Walking into Wearable Threats

Assessing business readiness for wearable devices

November 2014

TREND MICRO

Executive summary

The next phase of the Bring Your Own Device (BYOD) trend is underway, with wearable technology, such as smartwatches and health and fitness trackers, now being brought into the majority of UK organisations involved in this study.

As this report reveals, however, the influx is not only from employees bringing their own devices into work. A quarter of respondents said their organisation has deployed, or is deploying, wearables to boost productivity, enhance staff wellbeing or comply with business insurance policies.

With new devices in the workplace come new risks to corporate security. Trend Micro has partnered with Vanson Bourne to explore how prepared UK organisations are for this influx of new devices and the potential risks to IT security.

As this study shows, these threats include theft of highly personal information about employees – such as their health status – as well as business IP. These threats will only increase as wearables become more sophisticated and more of them enter the enterprise.

As with other smart mobile devices in the workplace, the challenge for businesses is to weigh up the potential benefits of wearables with their potential risks, and then act to maximise the former and minimise the latter.

This report explores these findings in more detail and provides some advice for businesses to help them prepare for the introduction of new personal devices.

This entails taking an approach that encompasses people, processes and technology. In particular, security policies should be adapted to account for wearables, and relevant technologies, such as endpoint security, vulnerability protection, data loss prevention (DLP) and encryption, should be implemented.

The rise of wearables in the workplace

If you're not wearing IT yet, chances are you will be in the near future. The rise of the wearable technology category, which includes smartwatches, fitness trackers and smart glasses, seems inexorable. Myriad market and analyst reports point towards continuing growth, both globally and in the UK:

- Futuresource Consulting says global wearable device shipments increased 40% to 12.7 million units in the third quarter of 2014, compared with the same quarter last year
- Juniper Research projects that 101.7 million smartwatches will be in use worldwide by 2019
- The Centre for Retail Research predicts that the value of the wearable market in the UK will total £313.6 million by the end of 2014

Trend Micro's study reveals growth in the number of UK employees bringing wearables to work. Over two-thirds of respondents at UK enterprises (69%) are seeing staff bring wearable devices into the workplace, and 91 per cent expect the number of employees doing so to increase in the next 12 months. None say it will decrease, which is understandable given its 'early adoption' status.

Raimund Genes, CTO of Trend Micro, said: "We're seeing the next phase of two related trends, Bring Your Own Device (BYOD) and consumerisation of IT. As was the case with smartphones in their early days, we're already seeing employees bring their own wearables into the workplace. We expect this will accelerate when the Apple Watch launches in Spring 2015."

Definition of wearables

By 'wearables' we mean smart electronic devices that people wear on or about their body as they go about their day. The purpose of these devices is usually measuring bodily functions or serving as an output of other devices. These two functions can overlap to provide an augmented or more rounded experience of the user's everyday reality as it happens.

There are three very broad categories that we can use to describe wearable devices:

- 'IN' devices. These are sensors that capture a user's data at all moments. Here, we find fitness sensors that measure the user's steps, distance, effort, calories, heartbeat, GPS coordinates etc. These devices usually store the information locally in the device, and then upload that data by synchronising with mobile phones or PCs and to the user's cloud account for historical logging and statistical display. Future devices that we have not yet seen are medical devices that could monitor health parameters, such as body temperature, oxygen in blood, etc.

- 'OUT' devices. These are devices that output data coming from other devices, usually mobile phones. Here, we find smartwatches and the like, which are able to display texts and any application data for ease of use. Data displayed usually comes from internet sources by means of the intermediate device.

- 'IN and OUT' devices. These are devices that capture data and use filters to display it differently. In here we find display devices such as Google Glass that have cameras that capture reality, but also feed data to the user by means of retina projection. These devices have the ability to enhance the user experience by filling in information on top of reality. Simpler devices also act as 'IN and OUT' by both gathering user data (steps taken, distance covered etc.) and streaming data from their companion mobile phone.

While these are distinct categories, the tendency is for devices to coalesce into IN and OUT because makers want to add as much value as possible. One example would be devices that record fitness information but also notify users of text messages, events, and other information from mobile devices.

