Attackers Would Rather Log In Than Break In

An Examination of Cybersecurity in 2026 for Retail Automotive Dealerships

Proton Dealership IT and Cybersecurity

October 2026

Introduction

Every year, major security vendors publish threat data, Proton Dealership IT and Cybersecurity included. These reports are generally built from one of three different vantage points: a quantitative survey of IT and security leaders, an adversary-tradecraft study of who is doing what and how fast, and a defender's account of how intrusions unfold. This year, they converge on a single conclusion. Attackers would rather log in than break in.

That sentence should reorder the priorities of a dealership. If the primary way into the business is a valid credential or a hijacked session rather than a piece of malware, the controls that mattered most for a decade remain necessary but are no longer where the outcome is decided. Nearly four in five ransomware attacks now begin with an identity-based approach, and 82% of detections involved no malware at all.

Retail Automotive dealerships feel this shift more sharply than most businesses of comparable size. That is because a store or a group typically runs a small IT team against a distributed rooftop footprint, has meaningful turnover in sales and service, and a concentration of customer financial and personally identifiable information inside a handful of systems: the DMS, the CRM, the F&I platform, and a long tail of SaaS applications connected over the years. The result is a large, trust-heavy attack surface maintained by a small and often understaffed team doing the best job it can with what it has.

The sections that follow build on that through-line. First, they show how the threat landscape shifted toward identity, cloud, and AI-enabled speed. Then they examine how those shifts are changing ransomware economics, phishing tactics, vulnerability management, and the expertise required to turn existing security tools into actual protection.

Cybersecurity Trends

The Four Shifts That Defined the Year

The clearest way to understand the year is not as five separate threats, but as four connected shifts. Each one reinforces the same idea: attackers are spending less energy forcing their way through technical defenses and more energy appearing to be legitimate users operating inside trusted systems.

- Identity became the front door. 79% of ransomware attacks now start with an identity-based approach, and two-thirds of victims (67%) said the ransomware incident was their most significant identity attack.
- Malware became optional. 82% of detections were malware-free, up from 51% in 2020, as attackers hijack legitimate administrative tools such as RMM software and PowerShell.
- Everything got faster, and AI is the reason. eCrime breakout time dropped to 29 minutes, with a fastest observed time of 27 seconds, against an 89% year-over-year rise in AI-enabled attacks.
- The fight moved to cloud and SaaS. Intrusions against cloud based targets rose 37% year over year.

That movement is partly a response to defensive success. Endpoint detection and patching programs became genuinely good at catching malware, so adversaries pivoted to the places where they still look legitimate: trusted identities and trusted tools. Artificial intelligence then made that pivot cheaper, faster, and easier to run at scale. For dealerships, the implication is immediate: the biggest risks are no longer limited to malicious files or unpatched machines. They increasingly sit in the gap between normal-looking activity and the expertise needed to recognize when "normal" is being abused.

"A year ago we were mostly fighting malware. Today we're fighting trust — stolen sessions, valid logins, legitimate tools used against us. Defenders got good at spotting 'bad,' so attackers got good at looking 'normal.'"

Sean Patronis
Proton Dealership IT

The Operational Challenge That Creates the Most Risk

That is why the operational data matters as much as the threat data. Asked where their real exposure sits, organizations surveyed did not point first at technology. The top root causes were security gaps, known or unknown (62%), a lack of people with the right expertise and skills (58%), and a lack of protection or poor-quality protection (57%). Human error was the only factor that rose year over year, reaching 35%.

In a dealership, those conditions compound one another. Lean IT staffing, a distributed store footprint, high turnover, and sensitive customer data concentrated in a few systems produce a wide attack surface watched by a small team. The constraint is rarely willingness or effort. It is capacity and visibility: when an alert happens, there may be no one free to determine whether the activity is a harmless anomaly or an intrusion in progress. That capacity gap becomes especially consequential when the intrusion turns into ransomware.

