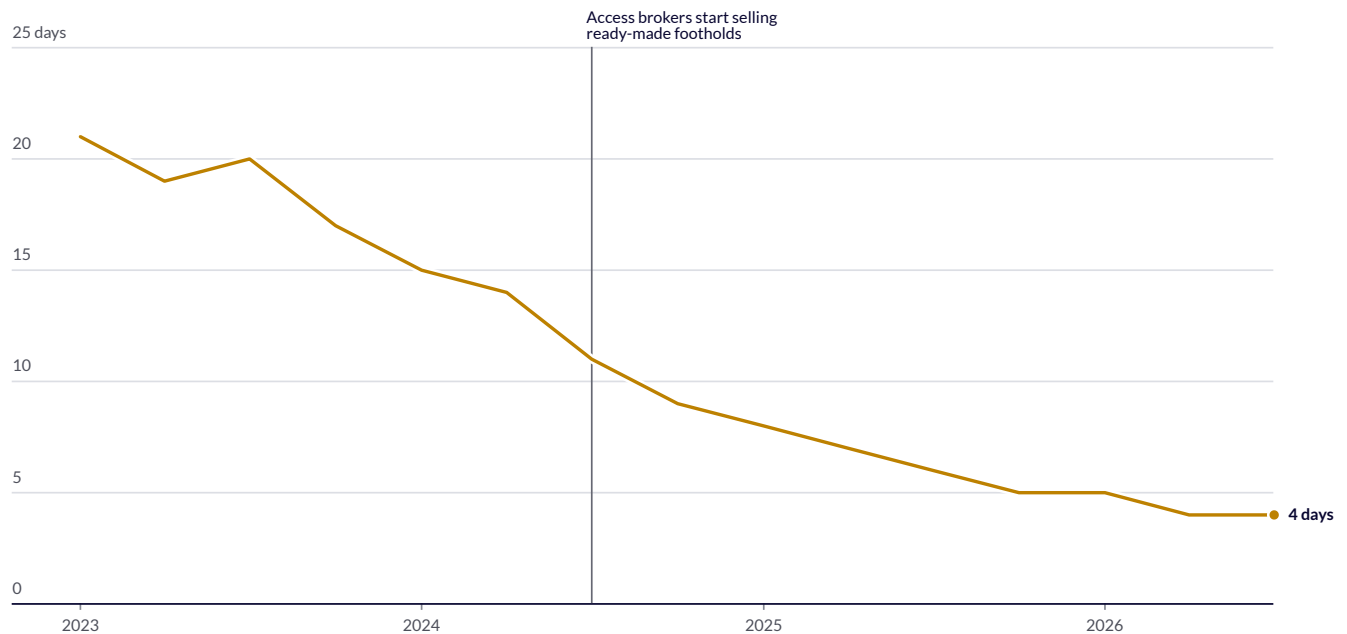


Intruders now act within days, not weeks

The time between break-in and impact has fallen from three weeks to four days

Median days from first access to encryption or theft, by quarter



Source: Hunt & Hackett incident response cases, 2023 to September 2026.

