority, 31 October 2024.
CrowdStrike outage: lessons for operational resilience.
Independent regulator source. Used for post-incident observations about testing software and content updates, phased release and third-party operational resilience. It is not an audit of CrowdStrike's remediation.

S15. CrowdStrike, 14 July 2025.
One Year Later: Reflecting on Building Resilience by Design.
Primary-party follow-through source. Used for later implementation statements concerning the Content Distribution System, ring-based deployment, self-recovery, remediation tooling, content controls, pinning, the Falcon Super Lab, resilience exercises and continuing outside expert review. Limitation: company-authored and not itself independent assurance.

S16. Center for Internet Security, post-incident guidance reviewed through 21 August 2026.
Guidance for CrowdStrike Windows Outage.
Independent implementation corroboration. Used for practical CrowdStrike customer update choices, including Early Access, General Availability and Pause Updates, and CIS's own stated use of General Availability.

S17. CrowdStrike, 7 August 2024.
Tech Analysis: Addressing Claims About Falcon Sensor Vulnerability.
Primary-party technical follow-up. Used only to establish that CrowdStrike described its exploitability analysis as peer reviewed. It is not treated as a public independent validation report for the full remediation program.

PRODUCT STATUS

Research status: Research Complete / Approved
Text version: 1.2
Evidence basis: Source Freeze SF2
Evidence Cut-off: 21 August 2026
Public demonstration status: V104 Public Demonstration Dossier produced and integrated by express instruction on 22 August 2026.
Professional boundary: Specialist code-quality or operating-effectiveness certification is not claimed.

Reality before reliance.

RELEASE-DATE CURRENT-STATUS CHECK

Release-date current-status check completed 23 August 2026. The latest located issuer filings through 21 August 2026 were routine ownership filings and no material official development was identified that changes the incident-causation or remediation-evidence assessment.

This release-date check does not silently extend the frozen evidence universe. A material new controlling source would require the matter to reopen under the v11.0 update trigger.

DOCUMENT 2

CLAIMS AND EVIDENCE MATRIX

Claim-level factual status, evidential confidence, reliance and qualification control

Claims-and-Evidence Matrix

ID	Claim / proposition	Factual status	Confidence	Sources	Qualification
C01	CrowdStrike's July 19 content update initiated the affected Windows crashes.	CORROBORATED	HIGH	S01; S03; S04; S11; S12; S13	Multiple independent official/ ecosystem sources corroborate the high-level cause; exact internal mechanism is separate.
C02	The incident was operational rather than caused by malicious cyber activity.	CORROBORATED	HIGH	S04; S12; S01	No contrary credible public evidence located through SF2.
C03	The low-level mechanism involved a 21/20 parameter mismatch and out-of-bounds read.	SUPPORTED	MODERATE-HIGH	S02; S05	Detailed mechanism is principally CrowdStrike-controlled evidence; it is not independently reproduced in public.
C04	Validation and testing failed to catch the relevant discrepancy before deployment.	CORROBORATED BY PRIMARY-PARTY ADMISSION	HIGH	S01; S02; S05	Admissions are detailed and against interest, but internal records are not public.

ID	Claim / proposition	Factual status	Confidence	Sources	Qualification
C05	CrowdStrike implemented stronger validation, testing, runtime safeguards and staged deployment after the incident.	SUBSTANTIALLY SUPPORTED	MODERATE-HIGH	S02; S05; S06; S15	Dated implementation statements and one-year follow-through strengthen the record; most internal evidence remains company-originated.
C06	CrowdStrike implemented customer-facing controls over content-update deployment.	CORROBORATED	HIGH	S07; S15; S16	Current developer documentation shows the controls and CIS independently corroborates practical update-ring choices.
C07	All RCA mitigations were independently validated.	PRIMARY-PARTY CLAIM WITH SUPPORTING REVIEW CONTEXT	MODERATE	S02; S05; S06; S17	Public evidence establishes review engagement and some peer/ independent review statements, but not the underlying full validation reports, reviewer identities, methods or exceptions.
C08	The remediation controls are independently proven effective enough to prevent future analogous failure over time.	NOT ESTABLISHED	HIGH that the stronger claim is unsupported	S08; S09; S15	Current public evidence supports implementation more strongly than operating effectiveness; CrowdStrike itself does not guarantee effectiveness.
C09	Post-incident customer control exists as an observable present capability rather than only a 2024 promise.	CORROBORATED	HIGH	S07; S16	Externally observable documentation plus independent CIS operational guidance.
C10	A later official source materially contradicting the established high-level root cause was located through the Evidence Cut-off.	NOT LOCATED	HIGH for the completed search, not a universal negative	S03; S04; S11; S12; S13; S14	Negative-evidence finding is bounded by the SF2 search universe and date.

