topics.watch Weekly Report

Edition Summary

Priority	Vendor	Category	Event
HIGH	**Adobe**	Product	Analytics 1.4 API hard shutdown August 12 — live integrations break on that date
HIGH	**Oracle**	Security	Oracle CSPU lands May 28 — CVE-2026-46840 CVSS 10 leads 35-patch first monthly release
MEDIUM	**Broadcom**	Product	VMware Cloud Foundation 9.1 ships May 5 with AI workload features and revised licensing tiers
MEDIUM	**Cloudera**	Regulatory	DOL suspends PERM processing 180 days; DOJ civil-rights lawsuit over INA hiring discrimination active
MEDIUM	**IBM**	Security	WebSphere identity-spoofing patch (CVE-2026-8644, CVSS 9.1) leads two-bulletin June 1 release
MEDIUM	**IBM**	Product	Project Lightwell: IBM and Red Hat commit $5B to open source security subscriptions
MEDIUM	**Tanium**	Security	CVE-2026-9207 and CVE-2026-9208 — twin CVSS 8.8 RCEs in Tanium Connect patched May 27
MEDIUM	**Workday**	Earnings	Workday FY27 Q1 subscription guide firms at $9.925–9.950B; AI ACV growth sustains
LOW	**Bottomline Technologies**	Product	Fraud Intelligence Exchange pilot launches with commercial bank cohort on June 2
LOW	**Broadcom**	Earnings	Q2 FY2026 earnings due after market close June 3; VMware software trajectory in focus
LOW	**Collibra**	Partnership	Collibra expands Snowflake integration with bi-directional AI governance; GA preview opens
LOW	**IBM**	Product	$10B quantum investment and Anderon foundry LOI signal IBM capital reallocation
LOW	**JetBrains**	Product	Fleet IDE sunsetted; successor 'Air' agentic environment announced with no pricing yet
LOW	**ServiceNow**	Partnership	Experian data partnership and BofA Buy reinstatement lift NOW 15% on May 29
LOW	**Tanium**	Product	Tanium demos Atlas autonomous IT platform at Gartner Security Summit through June 3

This report covers matters at the watched vendors with direct procurement relevance: (1) news, announcements, and reports that became public during the stated research window; (2) earlier matters whose deadline or procurement-relevant date falls within it; (3) ongoing matters whose status has changed.

Detailed Company Reports

Adobe — Product

HIGH — Analytics 1.4 API hard shutdown August 12 — live integrations break on that date

Confidence: High - official vendor source.

Adobe will permanently shut down the Adobe Analytics 1.4 API and its WSSE authentication legacy services on August 12, 2026; all endpoints using this API version will cease to work on that date, breaking any integration that has not migrated (**Adobe Developer Portal**). Integrations using the 1.4 API must migrate to the Analytics 2.0 API; those using WSSE authentication must move to OAuth-based credentials via the Adobe Developer Console (**Experience League EOL FAQ**).

With approximately 70 days remaining from this briefing date of June 3, 2026, organizations should audit their Adobe Analytics integrations now to identify any calling the legacy endpoints (api.omniture.com, api3–5.omniture.com) or using WSSE authentication. Third-party tools that connect to Adobe Analytics — such as ETL pipelines, Report Builder workbooks, and BI connectors — may also be affected, and their vendors should be contacted to confirm which API version they use.

What we are watching

- Audit all integrations calling api.omniture.com (and api3–5.omniture.com) endpoints and schedule migration to Analytics 2.0 API before August 12, 2026.
- Confirm with any third-party BI, ETL, or reporting vendors that their Adobe Analytics connectors have been updated to the 2.0 API ahead of the August 12, 2026 shutdown date.

TW-26W23-25-002

Bottomline Technologies — Product

LOW — Fraud Intelligence Exchange pilot launches with commercial bank cohort on June 2

On June 2, 2026, Bottomline Technologies announced it had begun piloting a Fraud Intelligence Exchange with a select group of commercial banking customers, enabling banks to share anonymized fraud signals across commercial payment flows to identify suspicious activity earlier (**GlobeNewswire, June 2, 2026**). The pilot phase focuses on validating the approach and refining risk signals before any broader rollout; timing for general availability has not been announced.

For organizations using Bottomline's Paymode network or commercial banking fraud tooling, the Exchange represents a directional shift toward consortium-based fraud detection. Buyers should note that no pricing, contractual, or integration change has been communicated at this stage — the pilot is operating with an undisclosed set of bank customers.