"The biggest risk at a dealership isn't always a missing product — it's not having enough skilled eyes on the systems you already own. Attackers exploit the gap between the alerts a tool fires and the people who can act on them."

Sean Patronis
Proton Dealership IT

Ransomware

A Mixed Picture: Real Progress Alongside Rising Cost

Seen through that lens, this year's ransomware data is not a separate story. It is the financial consequence of the same identity-led, trust-abusing tactics described above. Several defensive measures are working, and the cost of an incident still went up.

Recovery costs are up. The average recovery bill, excluding any ransom, is now $1.7 million, an 11% increase year over year.

Encryption success ticked back up. 56% of attacks succeeded in encrypting data, a six-point rise after two years of decline, including 16% in which data was both encrypted and stolen.

That said, backups are winning. Backup-based recovery surged to 66%, up twelve points, while paying to recover fell to 48%, the lowest figure in three years.

For an owner or executive, the operative number is not the ransom. The recovery bill arrives whether or not a ransom is paid, and it is both larger and more certain. Retail organizations' investment in recoverable backups is producing exactly the result it was meant to produce: restoring from backup has become the more common way out. But backups are a recovery answer, not an access-control answer. They reduce the damage after compromise; they do not prevent the identity-led entry that allowed the event to begin.

How Ransomware Crews Now Operate

That distinction matters because ransomware crews have changed their tradecraft as much as their economics. Two patterns define the current approach.

- From smash-and-encrypt to identity-led, cross-domain extortion. Big-game crews now minimize contact with monitored endpoints.
- Data theft as the leverage. The 'ShinyHunters' pattern grants OAuth access to a trusted application and exfiltrates directly. No malware runs, and no firewall is crossed.

"The bad news: cleanup still averages $1.7 million, and after two years of decline, attackers are encrypting successfully again."

Sean Patronis
Proton Dealership IT

"They've stopped kicking down the front door. Now they walk in with a stolen badge, take the data quietly, and only then decide whether encryption is even worth the risk."

Sean Patronis
Proton Dealership IT

Both patterns are especially relevant for dealerships. Virtualization hosts, the CRM, and the connected marketing, finance, and inventory applications are precisely the high-value, lightly monitored targets these techniques were designed for. An OAuth grant approved two years ago by an employee who has since left the store is not a malware event, and no endpoint product will treat it as one. That is why email and phishing now matter less as isolated awareness issues and more as the starting point for identity compromise.

Phishing and Malicious Email

Why Email Took the Top Spot

This is the headline root-cause shift of the year. Malicious email (26%) and phishing (24%) are now the first and second most common root causes of ransomware. Together they account for half of all incidents, displacing exploited vulnerabilities, which had led for three straight years. In other words, the inbox has become one of the primary ways attackers reach the identity layer.

There are two forces that drive the surge. The first is displacement: as patching programs and endpoint detection closed the technical door, attackers went back to people. The second is industrialization: AI now allows attackers to create more convincing, more personalized lures at a scale that was not practical before.

> "Phishing didn't get more common because attackers got lazy — it got more common because AI made it cheap, fluent, and personalized at massive scale. The typo-ridden phishing email is basically extinct."

Sean Patronis
Proton Dealership IT

CrowdStrike attributes an 89% rise in AI-enabled attacks partly to social engineering, with generative AI producing convincing fake personas and translating lures for regional targets. That means phishing emails are getting harder to spot because they increasingly resemble the routine business messages employees expect to receive.

SentinelOne documented AkiraBot generating unique, context-aware messages across hundreds of thousands of websites with CAPTCHA bypass and proxy rotation.

Why Convincing Emails Are Only Part of the Problem

These are now two separate engineering problems, and treating them as one is the most common mistake in dealership security conversations. A message can be convincing without defeating multi-factor authentication, and a technique can defeat multi-factor authentication without being especially convincing.

