EOTISEC

NATIONAL SECURITY INTELLIGENCE REPORT FOR BUSINESS

EOTISEC Analytical Division

SECTION 1: REPORT IDENTIFICATION

Report Title	Microsoft 365 and Exchange Online Service Disruption, 12 November 2026 (Incidents EX1550543 and MO1550821)
Report Number	EOTISEC-2026-081c
Date of Report	13 November 2026
Classification	BUSINESS SENSITIVE // EOTISEC SUBSCRIBER DISTRIBUTION
Originator	EOTISEC Analytical Division
Subject	Updated assessment, superseding EOTISEC-2026-081b, of the cause, severity, multi day duration, and the strategic, regulatory, and United States defense contract disclosability consequences of the Microsoft 365, Exchange Online, and multi service disruption that began on 12 November 2026.

SECTION 2: SCOPE AND PURPOSE

This report updates and supersedes EOTISEC-2026-081b and assesses the Microsoft 365 service disruption that Microsoft began tracking on 12 November 2026, first as Exchange Online incident EX1550543[3] and then as the broader multi service incident MO1550821.[4] It answers six questions. What is causing the disruption. Whether a cyberattack is a plausible explanation. How severe the impact is and how long it is running. Whether the concurrent reports of Amazon Web Services and Google outages reflect a shared failure or a reporting artifact. Whether the rumors attributing the outage to a rogue artificial intelligence have any basis. And what the outage means strategically and for disclosure obligations, including whether it is a reportable event for United States defense contractors. The report rests on Microsoft's own status communications and status page text, national, trade, and international press, independent active service checks, outage tracking data, provider status pages, primary regulatory and legal sources, and the published record of comparable incidents. It is current as of roughly 1900 UTC on 13 November 2026, which is 1400 Eastern, and it reflects a second day incident that is recovering in phases but still formally open. Vendor status pages are treated as weak evidence during an active outage, because they can lag or be degraded, so provider health claims are tested against independent probes rather than taken at face value. The report treats the concurrent and separate Windows update and Outlook vulnerability matters of the same week only as context for the broader Microsoft risk picture.

SECTION 3: KEY JUDGMENTS

Each judgment below is a primary analytical conclusion. ICD 203 probability language applies throughout. A confidence level with a rationale follows each judgment, and a business impact statement follows that.

KEY JUDGMENT 1: We assess that the disruption is very likely an internal fault, a cascading capacity loss now most consistent with a recent Microsoft configuration change, and that a cyberattack is very unlikely. Microsoft says a large number of its servers failed automated health checks and dropped out of service, which concentrated load on the rest, and it named a core process that establishes secure connections, and later an upstream authentication and routing configuration component, as the point of failure. Over the second day Microsoft began reverting a recent network configuration change that it says correlates with the start of impact, and reported that patching that authentication and routing component improved server stability. Microsoft states that overall traffic did not increase and has repeatedly reported no evidence of malicious activity.

Confidence: Moderate. *The internal fault finding is now strongly supported, and the attack alternative is weak. A denial of service presents as a traffic flood, and Microsoft describes the opposite, lost capacity under normal*

demand, with no actor claim more than a day in. The judgment that a specific configuration change is the trigger stays at Moderate, not High, because Microsoft has not published a confirmed root cause, its public account has shifted more than once, and the only party holding the logs is the vendor whose own change is implicated.

BUSINESS IMPACT: *Treat this as an availability event, not a breach. A configuration change trigger creates no data breach notification duty, but it sharpens vendor accountability and service credit questions. Keep security teams watching for opportunistic phishing and help desk impersonation while Microsoft Defender XDR access is degraded.*

KEY JUDGMENT 2: We assess that the event has very likely become a multi day degradation rather than a same day recovery. Microsoft's first day mitigations did not hold, restored servers failed again as traffic returned, and the incident remained open and formally degraded more than twenty six hours after it began, with no restoration time given. Recovery is proceeding in phases as Microsoft throttles traffic, rebuilds capacity, and reverts the implicated configuration, and residual mail flow and backlog effects will outlast the main incident.

Confidence: Moderate. *This supersedes the prior estimate of recovery within one business day, which the event overtook. The multi day course is now observed, not forecast. Confidence is held at Moderate on the forward question of when full stability returns, because recovery has been non linear and Microsoft has given no reliable timeline.*

BUSINESS IMPACT: *Plan for continued degraded access and residual mail delays into a second and possibly third day. Microsoft extended its email timeout window to forty eight hours to preserve delayed messages, a signal that clearing the backlog, not only restoring access, will take time. Do not stand down continuity measures on a green status board alone. Verify against your own tenant.*

KEY JUDGMENT 3: We assess that the disruption very likely caused material loss of email and collaboration capability across a wide and still growing set of Microsoft 365 services, in dozens of countries, with the heaviest effect falling across successive business days in the Americas, Europe, and Asia Pacific. Microsoft's affected service list grew from roughly eleven on the first evening to about twenty by the second day, spanning Exchange Online and the services that depend on it, and the admin center and security console were themselves intermittently unreachable. Reporting put the footprint at about seventy four countries, against a Microsoft 365 base the company puts at more than four hundred thirty million users.

Confidence: High. *The impact is directly observable across Microsoft's own expanding service list, more than one hundred thousand user reports at peak, and named disruptions to governments, police forces, financial venues, health providers, and transport operators across several continents.*

BUSINESS IMPACT: *Email and collaboration dependent operations slow or stop for the duration, and the degraded Defender XDR console weakens security monitoring at the same time. Organizations whose incident coordination runs on Teams or Exchange need an out of band channel now. Multinational operations should expect the effect to follow the business day across regions and should coordinate recovery checks accordingly. Finance and operations teams that rely on email approvals should expect delays and should not route time sensitive transactions through affected mailboxes until service is confirmed stable.*

KEY JUDGMENT 4: We assess that a comparable Microsoft cloud disruption is very likely to recur within the next 6 to 12 months. Microsoft absorbed major Microsoft 365 availability incidents in January and August 2026, a global Azure Front Door outage in October 2025, and further incidents in 2024, despite public commitments to staged rollouts and faster recovery.

Confidence: Moderate. *The recurrence pattern is well documented across multiple independent accounts and across more than one failure mode. The exact timing of the next incident is an inference, not an observation.*

BUSINESS IMPACT: *Organizations that treat this as a one off will be unprepared for the next one. Build Microsoft 365 availability failure into continuity planning as a recurring operational risk, not an exception. Budget for an independent secondary channel for critical communications and for periodic drills that assume*

Exchange, Teams, and the admin center are unavailable at the same time.

KEY JUDGMENT 5: We assess that the concurrent Amazon Web Services and Google outage reports were very likely secondary effects of the Microsoft event rather than a shared upstream failure. The signal was a mix of outage tracker cross reporting and genuine minor latency and errors on downstream providers as automated systems failed over and shifted load off the affected Microsoft services. Independent active checks and the providers' own status pages showed AWS and Google operating normally apart from minor regional items.

Confidence: Moderate. *Several independent observation methods agree that no broad AWS or Google outage was underway, and the most credible outlet attributes the signal to user reports rather than confirmed provider outages. Confidence stays at Moderate because status data can lag during a large event, and some real downstream degradation from load transfer is expected and hard to measure precisely.*

BUSINESS IMPACT: *Do not describe this to staff or clients as an internet wide or coordinated event. The confirmed disruption is Microsoft 365. Expect brief latency or errors on services that fail over or share integrations, and treat those as transient. Overstating scope triggers unnecessary failover and erodes trust when the broader claim does not hold.*

KEY JUDGMENT 6: We assess that the rumors attributing the outage to a rogue artificial intelligence or to AI automation are very likely false. The AI services in the Microsoft environment were downstream victims of the outage, not its cause. Microsoft 365 Copilot was among the degraded services, and third party assistants including OpenAI and Anthropic reported that their Microsoft 365 connectors stopped working. The only automation Microsoft has implicated is deterministic infrastructure automation, the server health check and traffic management systems, which is not artificial intelligence. Microsoft has named a secure connection and authentication routing fault and a configuration change, and nothing in its account or in independent reporting ties the event to an AI system acting on its own.