From a security standpoint, currently it's hard to say which category is more secure than the other. This is because the difference among the categories is primarily about attack vectors. The more things a device can do, the most possibilities exist for attackers.

For example, a device's connectivity capabilities, ability to add additional software (could be malicious), number of applications that could be exploited on that device, what data it holds and can be transferred to / from it etc. In this case,

IN and OUT devices have a larger attack surface, and the most potential for attacks. However, this doesn't mean that they are more insecure. Only time – and attacks by cybercriminals – will tell. Also the ecosystem they work within and the controls in place will increase / decrease their chance of attack / exploit.

Employers embracing wearables

Growth in wearables is expected in consumer and business markets alike, with implications for the UK workplace.

Analysts at Gartner predict that between 2018 and 2020, a quarter of smart wristbands and other fitness monitors will be sold through non-retail channels, and "offered increasingly by gyms, wellness providers, insurance providers, weight loss clinics or employers."

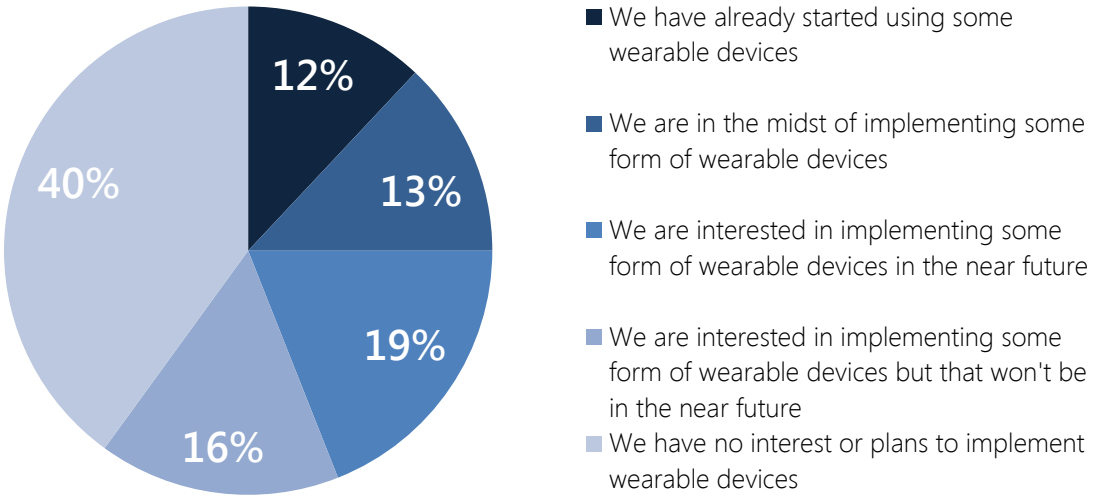
Trend Micro's research reveals that the majority (61%) of UK businesses involved in the study actively encourage the use of wearable technology in the office (39% discourage its use). A similar proportion (60%) say they have either implemented, have started to implement, or are interested in implementing wearables in the future. To break this total down:

- One quarter (25%) have implemented wearables or are in the midst of doing so
- 19% are interested in the near future
- 16% are interested in the distant future

The minority of respondents (40%) say their organisation currently has no plans regarding deploying wearables.