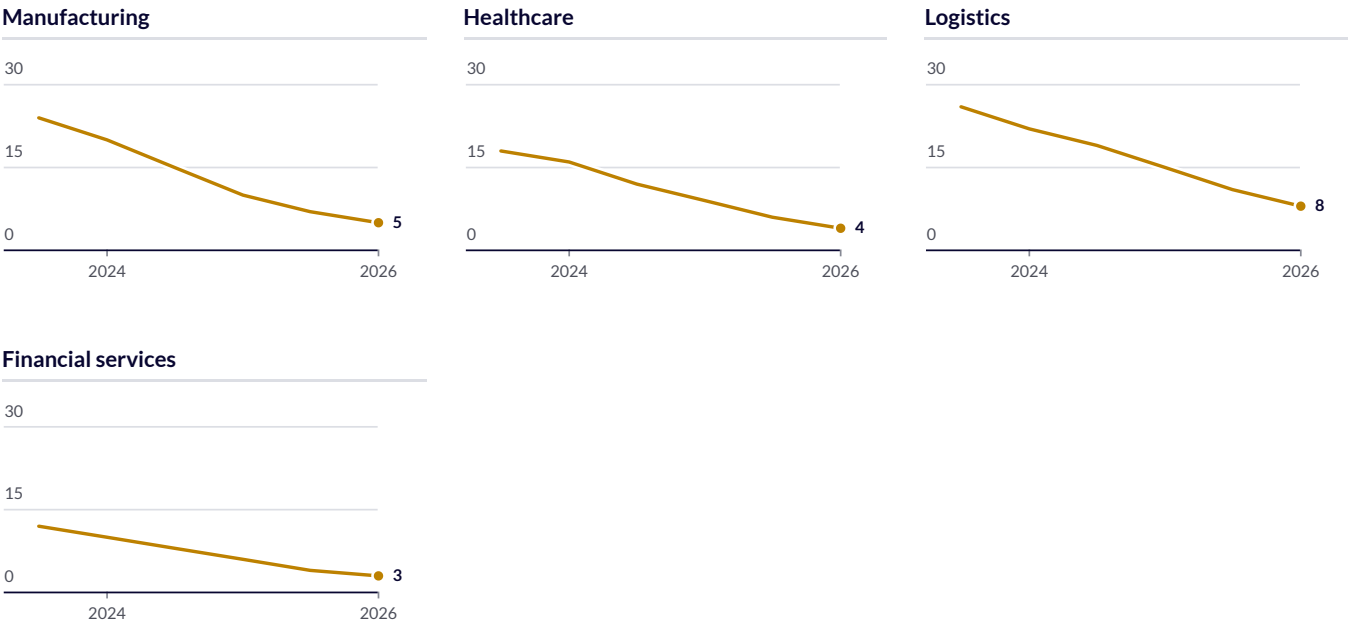
Hunt & Hackett Threat Intelligence, 10 October 2026. Based on 214 intrusions investigated since January 2023.

Every sector shortened, and logistics is still the slowest to be hit

The fall is not one group changing tactics. It shows in every sector we respond in, on the same scale. Logistics firms still get the most warning, because their networks are large and flat and take longer to map.

The same decline in four sectors

Median days from first access to impact, by half-year



Source: incident response cases. Sectors with at least 20 cases.

Four in ten intrusions began with a password that worked

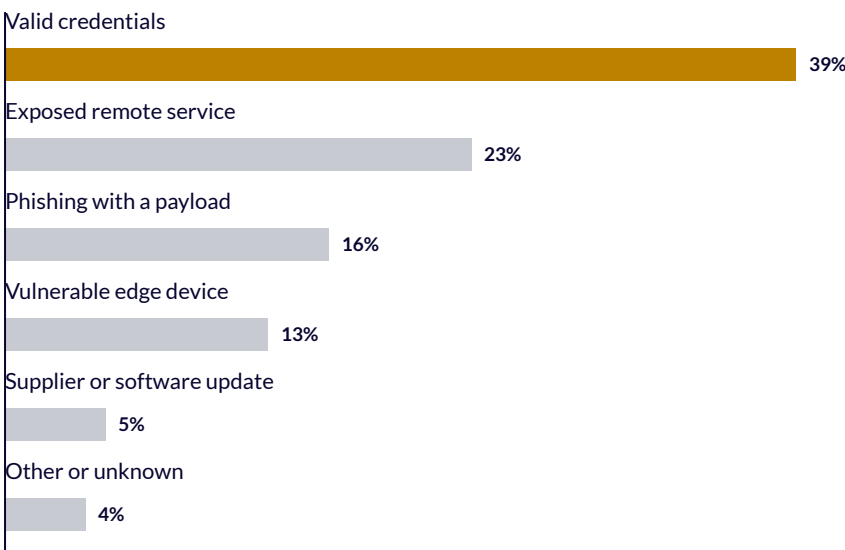
No exploit, no malware: the intruder signed in. Most of those passwords came from an earlier breach somewhere else, or from a session stolen through a relay page.

What counts as valid credentials

A password, token or session that the system accepted as genuine.
A password guessed against an exposed service is counted under that service.

