Acronis

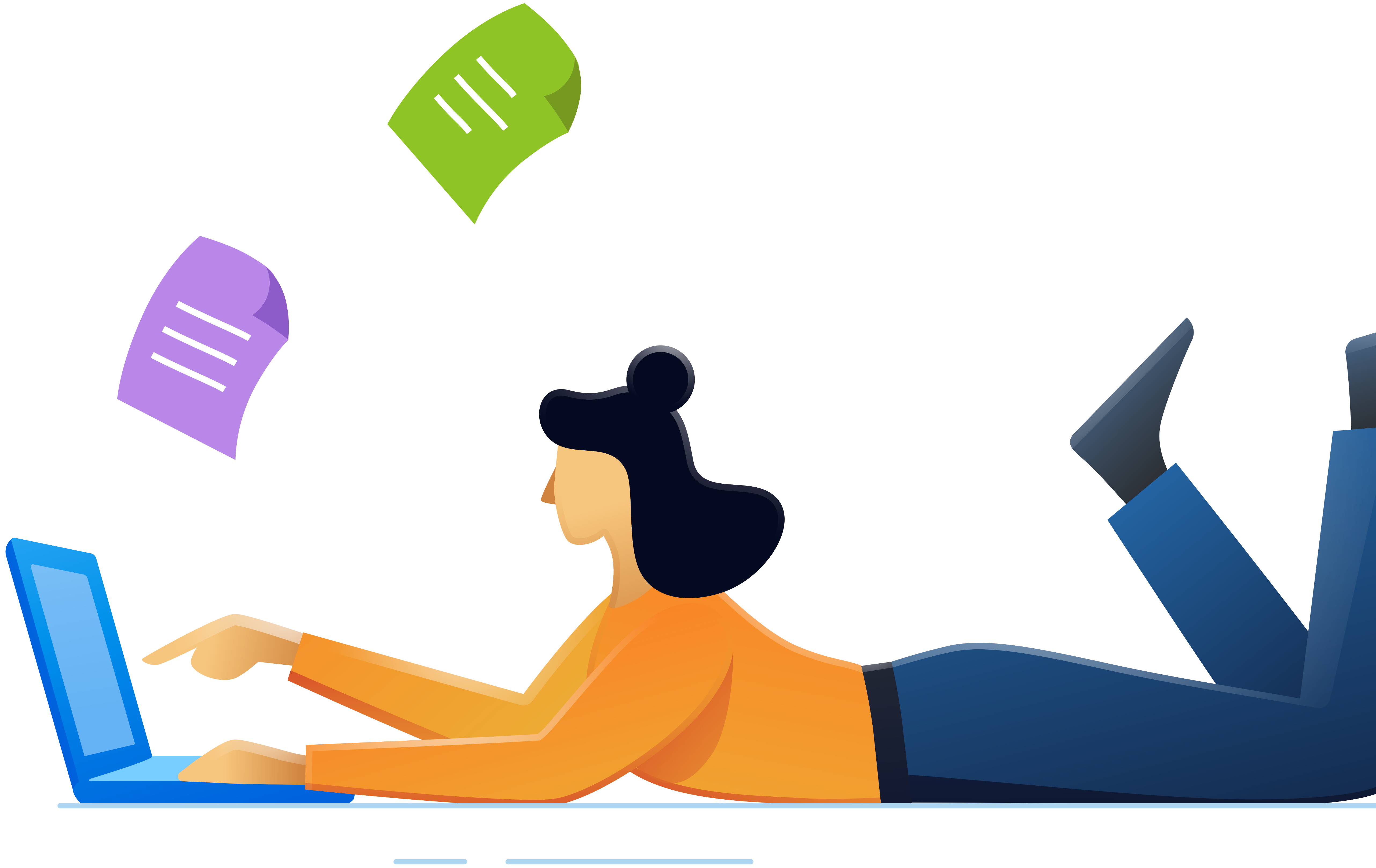
Planning and Optimizing WFH Networks for Security and Remote Management

While many of us are looking forward to a return to normalcy, remote work is a trend that is unlikely to change any time soon.

Why resist a shift that has led to increased productivity and a deeper talent pool? There are benefits to office work, but most employees appreciate the flexible hours, reduced commute, extra family time, and the ability to live and work anywhere.

There is a catch, though. Anywhere is a lot of territory for IT security professionals to protect. For those who view cybersecurity as a castle, with walls around it and threats looming on all sides, imagine what would happen if citizens could simply walk across the drawbridge – every one of them potentially holding a key to unlock the front gate.

