Automation in Cybersecurity: Making the Impossible Possible

As the world becomes heavily reliant on automation, the same needs to be said for cybersecurity. More and more threats are becoming automated, so fighting against them manually is described as bringing a knife to a gunfight – ineffective. Although it might seem impossible, new cybersecurity technology allows companies to be protected from attacks around the clock, all without the personnel necessary to monitor.

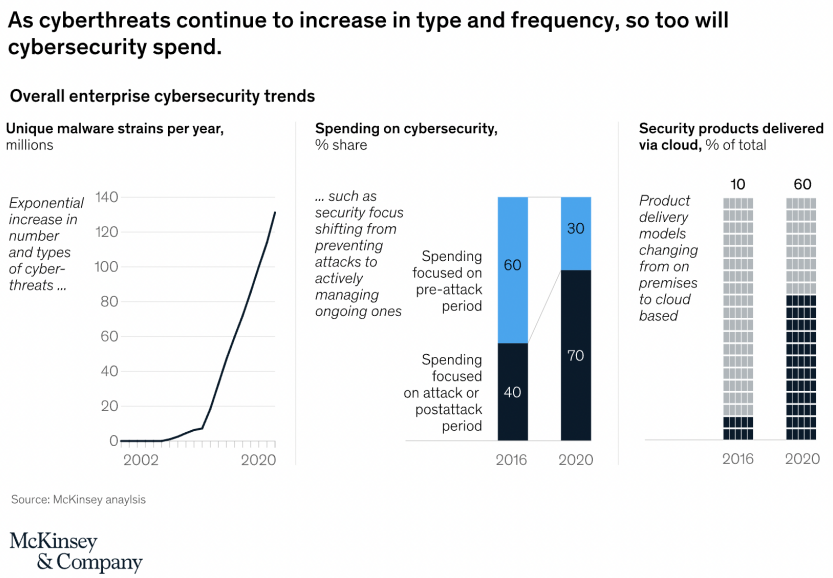
How cyber threats are changing

Businesses keep data and operational technology on the cloud, which is heavily prone to attacks. Attacks can happen on data integrity, confidentiality, and availability, with attacks on integrity having the most significant impact. Cybercriminals are leveraging techniques that can go undetected. These highly sophisticated and specialized programs can go unseen by personnel until it is too late. Cyberattacks are becoming more frequent, more refined, more expensive, and more threatening to businesses of all sizes. When cyber threats are highly advanced but cybersecurity is heavily reliant on human response, it is a recipe for failure.

Today, cyber threats are going beyond stealing data and can crumble the code-enabled infrastructure of companies and governments. New studies found that hackers can alter the vital signs of patients with connected medical devices in real time, which can cause medical staff to make inappropriate medical decisions. This is just one of many examples of how hackers can cost significant amounts of money and potentially lives when organizations are vulnerable to these attacks. Hackers are using AI and machine learning to launch attacks, so it is important to prevent and respond by using similar measures.

Some alarming statistics regarding cybersecurity and cyberattacks:

- Cybercriminals can penetrate 93% of company networks
- Businesses suffered 50% more cyberattack attempts per week in 2021 compared to 2020
- The education/research sector and government/military sectors were the hardest hit
- According to the FBI, over $43 billion has been lost since 2016 through Business Email Compromise attacks
- Half of US businesses do not have a cybersecurity risk plan in place
- 30 of the 50 biggest data breaches from 2004 to 2021 have happened since 2018



Reports from [McKinsey & Company] show that spending has shifted from preventing attacks to actively managing ongoing attacks. Funding for cybersecurity is much more effective when being spent on preventative measures rather than being reactionary.

Why we need automation in cybersecurity

There are plenty of security technologies out there, but there are not enough personnel that are trained that can implement and operate them. There is little standardization among cybersecurity techniques, which means they are heavily dependent on who is implementing them. Threat exposure to ransomware and other cyberattacks has exponentially increased, so old measures of cybersecurity are unable to keep up.

Automation in cybersecurity allows companies to provide an enhanced and structured way to identify, protect against, and respond to security threats around the clock. Hiring and training personnel to defend organizations against these advanced threats around the clock costs significantly more and leaves companies more vulnerable than allowing a machine to monitor and defend.

Automation helps small businesses and government agencies alike save significant money. [FedTech] found that “organizations that have invested in automation and orchestration have much lower costs for data breaches: $2.45 million versus over $6 million for those that did not.” Freeing up personnel also allows for more productivity in IT departments. Investing in automation can not only protect sensitive data but can save significant amounts of money.

Why Securitech180?

Securitech180 provides advanced protection for advanced threats. Once it has been installed, no maintenance is required from the companies it is defending. It works 24/7/365 to identify, defend, and resolve threats automatically every 180 seconds. When hackers use automated attacks, Securitech180 provides automatic protection.

One of the main issues previously with cybersecurity automation is the extremely expensive implementation of machinery and the cost of the talent necessary to operate and optimize them. Securitech180 fills this gap – no talent is needed. ST180 is continuously leveraging data from around the globe from global threat databases, local client environments, and ST180 subscribers' shared intelligence. This means that ST180 is constantly learning and adapting, even while you are sleeping.

ST180 is making the impossible possible. If hackers are getting more sophisticated, then so will our responses. To date, there have been 0 reported breaches amongst our subscribers. ST180 is the culmination of over 13 years in the cybersecurity industry, continuously working on new ways to keep clients safe. Schedule a demo today to see how ST180 can protect your company and save you money.