

HardenStance Briefing

Trusted research, analysis & insight in IT & telecom security

PUBLIC/SPONSORED

Airties' new cybersecurity portfolio

Sponsored by Airties

- With a large base of telco and ISP customers already using its market-leading Wi-Fi management and optimization software, Airties is seeking to disrupt the home networking market by launching its own cybersecurity apps to run on home routers.
- Leveraging an already mature, scalable edge and cloud architecture allows Airties to develop a cybersecurity portfolio at a small incremental cost.
- As well as enabling telcos to bring cybersecurity to the mass market among consumers and SMBs, Airties wants to be a leader in protecting against new threats. One example is an 'Agentic Shield' to protect against risk from agentic AI frameworks.

If you survey users on what router-hosted applications they value most, Wi-Fi optimization consistently comes first and cybersecurity comes second.

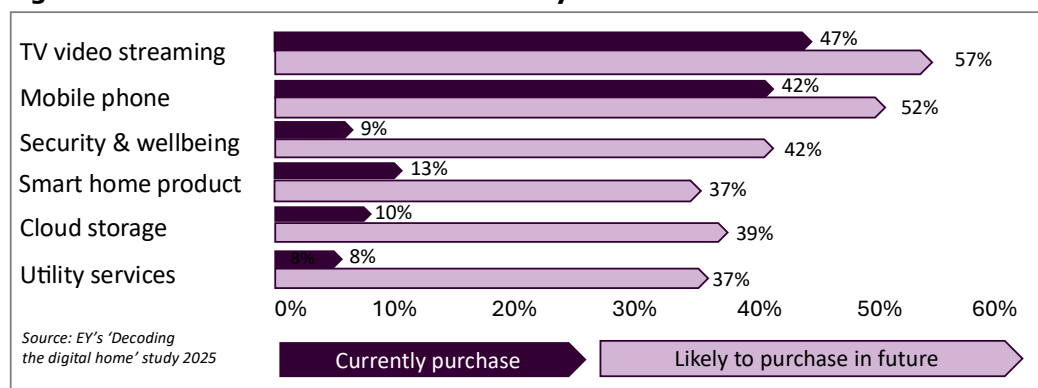
Security comes second only to Wi-Fi optimization

Ask them what application or service they value most on their home broadband network and consumers tend to answer in terms of cloud-hosted services like Netflix, Amazon Prime and home automation applications. Small businesses will answer in terms of any number of business applications. If you survey users on what router-hosted applications they value most, Wi-Fi optimization consistently comes first and cybersecurity comes second. Consumer research has shown this hierarchy in user preferences going back many years – almost without exception.

New EY research shown in **Figure 1** classifies security as a premium service, albeit EY also seems to assume Wi-Fi optimization is a given rather than a premium service. The data nevertheless reiterates the very high latent demand there is for cybersecurity in the home. **Figure 1** also highlights the opportunity for telcos to serve that demand by adding or embedding security into their consumer and small business service packages.

It should come as no surprise, then, when a leading vendor of Wi-Fi management and optimization software also invests in its own router security apps, which is exactly what Airties is doing. As will be shown, Airties has launched a portfolio of router security products that can run in proprietary environments or in either of the main open-source home router ecosystems - RDK-B (where Airties already has a large account footprint) and Prpl (which has started to see commercial roll out in 2026).

Figure 1: Consumers want to add security to their home broadband bundles



Telco strategies for protecting consumers and small businesses

In addition to the security features they already build into the network, router security applications are one of three types of cybersecurity software that telcos and ISPs are selling to consumers and small businesses:

- **Router security apps** block malicious traffic to and from every single smart device on the network using multiple protocols including IP and DNS.
- **Endpoint security** comes with multiple features that include scam protection as well as antivirus. It offers the richest possible protection but is only supported by high end devices with large OS footprints like PCs, smartphones and TVs.
- **DNS security** provides baseline security for 100% of the devices in the homes and businesses of 100% of a telco or ISP's customers. It requires little or no active engagement by the user. As with endpoint security, DNS security extends protection to high-end devices 'on the move', beyond the home or business premises. Among its limitations, though, are that protection only intervenes at the DNS layer. Users can also opt out of the telco or ISP's DNS service in favour of another one.

