

Gartner: 2018 Security Spending to Reach \$96bn

Written by Frederick Douglas
22 December 2017

According to Gartner global security spending will reach \$96.3 billion in 2018-- an 8% increase over 2017, driven by regulations, shifting buyer mindset, emerging threats and the evolution to a digital business strategy.

"Overall, a large portion of security spending is driven by an organisation's reaction toward security breaches as more high profile cyberattacks and data breaches affect organisations worldwide," the analyst says. "Cyberattacks such as WannaCry and NotPetya, and most recently the Equifax breach, have a direct effect on security spend, because these types of attacks last up to 3 years."

Table 1

Worldwide Security Spending by Segment, 2016-2018 (Millions of Current Dollars)

| Segment | 2016 | 2017 | 2018 |
|----------------------------|---------------|---------------|---------------|
| Identity Access Management | 3,911 | 4,279 | 4,695 |
| Infrastructure Protection | 15,156 | 16,217 | 17,467 |
| Network Security Equipment | 9,789 | 10,934 | 11,669 |
| Security Services | 48,796 | 53,065 | 57,719 |
| Consumer Security Software | 4,573 | 4,637 | 4,746 |
| Total | 82,225 | 89,133 | 96,296 |

Source: Gartner (December 2017)

A 2016 Gartner survey validates current security buyer behaviour. Of the 53% of organisations citing security risks as the top driver for overall security spending, the highest percentage of respondents say security breaches are the main security risk influencing their security spending.

Gartner: 2018 Security Spending to Reach \$96bn

Written by Frederick Douglas
22 December 2017

As a result, security testing, outsourcing and security information and event management (SIEM) are the fastest growing security subsegments driving the infrastructure protection and security services segments.

Another security spending driver is regulation. In the European case there is the General Data Protection Regulation (GDPR), which comes in place on 28 May 2018. Other regions have similar rules, such as the Health Insurance Portability and Accountability in the US or the Cybersecurity Law in China. Such regulations bring about increased spending in security tools, privileged access management and SIEM.

Gartner predicts over 60% of organisations will invest in multiple security tools by 2021, including data loss prevention, encryption and data-centric audit and protection tools, up from 35% in 2017. In addition, skill shortages, technical complexity and the threat landscape will drive the move to automation and outsourcing, leading to outsourcing becoming the 2nd largest security spending segment (after consulting) in 2018.

In 2019 total spending on security outsourcing spending will make 75% of spending on security software and hardware products, up from 63% in 2016.

A final spending shift involves detection and response-- a trend driving security market growth during the next 5 years. The increased focus on detection and response enables technologies such as endpoint detection and response, and user entity and behaviour analytics to disrupt endpoint protection platforms and SIEM.

Go [Gartner Forecasts WW Security Spending Will Reach \\$96bn in 2018](#)