We have seen the impact of cyber-attacks regularly reported in the news and many companies are having to handle cybersecurity issues on a daily basis. It’s hard to believe that only 10 years ago the concept of cybersecurity was new to the business world. It started from a government national security perspective only to break into the public domain during the 2016 US presidential election. Since then, it changed from being a neglected topic to being a C-level topic in 2019 — yet awareness remains too low. Cybersecurity has traditionally been delegated to the IT department of large organizations, while being neglected by SMEs who are most vulnerable to ransomware and nation-state attacks seeking IP.

Focusing on people

Today the actions of individuals can have major impact on businesses as they are the primary targets of cybercriminals’ attempts to infiltrate companies. As a result, the discussion surrounding cybersecurity technology has increasingly shifted to the decisions made by individuals. Technological quantum leaps in the last three years replaced legacy on-premise antivirus with cloud-native SaaS endpoint systems. Such systems offer managed endpoint protection by applying AI-based models, in which machine learning is applied to billions of data points to develop threat graphs.

Cybersecurity and the holistic view

The developments over the past few years reflect a paradigm shift and prove the importance of cybersecurity awareness for SMEs and global players alike. Global corporations and SMEs must employ a holistic view that embraces threat intelligence at the C-level all the way down to endpoint protection for the individual user. Employees at all levels must be trained in endpoint security awareness and be supported by the latest cybersecurity technology. But an effective cybersecurity strategy goes beyond internal individuals. A critical concept as a path to protection is “breakout time” — between when an external intruder gets on a machine and when they break out of the beachhead they’ve established. Only organizations that meet the “1-10-60 Minutes Rule” will be able to stop a potential breach from occurring. These three time objectives are technically critical to detect and respond to the intruder. The concept was first introduced by CrowdStrike, the global market leader for endpoint protection in the 2018 Global Threat Report.

* The 1-10-60 Minutes Rule: 1 minute to detect, 10 minutes to investigate, 60 minutes to remediate.