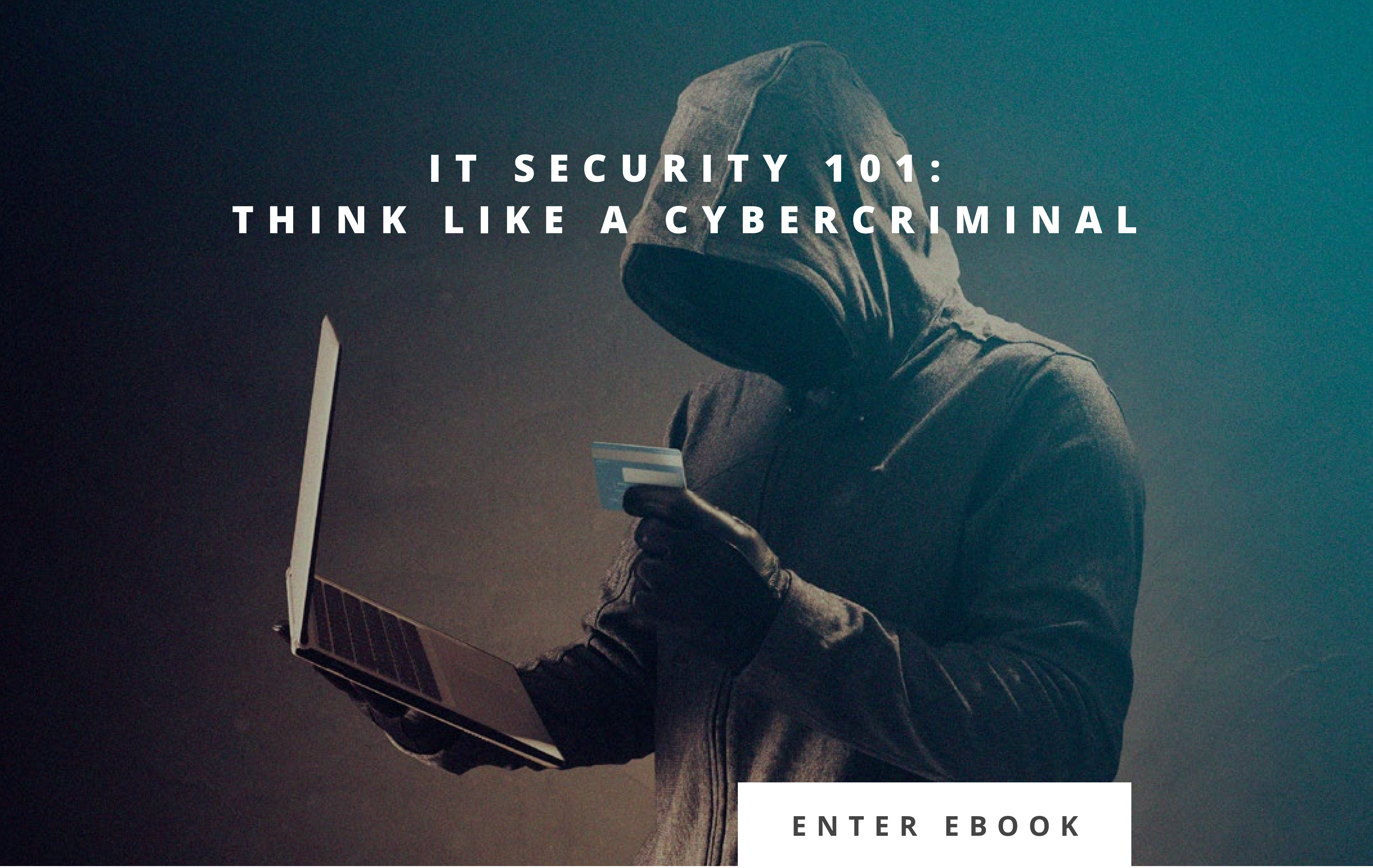
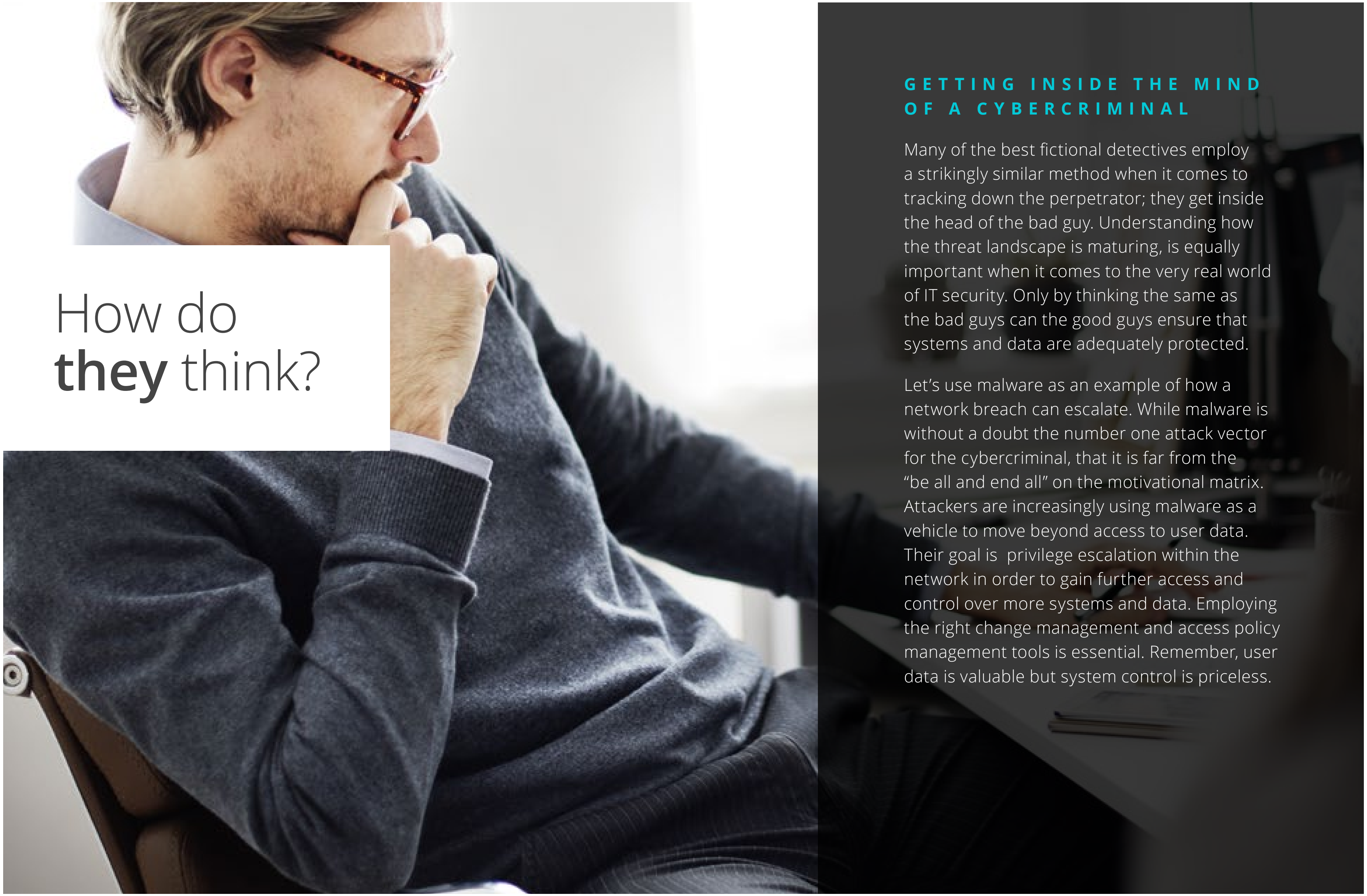
# IT SECURITY 101: THINK LIKE A CYBERCRIMINAL



