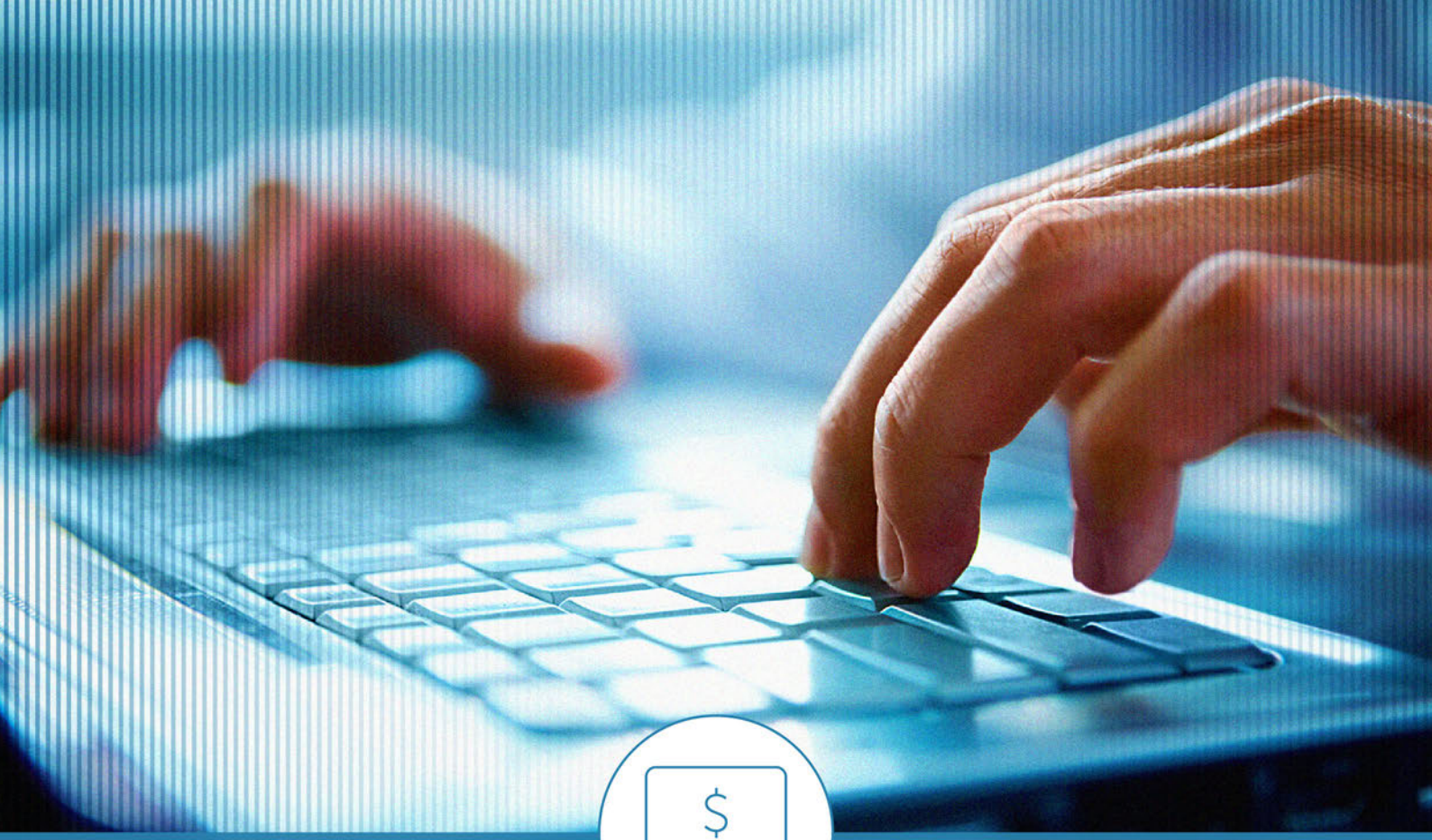
The Fine Line

2016 Trend Micro Security Predictions



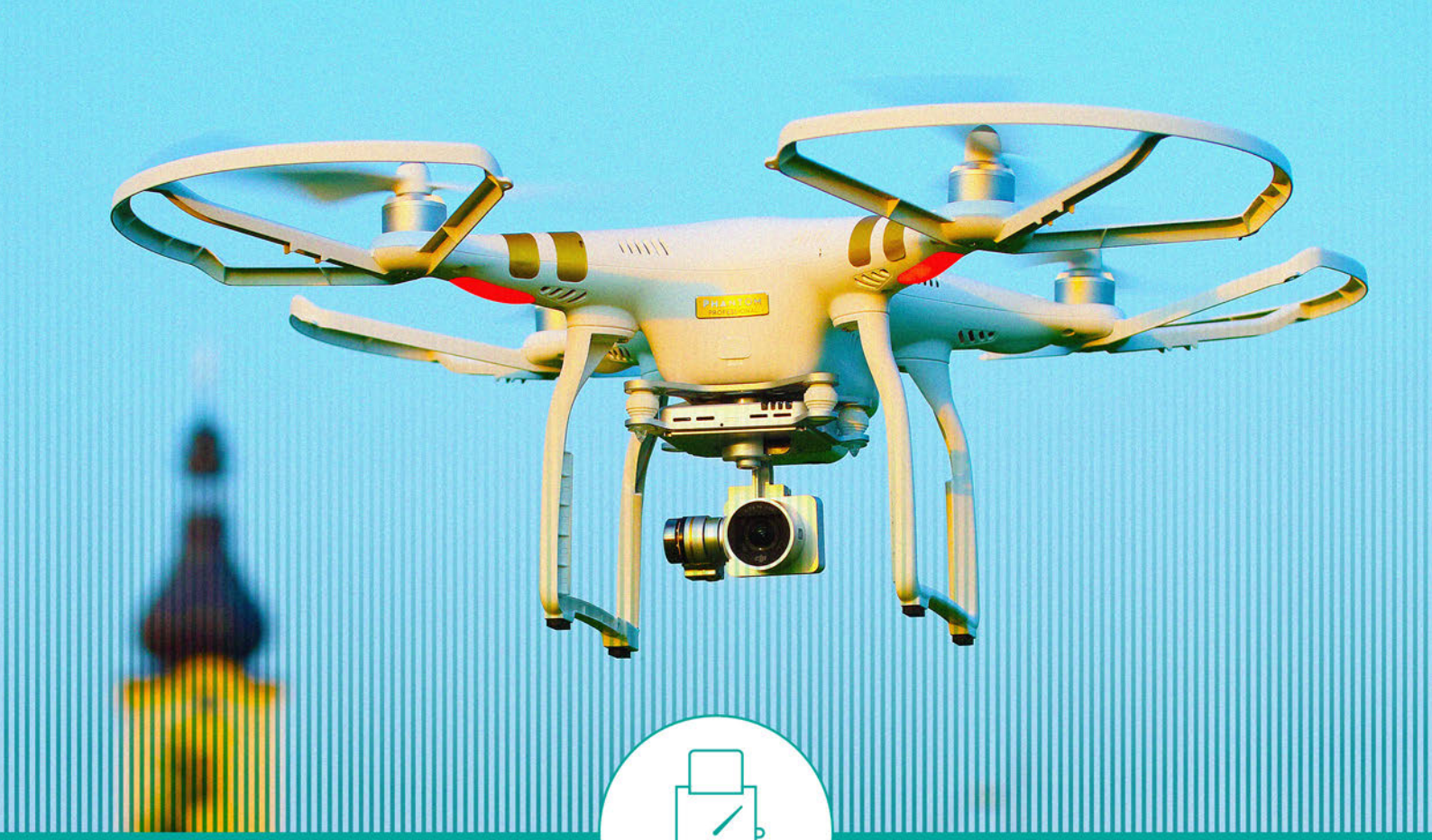
2016 will be the Year of Online Extortion.

In 2016, online threats will evolve to rely more on mastering the psychology behind each scheme than mastering the technical aspects of the operation. Attackers will continue to use fear as its main tool, as it has proven to be effective in the past.

In the past decade, cyber extortionists made use of ransomware to trick online users to make them fall for their tactics. This was done by exploiting one's fears to coerce victims into paying the ransom. The rogue/fake AV trap was set up to target those who feared computer infection. Earlier variants of ransomware locked screens of users, tricking them into paying to regain access. Police Trojans threatened users with arrests and charges for violations. And finally, with crypto-ransomware, cybercriminals aimed for the most valuable part of one's system, the data.