Confidence: High. *The victim not culprit pattern is directly observable, and the implicated components are conventional control plane automation. The kernel of truth that feeds the rumor is that an automated health check loop shed capacity faster than it could be restored, which is automation failure, not artificial intelligence.*

BUSINESS IMPACT: *Correct the rogue AI framing with staff and clients. Misattributing an infrastructure fault to AI distorts risk decisions and can drive misplaced controls. The governable AI exposure here runs the other way. Business processes that now depend on AI assistants inherit the availability risk of the platform beneath them, which this outage made concrete.*

KEY JUDGMENT 7: We assess that the outage will very likely intensify European and allied digital sovereignty and operational resilience pressure on Microsoft, that it is unlikely to drive material migration off the platform in the near term, and that Microsoft's direct financial and legal exposure for the outage itself is likely limited. European lawmakers and officials have already framed the event as a sovereignty test, but analysts across the same coverage note that no European provider can replace Microsoft 365 at the scale governments and banks require, so the realistic near term response is resilience investment and oversight pressure rather than departure. Microsoft's enterprise service level agreement caps the remedy for downtime at service credits, and the CrowdStrike litigation shows how liability caps and the economic loss rule blunt customer damage claims for outage losses.

Confidence: Moderate. *The sovereignty reaction and the oversight posture are observed. The forward call that behavior will not materially change rests on the absence of a credible alternative and on the CrowdStrike precedent, which is a strong analogy but not a certainty. A sovereign or sector mandate could change the picture over a multi year horizon.*

BUSINESS IMPACT: *Expect regulators in the European Union and the United Kingdom to treat this as evidence for the critical third party oversight regimes already in force, and expect customers to ask for exit plans and resilience commitments rather than to leave. Build continuity on the assumption that the platform stays and*

fails again, not on the assumption of a switch. Details and the United States defense contract disclosability question are in Sections 6 and 7.

SECTION 4: SITUATION AND BACKGROUND

Timeline and Current Situation

The day opened with a separate Microsoft Teams incident in North America, tracked as TM1550488, which Microsoft reported resolved by around noon Eastern after automated recovery reduced impact.[1112] Microsoft then began tracking the Exchange Online incident at 1617 UTC under EX1550543.[3] User visible impact built through late morning Eastern time. Outlook user reports on Downdetector passed one hundred thirty one thousand near 1:18 p.m. Eastern, Microsoft 365 reports ran into the tens of thousands, and Copilot and Teams drew several thousand each.[89] These are counts of user submitted reports, not counts of affected mailboxes, so they indicate scale rather than a precise victim total.

Microsoft first said it was investigating issues accessing Exchange Online mailboxes through multiple connection methods in the Americas, naming Outlook on the web, Messaging API, Exchange ActiveSync, and the REST API.[13] About thirteen minutes later it widened the stated scope to any region.[2] At 1826 UTC it opened the broader incident MO1550821, which grew over the afternoon to roughly eleven services, including Exchange Online, Teams, SharePoint Online, Copilot 365, Defender XDR, Planner, To Do, Purview, Intune, and Power BI, with OneDrive, Office for the web, and the Intune and apps admin tooling also affected.[43132] An early status update framed the event as elevated load across multiple regions and said Microsoft was reviewing an unexpected increase in a type of service traffic.[56] Microsoft then walked that framing back. At 1931 UTC it said the elevated load was not driven by an increase in traffic, but by a number of servers becoming unexpectedly unavailable and straining the remaining infrastructure.[26] The public status page and the admin center were themselves intermittently unreachable during the event.[10] A tenant level mirror also showed concurrent same day incidents for Intune, Purview, and SharePoint Online.[13]

Microsoft's account of the mechanism sharpened through the evening. It said the affected servers were failing automated health checks and being pulled from service, that it had not found any recent change correlated with the start of impact, and that the failed checks might originate from a specific component responsible for processing server health. It paused all deployments, moved traffic off the affected infrastructure, and restarted affected servers.[27] Near 2100 UTC it validated an alternative health check method that returned a subset of servers to service and began applying it more broadly.[28] Relief did not hold. Microsoft said the actions taken so far had not provided the anticipated relief, and it narrowed the mechanism to a core process that establishes secure connections becoming overwhelmed, with elevated processor use, which made servers stop responding and shed capacity. It prepared a configuration change for that behavior and validated it on a subset before a wider rollout. Microsoft also said it had identified a small number of recent configuration updates it might revert, which sat awkwardly against its separate statement that it had found no change correlated with the start of impact.[2932] Recovery stayed fragile overnight. Microsoft reported that restored servers initially stayed healthy but could fail again once they began receiving traffic, so it throttled load and rebuilt capacity in batches, and by late Thursday evening Eastern user reports had fallen well below a peak that trackers put between roughly 130,000 and 138,000, though tens of thousands of residual reports remained and neither incident was declared resolved.[3334]

The incident did not close overnight. Into the early hours of 13 November Microsoft adjusted traffic protocols, redistributed load, and applied deliberate traffic blocking, and reported that its own routing services were sending a surge of calls to the backend servers, partly a consequence of the traffic moves it had made during the event, a self inflicted retry storm layered on the original fault. It also began reverting a recent network configuration change that it now said correlated with the start of impact, a reversal of its earlier statement that no correlated change was found, and that revert was still not fully applied hours later.[36] Through the Friday business day in Europe and the Americas Microsoft reported marginal success, early stabilization, and gradually restored traffic, and said patching an upstream authentication and routing configuration component improved server stability.[3738] It extended its email timeout window to forty eight hours to preserve delayed messages. As of roughly 1900 UTC on 13 November, more than twenty six hours after the Exchange incident began, Microsoft still listed the service as degraded, said capacity

had not fully returned to baseline, reported no evidence of malicious activity, and had not published a root cause or a restoration time, with a full post incident review promised only after mitigation.[3739]

Multinational Impact

The footprint was global and reached into government and critical services. In the United Kingdom several police forces, among them the Metropolitan Police and forces in Lincolnshire, Hertfordshire, South Wales, and Merseyside, told the public to report by telephone, and councils, schools, Parliament, and the Insolvency Service reported email disruption, while Guy's and St Thomas' in London lost email but kept procedures running.[4041] In continental Europe the exchange operator Euronext said its email was unavailable, the Swiss luxury group Richemont postponed an earnings release, and Germany's Deutsche Bahn reported significant internal communication delays.[4140] In the Asia Pacific region government offices in Japan fell back to paper, and in Australia the domestic intelligence agency and the federal police were among those affected.[40] Third party artificial intelligence assistants from OpenAI and Anthropic reported that their Microsoft 365 connectors stopped working, a downstream effect that bears on the rogue AI question in Key Judgment 6.[3930] The breadth across governments, police, financial venues, health providers, and transport operators on several continents is the basis for the scope judgment and for the sovereignty assessment in Section 6.

The Multi-Provider Outage Question

Several outlets reported that Amazon Web Services and Google were down the same day, and some early comments tied the Microsoft disruption to Azure Front Door. The evidence did not support a shared upstream failure. The most credible outlet, CNBC, attributed the AWS and Google signal to user reports on Downdetector rather than confirmed provider outages.[7] A meta tracker that reads many sources at once found no internet wide outage on 12 November, with AWS, Google Cloud, and Azure all clear or showing no broad incidents, and only older events in searches for internet, cloud, and routing problems.[14] Because a status page can lag or be degraded during an outage, provider health was tested with methods that do not depend on a single vendor page. A direct server check reported aws.amazon.com online and responding in about 310 milliseconds, and the official AWS status page showed the large majority of components operational with only minor regional incidents.[15] Google Cloud reported no broad severe incidents, and independent checks showed the service operational.[16] Cloudflare's own status page listed only resolved minor issues and scheduled data center maintenance, while its user reports spiked at the same minute as the Microsoft surge, the signature of cross reporting.[17]

The downstream signal was not purely noise. When a platform the size of Microsoft degrades, automated failover and client retries shift load onto other providers, content delivery networks, and shared integrations, and that transferred load can produce real but minor latency and errors on those downstream services. This explains how AWS, Google, and Cloudflare could show small genuine blips while their own status pages and active probes still read healthy. Some Google Workspace users also reported trouble reaching Google hosted email through Outlook desktop and mobile clients, a Microsoft side failure surfacing as a Google problem.[30] The effect is secondary to the Microsoft event, not evidence of a common cause.