ENTER EBOOK

solarwinds msp

# How do **they** think?



## GETTING INSIDE THE MIND OF A CYBERCRIMINAL

Many of the best fictional detectives employ a strikingly similar method when it comes to tracking down the perpetrator; they get inside the head of the bad guy. Understanding how the threat landscape is maturing, is equally important when it comes to the very real world of IT security. Only by thinking the same as the bad guys can the good guys ensure that systems and data are adequately protected.

Let's use malware as an example of how a network breach can escalate. While malware is without a doubt the number one attack vector for the cybercriminal, that it is far from the "be all and end all" on the motivational matrix. Attackers are increasingly using malware as a vehicle to move beyond access to user data. Their goal is  privilege escalation within the network in order to gain further access and control over more systems and data. Employing the right change management and access policy management tools is essential. Remember, user data is valuable but system control is priceless.

# Where are they headed?

## YOU NEED TO GET THERE BEFORE THEY DO

Employing this same mindset in the dark web approach to the threat landscape, you also have to start thinking about where the cybercriminals are heading when it comes to threat distribution and obfuscation. The very clear answer is encryption or rather encrypted transactions, which mean that less resources have to be spent on creating sophisticated malware code in order to evade detection. Understanding that the bad guys are using encryption in this way, exploiting the lack of visibility into SSL traffic, means that you can focus on ways of countering the tactic by distinguishing between a genuine need for SSL traffic and 'hostile' usage. Granular control over encrypted traffic is key here.

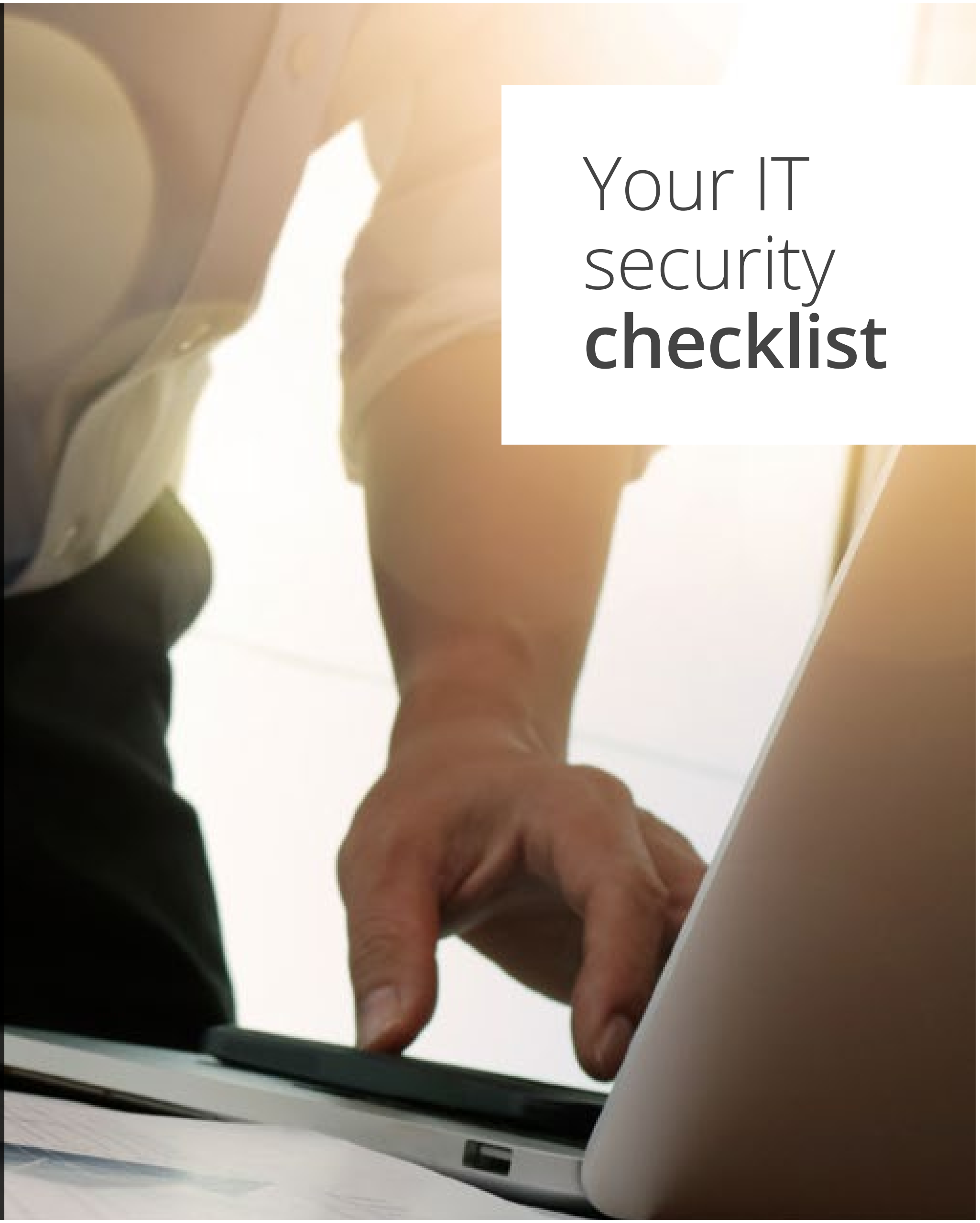
Don't think that all the emphasis is on the new. Old-school approaches like SQL injection and cross-site scripting continue to be popular; what is changing is the target. These days we are more likely to see criminals actively aiming at content management systems (CMS) and specifically CMS plug-ins. Equally, the old 'smoke and mirrors' routine continues to be used, whereby a DDoS attack or maybe a DNS poisoning threat is launched in order to tie up system resources and focus while the real target, most often a financial database, is penetrated.

