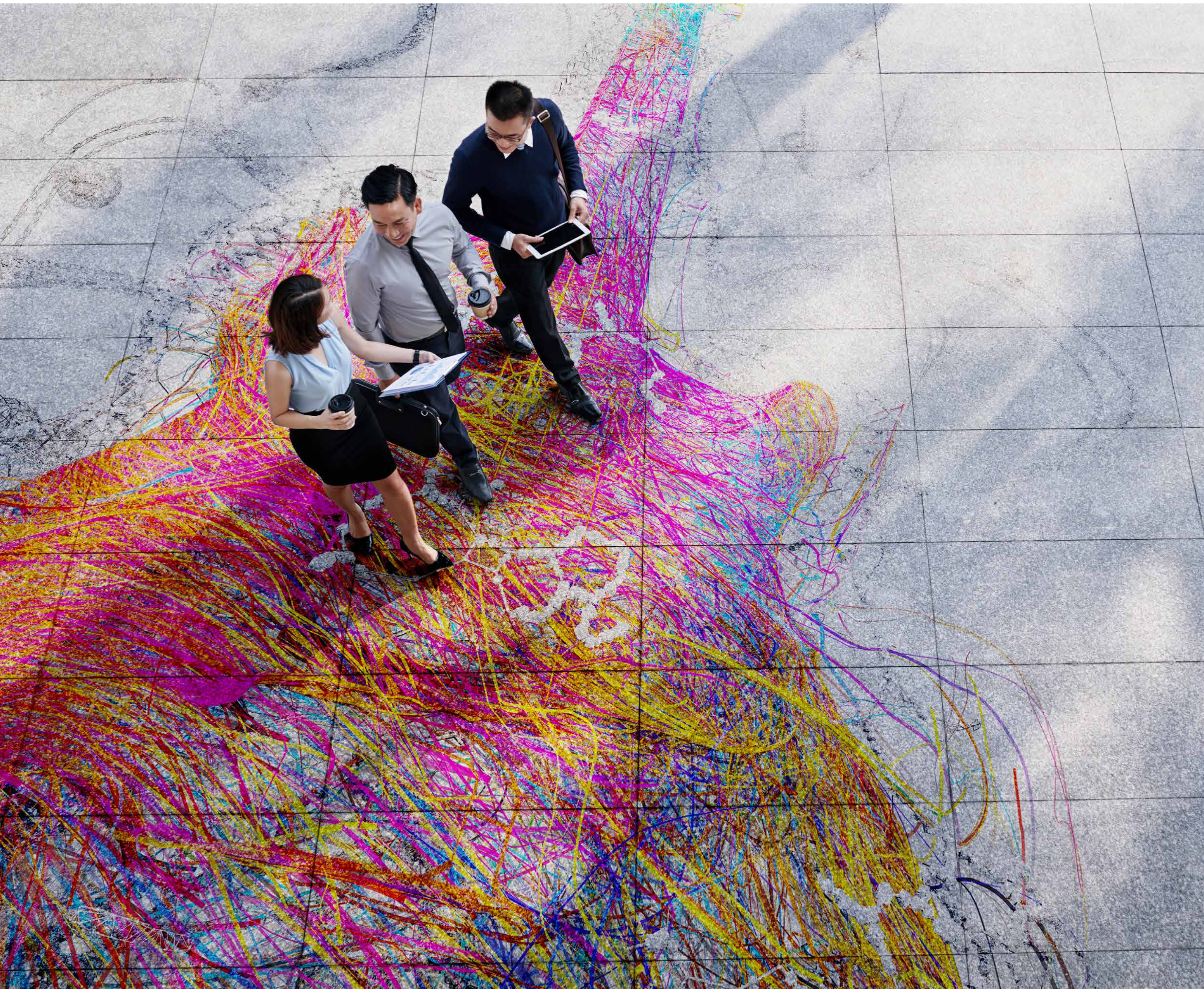
| Retail

Preventing misconfigurations in the cloud

Leveraging cloud security platforms to protect valuable assets



DOES THIS SOUND FAMILIAR?

Let's say you are developing a new web service for which you need a cloud database. Naturally, you have cloud experts on your team who are well informed about this. The new service should run on Amazon Web Services (AWS), since you will obtain a better price-performance ratio with that. However, your personnel are primarily familiar with Microsoft Azure, and the project should ideally have been ready yesterday, so everyone is working under high pressure. It is only human that errors will occur. But all it takes is a wrongly set tick in the configuration of an Amazon Simple Storage Service (S3) bucket, and before you know it, sensitive data is publicly accessible.

Unauthorized individuals might even have writing access. For example, hackers could then abuse the cloud services for crypto-jacking or use a script to access customers' payment information. **Gartner** predicts that by 2025, at least 99% of all cloud security incidents will be caused by programmers themselves.

EASIER SAID THAN DONE

Why is there such a high risk of cloud misconfigurations, and what are the main challenges?

Different configurations for different cloud service providers (CSP). To avoid errors, employees must know exactly what is going on, which is highly complex with a multi-cloud setting.

Documentation for configurations and best practices are arduous and time-consuming to read.

The setup and configuration of a cloud setting often spans more than 100 different services, each with their own authorization policies. It is nearly impossible to manually check all settings.

Cloud settings develop dynamically, and compliance requirements can change quickly. Security managers must continuously keep an eye on their configurations and compare them with current requirements.

Conventional security tools do not notice misconfigurations in the cloud, and do not sound the alarm when large data quantities are being leaked. Therefore, companies often only become aware of security breaches when cybercriminals have already caused damage or reach out with a ransom demand.

WHAT NOW?

Mean time for remediation (MTTR) is an important measure of cloud security. This is known as the time that elapses until a misconfiguration is corrected. The longer a vulnerability remains undetected, the greater the risk of a security incident. You can reduce MTTR to a few minutes with a solution that automatically detects dangerous configurations.

The solution should monitor the entire cloud infrastructure in real time and checks its configuration to ensure you are meeting compliance regulations such as PCI DSS or GDPR. If the solution finds an unsafe setting, it marks it as critical and sends an alert. It also should deliver step-by-step instructions or automated remediation. This way, you can solve the problem immediately without first having to dig through documentation.

TREND MICRO TIP

Conformity identifies an average of 230 million misconfigurations that compromise corporate access credentials and trade secrets every day. Read more about our current Cloud risks in our **white paper**.

WHAT WE CAN DO FOR YOU

- Avoid misconfigurations and therefore reduce the risk of data breaches and cyberattacks.
- More confidence that your cloud settings conform to current compliance requirements thanks to hundreds of best practice and compliance scans.
- Overview of the security status of your AWS and Azure environments from a central dashboard.
- Solve problems quickly without needing expert knowledge via step-by-step guides or auto-remediation.

TRUSTED CYBERSECURITY PARTNER BY YOUR SIDE

Trend Micro Cloud One™ – Conformity is part of Trend Micro Cloud One, a security solutions platform built for the cloud. According to **IDC**, Trend Micro has by far the largest market share in hybrid cloud workload security at 27.5%, and was named a **Leader in Forrester Wave™: Cloud Workload Security (4th quarter 2019)**.

Trend Micro (listed on the Tokyo stock market) has over 30 years of experience as a security solutions specialist. The company has been successfully managed for 15 years by its co-founder Eva Chen, internationally recognized as a leading woman in IT. Since its founding in 1988, Chen and her management team have ensured that the company has grown healthily and reinvests extensively in research and development, even in times of crisis.

Her motto: "Our only competition is cybercriminals, who must be stopped."

Securing Your Connected World