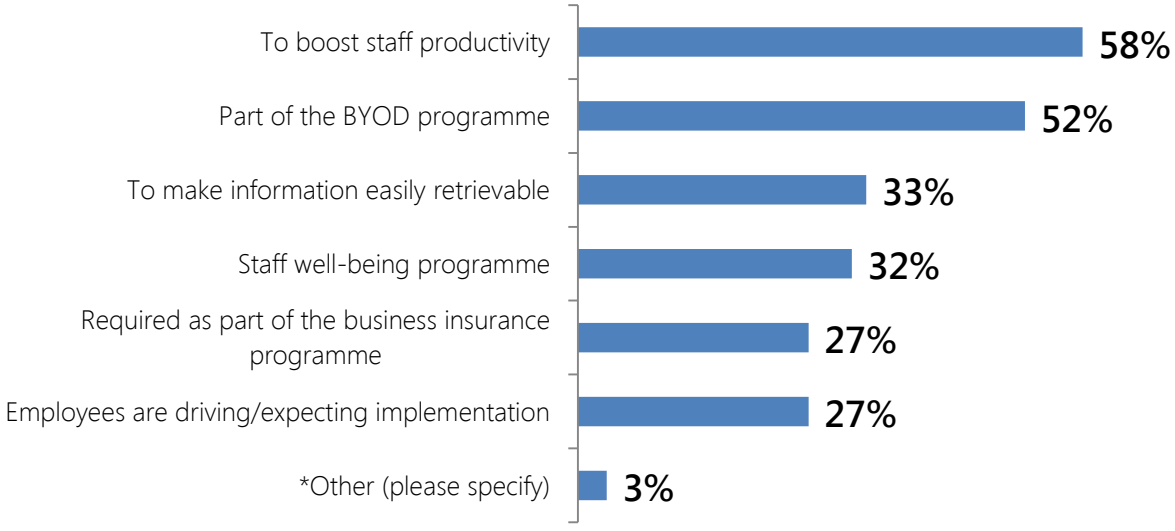
Of the same group of respondents, smartwatches (such as Pebble, Samsung Gear, Sony SmartWatch) are the most popular devices for deployment or potential deployment – favoured by 65 per cent – followed by activity trackers (such as Fitbit, Jawbone UP, Nike+ FuelBand), on 58 per cent, and smart glasses (such as Google Glass) on 40 per cent.

Which of the following statements best describes your company's position on the use of wearables within the organisation?



Of the organisations that are either rolling out wearables or intend to, increased productivity is the most popular reason to do so (58%). This is followed by incorporating wearables in a broader BYOD programme (52%), a staff wellbeing programme (32%), or a business insurance programme (27%).

Why has/ is/ would your organisation implemented/ implementing/ implement wearable devices? (multiple choice)



Cloud services company, Appirio, has introduced *CloudFit*, a voluntary wearable device programme, as part of a company-wide initiative to improve staff well-being. Tim Medforth, SVP at Appirio, said: "Technology is at the heart of everything we do at Appirio and since incorporating CloudFit we have witnessed the growth of a healthy competitive and collaborative environment.

"By using a Fitbit device and our voluntary CloudFit program, staff are not only getting healthier, but also working better as a team. An unintended benefit has been the reduction in our health insurance costs. But it's so much more than the insurance benefits – it's about being a great place to work and creating a productive, engaging and fun environment. Volunteer participation has gone from 10% to 50%. All employees choose what data they want to share; none of which is shared with 3rd parties.

"We see anything that raises awareness to an individuals' level of activity as a good thing. We've seen changes in individual's behaviour; rather than taking the lift, people take the stairs, rather than sitting down for a conference call they stand up and walk around. We also see great benefits in people collaborating in terms of the way they form teams – last week we had a team in London competing with a team in Indianapolis in terms of the distance walked over the course of a week. It's a bit of fun that ultimately leads to health and productivity benefits."

The corporate connection conundrum

It's inevitable, though, that at least some of these wearables operating in a work environment will connect to corporate data, just as smartphones do – personal or corporate. Indeed, three-quarters (76%) of UK respondents said their organisation allows staff to access corporate data (e.g. work emails) on their personal mobile devices in general. As wearables grow in functionality and sophistication, there's every reason to think that they too will access the corporate network in some way.

It's a truism that any new device entering the corporate environment presents a security risk, so an organisation needs to think about how they will manage the device to minimise that risk. The track record of businesses mitigating security risks from the BYOD trend shows that the earlier measures are implemented, the better. As this report uncovers, though, even now almost one in ten (9%) of respondents say their enterprise-sized organisation has no security protocols or guidelines for personal devices that connect to corporate data.

According to Vinod Bange, partner and data protection specialist at international law firm Taylor Wessing, "A smartwatch tracking health metrics like blood pressure and heart rate during a normal day, or perhaps during exercise, could mean people literally wear their hearts on their sleeve. The question inevitably focusses on whether the individual has any understanding of what happens to that data when the wearable is 'connected'?

