# Acquisitions are a standard way for cyber-security service providers to expand capabilities and presence

*June 2019*

Igor Babić

Most major cyber-security vendors acquired smaller security service providers during 2018 and 1Q 2019 in order to expand their portfolios and market reach. Telecoms operators also made M&A in the cyber-security space during this period. The main difference between the acquisitions carried out by these two company types is their purpose; vendors tend to acquire technology, while operators acquire people and consulting capabilities.

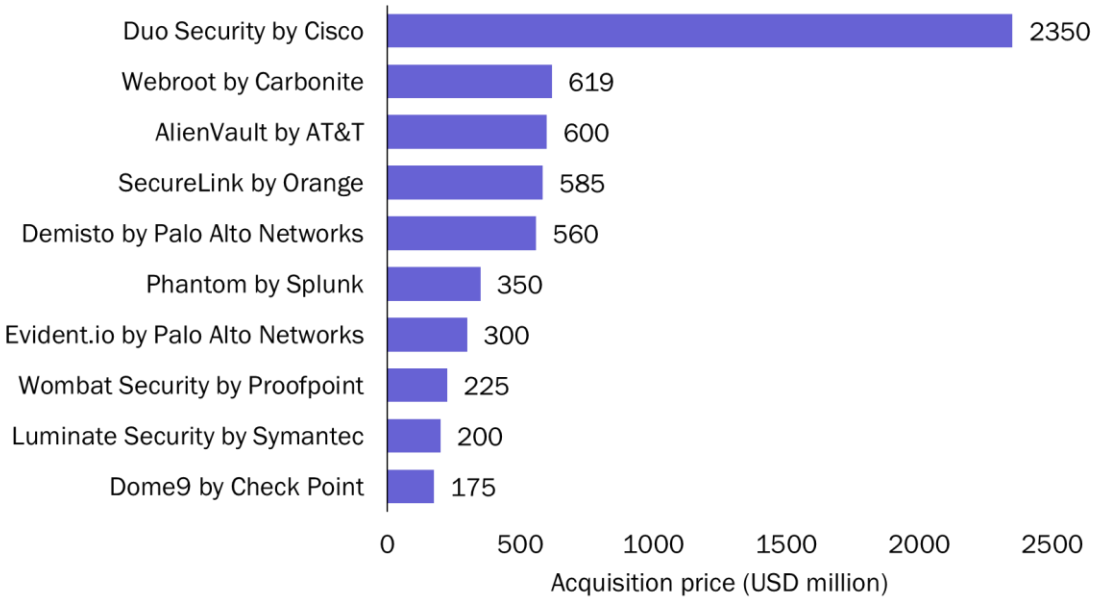
This article explores the acquisition activity of leading cyber-security vendors and telecoms operators that are competing in the cyber-security space. It draws upon Analysys Mason's *Cyber-security-related M&A tracker*.

## Both cyber-security vendors and telecoms operators are using acquisitions to expand their cyber-security capabilities

Cisco spent the most on acquisitions in 2018 and 1Q 2019 out of the vendors covered in Analysys Mason's *Cyber-security-related M&A tracker*. This is mainly due to its acquisition of Duo Security, a unified access security and cloud multi-factor authentication specialist, for USD2.35 billion (Figure 1). Duo Security generated over USD100 million in annual recurring revenue in 2017 and employed around 700 people at the time of the acquisition. It had reportedly raised a total of USD121.5 million prior to the acquisition.

Palo Alto Networks spent the second-largest amount on acquisitions in 2018 and 1Q 2019. It completed four cyber-security-related acquisitions during this period, and spent over USD1.1 billion in total (it acquired a further two companies in May 2019 for a total of around USD500 million). Its biggest acquisition was of Demisto (completed in March 2019), a security orchestration, automation and response specialist founded in 2015, for which Palo Alto Networks paid USD560 million. This acquisition will improve Palo Alto Networks's analytics and automation capabilities and will enable the vendor to accelerate its Application Framework strategy (which, in turn, will allow customers to deploy security innovations more quickly, through a suite of APIs).