While work-from-home (WFH) security might feel a bit like that, protecting remote employees is relatively simple with the right policies, training, and technology solutions. In this e-book, you'll learn how IT departments and service providers can build long-term plans to secure extended networks that stretch far beyond the office and directly into employees' homes. That includes best practices for discovery and inventory, onboarding and offboarding, forensics in remote environments, and other methods for keeping productivity levels high without sacrificing security.



Changing the IT landscape for remote work

For years, security professionals have known that the security perimeter they're responsible for is constantly expanding. Most companies no longer expect to shelter their employees within a constrained corporate network. Instead, the security perimeter extends wherever individuals go, and is based around their roles, the hardware and networking they use, and the software solutions they need to be productive and safe.

As the WFH trend keeps accelerating, more employees are bringing their own devices to work. Security stances have shifted in response. Newer approaches emphasize authorization and authentication. Zero-trust, role-based access, and privileged-access frameworks also create a bend-not-break approach to cyberdefense.

Of course, not everyone has adopted the bring-your-own-device (BYOD) approach. Some teams still prefer that their employees remotely connect to physical devices in the office using a VPN or remote-access software. Others try to provision virtual machines (VMs) from centrally controlled architecture that can be closely monitored. This e-book focuses on situations where employees connect from their own home networks using either their own devices or ones provided to them. Cyber protection in these scenarios includes managing, updating, maintaining, monitoring, and securing remote network assets in employees' homes.

Yet, don't forget that homes have become as complex in recent years as offices were a decade ago. BYOD has expanded to bring-your-own-WiFi, bring-your-own-docking-station, your own laptop, router, printer, smartphone and tablet – you can bring your entire home IT environment.

Additionally, Internet of Things (IoT) devices have become commonplace. IT security has to account for the risks that smart speakers, thermostats, home security systems, doorbell cameras, and even refrigerators can introduce. And even after issuing clear instructions to segment home networks, IT's endpoint security landscape has never been more complex.

At the highest level, the goal is to provide employees an engaging, productive WFH experience that supports the organization's mission and maintains high security standards. However, there are considerable challenges to this; for one, firms that try to lock down security too tightly soon notice that employees find workarounds or become frustrated by roadblocks. But on the other hand, security practices that are too loose are always moments away from becoming another gruesome statistic. Some of the basic steps to create a secure WFH environment without impacting productivity include requiring multi-factor authentication (MFA) and connecting via VPN – although that requires additional time configuring WiFi routers whenever employees are on-boarded or off-boarded.

To find the right balance, many organizations turn to professional services automation (PSA) vendors such as ServiceNow, ManageEngine, or BMC Remedy. Modern organizations increasingly rely on third-party ecosystems to operate at a high level. Keep in mind, however, that vetting vendors thoroughly is an important step.

While third-party providers are increasingly common points of attack, people are often the easiest targets for malicious actors. This is the case even though most professionals who work remotely have gone through enough training to be aware of several cybersecurity basics. (Avoid coffee shops and airport networks! Be cautious clicking on links in emails with a lot of exclamation points!)

Still, the threat landscape is evolving much faster than most people can keep up with while remaining productive in their roles. And people are capable of making basic mistakes, like reusing passwords between personal and company accounts – despite being aware of the risks. In fact, this may have been a contributing factor to an ongoing hack of the United Nations through credentials that were sold on the dark web.

In any case, with the right policies, training, and technologies, it's possible to reduce the chances of a cyberattack and minimize the damage done if one does occur.