Concurrent Security Context

Two separate Microsoft matters surfaced in the same week and should not be read as part of the outage. Microsoft's 10 November Patch Tuesday fixed more than a thousand flaws, including an actively exploited Outlook vulnerability tracked as CVE-2026-124194, which Microsoft's service advisories have not linked to the outage.[2430] Microsoft also confirmed Windows update installation failures and SQL Server performance problems tied to recent updates.[25] Neither is evidenced as a cause of the outage, but the Outlook flaw matters because the outage creates a social engineering window on the same product.

Historical Precedents

The recent record gives a base rate and two distinct failure modes. On 22 and 23 January 2026 a Microsoft 365 outage ran for nearly ten hours after Microsoft reported that a portion of service infrastructure in North America was not processing traffic as expected, recovered by restoring infrastructure and balancing traffic.[18] Microsoft reported further significant disruptions during 2026, including an Exchange Online incident that began 31 August and was mitigated on 3 September, which Microsoft tied to core authentication configuration used by multiple internal services, the closest analog to the authentication and routing component implicated this time.[1935] A different mode

appeared on 29 October 2025, when an inadvertent configuration change to Azure Front Door produced a global outage that Microsoft recovered by rolling back to a last known good configuration, a precedent that now looks directly relevant given the configuration revert under way in this event.[2223] The case that keeps the attack alternative from being fully closed is June 2023. Microsoft first declined to name a cause for a wave of Outlook and OneDrive outages, then confirmed they were denial of service attacks by the group known as Anonymous Sudan.[2021] Today's event most resembles the 2025 and 2026 configuration and load patterns, and Microsoft's own mechanism points inward, but the 2023 precedent is why the attack alternative is weakened rather than erased.

SECTION 5: ANALYSIS

Assumptions

Assumption 1: No threat actor is responsible and the cause is an internal fault. This is supported by Microsoft's stated server health mechanism, its capacity restart response, its own finding that traffic did not increase, and now by its reversion of a recent configuration change it says correlates with the start of impact. It fails if Microsoft links the server failures to malicious action, or if a credible attacker claim or intrusion indicator emerges.

Assumption 2: Microsoft's public and status page communications are materially accurate and do not understate scope or duration. The event has already shown this assumption strained, because Microsoft's affected service count rose over time and its cause account reversed on whether a configuration change was involved. It fails further if the true scope or length proves materially larger than Microsoft has stated.

Assumption 3: The recovery profile of comparable 2026 load incidents, roughly several hours to about one business day, was the initial guide for duration. This assumption did not hold. The event ran past one business day into a multi day course as load re amplified through client and service retries, and Key Judgment 2 has been revised accordingly. The failure of this assumption is recorded here as a correction, not buried.

Assumption 4: Subscriber organizations have at least a minimal out of band way to communicate and do not depend only on Exchange and Teams to coordinate their own response. It fails where the organization's incident bridge itself runs on the affected tenant.

LINCHPIN ASSUMPTION: Assumption 1 is the linchpin. The entire response posture, continuity rather than incident response, depends on this being an internal fault and not an attack. The configuration revert and the sustained absence of any actor claim more than a day in have strengthened the linchpin, so the posture holds. It still flips if Microsoft or an independent source links the failure to malicious action, in which case Key Judgment 1 inverts and the recommended actions change immediately. This assumption should be revisited at each update cycle and the moment Microsoft publishes a root cause.

Analysis of Alternatives

For Key Judgment 1, the primary alternative hypothesis is that a denial of service campaign or other external traffic event, rather than an internal fault, is driving the load. We assess this alternative as very unlikely, because Microsoft withdrew the traffic increase framing and stated that overall traffic did not increase, because the implicated fault is an internal configuration and secure connection process, and because no actor has claimed responsibility more than a day in. The June 2023 Anonymous Sudan precedent is the only reason it is not fully excluded.

For Key Judgment 2, the primary alternative hypothesis is now the reverse of the original one, that recovery completes quickly and cleanly within the first day. We assess that alternative as overtaken and very unlikely, because the first day mitigations did not hold and the event has run into a multi day course. The remaining forward uncertainty is how many more days full stability takes, not whether the one day estimate was right.

For Key Judgment 3, the primary alternative hypothesis is that impact is cosmetic or limited to a small subset of tenants with little business loss. We assess this alternative as very unlikely, given the growth to about twenty services, the footprint of about seventy four countries, the more than one hundred thousand user reports, and the named disruption to governments, police, financial venues, and health providers.

For Key Judgment 4, the primary alternative hypothesis is that Microsoft's hardening work reduces recurrence enough that no comparable outage occurs within twelve months. We assess this alternative as unlikely, because comparable incidents kept recurring across 2024, 2025, and 2026 despite earlier hardening commitments.

For Key Judgment 5, the primary alternative hypothesis is that AWS and Google suffered a genuine shared outage that their status pages failed to report because the reporting plane was itself degraded. We assess this alternative as unlikely, because independent active probes that bypass the status pages showed both providers responding normally, and a review of routing and domain name system incidents found nothing network wide, though some real downstream degradation from load transfer is expected.

For Key Judgment 6, the primary alternative hypothesis is that an artificial intelligence system or AI driven automation genuinely caused or materially worsened the outage. We assess this alternative as very unlikely, because the AI services were degraded victims and the implicated automation is conventional health check and traffic control rather than AI. The alternative cannot be fully closed until the post incident review details what the automation did, but nothing in the record supports an AI cause.

For Key Judgment 7, the primary alternative hypothesis is that the outage triggers material migration away from Microsoft and significant direct liability. We assess this alternative as unlikely, because no alternative provider matches Microsoft's scale for the largest customers and because service credit caps and the economic loss rule limit recoverable damages, as the CrowdStrike litigation shows. A sovereign procurement mandate or a sector rule could change this over a multi year horizon.

Implications by Customer Sector

Defense Industrial Base and Federal Contractors: Email and collaboration downtime slows proposal work, contract correspondence, and coordination with government counterparts on deadline, and the degraded Defender XDR console weakens monitoring during the window. Confirm that any contractual reporting clock does not require an email channel you cannot reach, document the outage window and its operational effect, and keep a security analyst watching endpoint and identity telemetry directly while the cloud console is degraded. Whether this event is itself a reportable cyber incident under United States defense rules is addressed in Section 7.

Financial Services: Email based approvals, client communications, and trade confirmations are exposed to delay. Do not route time sensitive or payment related instructions through affected mailboxes until service is confirmed stable, because delayed and later delivered mail raises both operational and fraud risk. Treat any payment change request received during the disruption with added scrutiny. European Union and United Kingdom financial entities should also map the event to the operational resilience regimes in Section 6.

Healthcare: Clinical and administrative email, scheduling, and secure messaging may degrade during the business day. Fall back to established downtime procedures and a non Microsoft contact method for urgent coordination. Verify that patient facing and on call communication paths do not depend solely on the affected services.

Small and Mid-Size Enterprises with their Managed Service Providers: Smaller organizations feel full business impact with the least slack and often no secondary channel. Service providers should expect a surge of client tickets and should send a single clear status note to clients using a channel outside Microsoft 365. Prioritize verifying client tenant recovery over relaying Microsoft's public status, which was itself unreachable at times during the event.

Multinational Subscribers: Readers outside the United States face their own reporting and resilience regimes rather than the United States defense rules in Section 7. European Union financial entities fall under the Digital Operational Resilience Act and United Kingdom financial firms under the critical third parties regime, both of which treat a major cloud availability failure as a resilience and oversight matter. Map the outage to the incident notification and operational resilience obligations that apply in your jurisdiction, and document the operational effect for your regulator.

Changes from Prior Assessment

This report, EOTISEC-2026-081c, supersedes EOTISEC-2026-081b of 12 November 2026 and extends it through roughly 1900 UTC on 13 November. Four things changed. First, the duration judgment was overtaken by events. The prior central estimate of recovery within one business day did not hold, and Key Judgment 2 now states a multi day course that is observed rather than forecast. Second, the cause picture firmed. Microsoft moved from finding no

correlated change to reverting a recent configuration change it says correlates with the start of impact and patching an authentication and routing component, so the internal fault finding is stronger and a configuration change trigger is now the leading unconfirmed explanation, while a cyberattack is very unlikely. Third, the scope grew, from roughly eleven services to about twenty and to a footprint of about seventy four countries, with named disruption across governments and critical services on several continents. Fourth, two questions were added that were not in the prior cut, the rogue artificial intelligence rumor, addressed and rejected in Key Judgment 6, and the strategic, regulatory, and disclosability consequences, addressed in Key Judgment 7 and in Sections 6 and 7. The report should be updated again when Microsoft publishes its post incident review and root cause, and the moment any credible evidence of an attack emerges.