With this in mind, cyber extortionists will devise new ways to target its victim's psyche to make each attack "personal"—either for an end user or an enterprise. Reputation is everything, and threats that can ruin an individual's or a business' reputation will prove to be effective and—more importantly—lucrative.

Businesses will also fall for elaborate tricks that use new social engineering lures. We will see a significant increase in successful ploys designed to persuade employees to transfer money to a cybercriminal-controlled account. Knowledge of ongoing business activities will camouflage these malicious schemes, done by intercepting communications between business partners just like the tactics used by cybercriminals behind HawkEye, Cuckoo Miner, and Predator Pain.

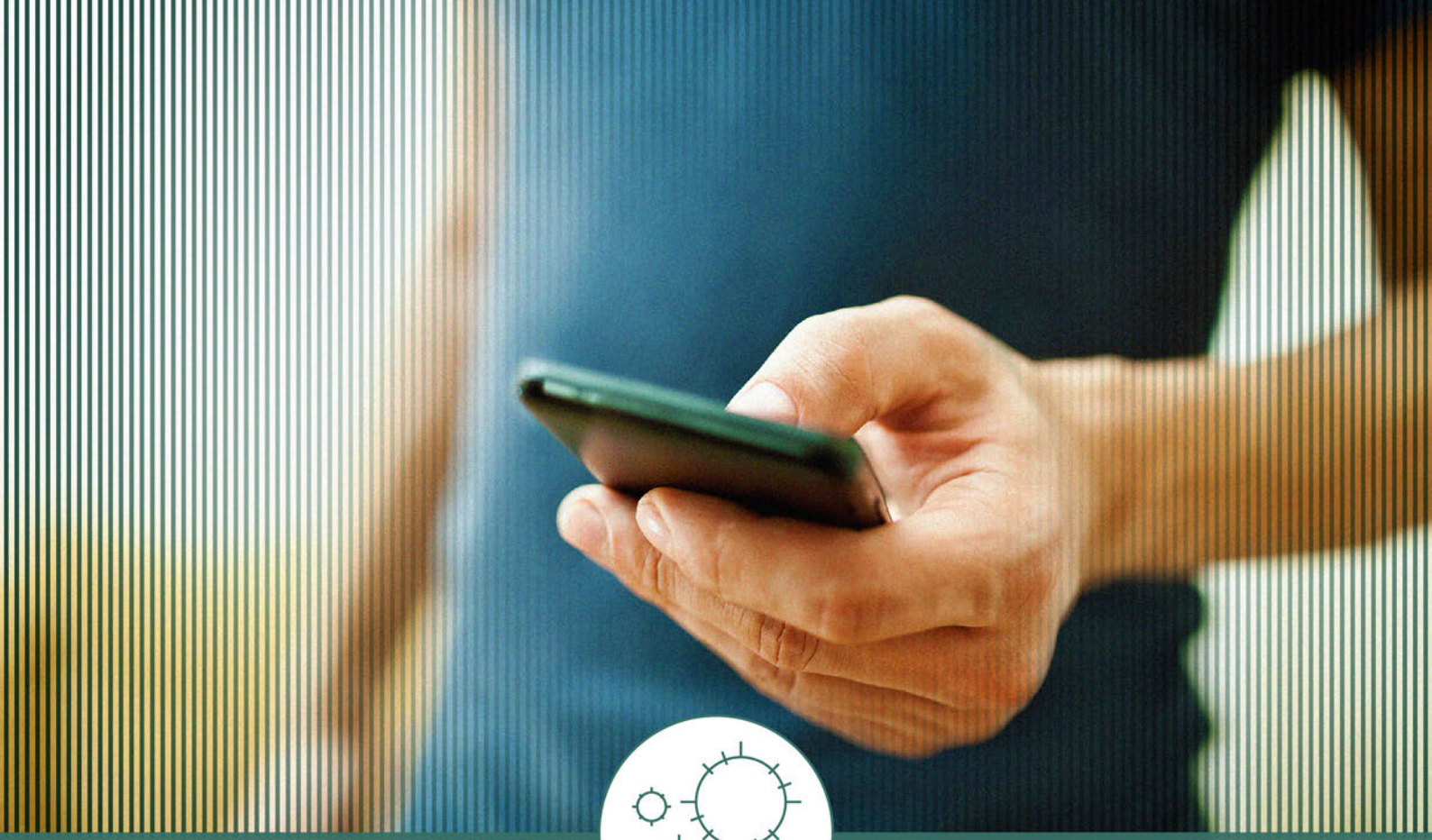


At least one consumer-grade smart device failure will be lethal in 2016.

