panda

Remote Work

|A Guide to Effective and Safe Telecommuting

pandasecurity.com/business/

/Contents

panda

|Introduction

Remote work is fast becoming one of the main benefits that a company can offer the employees that make up its staff nowadays. In the last decade, technology has evolved in such a way that almost anyone can carry out their day-to-day tasks from home.

Statistics on telework show how **this way of working has expanded 10 times faster** than other areas of the workforce. The same statistics also show that full-time employees are four times more likely to be offered the option of telecommuting than part-time employees. The data leaves no room for doubt: the number of people working remotely has increased 140% since 2005, which means that 52% of workers around the world now work from home at least once a week. What' s more, those who work from home at least once a month have **24% more chance of being happy and productive** when doing their work, while 21% of workers would give up part of their vacation time to obtain more flexible working options.

Years

2005-2020

140%

The increase in people working remotely

52%

Of workers

Work from home once a week

Alongside the human improvements, there are also great advantages for companies when it comes to implementing teleworking. One benefit is a 25% reduction in employee turnover compared to corporations that do not allow telework, thus promoting talent retention. It allows for greater diversityin terms of profiles, and better candidates when carrying out selection processes: more candidates can be reached if they are able to work remotely. Remote work is proven to directly reduce absences, allowing the worker more flexibility to manage their work-life balance. It is also important to bear in mind that costs are significantly reduced, by up to 30%, because no office infrastructure is needed.

30% Cost reduction for companies

Despite the multiple advantages that this increasingly popular way of working may provide at first glance, **a high proportion of companies are still reluctant to embrace telework for different reasons, Including security.** According to Eurostat, in Spain, only 4.3% of those in employment regularly worked from home in 2018, compared to the European average of 5.2%, and far below the rates in neighboring countries such as Germany (5%), Portugal (6.1%) and France (6.6%). In the United States, 4.3 million people regularly work from home, just 3.2% of the country' s workforce. All of this is quite some way off the experience of countries such as the Netherlands or Finland, where 14% and 13% of those in work telecommute, respectively. According to the data collected by the statistics of the Ministry of Labor, in Spain only 47 collective agreements (4% of the total) include among their clauses the conditions for applying telework to the 376,863 workers they cover (15.3% of those covered by collective agreements).

One thing is clear: Today, so-called millennials and Generation Z make up just 38% of the workforce, but by 2028, they will represent 58%. Given that they are digital natives, and that they cannot conceive of world where everyone is connected at all times and everywhere they go, the use of portable and mobile devices in the office and for work purposes will only increase. **This trend entails other consequences beyond the consumer market and affects the corporate environment as new generations enter the job market.** In this sense, the consultancy firm Markets & Markets calculates that the Bring Your Own Device (BYOD) market will reach 73.3 billion dollars by 2021, with a considerable percentage of the workforce already working remotely.

BYOD $73.3 billion by 2021

And now, getting ahead **of the statistics, suddenly the virus COVID-19 has come along, and has been able to make those who have been reluctant to adopt remote work measures in their organizations come around to teleworking,** either because they are being responsible or because they have no choice. Whatever the reason, there has been a considerable increase in the number connected devices outside office perimeters over the last few days. This will inevitably lead to difficulties for companies with no previous experience in this area and that don' t have adequate technology.

|COVID-19: hygiene and cybersecurity measures

Technical complexity and an increasingly dispersed perimeter have expanded the attack surface in recent years. For this reason, **even though perimeter security is still the first line of defense against attacks, endpoint security has become a vital issue when it comes to protecting the company.** This is because this where practically all files and sensitive information are stored. Now we must ensure that an endless array of endpoints, such as laptops, mobiles, tablets and many Internet of Things (IoT) devices are all protected. And more so in these times.

Security has become a vitally important issue for protecting companies >

And while the whole world is working to prevent the spread of coronavirus, organizations are transferring their employees to a remote work model at never before seen speeds. Because of these teleworking practices and **the connections that are being opened to facilitate communication between the company and its employees, organizations' systems are putting the technical capacity of our business fabric to the test.** Along with the tension that this implies for IT teams, network architectures and providers are now having to deal with new cybersecurity challenges.