SECTION 6: STRATEGIC IMPLICATIONS AND REGULATORY OUTLOOK

This section looks past the outage window to the consequences a national security executive will be asked about. What Microsoft owes, what it can be sued for, whether customers will leave, and who, if anyone, will independently establish what happened. The readership for this report is multinational, so the outlook spans the European Union, the United Kingdom, and allied jurisdictions as well as the United States.

Service Credits and Direct Cost

Microsoft's direct contractual exposure for the downtime is small and bounded. Its enterprise service level agreement commits to 99.9 percent monthly availability for Exchange Online and comparable services and makes service credits the customer's sole and exclusive remedy, calculated as a percentage of the monthly fee for the affected service and claimed by the customer within a set window.[48] Credits rise with the depth of downtime, commonly reaching twenty five, fifty, and one hundred percent of the affected service's monthly fee as availability falls, so even a full day of lost Exchange access converts to a fraction of one month of one service's subscription, not to compensation for the business a customer lost. The practical result is that the headline cost to Microsoft is reputational and regulatory, not the credits. Subscribers should still file for the credits they are owed, document the outage window precisely, and read the sole remedy and consequential damages exclusions in their own agreements before assuming any further recovery.

Litigation Exposure

Customer litigation against Microsoft for outage losses faces a steep climb, and the recent CrowdStrike experience is the clearest guide. After the July 2024 CrowdStrike update disrupted much of Delta Air Lines, Delta sued for more than five hundred million dollars, and in May 2025 a Georgia court let only its gross negligence and computer trespass claims proceed while dismissing fraud, product liability, and deceptive practices claims, holding that Georgia's economic loss rule and the parties' contractual liability cap barred tort recovery of economic losses.[45] CrowdStrike publicly estimated its worst case exposure in the single digit millions, and the passengers' own class claims were dismissed on federal preemption grounds. A Microsoft outage with no faulty code pushed onto customer systems, no compromise, and a service level agreement that names credits as the sole remedy gives a plaintiff even less to work with than Delta had. Absent proof of gross negligence or willful misconduct, which a configuration change finding would not by itself establish, direct liability to customers is likely limited. This is a central reason to expect little behavioral change, the same pattern seen after CrowdStrike, where few organizations actually left the vendor.

Digital Sovereignty and the Migration Question

The outage landed in the middle of Europe's digital sovereignty debate and has sharpened it. European lawmakers, including members of the European Parliament, and sovereignty advocates framed the event as a demonstration of overdependence on a single American provider, and a Spanish survey released the same week reported strong public support for European owned technology.[42] The strategic reality cuts against a migration, though. Analysts across the same coverage agree that no European provider can replace Microsoft 365 at the scale a bank, a ministry, or a hospital system requires, so the near term response is very likely to be resilience investment, exit plan and oversight pressure, and procurement leverage rather than departure. The judgment, stated in Key Judgment 7, is that the sovereignty wind is real and will shape policy and contract terms, but that it will not move material workloads off Microsoft in the near term for want of a credible alternative.

Regulatory Oversight and Investigations

The more concrete consequence is oversight. In the European Union, the Digital Operational Resilience Act gives the European Supervisory Authorities direct oversight of designated critical information and communications technology third party providers, and on 18 and 19 November 2025 those authorities named their first list of nineteen such providers, Microsoft Ireland Operations among them, which places Microsoft's service to the European financial sector under a standing resilience oversight regime.[44] The United Kingdom has built a parallel statutory critical third parties regime under which the Bank of England, the Prudential Regulation Authority, and the Financial Conduct Authority can oversee designated providers to the financial sector, including major cloud operators.[47] Neither regime is a fault finding investigation of this outage, but both give regulators a standing basis to demand resilience evidence and incident information, and an event of this visibility is the kind of case those regimes were built to examine. Subscribers in regulated sectors should expect their own regulators to ask how they depend on Microsoft and what their continuity plan is, independent of anything Microsoft discloses.

The Absent Forensic Reviewer

One structural gap shapes what the public will ever learn. The only authoritative account of the cause will be Microsoft's own post incident review, and the one body that previously performed an independent forensic review of a Microsoft failure no longer functions. The United States Cyber Safety Review Board, which in its review of the 2023 Storm-0558 intrusion found a cascade of avoidable Microsoft errors and called that intrusion preventable, had all of its members removed in January 2025 and was not reconstituted in the months that followed, despite calls from senators to restore it.[46] There is therefore no standing United States equivalent of an air safety board to examine this outage. For an availability event the absence matters less than it would for an intrusion, but the pattern holds. The party with the logs, the vendor whose own configuration change is implicated, is also the only party that will narrate what happened. Read Microsoft's eventual post incident review as the account of an interested party, corroborate it where independent telemetry allows, and weight it accordingly.

SECTION 7: DISCLOSABILITY UNDER UNITED STATES DEFENSE CONTRACTING RULES

Subscribers asked whether this outage is a disclosable event for United States defense contractors, specifically under the safeguarding and cyber incident reporting clause at DFARS 252.204-7012 and the Cybersecurity Maturity Model Certification program. The determination belongs to each covered contractor, with its contracting officer and legal counsel, and this section is analysis rather than legal advice. On the facts known as of this writing, the dominant reading is that the outage is not a reportable cyber incident under the clause, with two conditions that each contractor must check for itself.

The reporting trigger and why it probably does not attach

DFARS 252.204-7012 requires a contractor to rapidly report, within seventy two hours of discovery, a cyber incident that affects a covered contractor information system, the covered defense information residing on it, or the contractor's ability to perform requirements designated as operationally critical support, with reports filed to the Department of Defense at the DIBNet portal.[43] The clause defines a cyber incident as actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system or the information on it.[43] The operative words are actions taken through the use of computer networks, which contemplate an adversary act. Microsoft has stated repeatedly that it found no evidence of malicious activity and has described an internal capacity and configuration fault, and nothing in the record indicates a compromise of covered defense information or unauthorized access. An availability loss, without a compromise or an adversary action, does not fit the definition, so the seventy two hour report is generally not triggered by this event.

The two conditions to check

Two conditions can change that reading for a particular contractor. The first is operationally critical support. The clause's reporting duty extends to a cyber incident that affects a contractor's ability to perform support the Government has designated as operationally critical, a narrow category tied to airlift, sealift, and intermodal transportation and to the logistics that sustain the armed forces in a contingency operation.[43] A contractor that holds such a designation and whose performance was materially degraded by the outage should treat the question as live

and consult its contracting officer, even though the reporting duty still turns on there being a cyber incident in the first place. The second is where covered defense information actually resides. A contractor whose controlled unclassified information enclave runs inside the affected Microsoft environment, in a government cloud edition for example, should confirm that the outage touched availability only and did not expose or alter that information. If a contractor cannot rule out a confidentiality or integrity effect on covered defense information, the conservative course is to preserve evidence and consult the contracting officer before concluding that no report is due.

CMMC and the confidentiality frame

The Cybersecurity Maturity Model Certification program and its underlying control set in NIST Special Publication 800-171 protect the confidentiality of controlled unclassified information. They are an assessment and certification regime, not an incident reporting trigger, and an availability event with no confidentiality impact falls largely outside their reporting ambit. The outage is still relevant to a contractor's program as a documentation and lessons learned matter under the incident handling and risk assessment control families, and the companion lessons learned report LLR-2026-081 is structured for that use, but it does not by itself create a certification or disclosure obligation. Where a contractor's controlled unclassified information actually sat in the affected environment, the event should be recorded in the system security plan and reviewed at the next assessment, not reported as a breach.

Other regimes that may apply regardless

Three other regimes can apply on their own terms, and they use broader tests than the defense clause. For a publicly traded contractor, the United States Securities and Exchange Commission requires disclosure of a cybersecurity incident the company determines to be material, and that materiality test can capture a significant availability event even with no data compromise. For designated critical infrastructure entities, the reporting requirements under the Cyber Incident Reporting for Critical Infrastructure Act, once in effect, will use a definition that expressly includes a substantial loss of availability, which is broader than the defense clause's compromise test. And sector regulators, along with the European Union and United Kingdom resilience regimes in Section 6, impose their own notification duties on the organizations they supervise. The short answer for a United States defense contractor is that this outage is most likely not a DFARS 252.204-7012 reportable cyber incident, that the determination is the contractor's to make with its contracting officer and counsel, and that the live checks are operationally critical support, the actual location of covered defense information, and any broader materiality or availability based regime that applies to the organization independent of the defense clause.

