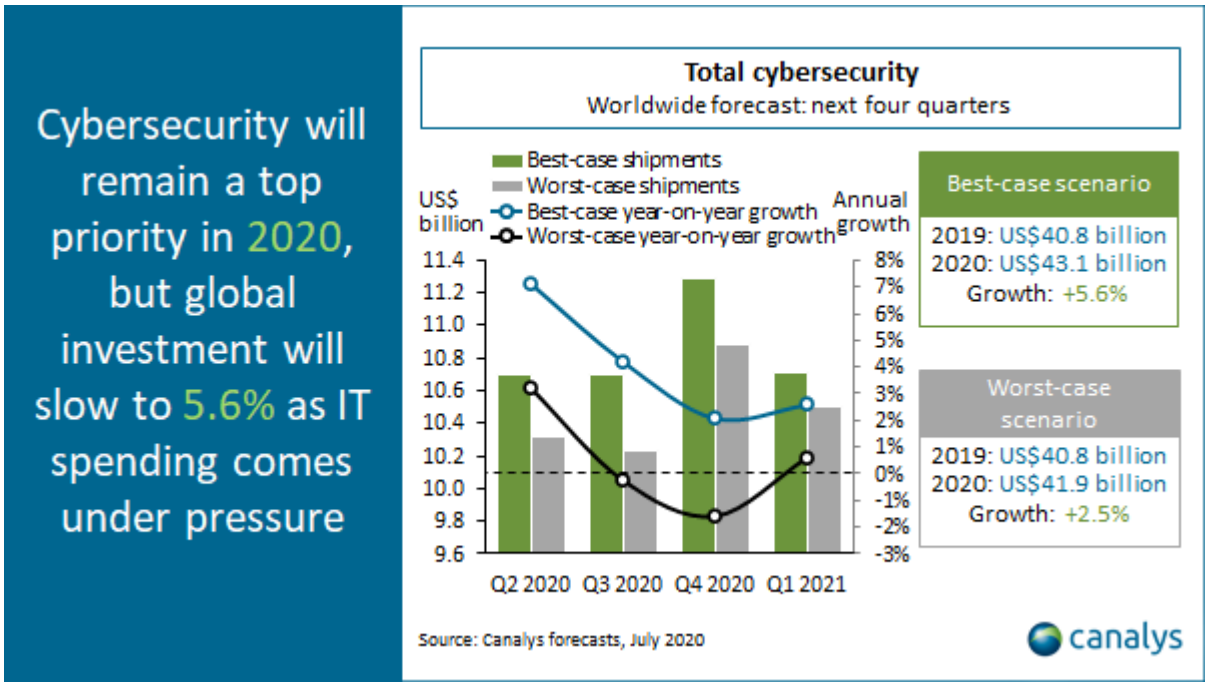
Canalys: Cybersecurity investment to grow by up to 6% in 2020

Shanghai (China), Bengaluru (India), Singapore, Reading (UK) and Portland (US) – Monday, 20 July 2020

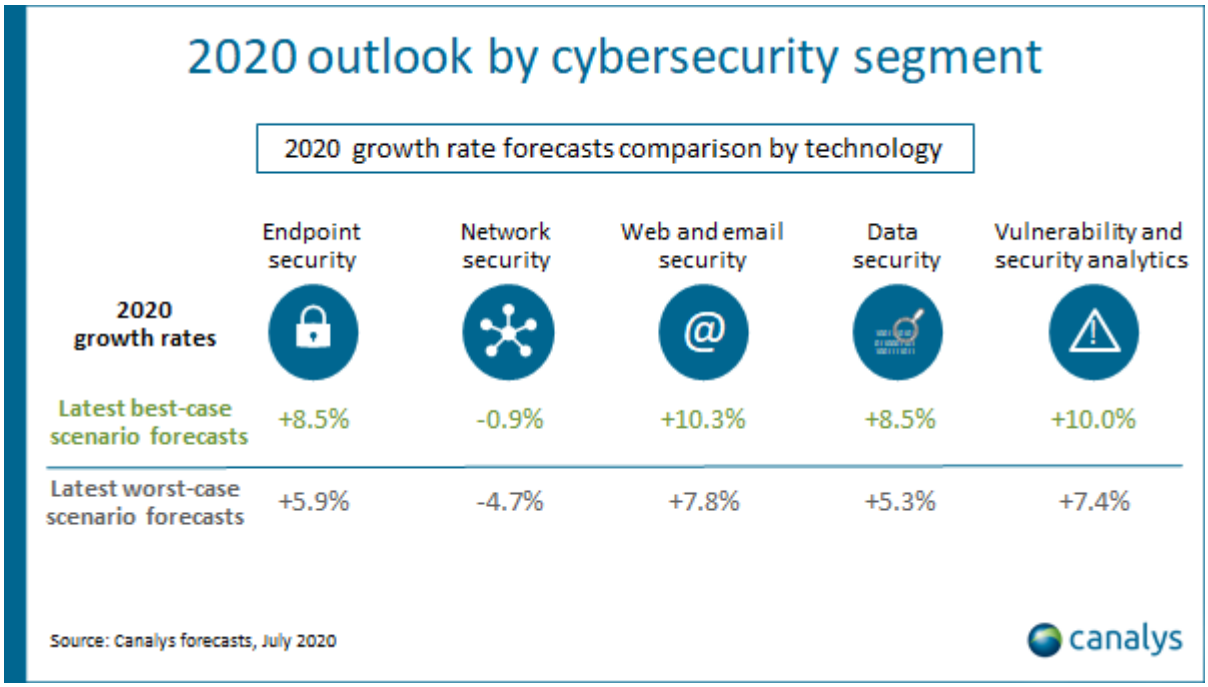
Canalys forecasts that worldwide cybersecurity spending will grow 5.6% in its best-case scenario, where investment continues to outpace the economy. The overall shipment value, covering endpoint security, network security, web and email security, data security, and vulnerability and security analytics, is expected to reach US$43.1 billion. Even in Canalys' worst-case scenario, if IT budgets come under serious pressure, the global cybersecurity market is still forecast to grow 2.5% in 2020. This assumes the maximum level of negative economic impact and duration of the COVID-19 pandemic.