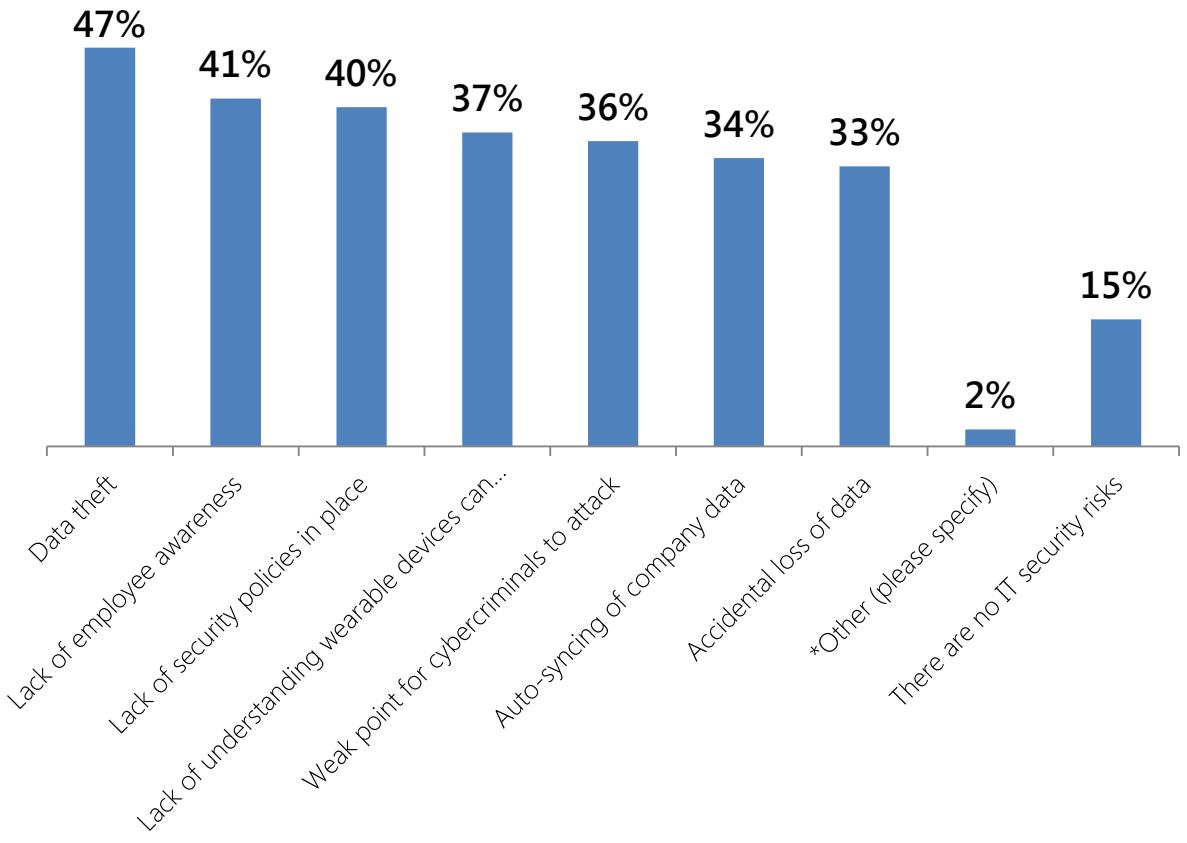
"Data Protection Regulators are increasingly concerned about the fundamental points of transparency and consent in relation to the sharing of such sensitive personal data. Regulators are keen that users are made fully aware of what will happen to such data and that 'choice' is prominently built into the use of the devices.

"There is no doubt that the entire data cycle flowing from wearables should be subject to stringent control measures as identified through a 'privacy by design' model," added Bange. "Privacy is increasingly becoming a lead concern for users of technology, and wearables is no exception. Being able to demonstrate to Regulators and users that privacy protection is at the core and not an afterthought could be the difference between success or failure of a product."