# What is your **weakness?**

## DON'T MAKE IT EASY FOR THEM

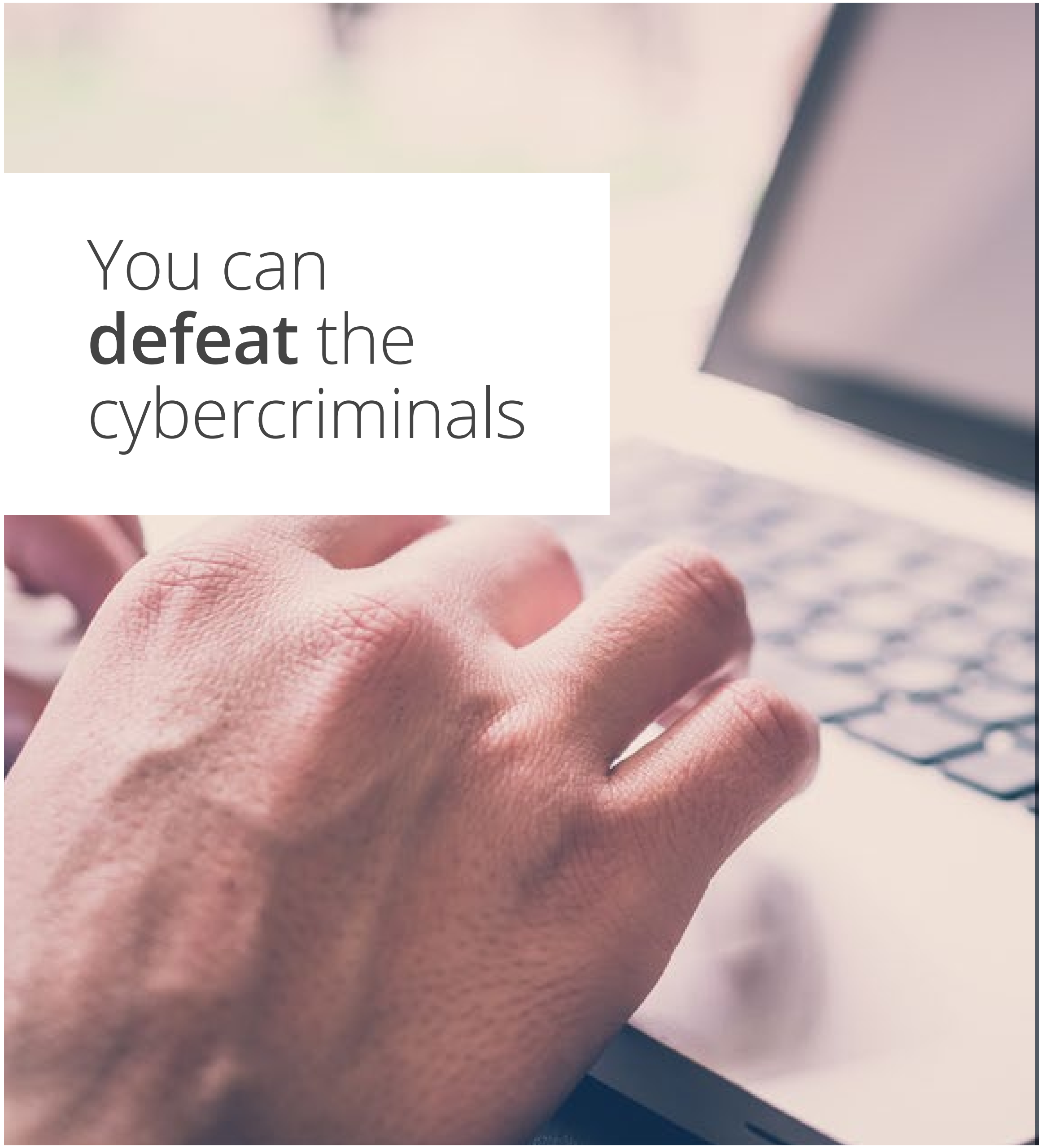
Take a sideways logic look at the threat landscape, and ask what would a cybercriminal like you to do to make life easier for them? Identifying your weaknesses in this way can be a real eye-opener for many IT admin teams. Take, for example, the small matter of maintaining network performance levels. It's at the core of what you do; it can also be at the expense of your enterprise security posture and quite literally open the door to increased breach opportunity. How so? Well, according to recent research from McAfee, one-third of IT admins admitted to disabling firewall functionality to increase performance; functionality such as deep packet inspection which can help detect malicious activity across your network traffic. Don't make things a lot easier for the bad guys just in order to make things a little easier for yourself.