At the same time, **cybercriminals are busy using new tactics and techniques designed to exploit this global situation of confusion and chaos,** causing critical IT security problems. Society is so impatient for up to date information about this disease that people will indiscriminately open any message, email, audio or file that they receive on their devices if it is related to coronavirus. *Blackhats* know this only too well.

The huge barrage of online messages has become the perfect camouflage for cybercriminals who want to make us download malware without our realizing. Since news started to spread regarding this disease, around 4,000 new Internet domains related to the term coronavirus have been registered, at least half of which are potentially dangerous in terms of cybersecurity. If we add to all this the thousands of social media accounts that have been registered, and the millions of messages circulating online, **we can see that any digital activity related to CoVID-19 is the perfect breeding ground for cyber criminals to spread a potential network of cyberthreats.**

Some cybercriminals try to impersonate public institutions sending out information about the virus; other cyberattacks are designed to look like a purchase order for face masks in order to trick a company into sending money straight to the cybercriminals. There have also been cases promising information about company policies regarding telework to try to steal credentials.

In fact, a campaign was seen in which messages were sent using the subject "Attention coronavirus", which installs a piece of malware via Microsoft Office to open a backdoor in the computer, which can then be used to attack the victim. Additionally, starting last Monday, mass mailings of emails have been observed, redirecting to a phishing website where a virus called Remcos RAT infects user devices. The attack is carried out using a supposed PDF file called "Security measures for Coronavirus". However, when the file is opened the malware is executed.

An APT group has also been detecting **carrying out a spear phishing campaign**, using the pandemic to spread their malware. The emails claim to contain information regarding the coronavirus, but actually contain two malicious RTF (Rich Text Format) files. If the victims opens these files, a RAT (Remote access Trojan) is launched, which is able to take screenshots, make lists of files and directories on the computer and download files among other capabilities. To weaponize this file, the attackers used RoyalRoad, a tool popular with Chinese threat actors, which allows them to create custom documents with embedded objects, which can exploit vulnerabilities in Equation Editor, the tool used to create complex equations in Word. The architecture of this malware, which is similar to a plugin, suggests that there are other modules, in addition to the payload that has been seen in this campaign.

Traditional threats, such as ransomware, remain especially active. Several campaigns have been seen that take advantage of the pandemic to infect their victims, and the notorious botnet Emotet, as well as the Trojan TrickBot, have also **exploited the situation** to reach even more systems.

/CEO

There is a high chance that a cybercriminal has stolen their identity and is sending us to a phishing page]

In addition to the cyberincidents that exploit this situation, there are certain incidents that have a direct impact on those who have been affected by the pandemic, hitting such critical infrastructure as research centers where people are working against the clock. A few days ago, in the Czech Republic, the research center at Brno University Hospital **was forced to halt its activity after a cyberattack paralyzed its systems.**

To make matters worse, many companies are sending out mass emails to all their customers, collaborators, and suppliers to inform them that, despite the coronavirus, they are still working. In this sense, although it is important to read the emails where a company CEO states that the company is taking strong measures to deal with COVID-19, it also vital to **distrust any message that includes external links.** Because, while the most likely case is that the person sending the message is who she claims to be, **There is always a strong possibility that a cybercriminal has stolen her identity and is trying to get us to visit a phishing website** or trying to get us to download a piece of malware that could lead to all our information being stolen.

These attacks are increasingly prepared to infringe our endpoint security. It is therefore vital to exercise extreme caution when receiving any email or message that sends you to a website where you have to perform some kind of action as a direct or indirect consequence of the coronavirus.

In light of so much instability, **how can you ensure that your cybersecurity is efficient and effective for all employees who are remote working?**

|Tips and best practices

is clear that if employees handle data at home, companies will not have so much control over protection measures. This could lead to an increased concern regarding the likelihood of this information being lost. This preoccupation is quite logical. A domestic environment can be far more dangerous than the office, where the software installed on the servers themselves offer security guarantees.

There is a great variety of risks. The loss of data can happen in several ways: a failure in a computer that deletes files that aren' t properly backed up, or a password being stolen, or even theft of the computer itself, which could lead to the thief ending up with confidential business information in their possession.