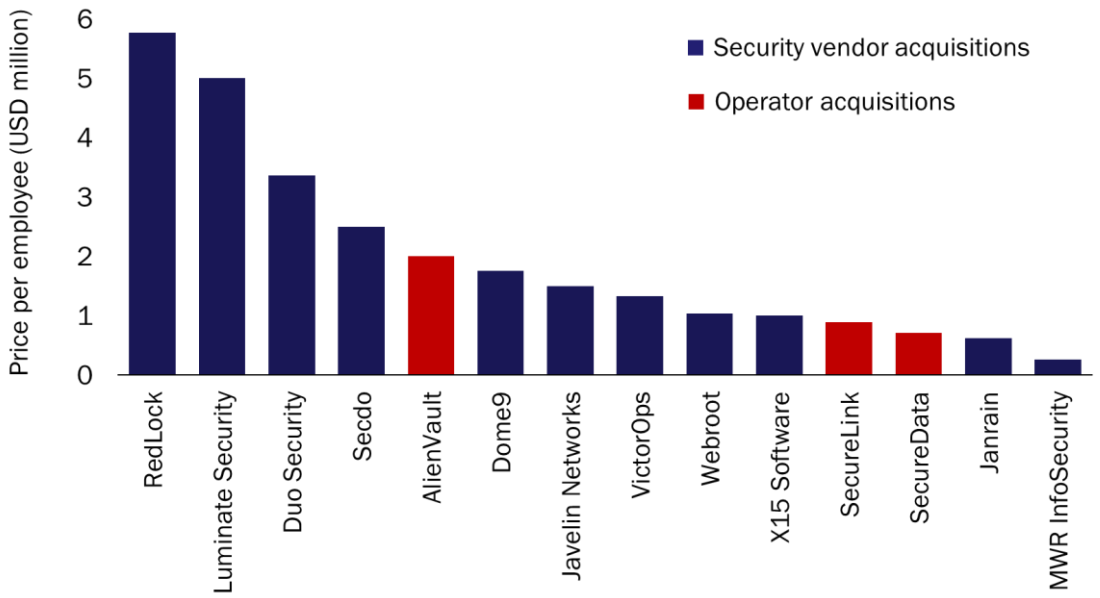
***Figure 1: Ten most-expensive cyber-security acquisitions (where the amount paid was disclosed or where reliable estimates are available), 2018 and 1Q 2019***




Source: Analysys Mason, 2019

Figure 2 illustrates how much each acquirer spent per employee to acquire the listed companies. The variation in these valuation multiples tells us a lot about the motives behind these acquisitions. Companies that were acquired mainly because they have developed unique and valuable technologies have higher per employee valuation multiples than more-established businesses that are primarily focused on providing consulting services. For example, the main reason behind Palo Alto Networks's acquisition of Redlock was to obtain Redlock's Cloud 360 AI-driven threat defence platform. Similarly, Symantec acquired Luminate Security primarily because of Luminate's Secure Access Cloud software-defined perimeter technology.

***Figure 2: Acquisition price per employee (for the cases where the number of employees and the acquisition price were both reported)***




Source: Analysys Mason, 2019

Telecoms operators have also made M&A deals in the cyber-security space. Orange spent nearly USD750 million in 2019 on its acquisitions of SecureData, a UK-based company providing integrated cyber-security solutions and consulting services, and SecureLink, a specialist in business solutions for secure remote access headquartered in the Netherlands. Both companies are well-established and focus primarily on consulting rather than technology development, explaining their position in Figure 2. Orange has added around 880 employees to its Cyberdefense business through these two acquisitions; it has extended its presence in Europe and has expanded into South Africa. Orange Cyberdefense generated USD358 million in revenue in 2018 (that is, prior to these acquisitions); SecureData generated USD57 million and SecureLink USD282 million during the same period. Orange will therefore roughly double its security revenue as a result of these acquisitions.

AT&T acquired AlienVault in 2018 for an estimated USD550 million–USD650 million and added around 300 employees as a result. AlienVault has reportedly raised a total of USD116 million since its inception in 2007. This acquisition allowed AT&T to significantly expand its cyber-security capabilities, and in 2019, the operator formed AT&T Cybersecurity, a standalone unit led by AlienVault's ex-CEO.

Orange's and AT&T's recent activities are not typical of operators (the acquisitions of AlienVault and SecureLink are the largest cyber-security acquisitions by operators since Singtel's USD810 million acquisition of Trustwave in 2015); most other operator cyber-security acquisitions have been far smaller. For example, Proximus acquired two companies in 2017 and 2018; one specialised in security analytics and vulnerability management and the other in providing managed security services. Each company had between 20 and 30 employees at the time of acquisition. KPN acquired malware protection specialist DearBytes (85 employees) in 2017 and TDC acquired Secu (11 employees) in 2019, a company focusing on vulnerability management services.

## The main difference between the acquisitions carried out by cyber-security vendors and those executed by telecoms operators is their purpose

All acquisitions in the cyber-security space enable the acquirer to expand its capabilities to some extent, but those carried out by vendors are more often executed to obtain technology or IP that can then be implemented into the vendors' offerings (as well as to acquire highly specialised talent). Acquisitions carried out by telecoms operators, on the other hand, are more often focused on gaining access to market segments that the operators are not already addressing sufficiently with their current offerings. For example, AT&T's acquisition of AlienVault enabled the operator to better target SMEs, Orange's two acquisitions in 2019 expanded the operator's cyber-security services geographical footprint and Proximus's acquisition of ION-IP in 2018 enabled the operator to expand its service portfolio in the Netherlands and increase the number of cyber-security vendors that it partners with. The aim of operators' acquisitions is often also to increase the cyber-security value chain coverage of their services (for example, through acquiring a company with managed services or software development capabilities).

More details regarding the acquisitions of the companies mentioned in this article are available in Analysys Mason's *Cyber-security-related M&A tracker*.