Adversary-in-the-Middle (AitM) phishing uses reverse-proxy pages to capture the authenticated session cookie after login. Multi-factor authentication worked, and the attacker got in anyway.

Infostealers such as Katz Stealer and PXA Stealer harvest session cookies and 'trusted device' status, so a replayed token inherits the identity without ever triggering a prompt.

Vishing and ClickFix lures deliver initial access, increasingly with AI-translated 'click to fix' prompts aimed at whichever language the target uses.

This is why multi-factor authentication was enabled in 97% of breaches that began with credentials. In most of those cases the control was present and correctly configured. It was simply never designed to defend a session that has already been authenticated. For a dealership, the practical implications are twofold. Email filtering has to be modern enough to catch AI-written lures that contain none of the tells staff were trained to look for, and security awareness training has to be continuous rather than annual, because the quality of the bait now improves every quarter. The same lesson applies to technical vulnerabilities: progress is real, but attackers will continue moving toward whichever path offers the least resistance.

"Modern phishing doesn't try to steal your password — it steals your session after you've already logged in with MFA. That's why 'we have MFA' is no longer a finish line."

Sean Patronis
Proton Dealership IT

The Exploited-Vulnerabilities Trend

Why the Number Fell

At first glance, exploited vulnerabilities appear to be the counterexample to the year's broader story. They fell from 32% to 18% of ransomware root causes — down fourteen points, and off the top spot after three years. But the decline does not mean vulnerabilities stopped mattering. It shows how quickly email and identity grew as preferred entry points.

Two things drove the decline. The first is genuine defensive progress: sustained investment in patching, helped by AI-assisted vulnerability prioritization. The second is arithmetic. Email and identity-based entry grew so quickly that vulnerabilities shrank as a share of the total even where the underlying risk did not fall. What took the top spot is identity: nearly four in five attacks (79%) now begin with an identity-based approach rather than a technical exploit. That makes vulnerability management less headline-grabbing this year, but not less important.

Why the Decline Is Expected to Reverse

The same technology that helped defenders prioritize patches is now helping attackers find and weaponize flaws faster than people can respond.

Sophos warns explicitly that frontier AI's vulnerability-discovery capability could push vulnerability-based ransomware back up in the year ahead. SentinelOne describes the end of the "needle in a haystack" advantage: actors scan the global IP space and weaponize edge vulnerabilities within hours. The same force that accelerated phishing is beginning to accelerate exploitation.

The dealership version of this problem is specific and physical. It is the firewall at a satellite store, the VPN appliance installed during a rooftop acquisition, the device that reached end of support two years ago and still terminates a site-to-site tunnel. Equipment of this kind cannot run endpoint detection, frequently sits outside the patch cycle, and in many groups does not appear on any

"Vulnerabilities didn't stop mattering — they got outcompeted. Why burn a zero-day when a stolen session cookie gets you in as a trusted user and trips no alarms?"

Sean Patronis
Proton Dealership IT

"The decline is a snapshot, not a trend line. Machine-speed exploitation of edge and perimeter devices — the ones that can't run EDR and often can't be patched — will pull that number right back up."

Sean Patronis
Proton Dealership IT

current inventory. Exposed applications and systems were already the number one entry point at 38%, which means the question is not whether vulnerability management still matters. It is whether dealerships can find and fix the exposed systems they may not know they have.

Expertise, Security Gaps, and Closing the Gap

Tools Are Table Stakes; Expertise Turns Them Into Outcomes

It is clear that security software is both necessary and no longer sufficient. The data makes the case plainly.

Controls were present and still failed. Multi-factor authentication was on in 97% of credential breaches, and firewalls detected 61% of attacks before payload delivery. Detection only helps if someone acts on it.

There is often nothing for a product to catch. 82% malware-free means defense depends on behavioral analysis and human threat hunting rather than signatures.

