VDC|Research
Insights for the Connected World

Press Release

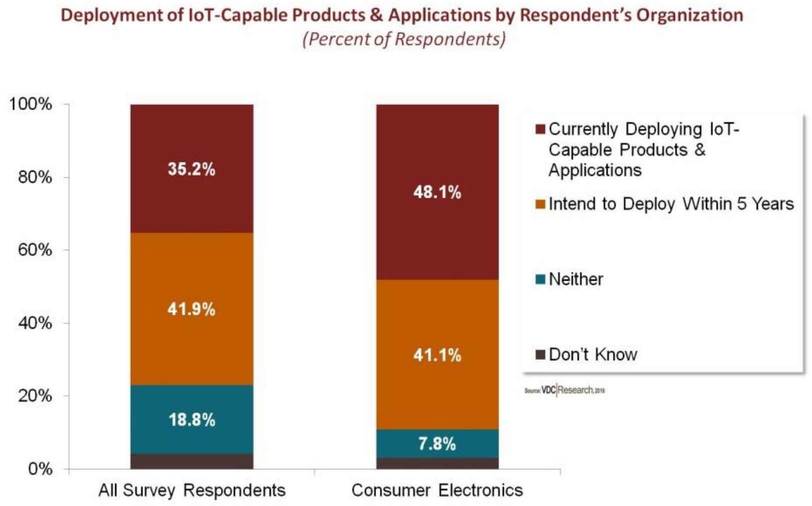
High Connectivity, Low Security in Home Automation and Wearables Market, According to VDC Research

Vendors need to walk the razor's edge between usability and security if they wish to see any success in the IoT consumer electronics market.

“The consumer electronics market has become the public face of the IoT. With many of these devices sitting so close to billions of consumers, comprehensive security solutions will be necessary to combat the growing threat of high publicity attacks.”

Natick, MA (PRWEB) March 02, 2016

Embedded software security revenue will grow at a rapid pace over the coming years as large service providers position themselves to take advantage of the burgeoning market for IoT services, according to a new report by VDC Research (click here to learn more). Vendors have unleashed a flood of wearables and home automation devices – connected white goods, HVAC systems, smart TVs, augmented reality glasses, smart watches, connected clothing – and show no signs of slowing down. Enabling consumer trust and peace of mind through security will be crucial if vendors wish to monetize the rapidly growing stream of consumer data.


Deployment of IoT-Capable Products & Applications by Respondent's Organization
(Percent of Respondents)

Source: VDC|Research, 2016

“Consumer electronics devices are much more likely to be connected – and at risk – than their less-visible counterparts,” says VDC research associate Roy Murdock. According to VDC Research's 2015 IoT & Embedded Engineering survey, engineers in the consumer electronics vertical are 13% more likely than the average engineer to be working for an organization that is already deploying an IoT-enabled device or application. Furthermore, 90% of consumer electronics engineers indicated that their organization would be deploying IoT-enabled solutions within the next 5 years as compared to only 78% in the industry at large.

With such a large volume of connected devices entering the market, consolidation around a common language for connecting these disparate devices and systems is becoming increasingly critical. The landscape is still filled with an overabundance of competing organizations, partnerships, and alliances that seek to push the adoption of their “open,” but often confining, solutions. Consequently, adoption among vendors and consumers is suffering. Uncertainty over the strength, strategy, and promises of various ecosystems is blocking investment decisions.

Common vulnerabilities in consumer electronics systems include weak (or sometimes missing) default usernames and passwords, obvious public-facing device identifiers, and a lack of any type of interface for resetting or reconfiguring security parameters. Additionally, implementing best-practice key management and data storage protocols remains a challenge within the industry. “With products in this market often protecting the safety of groceries, valuables, pets, and loved ones, consumers will patronize reliable, trustworthy, and hardened solutions,” says Murdock. “Getting security right is a huge opportunity for differentiation in a noisy, high-growth market. It is imperative that IoT services, device, and security vendors who accept the challenge operate responsibly and stay one step ahead of potentially life-threatening bugs and vulnerabilities."

About VDC Research

Founded in 1971, VDC Research provides in-depth insights to technology vendors, end users, and investors across the globe. As a market research and consulting firm, VDC's coverage of AutoID, enterprise mobility, industrial automation, and IoT and embedded technologies is among the most advanced in the industry, helping our clients make critical decisions with confidence. Offering syndicated reports and custom consultation, our methodologies consistently provide accurate forecasts and unmatched thought leadership for deeply technical markets. Located in Natick, Massachusetts, VDC prides itself on its close personal relationships with clients, delivering an attention to detail and a unique perspective that is second to none.