Control note: classifications are matter-specific and bounded by the Evidence Cut-off. A source ID refers to the Source and Evidence Register in Document 4.

DOCUMENT 3

MASTER CHRONOLOGY

Material events, dates, status and evidentiary significance

Controlled chronology

ID	Date / time	Event	Sources
C01	2024-07-19T04:09:00Z	CrowdStrike released the defective Rapid Response Content configuration update to affected Windows hosts.	S01
C02	2024-07-19T05:27:00Z	CrowdStrike reverted the defective content; systems online during the exposure window could experience crashes.	S01
C03	2024-07-19	NCSC, CISA and the Canadian Centre for Cyber Security issued official outage guidance identifying a CrowdStrike update and distinguishing the event from malicious cyber activity.	S04; S11; S12
C04	2024-07-20	Microsoft estimated approximately 8.5 million Windows devices were affected and described the incident as caused by a CrowdStrike update, not a Microsoft incident.	S03
C05	2024-07-24	CrowdStrike published its Preliminary Post Incident Review describing the content-update failure and initial mitigation plan.	S01
C06	2024-07-25	CrowdStrike states that runtime bounds checking and an additional input-array-size check were added.	S02
C07	2024-07-27	CrowdStrike states that the Sensor Content Compiler patch entered production.	S02

ID	Date / time	Event	Sources
C08	2024-08-06	CrowdStrike published its External Technical Root Cause Analysis, including the 21/20 parameter mismatch and broader validation/testing/deployment remediation.	S02
C09	2024-08-07	CrowdStrike published further technical material describing exploitability analysis and peer/independent review statements.	S17
C10	2024-09	CrowdStrike stated in an investor briefing that all RCA mitigations had been completed and independently validated.	S06
C11	2024-09-23	GAO published a government-wide operational account identifying the CrowdStrike software update as the initiating event.	S13
C12	2024-09-24	CrowdStrike testified before the U.S. House Committee on Homeland Security and described validation/testing failures and implemented remediation measures.	S05
C13	2024-10-31	UK FCA published operational-resilience observations arising from the CrowdStrike outage.	S14
C14	2025-07-14	CrowdStrike published a one-year resilience follow-up describing ring-based deployment, self-recovery, content pinning, expanded testing and continuing outside review.	S15
C15	2026-03	CrowdStrike fiscal 2026 SEC disclosure retained material risk language and stated that effectiveness of resilience/testing/customer-control enhancements cannot be guaranteed.	S08
C16	2026-08-21	Final current-status, source-locator and contrary-evidence checks completed; SF2 frozen.	S07; S09; S16

Chronology control: event dates are distinguished from later publication, filing and current-status dates where material. The chronology does not convert allegations into findings.

DOCUMENT 4

SOURCE AND EVIDENCE REGISTER

Controlling public sources, exact web locators, material use and reliance limitations

Source-control method

Each material public source is tied to the propositions attributed to it in this case pack. A source is not used to establish a proposition beyond its authority, scope or recorded limitation. Where a public source link is available, the descriptive Source link below is clickable.