SECTION 8: INFORMATION GAPS AND COLLECTION REQUIREMENTS

For each gap, the format is the gap statement, its analytical significance, and the collection requirement.

1. Gap: Microsoft has not published a confirmed root cause or its post incident review, and whether the implicated configuration change is the confirmed trigger is unresolved.
Analytical significance: Most sensitive to Key Judgments 1 and 2. The named cause decides whether this is cleanly a vendor configuration fault and how the duration is finally characterized.
Collection requirement: Obtain and read the post incident review when published, and compare its named cause against the configuration revert and authentication and routing component patch Microsoft applied during the event. Watch for any attack attribution.

2. Gap: The final geographic and service scope is still settling, after Microsoft's affected service count grew from roughly eleven to about twenty and reporting put the footprint near seventy four countries.
Analytical significance: Most sensitive to Key Judgment 3. Final scope sets aggregate business impact and strengthens the recurring enterprise risk case.
Collection requirement: Monitor admin center scope language, independent monitoring such as ThousandEyes and Cloudflare Radar, and whether more services are added to or cleared from MO1550821.

3. Gap: The size of genuine downstream degradation on AWS, Google, and Cloudflare from failover and load transfer is not precisely measured, and a shared upstream cause cannot be fully excluded while provider status pages may lag.
Analytical significance: Affects Key Judgment 5. A confirmed shared outage would change the event from a Microsoft fault with downstream ripple into a common cause failure.

Collection requirement: Track independent active probes alongside official status pages for AWS, Google, and Cloudflare, watch for any routing or domain name system incident, and separate confirmed provider incidents from cross reporting.

4. Gap: Microsoft has given no restoration time, recovery has been non linear with restored servers failing again under traffic, and it is unclear how many more days full stabilization and backlog clearance will take.
Analytical significance: Most sensitive to Key Judgment 2. It sets how long subscribers must sustain continuity measures.
Collection requirement: Track Microsoft's update cadence, whether restored servers hold under load, the email backlog and the forty eight hour timeout window, and the point at which Microsoft declares the incidents resolved.

5. Gap: Whether any mail was lost, bounced, or delayed rather than only made temporarily inaccessible, now material given the extended forty eight hour email timeout window.
Analytical significance: Affects the business impact under Key Judgment 3. Data integrity effects outlast the outage and carry compliance weight.
Collection requirement: After restoration, review non delivery reports, queue backlogs, and admin center detail on message handling during the window.

6. Gap: Whether degraded Microsoft Defender XDR access allowed any opportunistic activity to go undetected across a multi day window.
Analytical significance: Affects Key Judgment 1 and the security posture under Key Judgment 3. A monitoring gap during a high visibility outage is a known attacker opportunity.
Collection requirement: After restoration, backfill and review Defender and identity logs across the outage window for anomalous sign ins and mailbox rule changes.

7. Gap: Whether individual covered contractors and regulated entities will determine this a reportable event under DFARS 252.204-7012 or analogous non United States regimes is not yet known and is organization specific.
Analytical significance: Affects the disclosability analysis in Section 7. The determination turns on facts each organization must confirm, including operationally critical support and the location of covered defense information.
Collection requirement: Track contracting officer guidance, any Department of Defense or Cybersecurity and Infrastructure Security Agency advisory tied to the outage, and European Union and United Kingdom regulator statements.

8. Gap: Whether Microsoft's eventual root cause account can be independently corroborated, given that Microsoft is the sole holder of the relevant logs and there is no standing United States forensic review body.
Analytical significance: Affects confidence in Key Judgment 1 and the credibility weighting in Section 6. A vendor narrating its own failure has an advocacy interest.
Collection requirement: Seek independent telemetry from third party monitoring, customer tenant evidence, and any regulator findings, and weight the vendor account accordingly.

SECTION 9: SOURCE SUMMARY STATEMENT

This report draws on six source types. First, primary corporate communications from Microsoft, specifically the Microsoft 365 Status posts on X, the status.cloud.microsoft update text, and the admin center records for EX1550543, MO1550821, and TM1550488. These carry first party advocacy risk, because a vendor describing its own outage has reason to frame scope and cause favorably, and they are treated accordingly. The admin center text was read through third party university and research network status mirrors that republish the feed, not through the authenticated admin center, so the wording is reliable but the access path is indirect. Second, established national, trade, and international press, used for impact scale, multinational effects, and timeline. Third, independent monitoring and outage tracking data, used as indicators of user reported impact. Fourth, independent active service checks and provider status pages for Amazon Web Services, Google Cloud, and Cloudflare, with status pages read as weak evidence during an outage and cross checked against probes that do not depend on them. Fifth, primary regulatory and legal sources read directly, the DFARS clause text on the federal acquisition site, the European Supervisory Authorities' designation of critical third parties, and the public record of the CrowdStrike and Delta litigation. Sixth, the published record of comparable 2023 through 2026 incidents.

Source limitations are flagged. Downdetector figures are counts of user submitted reports, not counts of affected mailboxes or users, and different outlets cited different peaks, so they are used only as scale indicators. Recycled content was caught and excluded across both cuts, including one aggregator presenting 2024 CrowdStrike era impact such as grounded airlines and stock exchange disruption as current, one article describing the June 2025 Google Cloud outage as if it were today, and university status pages describing the separate January 2026 and November 2024 Microsoft outages, which were set aside. Microsoft's own account evolved during the event, from elevated load and a traffic review to an explicit statement that traffic did not increase, and from no correlated change to reverting a configuration change it says correlates with the start of impact, so earlier framings were superseded and the latest Microsoft statements are given precedence while the reversal itself is treated as a finding. One secondary claim, the exact date the United Kingdom began overseeing a designated critical third party, could not be confirmed at an authoritative source and is stated only at the level of the regime's existence and powers, not tied to a specific date. The CVE-2026-124194 Outlook flaw is carried as concurrent context only, not as a cause, consistent with Microsoft's advisories. No classified sources were used. EOTISEC products rely on open source reporting only.

SECTION 10: ICD 503 CONSIDERATIONS AND ATT&CK / D3FEND MAPPING

ICD 503 considerations apply because this incident degrades the confidentiality, integrity, and availability objectives of information systems that subscriber organizations depend on, with availability as the primary objective at risk. The event also degraded Microsoft Defender XDR and the admin center, which impairs an organization's own ability to detect and respond, a security relevant condition in its own right.

Risk to Information Systems and Data: The disruption removes reliable access to enterprise email and collaboration across Exchange Online, Teams, SharePoint, Copilot, and OneDrive, the backbone of most business communication and of many automated workflows. Data flows at risk include inbound and outbound mail, calendar and scheduling sync, and any application that authenticates or routes through the affected connection methods. The extended email timeout window raises the risk that delayed and backlogged mail arrives out of order or late, a data integrity concern. The degraded Defender XDR console is a secondary risk, because it weakens detection exactly when a high visibility outage invites opportunistic phishing and account abuse.

NIST RMF Alignment: The event implicates the Prepare, Assess, and Monitor steps most directly. Organizations should confirm that contingency planning controls in the SC and CP families reflect a single vendor cloud availability failure, that continuity assumptions account for a multi day rather than a same day outage, and that continuous monitoring can function when both the vendor management plane and the security console are degraded. Update system authorization documentation to record this dependency and the continuity path used during the outage.

Supply Chain Risk: Microsoft 365 is a concentrated third party dependency for most subscriber organizations. When the vendor's own service infrastructure fails under load or a configuration change, the effect cascades to every tenant at once, and geographic redundancy inside the same vendor does not protect against a fault that spans regions. This argues for a documented secondary communications path outside Microsoft and for treating vendor concentration as a standing supply chain risk in line with NIST 800-161 guidance. The European Union and United Kingdom critical third party oversight regimes in Section 6 are the regulatory expression of the same concentration concern.