However, telework does not have to be synonymous with danger. Of course, for companies to allow their employees to work from home with complete peace of mind, it is first essential to have a protocol that establishes how to act in terms of security when working remotely. In this case, it›s important to remember that the perimeter that needs to be secured is wherever the employee is. This is why the analytics firm Cybersecurity Ventures estimates that global cybersecurity spending will reach $1 trillion in the next five years.

However, many of these cybersecurity investments only protect devices and servers on the corporate network, **and with BYOD it is clear that protecting the physical perimeter is no longer enough.** It is important to remember that the organization carrying out the deployment must perform an analysis of the level of security required for the information that is going to be handled on remote or mobile workstations. Implementing a remote access solution is a challenge from a security and management point of view for any organization. Classic solutions based on deploying local or on-premise systems require personnel and infrastructure capabilities that are not always available in small or medium organizations.

/Remote work scenarios:

BYOD

Bring Your Own Device.

In a BYOD SCENARIO, the end user owns the device (cellphone, tablet, laptop) where the organization' s IT administrator creates a workspace, also called a container or WorkProfile. Here, it is possible to exclusively manage security restrictions and policies within the workspace, through a special agent application (Profile Owner).

COPE

Corporate Owned Personal Enabled.

In COBO and COPE scenarios, the device (cellphone, tablet, laptop) is the property of the organization, and the IT administrator has full control of the device, implementing security policies and restrictions. In the COPE scenario, there is an agent application in the personal area, called DO (Device owner), which will configure the policies of the whole device, such as Wi-Fi, as well as restrictions in the user' s personal area, which are usually minimum and basic security restrictions. Being a COPE scenario there will also be a Workspace, with its managing agent named (profile owner) within it. The organization' s IT manager will create stricter security settings in the workspace/container, which will complement the basic settings of the user' s personal area.

COBO

Corporate Owned Business Only.

The COBO scenario is used in deployments that require greater security, where the end users don' t have a personal area, since the whole device has strong restrictions. In a COBO scenario, there is only a DO agent, and no Workspace/Container is created.

It is therefore vital that the BYOD strategy includes specific guidelines and clear criteria.

Once these criteria for using programs have been established, the IT administrator must approve which employees can add them to their personal devices. On the other hand, it is not a question of the IT department having tight control over the content of employees' devices.

The ideal situation is to reach a **balance between maintaining the security of company data and safeguarding employees' privacy,** since they will continue to use their devices for personal matters.

Overly restrictive or invasive policies are therefore counterproductive.

With BYOD it is clear that protecting the perimeter is insufficient}

Finding the balance between the security of the company and the privacy of employees >

|Key points for an appropriate policy: BYOD

/WHO recommendations:

Wash your hands often and thoroughly with an alcohol-based hand rub or wash with soap and water.

Why? Washing your hands with soap or an alcohol-based hand sanitizer kills viruses that may be on your hands.

Practice social distancing: keep at least 1 meter (3 feet) away from anyone who is coughing or sneezing.

Why? When someone coughs or sneezes, small drops of liquid are sprayed through the nose or mouth, which may contain the virus. If you are too close, you may breathe in droplets, which may contain the COVID-19 virus if the person coughing has the disease.

Avoid touching your eyes, nose and mouth.

Why? Your hands touch many surfaces and can pick up the virus. Once contaminated, your hands can transfer the virus to your eyes, nose or mouth. From there, the virus can enter your body and make you sick.

panda

/Practical measures to mitigate cyber-risks:

VPN

Connect via to the company' s internal network through a VPN, avoiding the use of public or third-party Wi-Fi networks.

Continuous awareness training for employees is, of course, a fundamental element in this kind of crisis.

Just like when you' re in the office, only access websites that use HTTPS, guaranteeing a secure connection. It is also important to ensure that the passwords you use to access your accounts are robust and private.

Practice respiratory hygiene: Make sure that you and the people around you follow good respiratory hygiene. This means covering your mouth and nose with the corner of your elbow or with a tissue when you cough or sneeze. Then discard the used tissue immediately.