Discovery and inventory from a wide angle

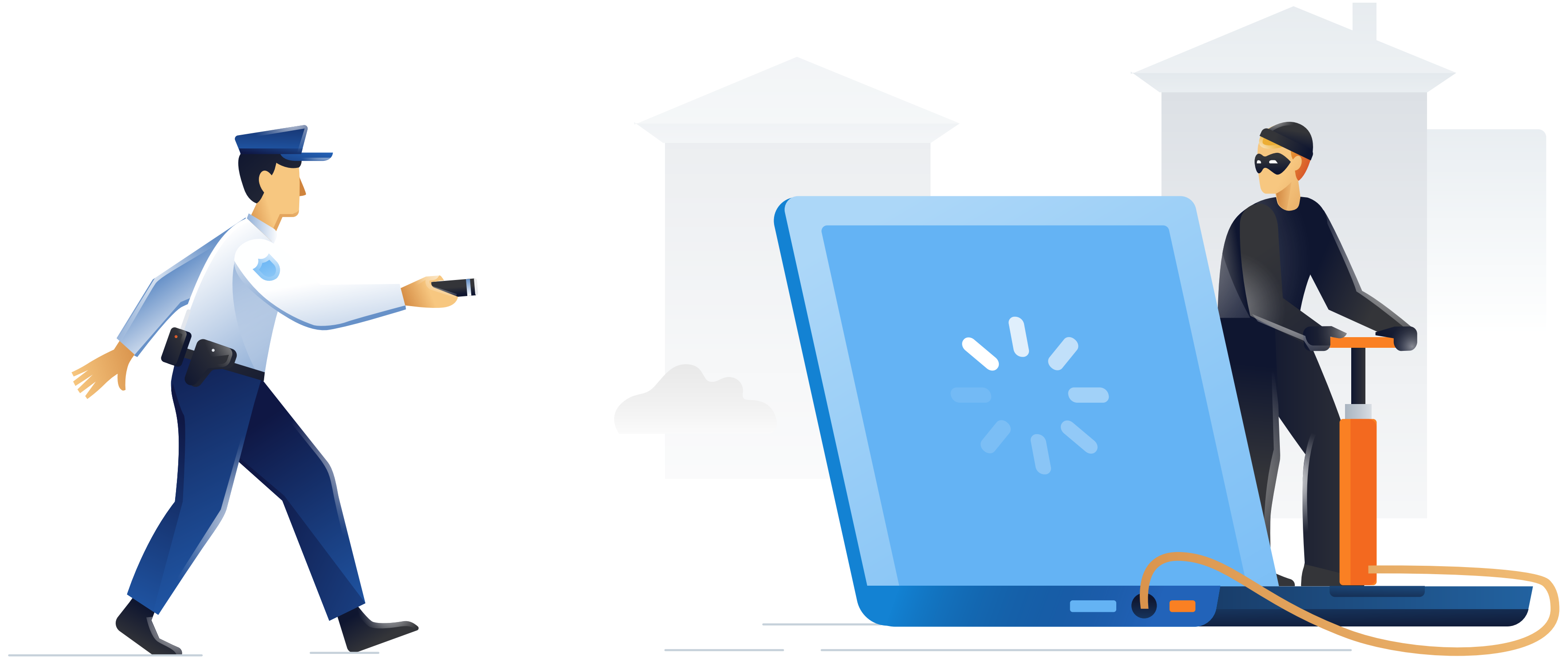
Now that cybercrime is a multi-billion-dollar industry, it seems like threats can arise from any angle. In fact, 86% of organizations were affected by a successful cyberattack last year. And without proper processes for discovery and inventory, any new device, application, server, or vendor is another potential point of weakness. After all, a remote worker is usually seen as an easier target than a corporate network.

There are monitoring solutions available that can scan and audit home networks, which can be an important step in the employee onboarding process. But that doesn't fully protect the company from threats that may emerge through employees' devices.

When IT teams could procure, deploy, and set up each application and piece of equipment within the office, security was easier. Now, imagine an IT team that has full visibility into each remote employee's home network environment. Some assets, such as a laptops, docking stations, or smartphones, might be company owned. Other assets, such as modems and routers, may be provided by a managed service provider (MSP). The rest are likely employee owned, including tablets and IoT devices. Keeping the core business secure means ensuring employees' home networks are properly configured and that every relevant piece of hardware and software is accounted for.

Your team should have a process in place for each type of asset. Typically, that process should include determining who is responsible for training, troubleshooting, support, patching, and pushing updates to ensure remote devices are harder to exploit – regardless of whether the company, a third-party provider, or the employee provides the asset.

Many companies turn to service providers to handle core security and business continuity functions, including data backup, disaster recovery (DR), and device failure procedures. Make sure to evaluate MSPs carefully and ensure they have established high security standards. If you go that route, it might also make sense to set clear guidelines for data segmentation between your business and other MSP clients. Recent CISA guidelines advise applying a zero-trust framework to MSPs that are involved in managing business networks.



Remote IT onboarding and offboarding

When it comes to employees, partners, vendors, or any other entity that needs network access, the biggest concerns come with onboarding and offboarding. Each time a remote employee or third-party vendor is brought on board or leaves, the attack surface for your organization grows or shrinks – along with the scope of endpoint protection. Of course, the first step in onboarding includes hiring, vetting, and training employees, as well as onboarding new vendors and partners.