No kill chain phase is supported by forensic evidence in this incident, because no adversary activity is confirmed. The ATT&CK table below maps the denial of service alternative, now assessed very unlikely after Microsoft withdrew the traffic increase framing and retained only for completeness, and the opportunistic threats that accompany any major outage. Every outage related technique is marked ASSESSED. The one REPORTED technique is the concurrent and separate Outlook vulnerability, included for attack surface awareness and labeled as not causal.

ATT&CK Technique Mapping

Technique ID	Technique Name	Tactic	Application to This Report	Status
T1498	Network Denial of	Impact	Primary alternative to the internal fault explanation, now	**ASSESSED**

Technique ID	Technique Name	Tactic	Application to This Report	Status
	Service		assessed very unlikely and retained for completeness. A volumetric or application layer flood would present as elevated load and connectivity errors, which was the early framing, but Microsoft withdrew the traffic increase statement and described lost capacity under normal demand. Microsoft confirmed a denial of service cause for a comparable Outlook and OneDrive outage in June 2023 only after first declining to name one, which is the sole reason this stays mapped.	
T1499	Endpoint Denial of Service	Impact	Application layer request floods against Exchange Online front ends would fit an elevated load pattern, but Microsoft has stated overall traffic did not increase and no actor has claimed responsibility more than a day into the event. Retained for completeness, assessed very unlikely.	**ASSESSED**
T1566	Phishing	Initial Access	Outage themed lures that ask users to reauthenticate Outlook or verify mailbox access are very likely to rise during and after the disruption. The public visibility of this event, with more than one hundred thousand user reports and coverage in dozens of countries, widens the target pool.	**ASSESSED**
T1656	Impersonation	Defense Evasion	Impersonation of Microsoft support, internal help desk, or a managed service provider to harvest credentials or push a malicious fix while users cannot verify through normal channels and the admin center itself is degraded.	**ASSESSED**
T1078	Valid Accounts	Persistence	Credentials captured through outage lures feed account takeover once service returns. Degraded Microsoft Defender XDR access during the window raises the risk that early misuse goes unseen.	**ASSESSED**
T1187	Forced Authentication	Credential Access	Concurrent, not causal. Microsoft's November 2026 Patch Tuesday fixed an actively exploited Outlook flaw that can expose Windows authentication information when a user opens a crafted file. It sits on the same attack surface in the same week.	**REPORTED**

D3FEND Countermeasure Mapping

D3FEND Technique	D3FEND ID	Addresses ATT&CK	Application and Priority
Multi-factor Authentication	D3-MFA	T1078, T1566	HIGH. Phishing resistant MFA blunts the credential theft and account takeover that follow outage themed lures. Confirm MFA stays enforced if any conditional access or sign in path degrades during the incident.
URL Analysis	D3-UA	T1566	HIGH. Filter and detonate links in reauthentication and outage notice lures. Lure volume tracks the public visibility of the outage, which is high across a second day of coverage.
Sender MTA Reputation Analysis	D3-SMRA	T1656, T1566	MODERATE. Catch spoofed Microsoft and help desk senders. Value is real but secondary to direct user warnings while mail flow itself is degraded.
Software Update	D3-SU	T1187	HIGH. Deploy the November 2026 Patch Tuesday release, including the actively exploited Outlook fix. This is independent of the outage and should not wait for it to clear.
Inbound Traffic Filtering	D3-ITF	T1498, T1499	MODERATE. Denial of service mitigation for Exchange Online sits with Microsoft. Subscriber action is limited to confirming that any internet

D3FEND Technique	D3FEND ID	Addresses ATT&CK	Application and Priority
			facing mail gateways and published endpoints sit behind filtering. The priority is not raised, because Microsoft withdrew the traffic increase framing and described lost capacity under normal demand.

Priority designations above are grounded in report specific data. The phishing, impersonation, credential, and patch items are rated HIGH because the public outage creates an active social engineering window across a second day and because the Outlook vulnerability is under active exploitation this week. The denial of service item is held at MODERATE and the control sits mainly with Microsoft, and it is not raised, because Microsoft withdrew the traffic increase framing and described lost capacity under normal demand.

SECTION 11: ANALYTIC TRADECRAFT SELF-CERTIFICATION

ICD 203 Requirement	Status	Notes
Objectivity: The analysis is free of advocacy, personal preference, or policy bias.	**CONFIRMED**	*The report states an availability event as an availability event, resists the breach narrative an outage invites and the reflex to clear the vendor, and states plainly that a prior duration judgment was overtaken by events and revises it.*
Independence of Political Consideration: No judgment was shaped to support a particular outcome or audience preference.	**CONFIRMED**	*Judgments follow the evidence. The duration judgment was revised against the vendor's framing when the event ran long, and the recurrence and limited accountability judgments are unfavorable to the vendor and are stated plainly.*
Timeliness: Source material is current and the report addresses matters actionable by the customer.	**CONFIRMED**	*Sources are tracked through roughly 1900 UTC on 13 November, and the report is written while the incident is open on its second day. Recommendations target the next 24 to 72 hours.*
Based on All Available Sources: All source material provided was considered. Gaps are documented in Section 8.	**CONFIRMED**	*Microsoft status posts and status page text, admin center incident records, national, trade, and international press, independent monitoring and active probes, primary regulatory and legal sources, and the record of comparable incidents were all used. Eight gaps are documented.*
Source Credibility Described: Source quality is addressed in Section 9.	**CONFIRMED**	*Section 9 names each source type, flags Downdetector figures as report counts rather than user counts, records the recycled content caught and excluded, and notes one secondary date that could not be confirmed and is stated only at the level of the regime.*
Uncertainty Expressed: Probability and confidence language conforms to ICD 203 standards.	**CONFIRMED**	*Each judgment carries one probability term and a separate confidence sentence with a rationale. Probability and confidence are never combined in one sentence.*
Assumptions Distinguished from Facts: All assumptions are labeled. Linchpin assumptions are identified.	**CONFIRMED**	*Four assumptions are numbered with failure conditions, one is marked as having failed and driven a revision, and the no adversary assumption is marked as the linchpin.*
Alternatives Incorporated: At least one alternative hypothesis is addressed for each major judgment.	**CONFIRMED**	*Section 5 gives one alternative hypothesis for each of the seven Key Judgments, including the rogue artificial intelligence hypothesis, which is stated and rejected, and the mass migration hypothesis, which is weighed against the absence of a credible alternative.*
Customer Relevance Addressed: Implications for the relevant stakeholder are stated specifically.	**CONFIRMED**	*Implications are written for defense contractors, financial services, healthcare, smaller enterprises and their service providers, and multinational subscribers, with a dedicated disclosability analysis for United States defense contractors in Section 7.*

ICD 203 Requirement	Status	Notes
Clear and Logical Argumentation: The main analytic message is stated up front in Section 3.	**CONFIRMED**	*The seven Key Judgments lead the report. Evidence in Section 4 and analysis in Sections 5 through 7 support them and are kept separate.*
ATT&CK and D3FEND Mapping Completed: REPORTED and ASSESSED attributions are correctly distinguished. Priority designations are grounded in the specific incident.	**CONFIRMED**	*The one REPORTED technique is the concurrent Outlook vulnerability, labeled as not causal. The denial of service techniques are ASSESSED and now rated very unlikely after Microsoft withdrew the traffic increase framing, retained only because June 2023 shows Microsoft has named a denial of service belatedly before. D3FEND priorities reflect the live social engineering window and the active Outlook exploit.*

SECTION 12: ENDNOTES

[1] Microsoft 365 Status (@MSFT365Status). Post on X acknowledging users experiencing issues accessing Exchange Online mailboxes through multiple connection methods in the Americas. 12 November 2026, approximately 1754 UTC.

[2] Microsoft 365 Status (@MSFT365Status). Post on X confirming the issue may affect Microsoft 365 service connectivity for users in any region, and directing admins unable to reach the admin center to an alternate update channel. 12 November 2026, approximately 1807 UTC.

[3] Microsoft 365 admin center, Service Health incident EX1550543, Exchange Online, serviceDegradation, start time 12 November 2026 at 1617 UTC. Incident text read through the University of Pennsylvania PennO365 Microsoft incident mirror and the Earlham College Microsoft 365 status mirror, which republish the admin center feed. The authenticated admin center was not accessed directly.

[4] Microsoft 365 admin center, Service Health incident MO1550821, Microsoft 365 suite, start time 12 November 2026 at 1826 UTC, next update by 2030 UTC. Potentially impacted services listed as Exchange Online, Microsoft Teams, SharePoint Online, Microsoft Copilot 365, and Microsoft Defender XDR. Read through the same status mirrors.