Material public-source register

S01 - Preliminary Post Incident Review: Content Configuration Update Impacting the Falcon Sensor and the Windows Operating System (BSOD)

Authority / issuer	CrowdStrike
Date	2024-07-24
Source type / tier	Primary-party incident review
Precise locator	Exact public web source at the linked URL; proposition-specific use and limitations are recorded below and in the Principal Investigative Dossier.
Material propositions supported / use	Incident timing, affected Windows sensor scope, reversion time, validator defect, early mitigation plan
Does not establish / limitations	CrowdStrike-authored; not independent corroboration
Reliance grade	Controlled source; reliance limited to the propositions and qualifications recorded here.

Public URL: Open public source

S02 - External Technical Root Cause Analysis: Channel File 291

Authority / issuer	CrowdStrike
Date	2024-08-06
Source type / tier	Technical root-cause analysis
Precise locator	Exact public web source at the linked URL; proposition-specific use and limitations are recorded below and in the Principal Investigative Dossier.
Material propositions supported / use	21/20 parameter mismatch, out-of-bounds read, dated technical mitigations, expanded testing, staged deployment, customer controls, independent review engagement
Does not establish / limitations	Detailed proprietary mechanism depends on vendor-controlled evidence
Reliance grade	Controlled source; reliance limited to the propositions and qualifications recorded here.

Public URL: Open public source

S03 - Helping our customers through the CrowdStrike outage

Authority / issuer	Microsoft
Date	2024-07-20
Source type / tier	Official ecosystem statement
Precise locator	Exact public web source at the linked URL; proposition-specific use and limitations are recorded below and in the Principal Investigative Dossier.
Material propositions supported / use	CrowdStrike faulty update, not a Microsoft incident, approximately 8.5 million Windows devices affected
Does not establish / limitations	Affected ecosystem/platform party; not a technical auditor of CrowdStrike
Reliance grade	Controlled source; reliance limited to the propositions and qualifications recorded here.

Public URL: Open public source

S04 - Statement on major IT outage

Authority / issuer	UK National Cyber Security Centre
Date	2024-07-19
Source type / tier	Government cyber authority statement
Precise locator	Exact public web source at the linked URL; proposition-specific use and limitations are recorded below and in the Principal Investigative Dossier.
Material propositions supported / use	Global disruption followed CrowdStrike security update; not malicious cyber activity
Does not establish / limitations	High-level characterization, not low-level RCA validation
Reliance grade	Controlled source; reliance limited to the propositions and qualifications recorded here.

Public URL: Open public source

S05 - An Outage Strikes: Assessing the Global Impact of CrowdStrike's Faulty Software Update

Authority / issuer	U.S. House Committee on Homeland Security
Date	2024-09-24
Source type / tier	Congressional hearing record
Precise locator	Exact public web source at the linked URL; proposition-specific use and limitations are recorded below and in the Principal Investigative Dossier.
Material propositions supported / use	Validation/testing admissions, remediation implementation, dated fixes, staged rollout, customer controls, safeguards and third-party reviews
Does not establish / limitations	CrowdStrike technical assertions remain company statements even though given in an official public record
Reliance grade	Controlled source; reliance limited to the propositions and qualifications recorded here.

Public URL: Open public source

S06 - CrowdStrike Investor Briefing: September 2024

Authority / issuer	CrowdStrike
Date	2024-09
Source type / tier	Investor presentation
Precise locator	Exact public web source at the linked URL; proposition-specific use and limitations are recorded below and in the Principal Investigative Dossier.
Material propositions supported / use	Claim that all RCA mitigations were completed and independently validated
Does not establish / limitations	Underlying reviewer identities, reports, methods and detailed findings not provided in presentation
Reliance grade	Controlled source; reliance limited to the propositions and qualifications recorded here.

Public URL: Open public source

S07 - Content Update Policies

Authority / issuer	CrowdStrike Developer Center
Date	2026-08-21
Source type / tier	Current product documentation
Precise locator	Exact public web source at the linked URL; proposition-specific use and limitations are recorded below and in the Principal Investigative Dossier.
Material propositions supported / use	How/when content update controls, host groups, EA/GA/Pause ring settings, delays and version pinning
Does not establish / limitations	Control interface existence does not prove full internal operating effectiveness
Reliance grade	Controlled source; reliance limited to the propositions and qualifications recorded here.