# Your IT security **checklist**



## 6 KEY THINGS TO CONSIDER

1. Know your network—Use a dedicated asset tracking service, instead of manually updating unwieldy spreadsheets, to map and check devices on your network. You will save time and eliminate data entry errors too.
2. Educate your employees—Employees are often the weak link in IT security. A phishing email that's obvious to an IT admin may prove completely believable to a non-techie. Help employees understand the IT security risks.
3. Use top-quality antivirus—In the instance that someone clicks on something they shouldn't have, the use of antivirus is essential. Choose a solution that's effective and fast—and easy to deploy and centrally manage.
4. Remember patch management—Antivirus doesn't provide protection against everything. An effective patch management process and schedule protects against additional vulnerabilities like web plug-ins and add-ons.
5. Protect users online—Malicious URLs can also trick your users into compromising business—and personal—information. A web filtering solution is another line of defence that blocks websites known to be malicious.
6. Proactively monitor—Nothing you do to ensure IT security matters if you turn your back and wait for problems to come to you. So, install a monitoring solution and, most importantly, use it.



# You can **defeat** the cybercriminals

## SOME CLOSING THOUGHTS

First, get inside the head of the bad guy. Know their intentions and which tools and methods they use to reach their malicious goals. When you think the same as the cybercriminals and understand where they are heading, you are on the right path.

Next, it's worth repeating: Don't make things a lot easier for the bad guys just in order to make things a little easier for yourself. Security breaches can prove to be embarrassing, costly and damaging to any organization. However, it is possible to make your life a little less stressful by putting in place layers of IT security with asset tracking, education, antivirus, patch management, performance monitoring and web protection.

Establishing an effective IT security system is a complex undertaking made even more difficult by the threat of new and unknown cybercriminal behavior. Start by employing the 6 simple steps outlined in this eBook, and proactively address potential threats by taking the time to regularly read the IT security news feeds, educate yourself about changes to the threatscape, and act accordingly.

# About SolarWinds® MSP

SolarWinds MSP empowers MSPs of every size and scale worldwide to create highly efficient and profitable businesses that drive a measurable competitive advantage. Integrated solutions including automation, security, and network and service management—both on-premises and in the cloud, backed by actionable data insights, help MSPs get the job done easier and faster.

SolarWinds MSP helps MSPs focus on what matters most—meeting their SLAs and creating a profitable business.

solarwindsmsp.com

solarwinds msp