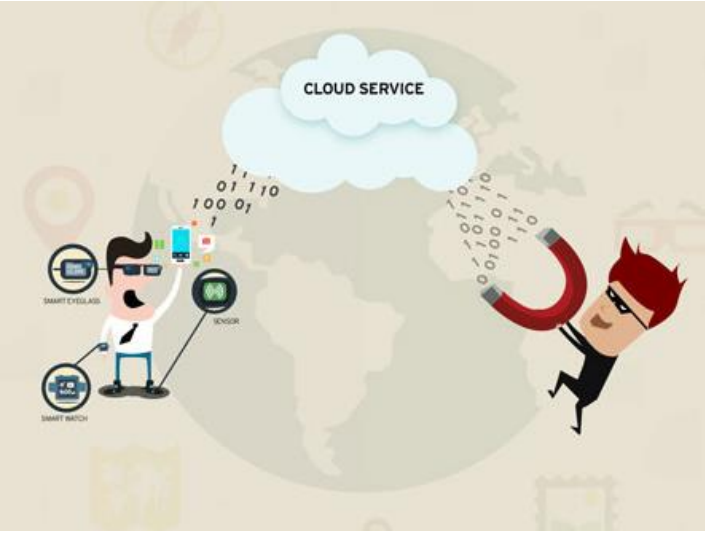
Assessing the risks

The study found that most respondents (85%) see at least one security risk arising from wearables. These include data theft (47%) and auto-syncing of company data (34%). Yet, almost two-thirds (64%) of respondents are not concerned about the potential influx of wearables into their workplace.

What IT security risks do you think wearable devices present for enterprise security? (multiple choice)



Key security risks associated with wearable devices



Low user risk, high feasibility attacks

These attacks are the easiest to pull off but they have the most limited application against the user. In this scenario, the attacker compromises the cloud provider and is able to access the data stored there.

Attackers will attempt to access cloud data by employing tactics such as utilising the provider's "forgot your password" mechanisms, using a keylogging Trojan, guessing the password based on data from the user's other breached accounts, or using a brute-force attack.

Once the account has been accessed, the attacker can see the data coming from the wearable devices and use it to create a better profile of the user in order to target them with specific spam campaigns. Attackers for this type of scenario are cybercriminals with the ability to create malware and whose main sources of profit come from spam/advertising campaigns. Hackers specialising in data breaches may also employ this attack as they can later sell the stolen information to others for monetisation.

High User Risk, Low Feasibility Attacks

These attacks are considered the most dangerous but these are also considered the least likely to happen. If an attacker manages to successfully compromise the hardware or network protocol of a wearable device, they would have access to the raw data in the 'IN' devices but also the ability to display arbitrary content on 'OUT' devices.

These scenarios range from personal data theft to mangling the reality of a camera device. These attacks might affect the wearer adversely and might even stop them from performing their daily routines.

The operating system (OS) or apps installed on the devices could also be exploited by vulnerabilities that exist within them. This can then enable the hacker to get back door access that can be used to steal data, add additional software or perform other malicious functions as listed above.

Medium user risk, medium feasibility attacks

These attacks are more dangerous, easier to pull off, but with more limited impact on the user. In this scenario, an attacker can compromise the intermediate device and capture the raw data. The attack can also act as a man-in-the-middle between the network and the physical device to alter the data coming from the Internet or the network.

The easiest way to accomplish this is by installing a Trojanised copy of the mobile app used by the hardware vendor. Nowadays, there are plenty of ways of installing rogue apps in Android mobile devices. Most attackers utilise third party app stores to do this. This attacker would look to gather a more complete profile of the victim in order to install malware that is more suitable for the particular victim.

An example of this would be when a malware attack can start by looking for the Google Glass app and using it to determine the user's current location at all moments. The malware will then download a new malicious app that performs click fraud based on that user's location.

The attacker in these scenarios would be someone who makes money from spam/ advertising campaigns and perhaps click fraud. These attacks can be done massively without any specific targets.