Cybersecurity will remain a top priority for most organizations in 2020, as threats and vulnerabilities persist and compliance, regulations and ecosystem requirements strengthen. It underpinned the mass shift to remote working during lockdown by securing newly provisioned

endpoints, providing secure access to corporate resources and extending perimeter defenses beyond physical corporate networks.

“The shift to subscriptions will shield cybersecurity from immediate IT spending cuts, but additional expenditure will be affected for the rest of the year as organizations begin the next stage in their response to the pandemic,” said Matthew Ball, Chief Analyst at Canalys. “The switch from free trials to paid-for subscriptions will be a factor in maintaining cybersecurity growth. But the mix of cost containment measures, workforce reduction and cashflow issues will result in greater scrutiny of existing projects and smaller deals. Delays and cancellations of new initiatives will increase, except those that enable cost reductions and secure high-priority digital transformation initiatives.”



2020 cybersecurity growth rates will vary by technology segment. Endpoint security will see high growth rates, as remote working practices are extended, though momentum will slow after strong investment in Q1, especially in SMB customer segments. Network security will remain the largest segment, at 36% of spending. But the reprioritization of budgets will defocus spending on traditional appliance-based perimeter defenses. This will lead to negative growth rates. Organizations will have to boost spending in other areas of their security stack to address new vulnerabilities created by a more decentralized workforce through multi-layer prevention plus detection and response. This will incorporate web and email security, data security, and vulnerability and security analytics. Spending will also shift to cloud deployment options and

securing cloud-deployed workloads, as organizations optimize business continuity measures and accelerate cloud migration.

“Large-scale remote working will be in place for a lot longer than previously envisioned when lockdown first took effect in March,” said Ketaki Borade, Canalys Research Analyst. “While some employees will return to the workplace over the coming months, organizations will have to maintain a highly decentralized workforce that can work anywhere for the foreseeable future. This includes a combination of remote-only and flexible workers, as well as on-site-only workers that can quickly transition to remote-only working if a localized or national lockdown arises again.” Latest Canalys research for Western Europe, for example, forecasts the proportion of workers working from home regularly will grow from 12% pre-COVID-19 to 28% in the post-COVID-19 pandemic era.

The implications for cybersecurity are far-reaching. “The emergence of COVID-19 in January saw a surge in targeted phishing campaigns and malicious domains established to lure end users searching for information,” said Borade. “These fell once lockdown took effect. But hackers continue to target organizations and individuals by compromising unsecured and poorly trained remote workers via numerous vectors, including email, social engineering and RDP brute force attacks. Organizations will to have reassess changes to workflows, application use, customer engagement and training for cybersecurity awareness in a more virtual workplace.”

For more information, please contact:

Canalys China
Nicole Peng: nicole_peng@canalys.com +86 150 2186 8330

Canalys India
Rushabh Doshi: rushabh_doshi@canalys.com +91 99728 54174

Canalys Singapore
Sharon Hiu: sharon_hiu@canalys.com +65 9777 9015
Yih Khai Wong: yih_khai_wong@canalys.com +65 9712 7835

Canalys UK
Matthew Ball: matthew_ball@canalys.com +44 7887 950 505
Alastair Edwards: alastair_edwards@canalys.com +44 7901 915 991
Kelly Wheeler: kelly_wheeler@canalys.com +44 7919 563 270

Canalys USA
Ketaki Borade: ketaki_borade@canalys.com +1 650 387 5389
Marcy Ryan: marcy_ryan@canalys.com +1 650 862 4299
Alex Smith: alex_smith@canalys.com +1 650 799 4483

About Canalys

Canalys is an independent analyst company that strives to guide clients on the future of the technology industry and to think beyond the business models of the past. We deliver smart market insights to IT, channel and service provider professionals around the world. We stake our reputation on the quality of our data, our innovative use of technology and our high level of customer service.

Receiving updates

To receive media alerts directly, or for more information about our events, services or custom research and consulting capabilities, please contact us or email press@canalys.com.

Please click here to unsubscribe