Public URL: Open public source

S08 - Form 10-K for fiscal year ended January 31, 2026

Authority / issuer	CrowdStrike Holdings, Inc.
Date	2026-03
Source type / tier	SEC filing
Precise locator	Exact public web source at the linked URL; proposition-specific use and limitations are recorded below and in the Principal Investigative Dossier.
Material propositions supported / use	Current incident consequences and express inability to guarantee effectiveness of resilience/testing/ customer-control enhancements
Does not establish / limitations	Issuer disclosure, not independent technical audit
Reliance grade	Controlled source; reliance limited to the propositions and qualifications recorded here.

Public URL: Open public source

S09 - 2026 Form 10-Q current-status disclosure

Authority / issuer	CrowdStrike Holdings, Inc.
Date	2026
Source type / tier	SEC filing
Precise locator	Exact public web source at the linked URL; proposition-specific use and limitations are recorded below and in the Principal Investigative Dossier.
Material propositions supported / use	Continuing July 19 incident risk, cost and effectiveness context
Does not establish / limitations	Issuer disclosure, not independent technical audit
Reliance grade	Controlled source; reliance limited to the propositions and qualifications recorded here.

Public URL: Open public source

S10 - Operational risks and resilience publication discussing the CrowdStrike outage

Authority / issuer	European Banking Authority
Date	2025-2026
Source type / tier	Institutional operational-risk publication
Precise locator	Exact public web source at the linked URL; proposition-specific use and limitations are recorded below and in the Principal Investigative Dossier.
Material propositions supported / use	Additional high-level cause and operational-resilience corroboration
Does not establish / limitations	Not a CrowdStrike technical audit
Reliance grade	Controlled source; reliance limited to the propositions and qualifications recorded here.

Public URL: Open public source

S11 - Alert AL24-010: Issue impacting CrowdStrike Falcon EDR

Authority / issuer	Canadian Centre for Cyber Security
Date	2024-07-19
Source type / tier	Government cyber authority alert
Precise locator	Exact public web source at the linked URL; proposition-specific use and limitations are recorded below and in the Principal Investigative Dossier.
Material propositions supported / use	Faulty CrowdStrike Falcon channel-file update, Windows crash behavior and C-00000291 recovery path
Does not establish / limitations	Operational incident alert, not low-level audit
Reliance grade	Controlled source; reliance limited to the propositions and qualifications recorded here.

Public URL: Open public source

S12 - Widespread IT Outage Due to CrowdStrike Update

Authority / issuer	U.S. Cybersecurity and Infrastructure Security Agency
Date	2024-07-19
Source type / tier	Government cybersecurity bulletin
Precise locator	Exact public web source at the linked URL; proposition-specific use and limitations are recorded below and in the Principal Investigative Dossier.
Material propositions supported / use	Windows outage due to CrowdStrike Falcon content update, not malicious cyber activity
Does not establish / limitations	High-level incident bulletin
Reliance grade	Controlled source; reliance limited to the propositions and qualifications recorded here.

Public URL: Open public source

S13 - Cyber Resiliency: CrowdStrike Outage Highlights Challenges, GAO-24-107733

Authority / issuer	U.S. Government Accountability Office
Date	2024-09-23
Source type / tier	Government accountability report
Precise locator	Exact public web source at the linked URL; proposition-specific use and limitations are recorded below and in the Principal Investigative Dossier.
Material propositions supported / use	High-level cause and critical-infrastructure resilience context
Does not establish / limitations	Does not independently audit proprietary RCA
Reliance grade	Controlled source; reliance limited to the propositions and qualifications recorded here.

Public URL: Open public source

S14 - CrowdStrike outage: lessons for operational resilience

Authority / issuer	UK Financial Conduct Authority
Date	2024-10-31
Source type / tier	Financial regulator guidance
Precise locator	Exact public web source at the linked URL; proposition-specific use and limitations are recorded below and in the Principal Investigative Dossier.
Material propositions supported / use	Testing, phased release and third-party resilience lessons after the outage
Does not establish / limitations	Does not audit CrowdStrike's remediation implementation
Reliance grade	Controlled source; reliance limited to the propositions and qualifications recorded here.