[5] Microsoft, status.cloud.microsoft update of 12 November 2026 at 1832 UTC. Current status text: the affected infrastructure is experiencing elevated load across multiple regions, which is likely contributing to the connectivity errors. Microsoft is restarting and repairing impacted portions of this infrastructure to restore capacity, is reviewing an unexpected increase in a specific type of service traffic to determine whether it is contributing to the elevated load, and is evaluating options to redirect traffic to alternate infrastructure. Relayed through the Hacker News discussion that quoted the status page verbatim.

[6] Deadline. Microsoft Outlook Goes Down In 365 Outage, Paralyzing Business Communication. 12 November 2026. Independently quotes the same Microsoft elevated load and traffic review statement.

[7] CNBC. Microsoft outage hits Outlook. AWS and Google users also report issues. 12 November 2026, published 3:54 p.m. Eastern. Reports that Microsoft determined the outage was caused by an increase in unavailable servers and launched a restart of impacted servers, with the shutdown possibly linked to failed health checks caused by a specific component responsible for processing server health. Attributes the Amazon Web Services and Google signal to user reports on Downdetector, not to confirmed provider outages.

[8] Investing.com. Microsoft services suffer outages affecting hundreds of thousands of users. 12 November 2026. Downdetector recorded more than 130,000 Outlook reports at 1:27 p.m. Eastern, more than 46,000 Microsoft 365 reports, and roughly 3,000 Teams reports, and notes the earlier North America Teams disruption was reported resolved.

[9] Daily Voice. Massive Outage Disrupts Microsoft Outlook, Online Services. 12 November 2026. Outlook more than 131,000 reports at 1:18 p.m. Eastern, Microsoft 365 more than 22,000 by 12:55 p.m., Copilot about 4,400, Teams roughly 2,000, earlier Teams issues resolved by around noon.

[10] Tom's Guide. Microsoft Outlook down for over 100,000 users, live updates. 12 and 13 November 2026. Reporter could not load the Microsoft 365 status page, which appeared to be affected. References EX1550543 and MO1550821, and on 13 November recorded the incident still unresolved with Downdetector above 40,000 reports.

[11] CybersecurityNews. Microsoft Teams Outage Hits Users in North America. 12 November 2026. Teams incident tracked as TM1550488, with automated recovery reducing impact.

[12] Microsoft 365 Status (@MSFT365Status). Post on X: mitigative actions have successfully restored service health and functionality, customer impact is now fully resolved, referencing TM1550488. 12 November 2026.

[13] Earlham College Microsoft 365 status mirror, snapshot at 1804 UTC on 12 November 2026. Shows concurrent same day incidents for Microsoft Intune (IT1549049), Microsoft Purview (MP1507695), and SharePoint Online (SP1548842).

[14] isinternetup.com. Internet and Cloud Outages Today. Updated 12 November 2026, 1935 UTC. Concludes no internet wide outage was detected on 12 November 2026, that searches for internet, cloud, and BGP incidents returned only older events, and that AWS, Google Cloud, and Azure were all clear or showed no broad severe incidents, with Cloudflare showing only routine data center maintenance.

[15] Independent active checks of Amazon Web Services on 12 November 2026. isitdown.page direct server check reported aws.amazon.com online and responding in 310 milliseconds at 2015 UTC. UptimeRobot reported AWS working normally at 1502 UTC. PulsAPI, reading the official AWS status page, reported 5,557 of 5,825 components operational with three active regional incidents, including elevated API and launch failures in the Tokyo region carried over from 11 November. These are observation methods that do not depend on a single vendor status page.

[16] Google Cloud Service Health page, status.cloud.google.com, Americas view, last updated 12 November 2026, 12:27 Pacific. States no broad severe incidents. Independent uptime checks of cloud.google.com reported the service operational with zero user issues in the prior 24 hours.

[17] Cloudflare System Status, cloudflarestatus.com, 12 November 2026. Lists only resolved minor incidents, including a Replicate customer issue and a DNSSEC configuration change, plus scheduled data center maintenance in Frankfurt, Houston, and Newark. No network wide outage. Separately, the Downdetector account on X reported user problems with Cloudflare beginning 1:27 p.m. Eastern, the same minute as the Microsoft report surge, consistent with cross reporting rather than a confirmed Cloudflare outage.

[18] The Register. Microsoft 365 outage drags on for nearly 10 hours during bad night for North American infra. 23 January 2026. Incident MO1221364. Microsoft attributed it to a portion of service infrastructure in North America not processing traffic as expected. Peak near 15,000 Downdetector reports. Recovery near ten hours.

[19] Tri-State Alert. Major Microsoft Outage Disrupts Outlook Email and Microsoft 365 Services Nationwide. 12 November 2026. Notes Microsoft experienced several significant disruptions during 2026, including a January outage and an August incident affecting Outlook, Teams, and other Microsoft 365 applications.

[20] Fortune. Microsoft on major Outlook and OneDrive outages: We were hacked. June 2023. Microsoft was initially reticent to name a cause, then disclosed that distributed denial of service attacks by the group known as Anonymous Sudan were responsible for the June 2023 Outlook, OneDrive, and Azure portal outages.

[21] CBS News. Microsoft blames Outlook and cloud outages on cyberattack. June 2023. Corroborates the Anonymous Sudan denial of service attribution and Microsoft's subsequent tuning of its Azure Web Application Firewall.

[22] ThousandEyes. Microsoft Azure Front Door Outage Analysis: October 29, 2025. Attributes that event to a global configuration push that caused nodes across the fleet to fail to load. Included as a distinct failure mode, different from the load based pattern seen on 12 November 2026.

[23] Microsoft Azure. Preliminary Post Incident Review for the Azure Front Door service disruption of 29 October 2025. Inadvertent configuration change deployed globally due to a defect in deployment safety systems. Mitigation blocked further changes and rolled back to a last known good configuration. Service restored by approximately 0005 UTC on 30 October 2025.

[24] TechRepublic and SecurityWeek. Microsoft November 2026 Patch Tuesday. Released 10 November 2026, including an actively exploited Outlook vulnerability. Outlet totals for the release differ, with SecurityWeek citing 1,094 vulnerabilities, so this report states only that more than a thousand were fixed.

[25] BleepingComputer. Microsoft confirms recent Windows updates cause SQL Server performance issues, and confirms November 2026 security update installation failures on Windows 11. 12 November 2026. Concurrent Windows reliability issues, separate from the Microsoft 365 outage.

[26] Microsoft 365 Status (@MSFT365Status). Post on X, 12 November 2026 at approximately 1931 UTC. The elevated load was not driven by an increase in traffic, but by a number of servers being unexpectedly unavailable, straining the remaining infrastructure.

[27] Microsoft 365 Status (@MSFT365Status). Posts on X, 12 November 2026 between approximately 1950 and 2020 UTC. Affected servers were failing automated health checks and becoming unavailable. Microsoft had not identified any recent change correlated with the start of impact, but its investigation indicated the failed health checks may originate from a specific component responsible for processing server health. Microsoft paused all deployments, moved traffic off the affected infrastructure, and restarted affected servers.

[28] Global News, and Microsoft 365 Status (@MSFT365Status) at approximately 2100 UTC, 12 November 2026. Microsoft validated an alternative service health check method that allowed a subset of affected servers to return to service and began applying it more broadly, and it prepared an automated process to detect and restart unresponsive servers.

[29] Microsoft 365 Status (@MSFT365Status). Posts on X, 12 November 2026 at approximately 2140 and 2210 UTC. The actions taken so far had not provided the anticipated relief. A core process on affected servers was becoming overwhelmed and causing capacity loss. Microsoft was isolating a portion of infrastructure to validate a recovery approach and assessing whether reverting a small number of recent configuration updates would help.

[30] SecurityWeek. Microsoft 365 Outage Disrupts Outlook, Exchange Online and Teams. 12 November 2026. Microsoft traced the increased load to a large number of servers becoming unavailable, said overall traffic had not increased, and disclosed no evidence of a cyberattack. Some Google Workspace users reported trouble reaching Google hosted email through Outlook desktop and mobile clients. The outage came two days after Microsoft's November Patch Tuesday, which included an actively exploited Outlook spoofing flaw tracked as CVE-2026-124194, and Microsoft's service advisories have not linked that flaw to the outage.