The gap is interpretation. Teams hold vast telemetry but often lack the context to distinguish an intrusion from an anomaly. In one SaaS compromise, the activity persisted for 71 days until analysis correlated a phishing campaign with unusual account geography. The lesson for dealerships is direct: the signal may already exist, but without skilled monitoring and response, it may not become action quickly enough.

"Buying security tools or platforms without the people with expertise to run it is like buying an MRI machine and no radiologist. '97% of credential breaches had MFA' tells you everything — the tool was there; the expertise to deploy, correctly configure, monitor, and respond wasn't."

Sean Patronis
Proton Dealership IT

Finding the Risks You Do Not Know You Have

"Unknown security gap" ranks among the top root causes of risk, and this year's blind spots are systemic across the industry rather than particular to any one store. For dealerships, closing those gaps starts with five practical disciplines:

1. **Assess and properly monitor who is logging into your systems.** MFA alone is not enough anymore. You need comprehensive, phishing-resistant methods to keep your system secure.
2. **Keep everything up to date with patches.** Exposed, unpatched devices can be that open window you need to avoid.
3. **Have quality email filtering that can detect malware and phishing and continually train your employees against social engineering and phishing scams.** That means test them, and if they fail, teach them how to spot or follow company policies that mitigate risk – such as not accessing personal email at work and not clicking on links without examining them first.
4. **Have an incident response and recovery plan.** Practice this at least once a year. You need to know who you are going to call, how to quickly get help, and what happens in the worst-case scenario.
5. **Continuous monitoring by experts, using a quality Managed Detection and Response program like Proton's.** Dealerships don't have the staff for 24/7 coverage, which is what is truly needed today with attack speeds reaching as fast at 27 seconds.

The One Priority Before Year-End

If those five disciplines have to be prioritized before the calendar turns, identity should come first. A dealership should make identities phishing-resistant and actually monitored, in this order:

1. Move from one-time passcodes and push approvals to phishing-resistant multi-factor authentication — passkeys or FIDO2 — across the DMS and every SaaS application, and retire legacy authentication.
2. Add identity threat detection with session and token monitoring, so that a login carrying a stolen session is flagged rather than waved through.

"If you do one thing before New Year's: make identity phishing-resistant and actually monitored by experts. Every major trend this year — ransomware, phishing, data theft — runs through a compromised identity. Fix that and you've addressed the current root cause, not the symptom."

Sean Patronis
Proton Dealership IT

Conclusion

The through-line of the 2026 reporting is a single sentence: attackers would rather log in than break in. Each of these key takeaways are another view of that same fact:

- Identity leads 79% of ransomware attacks.
- Malware is absent from 82% of detections.
- Email and phishing together account for half of all ransomware root causes.
- Multi-factor authentication was present in 97% of credential breaches and was not enough on its own.

The encouraging half of the data deserves equal weight because it shows that disciplined work changes outcomes. Backup-based recovery rose to 66%, and sustained patching pushed exploited vulnerabilities from 32% down to 18% of root causes. Those are the results of ordinary, disciplined work carried out consistently over several years. The same discipline applied to identity can produce the same kind of result, and it is the takeaway most worth acting on.

What the data does not support is the assumption that buying another product closes the gap. Firewalls detected 61% of attacks before payload delivery; whether that detection mattered depended on whether anyone was watching and able to act. The dealerships that come through the next twelve months well will be the ones that pair the tools they already own with the expertise to deploy, configure, monitor, and respond — whether that expertise is hired or partnered.

Sources

Figures and percentages in this paper are drawn from the four 2026 vendor threat reports below.

Proton Dealership IT and Cybersecurity — 2026 State of Cybersecurity.
Sophos — The State of Ransomware 2026.
CrowdStrike — 2026 Global Threat Report: Year of the Evasive Adversary.
SentinelOne — Annual Threat Report: A Defender's Guide from the Frontlines.

PROTON
DEALERSHIP IT | CYBERSECURITY

©2026 Proton Dealership IT. All rights reserved. 10/26