
THE INDUSTRY EDITION / 16 OCTOBER 2026

The haul road is now a network.

Autonomous fleets passed the thousand-truck mark, espionage against mining data stayed quiet by design, and a US\$264 billion sell-off will test whether security budgets hold.

MINING & METALS

THE OPPORTUNITY

Autonomy and plant AI at scale, with evidence you can audit.

THE CYBER QUESTION

Who can send a command to a truck, and from where?

THE ACTION

A 90-day agenda: find the edges, control them, prove it.

In this issue.

Seven sections for the people who run a mine's technology, secure its operations and have to sign off what automation is allowed to do.

01	The briefing	The highest-value systems sit outside the IT perimeter. Five signals, and what they do not establish.
02	AI in practice	Autonomy is the operating default at tier-one pits, and AI is moving into the processing plant.
03	Cyber front	Espionage stays silent by design, and a hosted ERP outage showed how far a supplier incident reaches.
04	The 90-day playbook	Find the edges, put controls where the risk is, then prove the fleet fails safe.
05	The decision desk	Production at risk, not incident counts. A worked example built on stated planning assumptions.
06	Monday's agenda	Lose the haulage network mid-shift, on paper, before it happens for real.
07	Sources & editorial notes	Twelve numbered references, each with what it does and does not establish.

HOW TO READ THIS EDITION

Reported events are attributed to their sources and were checked on 16 October 2026. Where a company has not confirmed something, we do not report it as fact. Figures that companies report about their own results are labeled that way.

The 90-day agenda, the worked example and the checklists are original editorial proposals and a practitioner heuristic, not a published standard and not verified Agents Stack customer results.

This edition draws on events in Australia, Chile, Brazil, China and North America. Have your legal or compliance specialist confirm which rules apply to your operations.

The highest-value systems sit outside the IT perimeter.

For mining CISOs, CIOs and OT leads: this month's story is quiet on the surface and structural underneath.

The editor's view

Mining's cyber risk moved in two directions at once. Down, into fleets of networked haul trucks and drills that now carry a large share of production at tier-one sites. Out, into geological, deal and investor data that state-linked actors want and that victims rarely disclose. Neither sits comfortably inside a classic IT security program.

The coverage window

Roughly 6 September to 16 October 2026, with earlier 2026 events and one 2024 case included as context where they explain the pattern.

What changed this month

The money changed. The 50 most valuable miners lost about US\$264 billion in market value in September. When margins tighten, programs with no recent visible incident are the easiest to defer. That is precisely the wrong moment for an industry whose production now runs through networked control systems. **[11]**

The common thread

Every signal in this edition points to the same gap: the systems with the highest consequence and the data with the highest value both sit at the edge of the network, with OEMs, consultants and hosted suppliers. The recommendation is to find those edges, put controls on them and prove they hold.

WHERE THE RISK SAT THIS MONTH

01

Autonomous fleets

Trucks and drills on the network.

02

Plant AI

Optimizers near the controls.

03

Exploration data

Wanted, and rarely reported.

04

Hosted suppliers

One outage, many sites.

Five signals behind the recommendation.

What the public record supports, and what it does not.

01 / Autonomy passed a thousand trucks

Komatsu said in April it had commissioned its 1,000th autonomous ultra-class haul truck, the first manufacturer to do so. In China, EACON says its system ran on more than 1,500 battery-electric trucks by early September, up from 800 in March. [1] [3]

02 / AI moved into the processing plant

Vale and ABB expanded an automation and AI cooperation across Vale's Brazilian iron ore plants in August. The company-reported results at the model plant include a 25% productivity gain. [4]

03 / Espionage stayed silent by design

A July feature in MINE describes state-linked theft of geological, operational and investor data, and why both sides keep it quiet. Recorded Future reported in April that criminal groups may act as access brokers for state operations. [5] [6]

04 / A supplier outage reached many sites

In May, a cyber incident at Scope Systems disrupted customers' hosted Pronto ERP. A week later, about half of its servers had been restored. The company said no client data was exfiltrated. [9]

05 / A sell-off will test the budget

The 50 most valuable miners were worth about US\$2.26 trillion at the end of September, after the second-largest monthly decline in the ranking's history. [11]

As more production runs through networked control systems, a cyber outage becomes a production outage.