Valid credentials are the most common way in

How the intruder first got access, % of cases in 2026



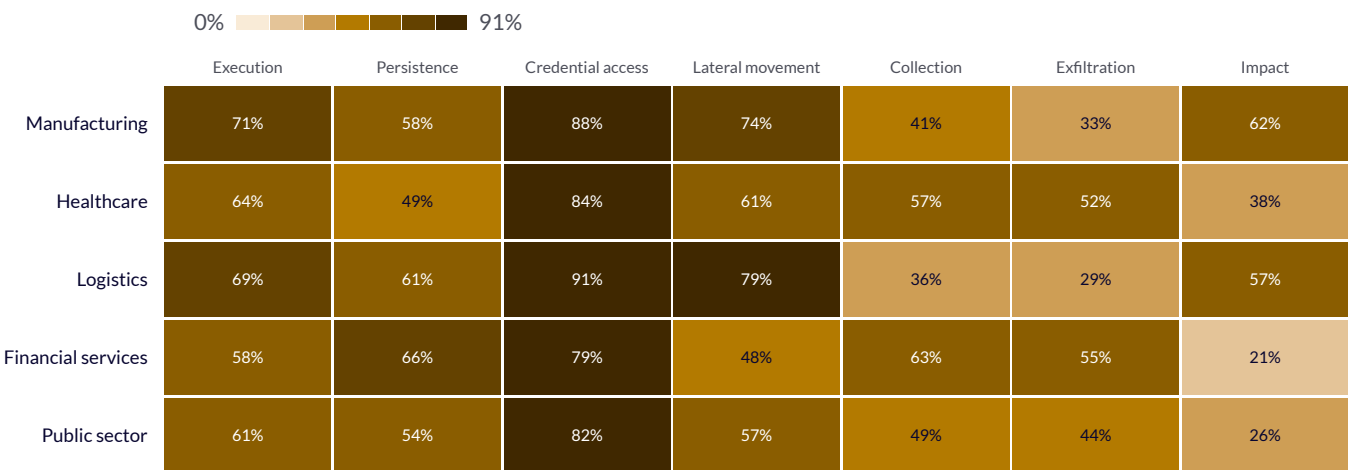
Source: 61 cases, January to September 2026.

Once inside, they go for credentials before anything else

Read across a row to see what an intrusion in that sector usually involves. Credential access stands out in every row: it is how one foothold becomes many. Exfiltration is what separates the sectors, and impact is rarest where data is worth more than downtime.

Credential access shows up in at least four of five cases, in every sector

Share of cases in which each tactic was seen, %, 2023 to 2026



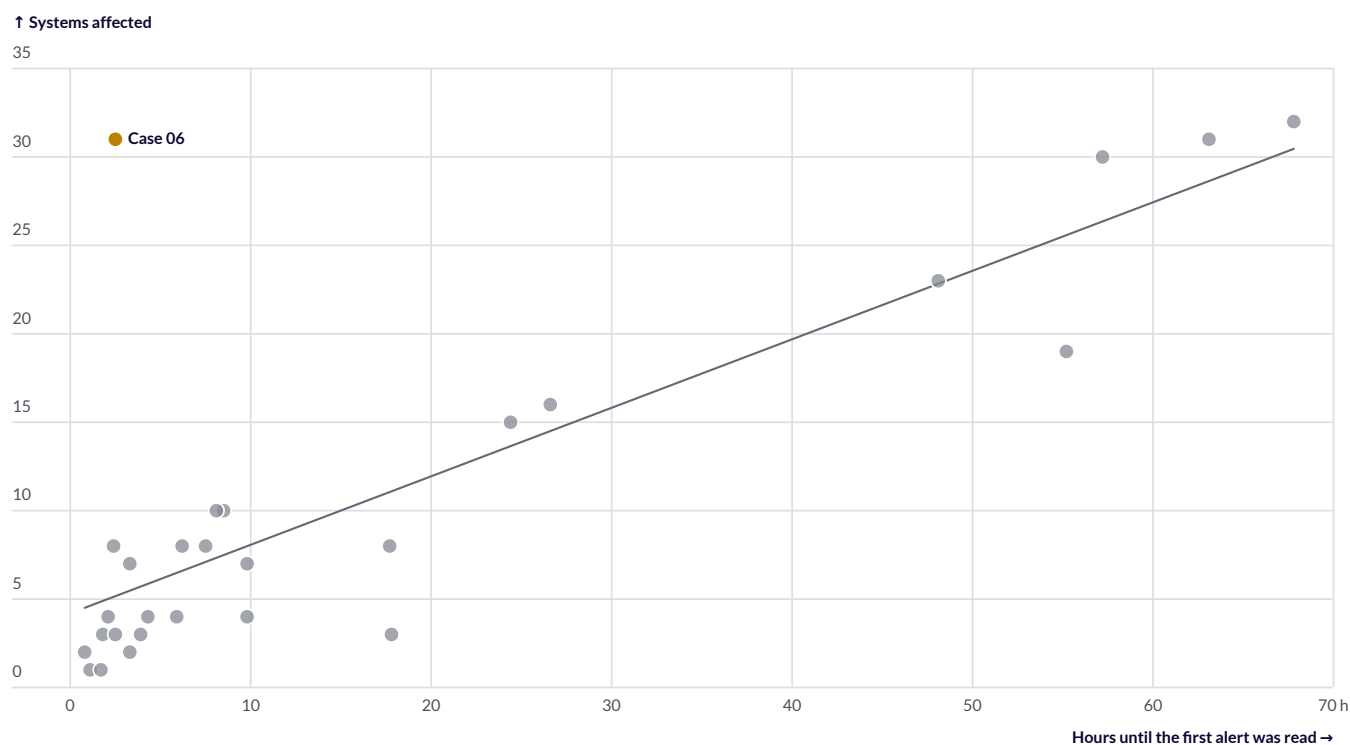
Source: incident response cases, tactics as named in MITRE ATT&CK.

