Customer Advisory

From Reaction to Foresight

Forecasting Malware Risk to Prevent the Next Incident

New research from TrendAI™, a business unit of Trend Micro, shines a light on a persistent gap in security operations. Most controls are designed to respond once malicious code has already breached the environment. This study shifts the focus upstream. It presents a method to assess the probability that a specific endpoint will experience a malware outbreak within the next 30 days, using observed user and system behavior as leading indicators of risk.

The model assesses risk across six malware classes: coinminer, hacktool, PUA, ransomware, trojan, and virus. Instead of issuing a single overall score, it calculates distinct probabilities for each class and connects them to the behaviors that increase exposure.

It was trained on two months of telemetry from more than 12 million Windows endpoints across 200 countries, and then applied to 10.7 million endpoints over a further month. The analysis reviewed web activity, software execution, application diversity, file prevalence, and other behavioral indicators, with a focus on first-stage infections.

The results show that risk is very specific. Different malware classes correlate with different patterns of device use. Business-critical systems face higher ransomware exposure, while download-heavy and gaming environments show greater PUA risk. The way a device is used plays a defining role in shaping future infection likelihood.

If you want to understand where future malware risk is building inside your environment and how to reduce it before impact, speak to your TrendAI™ representative to arrange a briefing or demonstration of how this capability can be applied within your organization.

Key takeaways for customers

Move from equal treatment to targeted prioritization

Not all endpoints carry the same likelihood of future compromise. Forecasting risk allows security teams to focus controls and monitoring on the machines most likely to be hit next.

Understand which threat type is most relevant

Risk is broken down by malware class. This enables more precise action, such as tightening controls around systems trending toward ransomware exposure while addressing other classes through application governance and web policy.

Act on observable behavioral drivers

Elevated risk is tied to measurable behaviors such as contact with suspicious or unclassified websites, high-diversity browsing, frequent software installation, and use of less common applications. These insights support concrete actions including stronger patch enforcement, restricted install rights, web filtering, and segmentation.

Strengthen business resilience before impact

By identifying elevated risk up to 30 days in advance, organizations can reduce the likelihood of disruption, data loss, and recovery costs, rather than relying solely on detection and response after an outbreak begins.

Operationalize risk within existing platforms

The research directly informs the evolution of TrendAI Vision One™ Cyber Risk Exposure Management (CREM), supporting risk-driven decision-making at the endpoint, user, and organizational level.

TrendMicro.com