2015 saw incidents that involved hacked or insecure devices, ranging from baby monitors, smart TVs, and connected cars. Even as users have increasingly become aware of the security risks of connecting appliances and devices to the Internet, the public interest in smartifying just about everything will continue to peak.

Smart-connected home device shipments are projected to grow at a compound annual rate of 67% in the next five years, and are expected to hit almost 2 billion units shipped in 2019—faster than the growth of smartphones and tablet devices. Given the diversity of operating systems and lack of regulation for these smart devices, there remains to be no signs of a possibility of a large-scale hacking attack. WiFi and Bluetooth networks, however, will become polluted and clogged as devices fight for connections. This will, in turn, push mission-critical tasks to suffer.

However, the likelihood that a failure in consumer-grade smart devices will result to physical harm is greater. As more drones encroach on public air space, more devices are used for healthcare-related services, and more appliances rely on an Internet connection to operate, the more likely we will see an incident involving a device malfunction, a hack, or a misuse that will trigger conversation on creating regulations on device production and usage.



China will drive mobile malware growth to 20M by the end of 2016; globally, mobile payment methods will be attacked.

Reports say that 3 in 4 apps in China are malware. Google, on the other hand, released a report that says less than 1% of apps found in Android devices are potentially harmful. Based on the data gathered by Trend Micro, this distinction stands, showing that 13% of apps found in Chinese markets are found to be malicious while Google Play only registered 0.16% malicious apps.

Mobile malware will continue to affect users in China due to the availability of third-party platforms and channels that offer free app downloads. Google Play, for example, is available in China, but reaches only 21 million of the estimated 800 million Chinese mobile users. Given this user behavior, there is no stopping the exponential growth of mobile malware at a rate that's projected to reach the 20 million mark by the end of 2016.

This will not be felt in other countries where users typically turn to official app stores for their apps. However, despite the slow adoption rate, the introduction of next generation mobile payment systems will inspire a renewed interest for threat actors to carry out real-world testing to steal information from new payment processing technologies like EMV credit cards, contactless RFID credit cards, and mobile wallets like Apple Pay and Google Wallet. In 2016, the improved security brought by these modes of payment will be challenged by online criminals.

Data breaches will be used to systematically destroy hacktivists' targets.

In 2016, we will see more hacktivists going the route of "destructive" attacks by going for data that can potentially damage their target's integrity. Cybercriminals will see the impact of data breaches on high-profile targets like Sony, Ashley Madison, and even the Hacking Team.

In the past, the hacktivist's playbook primarily consisted of default tactics like web defacement and DDoS attacks to disrupt targets. However, the recent success of high-impact breaches, driven by a common goal of exposing incriminating information like questionable corporate practices, classified messages, and suspicious transactions will drive cybercriminals to add data breach methods to their arsenal of tactics.

Threat actors will continue to upload stolen data publicly to make investigations and containment trickier. We will also see secondary infections that bank on a target's web presence and turn it against consumers, similar to watering hole attacks we have seen in the past. Data that has already been lost will also be used to lay the ground work for other attacks.

Despite the need for Data Protection Officers, less than 50% of organizations will have them by end of 2016.

Enterprises will finally realize the need for a job designation that focuses solely on ensuring the integrity of data within and outside the enterprise. Whether the company creates a separate Data Protection Officer, Chief Risk Officer or includes this among the tasks of the Chief Information Security Officer depends on company size, budget and other factors, but the set of responsibilities will be the same.

The iron cage put up by the EU Data Protection directive will mandate a high standard of protection on data and the role of the DPO/CISO will be vital in ensuring the integrity of data and compliance with rules and regulations of countries where company data is stored. DPOs and CISOs must be experts in data protection and data security regulations and must how these should be effectively implemented.