Rather than preferring one approach over another, the world's most advanced telcos recognize the value of layered security and invest in all three of these layers.

The cyber threat landscape in 2026

The cyber threat landscape against which Airties is entering this market is one that every adult (and every child approaching secondary school age) is in some way aware of. Among the different threats, online scams are top of mind. These continue to be generated at vast, industrial scale, due in part to so-called 'scam compounds.' People seeking work in mostly poor countries, many of them in Asia, are often lured by gangs into scam compounds with the promise of legitimate work. They're then forced to work as scam operatives in these compounds, according to a form of modern-day slavery.

As shown at the bottom of this page, the key findings from the Global Anti Scam Alliance's most recent 2026 research show that both the number of scam victims and the impact on victims remain intolerably high. GASA's other research shows this remains the case in all other regions as well as Europe and the United States. An increasing share of scams are now assisted by AI, whether in terms of automatically generating better-written phishing emails or high-quality fake audio and video. Users find fakes increasingly difficult, if not impossible, to distinguish from real content.

Highlights of 'State of the Scams, 2026': United States

- 86% of Americans are confident they can spot scams. But 56% nevertheless still engage with them.
- Among those who engaged with scams, 21% lost money, suffering an average loss of \$1,541.
- Half of Americans rely on simple heuristics such as "too good to be true" or spotting grammar issues.
- There is an average of 347 scam attempts per person per year in the U.S. - an average of almost one a day.
- 66% of victims now need to be informed they've been scammed, up from 45% last year.
- 59% saw their wellbeing impacted – a drop in self-assurance (29%) reduced access to credit (20%).

Highlights of 'State of the Scams 2026': Europe

- 75% of European adults encountered a scam in the last year.
- Seven in ten are confident they can spot scams but 44% of those exposed go on to engage with scams. 22% of these interactions result in financial loss.
- The average financial loss is €2,735.
- On average each victim suffers 2.7 scam incidents.
- Recovery is limited. It's 6% when reported to the police and 16% when reported to a bank.
- There is growing support for more proactive protection, like allowing banks to block suspicious high-value transactions without consent.

Source: Global Anti Scam Alliance (GASA) 'State of the Scams' research

Both the number of scam victims – and the impact on victims – remain intolerably high.

Hacking into a smart doorbell or its companion app can expose local IP addresses, geolocation data and installation addresses.

GASA’s conclusions on the state of scams echo those of other researchers. They point to a pretty clear picture of how consumers are coping with this problem in 2026.

- Users still tend to overestimate their own ability to spot scams.
- Users’ own efforts to avoid scams tend to be largely driven by habitual behaviours, such as ignoring unsolicited or suspicious-looking messages.
- Awareness is a necessary but insufficient condition for effective scam protection.

Most scams pose the same risk, whether they are delivered via a device connected to the home network, the mobile network or a third-party Wi-Fi network. In the home, a router security app should block any connected device from accessing a malicious URL or otherwise misbehaving. An endpoint security client on a PC or smartphone should go one step further by flagging risk before the user even tries to engage with a malicious application. It will also do that when the user is on the move as well as in the home. But endpoint security is relatively expensive, it requires significant user engagement, and it doesn’t protect all the other devices on a home or small business LAN.

Scams are just one of many types of cyber threat

Given how all-pervasive they are, and how easy it is to quantify the impact, media coverage of cyber risk is dominated by scams. But as shown in **Figure 3** there are many other types of cyber threat. A number of these are either unique to the home network environment or their impact can be exacerbated in the home context. In the case of these threats, router security apps offer the most effective protection. Some relevant examples of cyber threats that router security agents are uniquely or best placed to protect against include the following:

- **Targeted surveillance, disruption to household services and potential real-world physical threats.** Hacking into a smart doorbell or its companion app can expose local IP addresses, geolocation data and installation addresses. There have been real world instances of attackers pulling off remote takeover of heating, lighting or air conditioning systems. Among the most likely protagonists in household scenarios would be estranged partners with shared admin access to smart home apps. So far, there haven’t been any known instances of remote takeover of connected door or window locks leading to physical harm. But researchers have shown this scenario is plausible if vulnerabilities are not patched.