AGENTS STACK PERSPECTIVE

Research cut-off: 16 October 2026. Fleet counts and plant results are the companies' own figures; quote them with that attribution.

Autonomy is the operating default at tier-one pits.

The fleets are already here. The security questions are now about who can talk to them.

The scale

Komatsu says its FrontRunner system runs at mine sites across North America, South America, Australia and Europe, and that customers have moved more than 11.5 billion metric tons with it. Its 1,000th autonomous truck went to Nevada Gold Mines. **[1]**

One pit, fully autonomous

BHP's Escondida Norte pit in Chile runs 33 autonomous trucks and 11 autonomous drills. About 30% of Escondida's output comes from the autonomous zone, which moves more than 350,000 tonnes of material a day, according to BHP figures reported in January. **[2]**

Autonomy now schedules itself

EACON's system decides when its battery-electric trucks charge, drives them to the charging bay and sends them back to haul, weighing battery level, predicted energy use and production needs. Its named deployments are in China. **[3]**

Why this is a security question

An autonomous haulage system is a fleet of networked control systems sharing roads with people. The questions are concrete: who can send a command to a truck, how OEM remote support reaches the fleet, and what every truck does when the network is lost or spoofed. Those questions belong in the safety case, not only in the IT risk register.

FOUR THINGS TO SETTLE BEFORE THE FLEET GROWS

01

Command paths

Every route a command can take.

02

OEM remote access

Who approves each session.

03

Network loss

The safe state, tested.

04

Safety case owner

One name for cyber and safety.

An optimizer near the controls is a control change.

AI in the processing plant can show strong results. It also changes who and what can move a setpoint.

What Vale and ABB agreed

Vale and ABB formalized an expanded automation, AI and digitalization cooperation on 11 August, covering Vale's Brazilian iron ore operations. Conceição II in Itabira is the model plant. Brucutu is in implementation and is expected to run the new systems in early 2027. No contract value has been published. [4]

Read the results with care

The reported gains at the model plant are a 25% rise in productivity, 40% more premium ore for direct reduction and 26% lower iron losses in tailings. These come from company communications measured against the plant's earlier performance, not an audited report.

Where AI earns its place

Process plants are full of decisions made under time pressure: grind size, reagent dosing, throughput against recovery. Advisory AI that helps an operator make those calls faster is a credible first use. Closed-loop AI that writes setpoints directly is a different risk, and should be treated as a control-system change.

Four questions to ask

Does the model advise, or does it act? Which setpoints can it change, and within what limits? Who can update the model, and is each version logged? If it is switched off mid-shift, can the operators run the circuit without it?

If the AI can move a setpoint, it belongs in the control-system change process.

AGENTS STACK PERSPECTIVE

Espionage stays silent by design.

The most valuable data in a mining company rarely sits in the main ERP. It sits with geologists, advisers and consultants.

What the July feature describes

MINE magazine reports that state-linked actors target pre-commercial survey and exploration data, pricing forecasts, OT and SCADA information, and merger, investor and shareholder data. Its main expert source, American University's William Akoto, says: "There are incentives for both the target and the attacker to keep cyber espionage quiet." [5]

What Recorded Future found

Its Insikt Group research identified state-sponsored and criminal actors targeting mining organizations, including a 2025 campaign by Chinese state-sponsored actors against an organization that regulates seabed mining. It warns that criminal intrusions may be more than financially motivated. [6]

The case that shows the pattern

Australian rare earths producer Northern Minerals detected a breach in March 2024. In June it disclosed that exfiltrated corporate, operational and financial data, plus some staff and shareholder details, had been posted online. The filing came a day after the government ordered China-affiliated investors to sell their shares. [7]

What is not established

Who was behind it. The data was posted by the BianLian ransomware group, and government sources later told The West Australian the hack almost certainly came from Russia or a jurisdiction with Russian ties. That attribution is unconfirmed. [8]

Treat the ISAC as a sensor

Industry sharing groups such as the Mining and Metals ISAC exist because individual companies rarely see the whole campaign. Membership is useful as a detection source, not a badge: feed its indicators into monitoring and report back what you see.