Attacking the App Layer

Another possible attack vector for wearables is attacking the app layer and hijacking the data going to the cloud. This attack may allow bad guys to perform the following:

- Listen to the information being sent by the local app
- Tap the data being stored in the mobile device

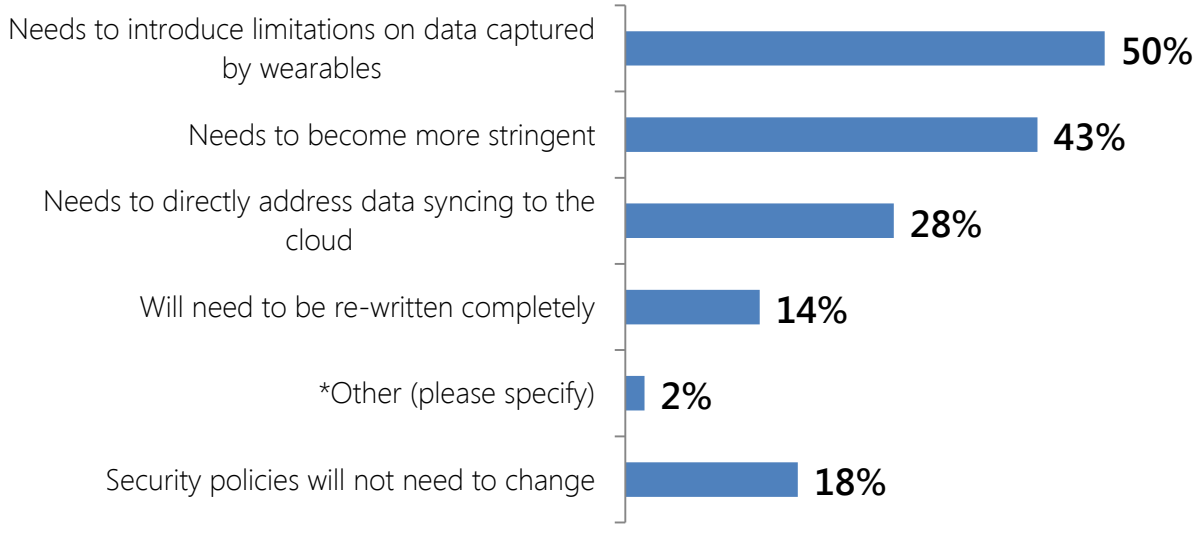
Putting the right security in place to minimise risk

Responses to questions about the impact of wearables on security policies and protocols indicate that the majority of IT decision makers appreciate that something has got to change: 82 per cent of all respondents say that their organisation's IT or BYOD security policies will have to change to account for wearable devices.

Specifically, half of UK businesses (50%) think they need to introduce to their policies limitations on corporate data captured by wearables, and 43 per cent believe their policies will need to become more stringent to account for risks from wearables.

Almost three quarters of respondents (73%) agree that organisations need to introduce a wearable device policy.

How do you think your organisation's IT or BYOD security policies will change to account for wearable devices? (multiple choice)



How can businesses prepare for the influx of wearables in the workplace?

1. Accept BYOD and new technologies by not being a 'Department of No' - Saying 'no' too often drives employees from Shadow IT to Rogue IT. Have a policy detailing how various devices can be used. For example, how to connect to the PC and other corporate devices, what network (if any) they can connect to, whether they can view corporate data etc.

2. Identify the risk for your company and think about how you could mitigate the risks. For example, limit access to sensitive data to a certain group of people, or just with authorised devices. Accept that there might be a breach, and do fire drills for it to ensure you respond in the right way.

3. User education is key - employees are responsible for your company secrets as well. If they feel responsible and empowered, they will act responsibly.

4. If security solutions exist for these devices, ensure that they are installed. App reputation checking is one for example. Ensure devices have the latest software version to stop older vulnerabilities being used to compromise the device.

5. Accept that there is no silver bullet - the latest offer from a security company will not solve all of your problems. Defence in depth with multiple components is needed - not a one-trick pony.

About the research

The research was carried out in November 2014 by Vanson Bourne and surveyed 100 UK senior IT decision makers from organisations with over 500 employees.

About Trend Micro

Trend Micro Incorporated (TYO: 4704), a global leader in security software, strives to make the world safe for exchanging digital information. Our solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. Trend Micro enables the smart protection of information, with innovative security technology that is simple to deploy and manage, and fits an evolving ecosystem. Leveraging these solutions, organizations can protect their end users, their evolving data center and cloud resources, and their information threatened by sophisticated targeted attacks.

All of solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe.
For more information, visit www.trendmicro.co.uk Or follow our news on Twitter at @TrendMicroUK.

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice. Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an “as is” condition.

Securing Your Journey to the Cloud