Figure 3: Cyber threats to consumers and available protections from telcos

1. Type of Threat	2. Type of attacker	3. Threat vectors	4. Attacker's tools	5. User's location	6. User protection
Financial scam	Scammer	Phone call	AI	At home (Wi-Fi)	User awareness
Personal data theft	Third party data broker	Phishing email	Vulnerability scans & exploits		Endpoint security +Scam protection +ID protection
Random and targeted Surveillance	Cryptojacker	Smishing text	Botnets	On the go (mobile)	Home router security app
Identity theft	Cyber Stalker	Malware	Bullet proof hosts		Network-based security DNS or DPI
Doxing	Identity fraudster	Botnet enslavement	Anonymization & spoofing	On the go (3 rd party Wi-Fi)	
Harm to children	Online voyeur	DDoS attacks	Dark web		
Broadband service outages & degradations		Malicious apps	Abuse of DNS		
		Malvertising & adware	Malicious TDS		
		Location tracking	Abuse of agentic AI frameworks		
			Malicious sites		
			Scam compounds		

Source: HardenStance

- **Random surveillance in and around the home.** In June 2025, a Milan court jailed five men for running a 'voyeurism as-a-service' business. They scanned the Internet and obtained access to tens of thousands of live video camera feeds throughout Italy. These cameras all had factory default credentials or other weaknesses. They live-streamed the private moments of Italians in retail fitting rooms, swimming pools and at home. Clips were shared on social media with degrading comments and location tags.
- **Broadband service outages and performance degradations.** The defining trend in the DDoS threat landscape over the last 18 months has been the enslavement of millions of insecure household IoT devices into malicious botnets. The botnets then use those enslaved devices as a platform from which to direct DDoS and other threats at other targets. Householders are typically not even aware that their devices have been compromised. They can nevertheless suffer from degraded service and application performance as a result of their devices misbehaving. Cryptojacking, where an infected device's processing power is 'hijacked' for cryptocurrency mining, is another way that performance of home or small business LANs can be compromised.

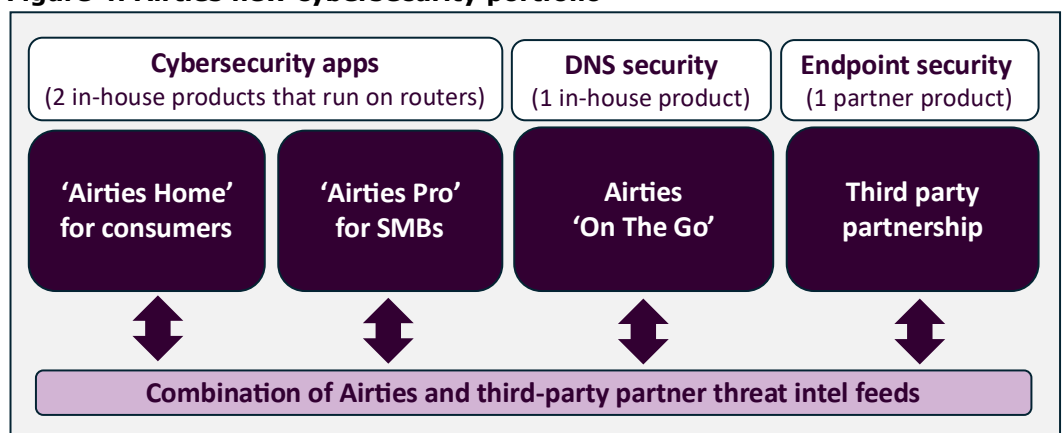
There are four components of Airties' new cybersecurity portfolio, available to consumers and small businesses.

Airties' new cybersecurity portfolio

Until now Airties has offered router security through a third-party partnership. Now the company is among smart home vendors that are augmenting core performance optimization software with their own, in-house, router security applications. HardenStance forecasts that telcos worldwide will grow their spending on router security apps to \$93 million in 2030, up from \$40 million in 2025. 63% of that spending is expected to be on RDK-B routers. Operators like Comcast, Charter, T-Mobile, Deutsche Telekom and Vodafone are deploying these at scale with embedded security apps. The remaining 29% of spending will be on Prpl. 8% will be on proprietary implementations.