It's important to develop processes, documentation, and training regarding how equipment is issued, set up, tracked, replaced, or returned. Even a WiFi-protected setup (WPS) can be a point of attack through a remote employee's home network, so disabling WPS is a best practice. Make sure the router's firmware is up to date, or implement software firewalls and limit access others have to the router. Typically, employees should set up a separate network segment for work, which can only be accessed by approved devices.

It's imperative that a company give clear guidance on VPN usage, anti-malware, and hard-drive encryption guidelines for personal devices being used to store or process company data. Also, make sure the virtual network is properly configured to handle the volume of traffic you expect at peak hours. While onboarding, your team should consider requesting a security audit of home networks.

Well-defined policies are tremendously helpful in ensuring your team has clear expectations. It's also a good idea to set guidelines for pushing patches and updates, and for where employees and partners can find support and help-desk resources. If a device goes missing, your team should be prepared to remotely wipe it. Introduce processes for managing and offboarding vendors, including when to shut off access if a vendor's contract ends. Also consider guidance regarding use of tools like RDP (Microsoft's remote desktop protocol) for remotely connecting to devices, since there is always a risk of reverse RDP exploits.

While onboarding and offboarding are vulnerable processes, keep in mind that ongoing IT support that extends into employee networks adds complexity on a daily basis – and that's where people become more inclined to look for shortcuts and workarounds. Yet with the right tools and processes, those everyday risks can be diminished.

Forensics in remote IT environments

What if you took it as a given that employee devices are likely to be compromised at some point? According to the National Institute of Standards and Technology (NIST), that should be the expectation. When cybersecurity is extended and flexible, IT security's role is to minimize any damage by providing access privileges appropriate for remote employees.

In a modern IT environment, assessing where an attack (or other issue) originated can be a real challenge. If you've followed the guidelines outlined above, you'll be in better shape to view the full scope of the extended network, and you'll have a complete asset inventory as a starting point.

Keep in mind that a good strategy must include training for insider threats, as they can often be the most damaging. Be sure to have a data-loss-prevention (DLP) plan in place in the event of an insider attack, as well as remote attacks via vendors, service providers, partners and suppliers.

As mentioned earlier, a compromised employee device is almost inevitable. This is why a least-privilege access model is recommended: Make sure employees only have access to applications, devices, software, network segments, etc. that their roles demand.

Depending on the sophistication of the remote access tools you use, it might be possible to limit employee and vendor access to specific IP addresses or set time-of-day windows where devices, networks, or applications can be accessed. This simplifies remote environment monitoring dramatically: If a profile associated with a vendor is attempting to connect in the middle of the night from a fjord in Greenland, it's easier to identify and shut down the activity, if needed.

Keep in mind that detailed audit logging and records are important in forensics – not just for regulatory compliance purposes, but also to follow the tracks of a potential intruder. Knowing where a malicious actor has been can help identify weaknesses in system security and ensure the intruder has been fully locked out. Note that there is a balance to be struck between recording so much that the data becomes noise, versus recording so little that something gets missed.

Finally, make sure to have an incident response plan in place whenever there is a cyberthreat, no matter how minor or unsuccessful it might be. Depending on your industry and organization's own reporting requirements, there are steps that can be automated, regardless of where the incident originated.

ABOUT ACRONIS

Acronis unifies data protection and cybersecurity to deliver integrated, automated cyber protection that solves the safety, accessibility, privacy, authenticity, and security (SAPAS) challenges of the modern digital world. With flexible deployment models that fit the demands of service providers and IT professionals, Acronis provides superior cyber protection for data, applications, and systems with innovative next-generation antivirus, backup, disaster recovery, and endpoint protection management solutions powered by AI. With advanced anti-malware powered by cutting-edge machine intelligence and blockchain based data authentication technologies, Acronis protects any environment – from cloud to hybrid to on premises – at a low and predictable cost.

Founded in Singapore in 2003 and incorporated in Switzerland in 2008, Acronis now has more than 1,700 employees in 34 locations in 19 countries. Its solutions are trusted by more than 5.5 million home users and 500,000 companies, and top-tier professional sports teams. Acronis products are available through over 50,000 partners and service providers in over 150 countries and 25 languages. For more information, visit www.acronis.com

Acronis

Copyright © 2002-2021 Acronis International GmbH. All rights reserved. Acronis and the Acronis logo are trademarks of Acronis International GmbH in the United States and/or other countries. All other trademarks or registered trademarks are the property of their respective owners. Technical changes and Differences from the illustrations are reserved; errors are excepted. 2021-11