THREE QUESTIONS TO ASK THIS QUARTER

01

Where it lives

Where are resource models and deal files, including copies held by consultants?

02

Who can see it

Is access to geology and corporate development data logged?

03

Who would notice

Would an export of exploration data trigger an alert?

One hosted supplier, many sites.

A May outage at an ERP hosting partner is a useful rehearsal for the incident most mines are least ready for.

Scope Systems, May 2026

The incident began in the early hours of 5 May and disrupted customers' access to Pronto Xi hosted on the Scope Systems Cloud, along with its support portal and hosted APIs. Restoration from backups had begun by 9 May. By 12 May, 53% of servers had been restored. [9]

What was confirmed

Scope Systems said it had found no data loss and no exfiltration from client systems. It did not disclose the nature of the incident, and no group claimed responsibility. Pronto said there was no compromise to Pronto Cloud or to the Pronto Xi application. [9] [10]

The recovery curve

Four days to begin restoring from backups and a week to bring back about half the servers is not unusual for a hosted environment. Plan for that curve, not for the vendor's best case. The question is what your sites do on day three.

Why a mine should care

ERP sits behind maintenance work orders, spare parts, procurement and payroll. A week without it does not stop the trucks on day one. It stops the parts arriving, the contractors being paid and the work orders being raised, a few days later.

Three questions for every hosted supplier

How fast must they tell you about an incident? Where are your backups, and can you restore without them? Which work could run on paper for a week, and who decides when to switch?

What we left out

Ransomware leak sites have named several mining companies in recent months. Those are attacker claims, not confirmed incidents, so they are not reported here.

A supplier's outage is your outage. Rehearse it like one.

AGENTS STACK PERSPECTIVE

Find the edges. Control them. Prove it.

An Agents Stack agenda for mining CISOs and OT leads. It is a practitioner heuristic, not a published standard.

DAYS 0 TO 30

Find the edges

Map every command path into autonomous fleets and plant control systems, including OEM remote support and wireless links. Locate exploration data, resource models and deal files, including copies held by consultants and advisers. List the hosted suppliers that operations could not run a week without.

DAYS 31 TO 60

Put controls where the risk is

Add network-loss and spoofed-command scenarios to the autonomy safety case. Require approval and logging for each OEM remote session. Apply access logging and data-loss controls to geology and corporate development teams. Join or re-engage with the Mining and Metals ISAC.

DAYS 61 TO 90

Prove it

Run a tabletop where the haulage network is lost mid-shift, with the OEM in the room. Test a week without the hosted ERP. Present the board with production at risk, not incident counts, as the case for the security budget.

THROUGHOUT

Keep the evidence

Retain the command path map, the data location register, the supplier list, OEM session logs and the tabletop record. This becomes the starting audit trail. It is not a claim of regulatory compliance or certification.

Review group: security · OT and automation · mine operations · geology and corporate development · procurement.

Two gates decide whether autonomy keeps running.

Write both down before the next fleet expansion or plant AI goes live, not after the first unexplained stop.

GATE ONE

Control gate

Confirm that only approved systems can send commands to the fleet, that each OEM session is approved and logged, and that any AI near the plant controls advises within set limits. Keep a record of each test and of the configuration tested.

GATE TWO

Safe-state conditions

Define what triggers a fleet-wide stop: unexplained commands, loss of network integrity, an unapproved remote session or loss of the logs. Route the event through the incident process and the safety process before any restart.