As shown in **Figure 4**, there are four components of Airties' new cybersecurity portfolio, available to consumers and small businesses. The router security app comprises two modules. A number of baseline cybersecurity features are supported across Airties Home and Airties Pro. This blocks access to malicious sites using threat intelligence spanning DNS and IP protocols and other sources. It also filters content according to predefined rules to restrict access to inappropriate content. These aren't leading edge features, but in an otherwise unprotected home or small business, they can significantly raise the level of protection. With more advanced features, however, Airties wants to compete head-on with specialist cybersecurity vendors.

Figure 4: Airties new cybersecurity portfolio



Source: HardenStance/Airties

More advanced features supported in 'Airties Home' and 'Airties Pro' editions include:

- additional firewall features to augment router hardening;
- ad blocking to assure a better user experience as well as protect against cyber risk;
- threat detection and remediation like quarantining or isolation of infected devices.
- integration of observed cyber threat insights into Airties' existing telco and ISP dashboard, as well as correlation with existing application and device level analytics.
- protection against risk arising with the increasing adoption of autonomous AI agent frameworks (see below).

More advanced features include additional firewall features to augment router hardening.

Airties Business – cybersecurity tailored to small businesses

'Airties Pro' for small and medium sized businesses supports all the features supported in Airties Home. In addition, it also includes features that are tailored to the unique IT architecture and cybersecurity requirements of small and medium sized businesses, which Airties defines as businesses with up to 50 employees. Key features include network segmentation to divide the organization's LAN into unique secure zones, each with its own security policies; ethernet blocking to disable ports; and client isolation to prevent connected devices from communicating with one another.

An 'Agentic Shield' to protect against OpenClaw risk

Many of the features Airties is rolling out offer familiar baseline cybersecurity. However, the company also wants to lead by protecting against emerging cyber risk. One of these areas is risk from new autonomous AI agent frameworks like OpenClaw that run on a user's PC or server on their own premises.

It's clear from CEO Tim Cook's public comments at the end of April that Apple couldn't keep up with a sharp upward spike in demand for the Mac Mini. This has mainly been driven by OpenClaw's appeal among all kinds of advanced users, including some consumers. Many early adopters of OpenClaw and other agentic AI frameworks are embracing these tools at pace with little or no security controls.

Consistent with the key principle of layered security, an early adopter's own cybersecurity hygiene should provide an important baseline of protection. Users shouldn't be enabling admin privileges that allow OpenClaw to control their PC or workstation's OS or their network. They should be wary of unhardened Chinese AI models. Even with hardened models like Google Gemini, the cadence of releases is so frequent that users need to be sure they're using the very latest one. Being careful not to enable port forwarding sounds incredibly basic but it's still key in managing these new risks. Unfortunately, it's clear from vendor and media reporting that many early adopters are disregarding these basics.

For a high level of security efficacy, layered security assumes that even good basic cyber hygiene needs augmenting with threat monitoring, detection and mitigation. Endpoint security vendors Bitdefender, F-Secure and Gen Digital have already launched scanning features targeting the new risk from OpenClaw and other frameworks. These look for vulnerabilities and malicious behaviours in so-called 'skills' files that direct AI agents as well as in Model Context Protocol (MCP) traffic between AI agents and models.

Airties aims to lead in bringing equivalent protection to routers, using firewalling and other router security extensions. For its 'Advanced' edition, Airties is therefore building what it calls an 'Agentic Shield'. This will do things like block port forwarding; detect shadow AI gateways; validate the integrity of external AI skills; and restrict lateral movement with rate-limiting rogue agent loops. It will also use an AI sandbox to run and test AI agents. The main goal isn't to defend against AI specifically. It is to protect against any of the AI and non-AI threats that agentic AI platforms can expose a network to.

Rounding out the portfolio of four cybersecurity products depicted in **Figure 4**, Airties offers an 'On the Go' DNS filtering solution to protect users' mobile devices once they're out of range of the home or small business network. This is supported by a variety of partner threat intel feeds. Lastly, Airties offers its telco customers endpoint security via a third-party partnership with a leading endpoint security vendor.

Security built on a mature solution architecture

A core driver of Airties security strategy is leveraging its Wi-Fi optimization and management software architecture to build additional apps like cybersecurity at low incremental cost. **Figure 5** depicts how the cybersecurity portfolio is deployed across Airties Edge software on the router, in the Airties Cloud, as well as in the telco or ISP's cloud. This is Airties' unique core architecture but the fundamentals are the same three-layered architecture that any vendor in this space needs to use in order to balance cost and performance, agility and scalability.