Why? Droplets spread the virus. Following good respiratory hygiene helps protect the people around you against viruses such as the common cold, the flu, and COVID-19.

If you have a fever, a cough, and shortness of breath, seek medical attention immediately. Stay at home if you feel unwell. If you have a fever, cough, and shortness of breath, seek medical attention and call ahead. Follow the instructions provided by your local health authority.

Why? National and local authorities will have the most up-to-date information on the situation in your area. Calling ahead will allow your healthcare provider to quickly direct you to the right health center. This will also protect you and help prevent the spread of viruses and other infections.

Stay informed about the latest developments regarding COVID-19. Follow the advice of your healthcare provider, your national and local public health authority, or your employer on how to protect yourself and others from COVID-19.

Why? National and local authorities will have the most up-to-date information on whether COVID-19 is spreading in your area. They are best suited to advise on what people in your area should do to protect themselves.

Cybersecurity solutions must be advanced and up to date, considering using endpoint detection and response programs to remotely limit the impact of a compromised device. Advanced security solutions must include full EPP and/or EDR capabilities that monitor activity at the endpoint and offer continuous, comprehensive and detailed visibility. This monitoring is the basis of our Zero-Trust App Service, which is the only one of its kind of the market.

Companies should review, evaluate and update, where necessary, their incident response and business continuity plans. Our incident response services often begin by deploying our agents on clients' endpoints. These agents provide visibility of indicators of attackers on your network and about assets that have been compromised. Using this, a personalized remediation plan is established, providing a strategy to eradicate attackers from the network.

Regularly make backups to ensure that no information is lost in the event of an incident". Even in the worst-case scenario, you will always have the possibility to recover the data, which is the lifeblood of many companies.

/ Other recommendations >

- ✓ Enable **communications channels** to hold meetings **online.**
- ✓ **Close** all connections that are not **strictly necessary.**
- ✓ Avoid **“Split-Tunneling”** options on insecure computers or those that do not fulfill safety measures.
- ✓ Prevent mechanisms that allow computers to be restarted remotely and accessed through established channels once they have been restarted.
- ✓ Carry out **scheduled (exhaustive) antivirus scans** on workstations, even if computers are not restarted.
- ✓ Restrict mounting the **organism’ s mapped units** to insecure remote computers.
- ✓ **Close** all applications when not in use.
- ✓ Apply **updates scheduled in the organization;** to do so it may be necessary to restart computers periodically.
- ✓ Have **lists** of people, IP addresses, phones, and corporate and alternative email addresses related to having **remote access to the system.**
- ✓ Have easily accessible **phone lists** to communicate with people from different areas.
- ✓ Have monitoring services activated with defined alerts.
- ✓ Revise or increase supervision of **units where information is exchanged.**
- ✓ Have an updated **list of people** who can remotely access the organization’ s computers, with their IP address and means of connection.
- ✓ Check whether cybersecurity solutions scan **USB devices** connected to remote computers or if USB access is blocked on those computers.
- ✓ Revise **logs and audits** of remote connections.

*Points shared with the measures published by the CCN-CERT in abstract, entitles: “Security Measures for Remote Access”.

|Monitoring solutions for the endpoint

Given the nature of the security risks that remote working can entail, organizations should implement solutions that apply constant, real-time monitoring of the corporate network and all its access elements.

At the moment, cybersecurity teams are taking on a vast amount of work, especially those responsible for computer security. And this high workload means that real threats may be sidelined, and could be overlooked, putting the whole company' s security at risk.

The remote work taken on these days means that security must be addressed with an endpoint detection and response service capable of accurately classifying all the organization' s applications and blocking advanced threats, targeted attacks and zero-days that other traditional solutions are not able to detect.

Let' s not forget that, even though BYOD presents new security risks, the opportunities it offers companies and employees are much greater if it is implemented with the necessary precautionary measures.

Risk prevention based on appropriate policies and real-time monitoring solutions that can reach all devices is the best way to harness the full potential of remote work.

|Passwords and encryption

Passwords are another key element to ensure that teleworking is secure. If the password an employee uses to access the company network is stolen, it could cause a critical security incident, as it would give cybercriminals access to a vast quantity of information.