However, not all enterprises will be up to the task. In a survey in the finance sector, 22.8% of respondents admitted to not knowing anything about the law, while 50% said that there were no plans to review policies in line with the new regulation.

Awareness around data protection will pave the way to a significant shift in the enterprise mindset and strategy against cyber-attacks. We will see more enterprises taking on the role of the ‘hunter’ instead of the ‘hunted’, in that they will begin to make use of threat intelligence and next-generation security solutions with custom defense to detect intrusions earlier.

Ad-blocking will shake up the advertising business model and kill malvertisements.

The growing aversion of online users to unwanted ads, combined with the spike in malvertising attacks seen throughout the 2015, have given vendors reason to push ad-blocking options in their products and services.

In the first half of this year, we saw how exploit kits were used in malvertising schemes. In September 2015, 3,000 high-profile Japanese sites got affected by a massive malvertising campaign that exposed almost half a million users. In February 2015, Trend Micro discovered a zero-day exploit in Adobe Flash that was used in malvertisement attacks.

This explains the seemingly heightened sense of awareness among consumers who want to block ads. Users are no longer just "annoyed" by unwanted ads, they are fully aware of the kind of risks these pose. In fact, the PageFair and Adobe 2015 Ad Blocking report shows that more consumers are doing so, with a 41% increase in global ad blocking software use in 2015.

In the U.S. alone, the number has increased to 48%, with monthly active users during the second quarter expanding to 45 million. This figure seeks to shake the very foundation by which advertising business models operate, which will, in turn, propel advertisers to seek new ways to advertise online. Likewise, cybercriminals will find other ways to get closer to victims, effectively delivering a blow to malvertisements.

Cybercrime legislation will take a significant step towards becoming a truly global movement.

The next 12 months will see more concrete changes as a result of efforts to fight cybercrime. The good guys will see more indicators of success, be it in faster legislation, successful takedowns, more cybercriminal arrests, and convictions.

Governments and authorities will act faster and will give more rapid response to cyber offenses. We have seen it in the continued arrests and sentencing of various individuals like the Russian national behind the CITADEL malware and another Russian cybercriminal who pleaded guilty of targeting payment processors, both in September 2015. This year, the cloak of anonymity that hid underground forums was removed, allowing law enforcement agencies to take down the hacking forum Darkode.

Cooperation and partnership will also flourish, as shown by the concerted efforts of Trend Micro, INTERPOL, the Cyber Defense Institute and other security firms that resulted in the SIMDA botnet takedown in April. Just recently, we have seen multiple servers used by the online credential-stealing DRIDEX botnet shut down by the FBI as a result of its partnership with security researchers. We will also see enhanced international cooperation, as spearheaded by major regions like the US and Europe, in their recent data-sharing agreement on investigations.

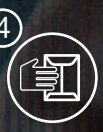
The Internet has operated with very lax regulations for years. 2016 will see a significant shift in the mindset of governments and regulators to take on an even more active role in protecting the Internet and safeguarding its users. Cybercrime laws will be in discussion, and changes to outdated cybersecurity standards will be mandated to bolster an improved stance on security.

Which solutions best help your company face the security challenges of 2016?

1. Protects against online extortion

2. Decreases liabilities from smart device failures

3. Protects against mobile malware and mobile payment attacks



4. Protects against attacks involving data breach dumps

5. Meets the need for data protection officers

6. Shields ad companies from business effects of ad-blocking

Creation/revision of security policies	①	②	③	④	⑤	⑥
Backup policy	•					
BYOD policy		•	•			
Smart device purchase policy		•				
Smart device usage policy		•	•			

Creation/revision of security strategies						
Alternative advertising strategy						•
Customized threat defense strategy	•		•	•		
Encryption strategy				•		

Investment in solutions/infrastructure						
Investment in HTML5 development						•
Mobile solutions (MDM, MAM, VMI)		•	•			

Investment in information security personnel						
Creation of data protection officer roles				•	•	
Formation of incident response teams	•			•	•	

Internal training and audits						
Phishing simulation	•			•		
Employee security awareness	•	•	•	•		
Audit of assets for vulnerabilities		•	•	•		

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.

Created by:

TrendLabs

The Global Technical Support and R&D Center of TREND MICRO

TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver topranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit **www.trendmicro.com**.

TREND MICRO™

Securing Your Journey to the Cloud