Public URL: Open public source

S15 - One Year Later: Reflecting on Building Resilience by Design

Authority / issuer	CrowdStrike
Date	2025-07-14
Source type / tier	One-year remediation follow-through
Precise locator	Exact public web source at the linked URL; proposition-specific use and limitations are recorded below and in the Principal Investigative Dossier.
Material propositions supported / use	New Content Distribution System, ring-based deployment, recovery tooling, content controls, pinning, Super Lab, resilience exercises and continuing outside review
Does not establish / limitations	Company-authored; not independent assurance
Reliance grade	Controlled source; reliance limited to the propositions and qualifications recorded here.

Public URL: Open public source

S16 - Guidance for CrowdStrike Windows Outage

Authority / issuer	Center for Internet Security
Date	2024-2026
Source type / tier	Independent operational guidance
Precise locator	Exact public web source at the linked URL; proposition-specific use and limitations are recorded below and in the Principal Investigative Dossier.
Material propositions supported / use	Early Access, General Availability and Pause content-update choices and CIS deployment practice
Does not establish / limitations	Operational guidance, not full audit of CrowdStrike internal controls
Reliance grade	Controlled source; reliance limited to the propositions and qualifications recorded here.

Public URL: Open public source

S17 - Tech Analysis: Addressing Claims About Falcon Sensor Vulnerability

Authority / issuer	CrowdStrike
Date	2024-08-07
Source type / tier	Technical follow-up
Precise locator	Exact public web source at the linked URL; proposition-specific use and limitations are recorded below and in the Principal Investigative Dossier.
Material propositions supported / use	CrowdStrike statement that exploitability analysis was peer reviewed
Does not establish / limitations	Does not disclose full independent reviewer work product or validate the entire remediation program
Reliance grade	Controlled source; reliance limited to the propositions and qualifications recorded here.

Public URL: Open public source

DOCUMENT 5

PUBLIC PORTFOLIO EDITION

Decision-focused public summary of the controlled research record

Public Portfolio Edition

> INDEPENDENT PUBLIC-SOURCE CASE STUDY - NOT A CLIENT ENGAGEMENT. This Public Portfolio Edition summarises the controlled evidence record. It is not a substitute for the complete case pack, specialist advice or a commissioned matter-specific engagement.

Central Question

Did the public evidence sufficiently corroborate CrowdStrike's account that the 19 July 2024 global Windows outage resulted from a defective Falcon Rapid Response Content update, and does the available public record sufficiently support CrowdStrike's claim that the principal validation, testing, deployment and customer-control weaknesses identified after the incident were materially remediated?

Principal evidence-led assessment

On 19 July 2024, a CrowdStrike Falcon content configuration update caused Windows systems around the world to crash. Microsoft estimated that approximately 8.5 million Windows devices were affected, while the UK National Cyber Security Centre, the U.S. Cybersecurity and Infrastructure Security Agency, the Canadian Centre for Cyber Security and the U.S. Government Accountability Office separately identified a CrowdStrike update as the initiating event. The strongest official evidence also supports that this was an operational software failure rather than a malicious cyberattack. [S03][S04][S11][S12][S13]

The important evidence question is narrower than the public controversy. It is not whether the outage happened or whether CrowdStrike was involved. Those propositions are well established. The useful decision question is whether the public record supports two more demanding conclusions: first, that CrowdStrike's technical root-cause account is sufficiently corroborated for responsible factual reliance; and second, that the principal controls introduced after the incident can be treated as materially implemented rather than merely promised.

This Focused Evidence Review tests both propositions, separates independently corroborated facts from vendor-dependent technical detail, tests alternative explanations, examines the post-incident control record through August 2026 and identifies the point at which public-source research reaches a genuine non-public evidence ceiling.

Reliance boundary

This public portfolio summary must be read with the full dossier, Claims-and-Evidence Matrix, Master Chronology and Source and Evidence Register. Evidence Cut-off: 21 August 2026. Status: APPROVED FINAL PUBLIC EDITION.