What we are watching

- Track whether general availability of the Fraud Intelligence Exchange introduces new subscription tiers or data-sharing obligations at next Paymode or fraud-platform renewal.
- Confirm with your Bottomline account team whether your organization is eligible or has been invited to the pilot, and what contractual terms apply to anonymized signal sharing.

TW-26W23-25-009

Broadcom — Product

MEDIUM — VMware Cloud Foundation 9.1 ships May 5 with AI workload features and revised licensing tiers

On May 5, 2026, Broadcom released VMware Cloud Foundation (VCF) 9.1, positioning it as a production AI infrastructure platform with accelerated workload deployment, enhanced security controls, and an open hardware ecosystem extending to ODM self-certification partners including Cisco, Intel, and Supermicro (**Broadcom News Releases**). The release follows VCF 9.0 and expands the licensing footprint required for customers running AI-adjacent private cloud workloads.

Separately, on May 14, 2026, Broadcom published security advisory VMSA-2026-0003, addressing a privilege escalation vulnerability (CVE-2026-41702) in VMware Fusion versions prior to 26H1; CVSS score was not confirmed in available sources (**Canadian Centre for Cyber Security AV26-469**). No CVSS ≥ 9.0 advisory for an enterprise-class VMware product was identified in the research window. Buyers running Fusion in developer or lab environments should verify upgrade status.

What we are watching

- Confirm whether existing VCF 9.0 subscription terms require a paid upgrade to access VCF 9.1 AI workload features, and capture the effective license change date before the next renewal cycle.
- Verify VMware Fusion CVE-2026-41702 patch status in developer and lab environments; check whether affected versions (prior to 26H1) are in scope under your enterprise support contract.

TW-26W23-25-007

Broadcom — Earnings

LOW — Q2 FY2026 earnings due after market close June 3; VMware software trajectory in focus

Broadcom is scheduled to report Q2 FY2026 results after market close on June 3, 2026. At Q1 results on March 4, 2026, Broadcom guided Q2 revenue of approximately $22.0 billion (+47% year-over-year) with adjusted EBITDA of roughly 68% of revenue (**Broadcom Q1 FY2026 8-K, SEC EDGAR**).

Outlook as of 2026-06-03: if Broadcom meets or exceeds its Q2 infrastructure software guidance of approximately $7.2 billion (+9% year-over-year) when it reports after close on June 3, 2026, VMware subscription conversion progress may accelerate renewal pricing pressure in H2 2026.

Analysts including Susquehanna (June 2, 2026 price target raised to $490) have begun separately valuing Broadcom's VMware software franchise from its semiconductor segment, with VMware approaching $30 billion in annual revenue at margins above 78% as the perpetual-to-subscription transition is expected to complete in late 2026 (**IndMoney earnings preview, June 2, 2026**). Enterprise buyers whose perpetual VMware licenses remain active should track whether Broadcom's subscription attach-rate commentary on June 3, 2026 signals accelerated end-of-support for remaining perpetual entitlements.

What we are watching

- Track Broadcom's June 3, 2026 earnings commentary on VMware subscription attach rates; accelerated perpetual-license end-of-support messaging would require immediate renewal re-costing.
- Monitor VMware infrastructure software revenue growth rate; a deceleration below Q1's trajectory may signal Broadcom increasing bundle pressure or price adjustments to sustain software margins.

TW-26W23-25-013

Cloudera — Regulatory

MEDIUM — DOL suspends PERM processing 180 days; DOJ civil-rights lawsuit over INA hiring discrimination active

On May 12, 2026, the U.S. Department of Labor announced an enforcement action against Cloudera, suspending all processing of permanent labor certification (PERM) applications filed by or on behalf of the company for 180 days — a constraint that remained in active effect during the research window closing June 3, 2026 (**DOL release**). The action followed allegations that Cloudera violated the Immigration and Nationality Act by engineering a non-functional recruitment process that excluded qualified U.S. workers while certifying to the government that none were available.

The DOL enforcement is the downstream result of a DOJ Civil Rights Division lawsuit filed on April 28, 2026, with the Office of the Chief Administrative Hearing Officer (**Washington Times**). The DOL noted the 180-day suspension may be extended pending DOJ investigation outcomes (**Miller Mayer**). The enforcement aligns with Project Firewall, a 2025 inter-agency initiative targeting tech-sector PERM compliance.

For procurement teams, the PERM freeze constrains Cloudera's ability to hire and retain skilled foreign-national technical staff for the duration of the suspension, which runs through approximately November 2026. Buyers with active or upcoming engagements dependent on Cloudera's delivery capacity should assess whether contractual staffing and service-level commitments remain achievable under these workforce restrictions.