[31] WebProNews, citing Associated Press and TechCrunch. Microsoft 365 Outage Cuts Off Outlook for Hours. 12 November 2026. As of the 3:56 p.m. Eastern update Microsoft had not fully restored service or named a root cause. Downdetector peaked near 130,000 Outlook reports. The MO1550821 notice expanded to list Planner, To Do, and Purview among affected services.

[32] The Register. Microsoft struggling to fix massive cloud outage that's taken down email and Intune. 12 November 2026. Microsoft blamed a problem causing servers to fail automated health checks and become unavailable, said it had found no correlated change, described a core process on affected servers becoming overwhelmed and causing capacity loss, and said admin tools including Intune and the Microsoft 365 Apps Admin Center were also unreachable. The Register noted that Microsoft's reference to reverting a small number of recent configuration updates sat in tension with its statement that no correlated change was found, and that in a 00:35 UTC 13 November update returned servers initially stayed healthy but could become unresponsive again once they began receiving traffic.

[33] Pouyam.com. When Will Outlook Be Back Up. Updated 13 November 2026. As of 00:55 UTC on 13 November Microsoft had not declared EX1550543 resolved and had given no time for full recovery, and a 00:06 UTC update noted that restored servers could fail again under traffic, with traffic limits and rebuilds under way.

[34] Flavorist. Microsoft Outage Today: Outlook, Microsoft 365 Recovery Update. 12 November 2026. Records a Downdetector peak of 138,058 reports, notes engineering teams were examining whether recent configuration changes contributed, states the definitive root cause remained under investigation, and reports that complaints declined and some infrastructure recovered while restoration remained incomplete.

[35] Enrow.io. Microsoft Outlook Outage of November 12, 2026: Timeline, Cause, and What Happened to Your Emails. 12 November 2026. Records that the incident reached roughly eleven services by evening, with the incident record reading root cause not available as of 21:45 UTC, and lists prior Exchange Online incidents including one that began 31 August 2026 and was mitigated on 3 September 2026, tied to core authentication configuration used by multiple internal services.

[36] systemdesign.academy and kbytechnologies.com, Microsoft 365 outage coverage checked 05:50 UTC and later on 13 November 2026, relaying Microsoft 365 Status updates. At 04:11 UTC Microsoft said there was no indication the incident was the result of malicious activity. At 04:57 UTC Microsoft said its own routing services were sending a surge of calls to the backend servers, partly as a result of the traffic moves it had made during the event. From about 05:00 UTC Microsoft began reverting a recent network configuration change that it said correlated with the start of impact, a reversal of its earlier statement that no correlated change was found, and that revert was still not fully applied hours later.

[37] Tokai National Higher Education and Research System Microsoft 365 status mirror, incident MO1550821, updates on 13 November 2026 at 16:24, 17:09, 18:03, and 18:57 UTC, which republish the admin center feed. Microsoft reported positive results for server stability after applying an upstream authentication and routing configuration component patch to a portion of its infrastructure, described phased recovery with service health still variable and capacity not yet returned to baseline, said network and traffic management actions remained active, and stated it had extended the email timeout window to 48 hours to preserve delayed messages.

[38] FourWeekMBA. Microsoft 365 Outage Hits 74 Countries, Passes 18 Hours. 13 November 2026. Records that Microsoft's 12:00 UTC service health post on 13 November still listed the service as degraded, that the affected service count had grown from about eleven on the first evening to about twenty, that the outage had passed eighteen hours, that Microsoft reaffirmed no evidence of malicious activity, and that a full post incident report with root cause was promised only after mitigation.

[39] Euronews. Microsoft outage explained: what went wrong and is your data at risk. 13 November 2026. Reports that Microsoft executive vice president Charles Lamanna said the outage did not appear to be a cyberattack, that Microsoft says more than 430 million people use its Microsoft 365 apps, and that Microsoft's explanation shifted over the course of the outage.

[40] CNN and Reuters live coverage. Microsoft global outage, 12 and 13 November 2026. Reports that several United Kingdom police forces told the public to report by telephone, that Germany's Deutsche Bahn reported significant internal communication delays, that in Australia the domestic intelligence agency and the federal police were among those affected, and that a Microsoft executive confirmed the outage was not the result of a security breach.

[41] European Business Magazine and International Business Times. Microsoft outage second day coverage. 13 November 2026. Report that Euronext said its email was unavailable, that the Swiss luxury group Richemont postponed an earnings release, that Guy's and St Thomas' in London lost email while procedures went ahead, that United Kingdom councils, schools, Parliament, and the Insolvency Service reported disruption, and that Microsoft said its fix was not taking as expected.

[42] Al Jazeera, Rapporteur, and trendingtopics.eu. Microsoft outage and European digital sovereignty. 13 November 2026. Report that members of the European Parliament and sovereignty advocates framed the outage as a test of Europe's digital sovereignty, that a Spanish survey reported strong support for European owned technology, and that analysts assessed no European provider could replace Microsoft 365 at the scale governments and banks require, so the likely response is resilience and oversight rather than migration.

[43] United States Department of Defense. DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. Read at acquisition.gov. Defines a cyber incident as actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system or the information residing on it. It defines operationally critical support as supplies or services designated by the Government as critical for airlift, sealift, and intermodal transportation and for logistical support that sustains the Armed Forces in a contingency operation. It requires the contractor to rapidly report, within 72 hours of discovery, a cyber incident that affects a covered contractor information system, the covered defense information on it, or the contractor's ability to perform operationally critical support, with reports filed at the DIBNet portal.

[44] European Supervisory Authorities (European Banking Authority, EIOPA, and the European Securities and Markets Authority). First designation of critical ICT third party providers under Article 31 of the Digital Operational Resilience Act, published 18 and 19 November 2025. The list of nineteen designated providers includes Microsoft Ireland Operations Limited, Amazon Web Services EMEA, Google Cloud, Oracle, IBM, and SAP, bringing those providers under the direct oversight of the European Supervisory Authorities. Confirmed through the ESMA list and the Microsoft Learn DORA compliance page, which states that Microsoft Ireland Operations Limited is identified as a critical third party provider subject to oversight.

[45] CrowdStrike and Delta litigation record. Delta Air Lines sued CrowdStrike in Fulton County, Georgia, over the July 2024 update that disrupted its operations, claiming losses above 500 million dollars. In a 16 May 2025 ruling, Judge Kelly Lee Ellerbe allowed Delta's gross negligence and computer trespass claims to proceed but dismissed its fraud, product liability, and deceptive practices claims, holding that Georgia's economic loss rule and the parties' contractual liability cap bar tort recovery of economic losses. CrowdStrike publicly estimated its worst case exposure in the single digit millions, and separate passenger class claims were dismissed on federal preemption grounds. Reuters, FOX 5 Atlanta, The Register, and CrowdStrike's own annual report filing with the Securities and Exchange Commission.

[46] SecurityWeek, CSO Online, and the 30 May 2025 letter from Senator Mark Warner and colleagues. The Department of Homeland Security removed all members of the Cyber Safety Review Board in January 2025, halting its investigation into the Salt Typhoon telecommunications intrusions. The board had previously reviewed the 2023 Microsoft Exchange Online intrusion attributed to Storm-0558 and found a cascade of avoidable Microsoft errors, concluding the intrusion was preventable. As of mid 2025 the board had not been reconstituted despite calls from senators to restore it.

[47] United Kingdom critical third parties regime. Under the Financial Services and Markets Act 2023 and the rules made by the Bank of England, the Prudential Regulation Authority, and the Financial Conduct Authority, United Kingdom financial regulators can designate and directly oversee critical third parties to the financial sector, including major cloud service providers. Stated here at the level of the regime's existence and powers. The specific date on which a given provider was designated was not independently confirmed at an authoritative source for this report.

[48] Microsoft Online Services service level agreement, as published by Microsoft. Microsoft commits to 99.9 percent monthly uptime for Exchange Online and comparable Microsoft 365 services and makes service credits the customer's sole and exclusive remedy for failing to meet that commitment, calculated as a percentage of the monthly fee for the affected service and claimed by the customer within a defined window, with the credit percentage rising as monthly uptime falls. Cited for the structure of the remedy. Subscribers should read the credit tiers and the sole remedy and consequential damages terms in their own agreements.