Beyond the password for the corporate server, employees working from home should bear in mind that, when using cloud services and tools, it is important to follow certain tips to create strong and reliable passwords: **Do no repeat passwords; change it every so often; and use a password manager to prevent password theft.**

However, passwords are not always enough. Although a remote desktop is useful to avoid storing **corporate information** on your home computer, sometimes saving something on the computer itself is unavoidable.

In this case, as well as using strong passwords, it is **important to encrypt any confidential information.** This way, the loss (or theft) of a laptop doesn' t mean the theft of information. Encrypting specific files through the operating system or encrypting the whole hard drive can stop the risk.

✓ Do not repeat passwords

✓ Change your password from time to time

|Conclusions

What should you ask of a cybersecurity solution to protect your device when remote working?

1-Preventively blocking known and unknown threats

To avoid security breaches, there needs to be a change: to shift from detecting and responding to incidents after they occur, to preventing these breaches in the first place. Endpoints must be protected against known, unknown and zero-day threats that are sent to computers via malware. These computers may be online or offline, on-premise or off-site, or connected to the company network or a different network. A key step to achieve this is incorporating cloud-based and local threat analysis to detect and avoid unknown threats.

2-Have no negative impact on user productivity

An advanced endpoint security solution must allow end users to carry out their normal work and use mobile and cloud-based technologies without having to worry about infection. They must be able to focus on their responsibilities instead of having to worry about security patches and updates. Lastly, they should be able to be confident that they are protected against malware or exploits that run without their realizing and that may endanger the security of their systems.

It must allow users to carry out their normal work and use cloud-based and mobile technologies without worrying about infection[

panda

3-Automatically convert threat intelligence into prevention

Threat intelligence gained from dealing with new attacks should allow endpoint agents to instantly prevent known malware, identify and block unknown malware, and prevent both from infecting endpoints. Likewise, threat data must be collected within the organization: network, cloud and endpoint. Automation should be used to correlate data, recognize indicators of compromise, create protections, and expand them across the organization.

4-Protect all applications

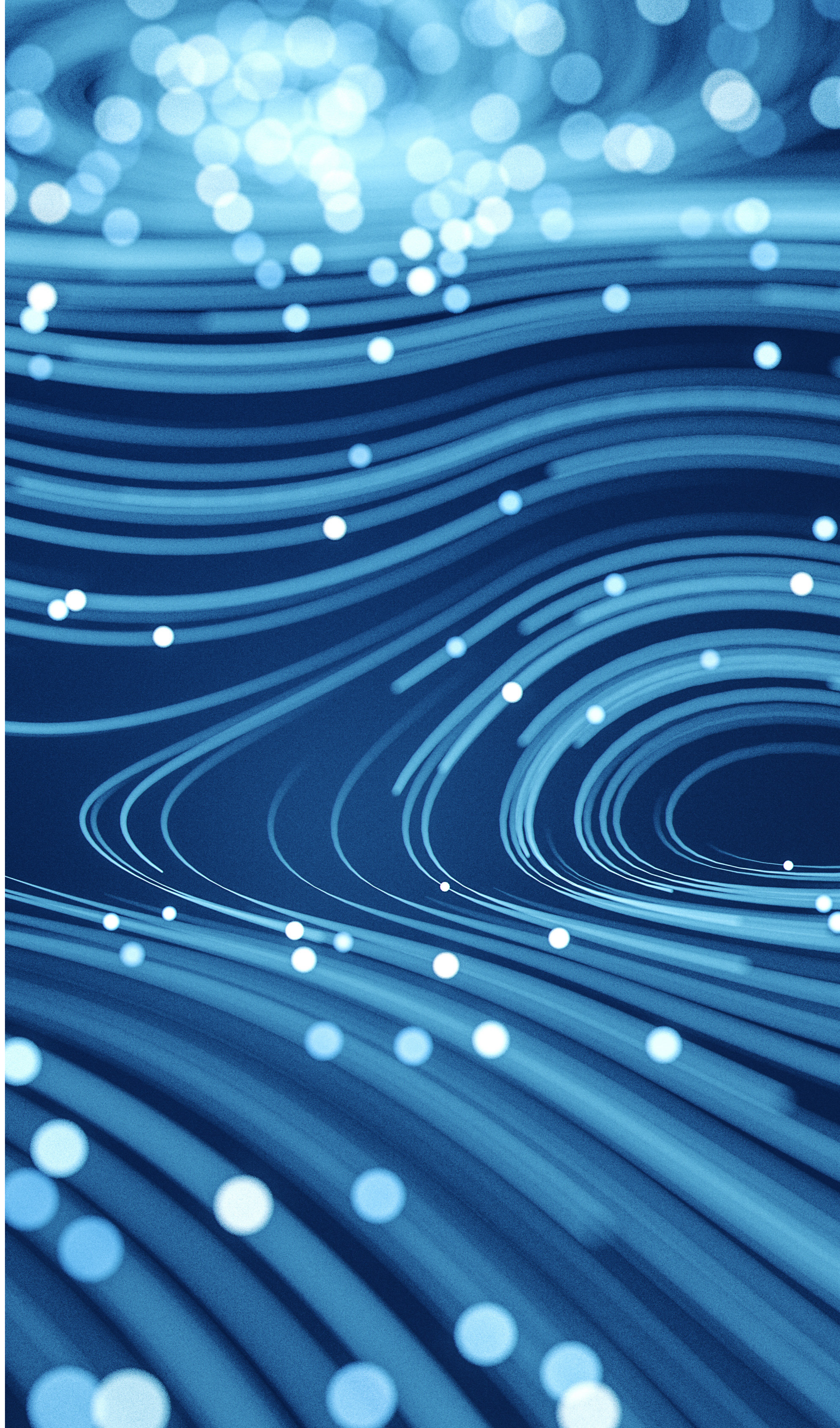
Errors or bugs in applications provide cybercriminals with an expansive attack surface that traditional antivirus cannot protect. An organization' s security infrastructure should be able to offer full exploit protection for all applications, including third-party and proprietary applications. It should also be able to streamline the process of approving new applications as they are installed in the environment by issuing quick security responses.