What we are watching

- Confirm whether Cloudera's delivery teams supporting your engagement include PERM-dependent staff; request written assurance of staffing continuity through November 2026.
- Track DOJ litigation progress — an adverse ruling or extended DOL suspension beyond 180 days may further constrain Cloudera's technical hiring pipeline and affect roadmap execution.
- At next renewal, include contractual staffing-continuity obligations and a service-credit mechanism tied to delivery shortfalls attributable to workforce restrictions.

TW-26W23-25-008

Collibra — Partnership

LOW — Collibra expands Snowflake integration with bi-directional AI governance; GA preview opens

On June 2, 2026, Collibra announced at Snowflake Summit 26 an expanded integration with Snowflake, enabling bi-directional flow of governed metadata, semantic models, and access policies between the two platforms (**PRNewswire, June 2, 2026**). The expanded collaboration extends Collibra's AI Command Center into Snowflake Horizon Catalog, Cortex Analyst, and Cortex Agents. The new integrations are available in preview to a select group of joint customers, with broader availability planned for Q3 2026.

For joint Collibra–Snowflake customers, the integration may affect module selection — particularly the AI Governance module — and connector-tier licensing decisions ahead of Q3 2026 general availability (**Collibra Newsroom**). Organisations with lineage-completeness requirements should note that unlimited technical lineage connectors are restricted to Collibra's Ultimate tier; the integration may surface that constraint earlier than a standard renewal cycle would.

What we are watching

- Confirm whether the Q3 2026 Snowflake bi-directional integration requires an AI Governance module add-on or is covered within existing contract scope.
- Audit current connector tier — if unlimited technical lineage connectors are a requirement, verify whether the Ultimate tier is already contracted before Q3 2026 GA.

TW-26W23-25-010

IBM — Security

MEDIUM — WebSphere identity-spoofing patch (CVE-2026-8644, CVSS 9.1) leads two-bulletin June 1 release

IBM published two WebSphere Application Server security bulletins on June 1, 2026. The higher-severity bulletin covers CVE-2026-8644 (CVSS 9.1), an authentication-bypass-by-spoofing flaw allowing unauthenticated identity spoofing affecting versions 8.5.0.0 through 8.5.5.29 and 9.0.0.0 through 9.0.5.28 (**IBM Security Bulletin**). IBM strongly recommends applying the available interim fix for APAR PH71422 immediately; fix pack 9.0.5.29 or 8.5.5.30 is targeted for Q3 2026.

The second bulletin, also dated June 1, 2026, addresses CVE-2026-9319 (CVSS 9.0), a remote code execution flaw via deserialization of untrusted data through JAX-WS endpoints with WS-Security (**IBM Security Bulletin**). The interim fix for APAR PH71454 is available now. Neither advisory carries a CISA KEV designation or vendor out-of-band label; no active exploitation has been reported as of June 3, 2026.

What we are watching

- Confirm interim fix deployment status for APAR PH71422 and PH71454 with WebSphere operators before next steering cycle.
- Validate whether WebSphere renewal terms include SLA commitments covering interim-fix delivery timelines; flag gap if fix packs remain in Q3 2026.

TW-26W23-25-003

IBM — Product

MEDIUM — Project Lightwell: IBM and Red Hat commit $5B to open source security subscriptions

On May 28, 2026, IBM and Red Hat (acquired by IBM in 2019) announced Project Lightwell, a $5 billion commitment to secure open source software supply chains via a new AI-assisted enterprise clearinghouse (**IBM Newsroom**; **Red Hat press release**). The clearinghouse will use AI to identify, triage, and validate fixes across open source codebases at scale, backed by a workforce of more than 20,000 engineers.

Critically for procurement, Project Lightwell capabilities will be delivered through commercial subscriptions, integrating validated patches into enterprise software supply chains (**SecurityWeek**). Buyers on RHEL, OpenShift, or IBM open source bundles should expect new subscription tiers or add-on offerings to emerge from this initiative and factor potential uplift into 12-month renewal models.

What we are watching

- Request IBM and Red Hat account teams to clarify Project Lightwell subscription pricing and packaging before next RHEL or OpenShift renewal cycle.
- Audit current open source components in scope to assess whether Lightwell's commercial patch validation may be positioned as a mandatory upgrade at renewal.

TW-26W23-25-006

IBM — Product

LOW — $10B quantum investment and Anderon foundry LOI signal IBM capital reallocation

On May 28, 2026, IBM filed an SEC disclosure announcing a plan to invest more than $10 billion in quantum computing over the next five years, spanning R&D, manufacturing, ecosystem partnerships, and M&A (**The Quantum Insider**). The disclosure also referenced a Letter of Intent with the U.S. Department of Commerce to establish Anderon, a purpose-built U.S. quantum chip foundry backed by a proposed $1 billion CHIPS Act award, announced May 21, 2026 on the IBM Newsroom (**IBM Newsroom**).