Why the map comes first

Segmentation, session approval and safe states all depend on a complete list of command paths. An unlisted wireless bridge or a forgotten vendor connection defeats the control without anyone having to bypass it. [12]

What a safe stop should look like

A named person on every shift with the authority to stop the fleet without a committee, and a rehearsed path back to production. Industry guidance from the Mining and Metals ISAC says autonomous haulage security should be designed alongside the deployment, not added afterward. [12]

A fleet that has never practiced losing the network has not proved it fails safe.

AGENTS STACK PERSPECTIVE

Count production at risk, not incidents.

A worked example for one hypothetical open-pit operation. Every input is a planning assumption to replace with your own numbers.

ONE HAULAGE NETWORK OUTAGE, THREE WAYS

US\$1.25M

Rehearsed fallback, 3-day outage

US\$2.5M

No fallback, 3-day outage

US\$11.25M

Downside, 10-day outage

Lost contribution in US dollars under the planning assumptions below. Illustrative only. Not a forecast, a benchmark or a client result.

The assumptions

The plant processes 50,000 tonnes of ore a day at a contribution of US\$25 a tonne, so a full day of lost feed costs US\$1.25 million. A run-of-mine stockpile keeps the plant fed for the first day. Without a fallback, feed stops after that. A rehearsed fallback restores half of the feed from day two.

What it means for the business case

The case does not need a breach probability. It needs the board to agree that one multi-day outage costs more than the program that shortens it. In this example, rehearsal alone is worth US\$1.25 million per event. Replace every input before you use it.

THE INPUTS BEHIND THE EXAMPLE

50,000 t

Ore processed per day

Planning assumption.

US\$25/t

Contribution per tonne

Planning assumption.

1 day

Stockpile buffer

Planning assumption.

50%

Feed restored by fallback

Planning assumption.

Margins fell. The exposure did not.

September's sell-off is a real pressure on budgets. It is also the reason to make the case in production terms.

What the market did

MINING.COM's ranking of the 50 most valuable miners fell by about US\$264 billion in September to roughly US\$2.26 trillion. Only March was worse. Gold miners lost US\$79 billion, or 12.7%, and lithium carbonate futures in Guangzhou fell 22.5%. **[11]**

The Agents Stack view

This is our view, not a reported trend. When margins tighten, security and OT resilience work with no recent incident is easy to defer. The counter-argument is the autonomy point from section 02. The more production runs through networked control systems, the more a cyber outage looks like a production outage.

How to frame the ask

Lead with production at risk from the worked example, using your own figures. Then show the 90-day agenda as the program that shortens the outage and narrows the edges. Keep incident counts out of the opening slide. In an industry that under-reports, they understate the exposure.

What to protect from cuts

The command path map, OEM session approval and the network-loss tabletop. All three are low in cost and high in consequence, and none of them depends on buying a new product.

THREE CONTROLS TO PROTECT FROM CUTS

01

Command path map

Cheap to make, costly to lack.

02

OEM session approval

A process change, not a product.

03

Network-loss tabletop

One shift, with the OEM.

Before you reuse the figures: the market data is from a media ranking at the end of September 2026. Check the latest values before they go into a board paper.

Put a name on every edge.

A conversation for security, OT and automation, mine operations, geology and the executive sponsor.

Ask OT for the command path map

Which systems can send a command to a truck, a drill or the plant? Which OEMs can reach them remotely, over which links, and who approves each session? If nobody can draw it on one page, that is the first finding.

Ask operations for the safe state

What does every truck do when the network drops, and who decides when the fleet restarts? Has anyone tested it outside the commissioning period?

Ask the OEMs for their access list

Which of their staff and systems can reach your fleet or plant today, from where, and under which contract clause? Ask for it in writing, and compare it with what your own logs show.

Ask geology and corporate development for the data

Where do exploration results, resource models and deal plans live, including copies with consultants and advisers? Who can export them, and would anyone notice?

Ask procurement for the supplier list

Which hosted systems could operations not run a week without? What does each contract say about notification, restoration and backups?

Ask finance for the production figures

Tonnes processed per day, contribution per tonne and the size of the stockpile buffer. Those three numbers turn the worked example in section 05 into your own case.