5-Stop security from affecting system performance

Security solutions should not put a strain on system resources, such as RAM, CPU, or disk storage space. Endpoint protection should be lightweight enough not to require a lot of system resources or it will hinder system performance and degrade user experience.

6-Protect previous systems

Organizations may not always install system updates and security patches as soon as they become available. This may be because doing so would interfere with, decrease, or eliminate critical operational capabilities. It may also be the case that patches are not available for legacy systems and older programs that have reached EoL. A complete endpoint security solution must be able to support systems where patches cannot be installed, thus stopping the exploitation of known and unknown vulnerabilities in programs, regardless of whether security patches are available or if they are applied.



7-Be prepared for use in business environments
company implements its IT resources, expanding to as many endpoints as necessary, and supporting deployments that cover geographically dispersed environments. It must also be flexible when providing comprehensive protection, while continuing to support business needs without unduly restricting activity. This flexibility is vital, since the needs of one part of an organization may be completely different from those of another. What' s more, the solution must be easily manageable for the same group that manages security in other parts of the organization. It must be designed with business management in mind, without adding extra operational burdens.

8-Provide independent verification of sector regulatory compliance requirements
Regulatory compliance often requires organizations within a given jurisdiction to implement antivirus programs to protect their endpoints. To proactively protect endpoints while still meeting regulatory compliance requirements, such as the latest data protection regulations (GDPR), endpoint security providers that replace existing antivirus solutions should be able to provide third-party validation to help clients achieve or maintain compliance.

9-Provide independent verification as an antivirus replacement
Any security product intended to replace the existing antivirus should ideally be verified and validated by an independent third party for performance. Independent reviews provide an essential control element that organizations seeking to replace antivirus cannot do without.

10-Be recognized by the market and industry analysts
Any company that wants to implement an advanced cybersecurity solution must ensure that this solution has been endorsed by an accredited endpoint security analyst or company This way, you can rest assured that the solution and its vendor meet standard viability requirements as an endpoint security provider.

panda

Get in touch with us]

pandasecurity.com/business/

More info at: www.pandasecurity.com/business/