Businesses Expect Advanced Security to Lessen Reliance on Human Judgement in Fighting Global Cyber Battle

Latest Trend Micro research shows increasing reliance on machine learning to fight cyber threats, yet skepticism remains

DALLAS--(BUSINESS WIRE)--Latest research from Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, reveals that three quarters of businesses (76 percent) foresee advanced security techniques will lessen the need to rely on human judgement to capture subtle differences between threat anomalies in the future. This displacement will reduce the strain on IT resources leaving time for other strategic activities. Nearly 45 percent expecting this change to occur within the next five years.

The research, which is the second phase of Trend Micro's investigation into the state of cybersecurity, surveyed 2,402 IT decision makers across Europe and the US. It reveals that transformation is potentially already under way with two-thirds of organizations (67 percent) currently using advanced techniques within their cybersecurity solutions, and a further 43 percent of those who currently do not, planning to introduce them in the next 12-18 months.

Despite the majority of businesses advocating advanced security techniques, there is still skepticism and confusion. Looking specifically at machine learning, more than 20 percent of respondents feel it is a marketing buzzword and a further 11 percent believe it only exists in movies, demonstrating a clear disparity in how businesses feel best to protect themselves. In addition, 15 percent of businesses don't yet know how effective machine learning and behavioral analysis are at preventing attacks. This indicates as enterprise security evolves, there remains an opportunity for technology professionals to meet the demand to maintain these systems with advanced training.

Leah MacMillan, senior vice president of global marketing at Trend Micro, stated, "Cyber threats are becoming increasingly stealthy and destructive, meaning businesses must also adapt their defenses. Following the explosion of ransomware and other damaging cyber-attacks like those highlighted in our latest Pawn Storm report, organizations now face a very real threat to their operations and competitive advantage. While the opportunity now exists to focus more on the newest, most advanced technology to circumvent the potential for human error, it's evident that companies aren't clear on their strategy here yet."

"Companies cited that their lack of understanding may be a result of the ever-changing attacks and over-hyped claims," said MacMillian. "The reality is that there is no silver bullet. It takes a layered technology approach, directed and managed by security experts trained in best practices to defend against threats and to make stakeholders feel safe."

The latest report also exposes the lack of awareness around false positives within cyber-security, when a security system believes it has detected a threat and takes action but no such threat actually exists. These protective actions are hugely time constraining and can disrupt the functioning of the organization by rendering programs and operating systems unusable. Forty percent of businesses have not accounted for this, but the problem is particularly prevalent throughout Europe with the majority of businesses in Norway (78 percent), Sweden (64 percent), Austria (60 percent) and Switzerland (59 percent) having never previously considered this issue.

Businesses now face up 500,000 new, unique threats every day, and 2016 alone saw a 752 percent spike in ransomware attacks. The very real danger ransomware poses to business continuity was demonstrated last week with WannaCry spreading across the globe. Trend Micro suggests a blend of cross-generational threat defense techniques, which include advanced technologies such as machine learning, as the best way to detect and handle the full range of threats faced by organizations today.

MacMillian continued, "Businesses require a connected threat defense, allowing them to share threat intelligence across layers with the visibility and control to protect, detect and respond – this is where we'll see the best results. Advanced cybersecurity technologies must be comprehended before they can be integrated into an efficient system, and businesses will still require human expertise to evolve their security strategies and optimize security procedures."

Notes to editors

The survey of 2,402 IT decision makers (ITDMs) in the UK, U.S., France, Germany, Italy, Netherlands, Sweden, Norway, Austria and Switzerland was commissioned by Trend Micro and conducted by Opinium in February 2017.

About Trend Micro

Trend Micro Incorporated, a global leader in cybersecurity solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks and endpoints. All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and control, enabling better, faster protection. With more than 5,000

employees in over 50 countries and the world's most advanced global threat intelligence, Trend Micro enables organizations to secure their journey to the cloud. For more information, visit www.trendmicro.com.

Contact:

Trend Micro Incorporated
Sarah Ferguson, 972-499-6648
publicrelations@trendmicro.com

Public Company Information:

TOKYO:
4704
JP3637300009
NQB:
TMICY