No customer-facing deadline or procurement trigger is attached to this announcement. The capital commitment signals IBM's long-term platform priorities — quantum and hybrid cloud — but the Anderon LOI carries no stated close date communicated to customers. Procurement teams with multi-year IBM software or consulting agreements may wish to note this reallocation as context for future roadmap conversations.

What we are watching

- Monitor whether quantum-focused roadmap messaging affects IBM software and consulting renewal positioning over the next 12 months.

TW-26W23-25-015

JetBrains — Product

LOW — Fleet IDE sunsetted; successor 'Air' agentic environment announced with no pricing yet

As of May 2026, JetBrains confirmed that Fleet has evolved into 'Air,' a new Agentic Development Environment, per a **JetBrains blog update** posted in May 2026. Fleet was withdrawn from download on December 22, 2025; existing installations retain basic functionality, but server-side services including AI Assistant may degrade over time.

InfoWorld reported on June 2, 2026 that JetBrains determined maintaining two overlapping product lines created confusion, and AI workflows developed for Fleet will be carried forward into the IntelliJ-based IDE family instead. No commercial terms or pricing for Air had been published as of the research window close on June 3, 2026.

What we are watching

- Audit any Fleet IDE seats in active renewal or procurement pipeline and confirm whether Air licensing will be a net-new purchase or an upgrade path from existing JetBrains All Products Pack subscriptions.
- Track Air commercial announcement — no pricing or licensing model published as of June 3, 2026; hold budget placeholder at current JetBrains subscription spend until terms are confirmed.
- Confirm that IntelliJ-based IDE versions (2026.1 or later) cover all developer workflows previously assigned to Fleet seats, to avoid a gap in tooling coverage during the transition.

TW-26W23-25-011

Oracle — Security

HIGH — Oracle CSPU lands May 28 — CVE-2026-46840 CVSS 10 leads 35-patch first monthly release

Confidence: High - official vendor source.

On May 28, 2026, Oracle released its first Critical Security Patch Update (CSPU), delivering **35 new security patches** across on-premises product families. The lead advisory is CVE-2026-46840, a CVSS 10 flaw in the backend-as-a-service component of **Oracle REST Data Services** versions 24.2.0 through 26.1.0 — exploitable by an unauthenticated attacker over HTTPS, resulting in full gateway takeover. Two companion REST Data Services flaws, CVE-2026-46775 and CVE-2026-46839, both score CVSS 9.9.

Separate high-severity patches released May 28 cover Oracle E-Business Suite (CVE-2026-46822), Oracle Payments (CVE-2026-46817), and the Oracle Universal Work Queue portal (CVE-2026-46824). Security teams should also prioritize CVE-2026-2332 and CVE-2025-58050 in Oracle Communications products, for which **proof-of-concept exploit code reportedly exists**. Oracle cloud customers receive these fixes automatically; on-premises and customer-managed OCI deployments require manual application and remain unpatched until teams act.

Outlook as of 2026-06-03: Oracle has established a new third-Tuesday monthly cadence; the **next CSPU is scheduled for June 16, 2026**, and procurement teams should confirm their patch-governance calendar includes a monthly Oracle lane by that date.

What we are watching

- Confirm the May 28, 2026 CSPU has been applied to all on-premises Oracle REST Data Services deployments — CVE-2026-46840 is CVSS 10 with an unauthenticated remote exploit vector and is the highest-risk fix in the bundle.
- Update your Oracle patching SLA to add a monthly CSPU lane alongside the quarterly CPU lane; the June 16, 2026 CSPU is the first third-Tuesday release and will test whether the new governance calendar is operational.
- Verify Oracle E-Business Suite and Oracle Payments patch owners have reviewed the May 28, 2026 CSPU advisory and confirmed applicability to your EBS release 12.2 environment.

TW-26W23-25-001

ServiceNow — Partnership

LOW — Experian data partnership and BofA Buy reinstatement lift NOW 15% on May 29

On May 29, 2026, ServiceNow announced a global multi-year partnership with Experian, embedding Experian's Ascend data into the ServiceNow AI Platform to support agentic AI workflows in risk, fraud, and customer onboarding use cases (**StocksToTrade, May 29, 2026**). On the same date, Bank of America reinstated coverage with a Buy rating, citing the platform's positioning in agentic AI adoption.