Cases where the first alert was read within a day stayed small

In all but one of the cases an alert had fired before the damage. What differed was how long it sat unread. Each dot is a case from the last twelve months.

The longer the first alert waited, the more systems were lost

Hours until the first alert was read, against systems affected



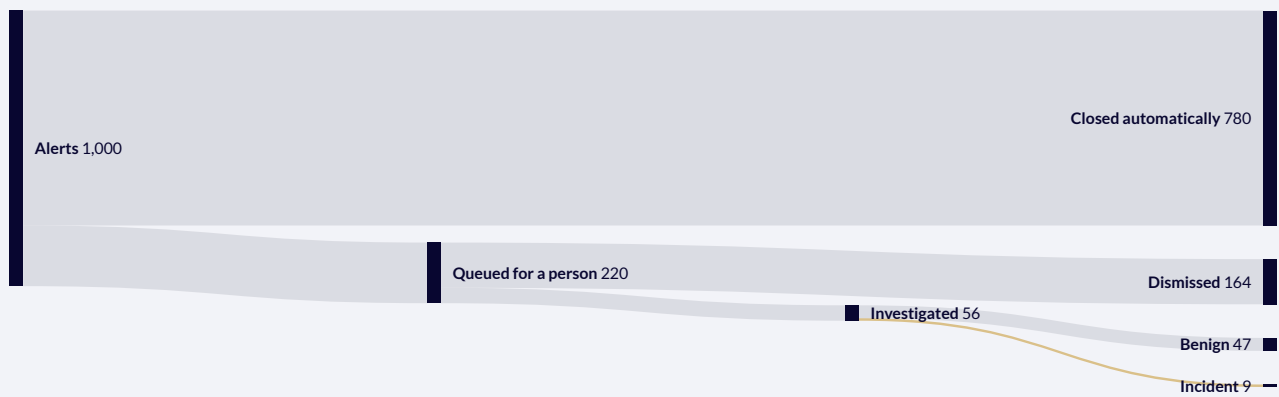
Source: 28 cases, October 2025 to September 2026. Case 06 was read in under three hours and dismissed.

Four days is shorter than most alert queues

A detection only helps if someone reads it in time. Most alerts close without a person looking; the ones that matter are a thin stream.

Of a thousand alerts, nine become incidents

Where 1,000 alerts go in a typical month at a mid-sized organisation



Source: median of 14 organisations before they joined our detection service.

If the queue takes longer than four days to reach an alert, the alert arrives after the damage.

Method

Figures come from intrusions Hunt & Hackett investigated between January 2023 and September 2026. "Impact" is the first encryption, destruction or confirmed theft of data. Cases stopped before impact are left out of the time to impact, and included everywhere else.