WHO HAS TO BE IN THE ROOM

01

Security lead

Owens the risk register.

02

OT and automation

Brings the command path map.

03

Mine operations

Owens the safe state.

04

Executive sponsor

Assigns the owners.

Lose the haulage network mid-shift, on paper first.

A tabletop with the OEM in the room tells you more than the written plan does.

Run the scenario

The fleet management network is lost at 2 a.m. on night shift. Which trucks stop, and where? Who calls the OEM, and how fast can they join? How long does the stockpile feed the plant? When is it safe to restart, and who says so?

Ask the sponsor for one decision

Pick the date by which every command path, every hosted supplier and every sensitive data store has a named owner. Do not mix that with a wider automation strategy discussion. Ownership is the deliverable.

The question to take to your team

Which system, supplier or data store in our operation could fail this week without appearing on anyone's list?

What to leave the meeting with

A command path map, a data location register, a hosted supplier list and a date for the tabletop. If any of the four is missing, the plan is not yet testable.

A safe state nobody has tested is an assumption, not a control.

AGENTS STACK PERSPECTIVE

Planned next edition: retail and e-commerce. Not yet written or researched.

Evidence you can inspect.

Numbered references match the articles. All sources were checked on 16 October 2026.

[1] Komatsu becomes first OEM to commission 1,000 ultra-class autonomous haul trucks

Komatsu newsroom · 21 April 2026 · Primary source. The company's own milestone and tonnage figures; makes no security claims.

[2] The autonomous electric vehicles inside BHP's mines

EV Magazine · 27 January 2026 · Trade press reporting BHP's figures for Escondida Norte. Not independently verified.

[3] EACON's autonomous solution deployed on more than 1,500 battery-electric mining trucks

Global Mining Review · September 2026 · Trade press based on company figures. Describes no connectivity or remote operations detail.

[4] Vale puts ABB robotics into more iron ore plants after big gains

The Rio Times · 20 August 2026 · News summary of company communications. Results are company-reported, not audited.

[5] Cyber espionage in mining

MINE / Mining Technology · July 2026 · Feature article with expert interviews. Describes targets and incentives; quantifies no gap.

[6] Critical minerals and cyber operations

Recorded Future, Insikt Group · 23 April 2026 · Threat intelligence research by a security vendor. Several targets are unnamed.

[7] Australian rare earths miner hit by cybersecurity breach

Mining Weekly (Bloomberg) · 4 June 2024 · Reports Northern Minerals' own filing. Does not establish who carried out the attack.

[8] Northern Minerals hack 'almost certainly' not from China, sources say

The Nightly · 21 June 2024 · Reporting based on anonymous government sources. Attribution unconfirmed.

[9] Scope Systems confirms cyber incident, says no data loss occurred

Cyber Daily · 13 May 2026 · Trade press quoting the company's statements. Nature of the incident not disclosed.

[10] Scope Systems cyber incident

Pronto Software · 8 May 2026 · Primary source. Pronto's statement on its own systems; does not cover Scope's customers.

[11] Top 50 mining companies take \$264 billion hit as gold trade unwinds, lithium stocks exit

MINING.COM · 4 October 2026 · Media market ranking. Values move daily; check before reuse.

[12] MM-ISAC secure deployment of autonomous haulage systems

Global Mining Guidelines Group · December 2022 · Industry case study summary. Guidance, not a standard; the full paper sits behind the summary.

EDITORIAL NOTES

Reported events are attributed to their sources. Attacker claims that a company has not confirmed are not reported. The 90-day agenda, the worked example and the checklists are original editorial proposals, not verified Agents Stack customer results.

This magazine does not provide legal, safety, financial or regulatory advice. Publication requires a named editor's approval and a final source check. No affiliation or endorsement by cited organizations is implied.



NEXT IN THE SERIES

Retail & e-commerce

Planned, and not yet written or researched.



Agents Stack

One industry. Useful AI. Accountable cybersecurity.

agentsstack.com