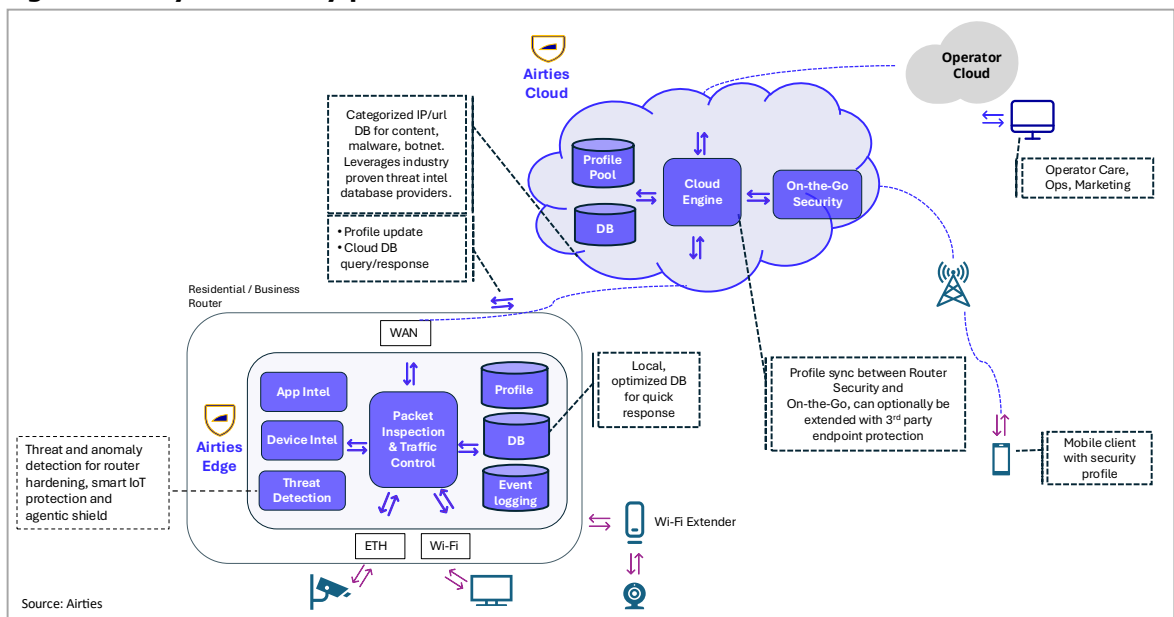
A core driver of Airties security strategy is leveraging its Wi-Fi optimization and management software to build additional apps at incremental cost.

The cost of a core management system that registers to a cloud, manages live connections, and sends and receives data is significant. Hence sharing that cost across multiple revenue-generating application creates more flexible commercial options for any vendor. Moreover, there is also a lot of obvious complementarity and re-use across the specific application areas that Airties is targeting now. The security portfolio builds on the device and application intelligence that already forms part of the core Wi-Fi optimization and management software. These ingest and process granular analytics on the type, model, brand and OS of every device on the network - and on all the applications these devices are using down to the packet level. Airties security portfolio re-uses and builds on these existing device and application intelligence microservices.

Building and selling several apps is consistent with open source ideals

The opensource RDK-B and Prpl ecosystems are designed to allow any standard-compliant apps to run on any standard compliant hardware. A vendor evolving its portfolio to support more than one app therefore isn't at variance with that. So long as the software is fully compliant with the open standard, telcos and ISPs can benefit from capex and opex savings by buying multiple apps from one vendor.

Figure 5: A cybersecurity portfolio driven off Airties' mature solution architecture



An AI-powered development environment

'AI Native' is a key trend in software development. It uses AI agents as the primary foundation around which devops teams and workflows are built rather than just leveraging AI as a supporting tool. During the first half of 2026 Airties has embraced a native AI roadmap by introducing one of the primary generative AI chatbots and large language models (LLMs) into its development environment.

The cybersecurity suite is among the first new capabilities to benefit from this. This should enable the cybersecurity releases to be iterated with better agility and scalability. Given how important frequent updates are in cybersecurity, an agile development model is especially important for security apps. Airties is also using AI-assisted 'detection as code'. This uses threat detection logic as software code, enabling things like version control and quality assurance to be managed by the core software.