ServiceNow shares rose 15.66% on May 29, 2026, reflecting combined momentum from the Experian deal, the BofA reinstatement, and an expanded Boomi integration deepening real-time data access for AI agents (**StocksToTrade, May 29, 2026**). No pricing change, contract trigger, or renewal deadline was named in connection with the partnership.

What we are watching

- At next ServiceNow renewal, confirm whether Experian Ascend data features carry a separate consumption charge or are bundled into existing Now Assist SKU entitlements.
- Track whether BofA's price-target reinstatement tightens ServiceNow's discount posture on multi-year deals in H2 2026.

TW-26W23-25-012

Tanium — Security

MEDIUM — CVE-2026-9207 and CVE-2026-9208 — twin CVSS 8.8 RCEs in Tanium Connect patched May 27

Confidence: Medium - trade press reporting.

On May 27, 2026, Tanium published patches for two unauthorized code-execution vulnerabilities in Tanium Connect: **CVE-2026-9207** and **CVE-2026-9208**, both scoring CVSS 8.8 (High). Neither CVE requires authentication to exploit, meaning an unauthenticated attacker with network access to a Tanium Connect instance could execute arbitrary code on the host. No CISA KEV listing or confirmed active exploitation was identified as of June 3, 2026.

Both CVEs extend the thread first reported in the prior edition (entry 1385). Tanium addressed the vulnerabilities via its advisory channel on May 27, 2026; organizations should confirm the patched Connect version is deployed across all instances and verify that Tanium Connect is not exposed on internet-facing segments without network-level access controls.

What we are watching

- Confirm patched Tanium Connect version is deployed on all instances; validate network segmentation blocks unauthenticated access to Connect endpoints.
- At next renewal, verify Tanium's patch-cycle SLA commitments for critical Connect components are contractually defined.

TW-26W23-25-004

Tanium — Product

LOW — Tanium demos Atlas autonomous IT platform at Gartner Security Summit through June 3

Tanium is exhibiting as a Platinum Exhibitor at the Gartner Security and Risk Management Summit in National Harbor, MD, running June 1–3, 2026, showcasing **Tanium Atlas** — its autonomous IT operating platform announced approximately one month prior — alongside practitioner-led sessions on exposure management. The event is a positioning signal for Tanium's enterprise pipeline but carries no immediate pricing or contract trigger for procurement teams.

What we are watching

- Monitor Tanium Atlas licensing model announcements; if Atlas moves to a separate SKU or bundling tier, re-cost existing endpoint-management subscriptions at next renewal.

TW-26W23-25-014

Workday — Earnings

MEDIUM — Workday FY27 Q1 subscription guide firms at $9.925–9.950B; AI ACV growth sustains

Workday reported Q1 FY27 results on May 29, 2026, posting subscription revenue of $2.30 billion (+14% year-over-year) and total revenue of $2.54 billion (+13.5%) **Workday IR**. The company maintained its full-year FY27 subscription revenue guidance at $9.925–$9.950 billion, signalling confidence in the pipeline even as macro headwinds persist **Reuters**.

AI-attached new annual contract value grew approximately 200% year-over-year in Q1 FY27, according to the May 29, 2026 earnings call, driven by Workday Illuminate and agent-based HR and finance SKUs **Workday IR**. Channel partners reported rising AI workflow attach rates on new and renewal contracts as of late May 2026 **CRN**. Buyers renewing in the next two quarters should expect Workday to price AI SKUs as incremental add-ons rather than bundled, consistent with the ACV acceleration pattern disclosed on May 29, 2026.

What we are watching

- Audit upcoming Workday renewal quotes for new AI SKU line items (Illuminate, agent add-ons) that may inflate the base subscription cost beyond the FY27 guide rate.
- Confirm whether current contract language covers AI feature parity or treats each Illuminate module as an out-of-scope upsell requiring a new order form.
- Track Q2 FY27 results (expected late August 2026) for any subscription-guide revision that would shift Workday's discount posture at renewal.

TW-26W23-25-005

Nothing to Report (28 May – 3 June 2026 (UTC))

These vendors had no material new news in sources checked for this cover window. Where a recent event sits just outside the window, the date is noted.

Vendor
BMC Software
NICE
Nasdaq
Quantitative Risk Management (QRM)
SAS Institute

Previously Reported (28 May – 3 June 2026 (UTC))

These vendors had a HIGH or MEDIUM alert in a prior edition and no material new development this week. The alert remains on file; we will return to it if the situation changes.

Vendor	Prior alert
Coupa Software	Coupa acquires Tonkean on May 21, second AI deal in nine days, deepening agentic orchestration stack

This briefing references 31 public sources, all linked inline.