What the complete case pack demonstrates

The Focused Evidence Review demonstrates how Aperture Research Works separates claims, source authority, contrary evidence, unresolved gaps and the level of reliance the record can responsibly support. It does not imply that the subject commissioned or endorsed the work.

DOCUMENT 6

FINAL DELIVERY MANIFEST

File-level control, release status and technical production record

Final Delivery Manifest

Control	Recorded value
Public brand	Aperture Research Works
Matter	CrowdStrike: Did the Evidence Verify Both the Cause and the Fix?
Product / capability	Focused Evidence Review
Document	Complete Case Pack (CCP)
Document version	1.0
Governing master	PHW Research AI v11.0
Operating mode	Independent Public-Source Case Study - Not a Client Engagement
Evidence Cut-off	21 August 2026
PDF production date	23 August 2026
Package status	APPROVED FINAL PUBLIC EDITION
Human approval of exact PDF	Paul Hattingh | 23 August 2026 | Human-approved for public release
Public-source links	17 clickable descriptive public-source links in the Source and Evidence Register
Output filename	APERTURE_CROWDSTRIKE_CCP_APPROVED_FINAL_PUBLIC_V1.0.pdf

Control	Recorded value
Technical PDF preflight	PASS - final PDF opens correctly, is A4 throughout, text is searchable/selectable, no blank pages or out-of-bounds text blocks were detected, and final preflight was repeated after release metadata. Page count: 30.
Page-by-page render inspection	PASS - all 30 pages rendered at 200 DPI and visually inspected after final release metadata; no clipping, overlap, broken glyphs or unintended blank pages detected.
Font audit	PASS - only permitted embedded Carlito and Liberation Sans families detected; no silent font substitution detected.
Hyperlink audit	PASS - 19 hyperlink annotations detected, including 17 unique descriptive public-source URLs; links preserved in the final PDF.
External SHA-256	Recorded in companion V105 SHA-256 manifest after the final immutable PDF bytes are created.
Release restriction	Approved for public display as an independent public-source case study. This is not a client engagement, legal opinion, specialist certification or permanent-currentness guarantee.
Final page count	30
Authorised release status	APPROVED FINAL PUBLIC EDITION
Human approver	Paul Hattingh
Human approval date	23 August 2026
Scope of approval	Complete combined case-pack PDF, substantive findings and qualifications, public portfolio presentation, source register, release wording and publication status.
Corrections required by approver	None specified in the 23 August 2026 approval instruction; production-control corrections and release-state corrections implemented under v11.0.
Release-date current-status check	Release-date current-status check completed 23 August 2026. The latest located issuer filings through 21 August 2026 were routine ownership filings and no material official development was identified that changes the incident-causation or remediation-evidence assessment.
Bookmarks and navigation	PASS - 68 top-level/internal bookmark entries detected; document order and navigation checked.
Production Conformity	PASS for Approved Final Public Edition, subject to stated future update triggers.
Mandatory review status	Completed / Not Applicable as recorded for the approved public wording; future-trigger obligations remain controlling.
Final ZIP and hash audit	Performed at package level after the immutable PDF set is frozen; authoritative PDF and ZIP SHA-256 values are recorded in the companion V105 release manifest and QC report.
Included professional functions	Principal Investigative Dossier; Claims-and-Evidence Matrix; Master Chronology; Source and Evidence Register; Public Portfolio Edition; Final Delivery Manifest. The combined PDF is the complete public case pack.
Specialist Appendix status	Not created as a repetitive standalone component. Any genuine specialist-review requirement or technical limitation is disclosed in the relevant dossier and release-control sections.

END OF COMPLETE CASE PACK

CrowdStrike: Did the Evidence Verify Both the Cause and the Fix?

Approved Final Public Edition

REALITY BEFORE RELIANCE.
VERIFICATION BEFORE INTERPRETATION.
EVIDENCE BEFORE NARRATIVE.

Paul Hattingh
Aperture Research Works
info@apertureforensic.com
apertureforensic.com