Opportunities and challenges for Airties

As shown, Airties has an advanced software architecture for delivering new applications like cybersecurity. The security portfolio is comprehensive, complementing the core router security apps with DNS-based network security and endpoint security. The router security apps are also designed to serve different market segments. Putting together the segmentation of the portfolio with the cost advantages the company can accrue from developing multiple apps, Airties has potential to be a cybersecurity disruptor in the home and small business markets.

The baseline expectation of most telcos and ISPs is that they should be able to charge for most router apps and cybersecurity is no exception.

The baseline expectation of most telcos and ISPs is that they should be able to charge for most router apps and cybersecurity is no exception. In terms of how telcos and ISPs go about charging, several models are in operation today. Some operators embed a cybersecurity app in all their new generations of routers and all their broadband service packages by default. Examples of operators pursuing this strategy with RDK-B products are some of the big cable operators in North America as well as Deutsche Telekom in Europe. Others are only embedding security in their premium packages. They're either recouping their costs via the price premium or making additional margin on top. These are the most user-friendly models, requiring no specific action on the part of the end user. Some telcos and ISPs prefer to offer a router security app as a one-off purchase for a recurring fee. That may require a user manually uploading the security app.

The baseline consumer proposition represents low hanging fruit for Airties. Whether it be to embed security as a core brand value and differentiator, or to grow incremental revenue, or to meet regulatory expectations, some telcos will be drawn to a proposition that enables them to extend baseline cybersecurity across all their new generations of home routers at low cost. Executing well on the small business edition – and some of the advanced features that span both editions – will be more challenging.

Most obviously, the feature requirements are more technically challenging. More than that, while a telco's own brand can be good enough for some advanced users, others will need to be persuaded not to prefer a more well-known cybersecurity brand under the hood of a telco's offer. Good execution and marquis customer references will therefore be key to succeeding in these segments. ■

"Airties' new cybersecurity portfolio", Copyright: Patrick Donegan, HardenStance Ltd, 2026

More Information

- HardenStance Briefing: [“Telco Strategies for Consumer Security 2026”](#)

About Airties

Airties empowers operators to provide smooth, smart, secure connectivity. Airties turns smart connectivity into a competitive advantage for operators and enhances how subscribers experience connectivity in the real world: making every connection more intelligent, reliable and secure. Airties’ AI-driven insights enable operators to lower churn, reduce expenses, boost satisfaction, and attract new customers.

Across departments, from engineering to marketing, Airties helps increase efficiency, accelerate innovation, and design smarter campaigns. Airties’ holistic suite of hardware-agnostic software enables ISPs to manage connectivity, based on leading industry standards and open-source software, across their fibre, cable/DSL, and fixed wireless access (FWA) deployments. Airties’ customers include leading service providers such as AT&T, Bouygues Telecom, BT, Cox, Deutsche Telekom, Telia, Telstra, T-Mobile US, Vodafone, and many others across the world. More information is available at www.airties.com

About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a leader in custom cyber security research and leading publisher of cyber security reports. HardenStance is also a strong advocate of industry collaboration in cyber security and is the organizer and host of the Telecom Threat Intelligence Summit. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, The GSM Association, MEF, OASIS, ETSI. The Cyber Threat Alliance. HardenStance is also a recognized Cyber Threat Alliance ‘Champion’. www.hardenstance.com

HardenStance Disclaimer

HardenStance Ltd has used its best efforts in collecting and preparing this report. HardenStance Ltd does not warrant the accuracy, completeness, currentness, noninfringement, merchantability or fitness for a particular purpose of any material covered by this report.

HardenStance Ltd shall not be liable for losses or injury caused in whole or part by HardenStance Ltd’s negligence or by contingencies beyond HardenStance Ltd’s control in compiling, preparing or disseminating this report, or for any decision made or action taken by user of this report in reliance on such information, or for any consequential, special, indirect or similar damages (including lost profits), even if HardenStance Ltd was advised of the possibility of the same.

The user of this report agrees that there is zero liability of HardenStance Ltd and its employees arising out of any kind of legal claim (whether in contract, tort or otherwise) arising in relation to the contents of this report.