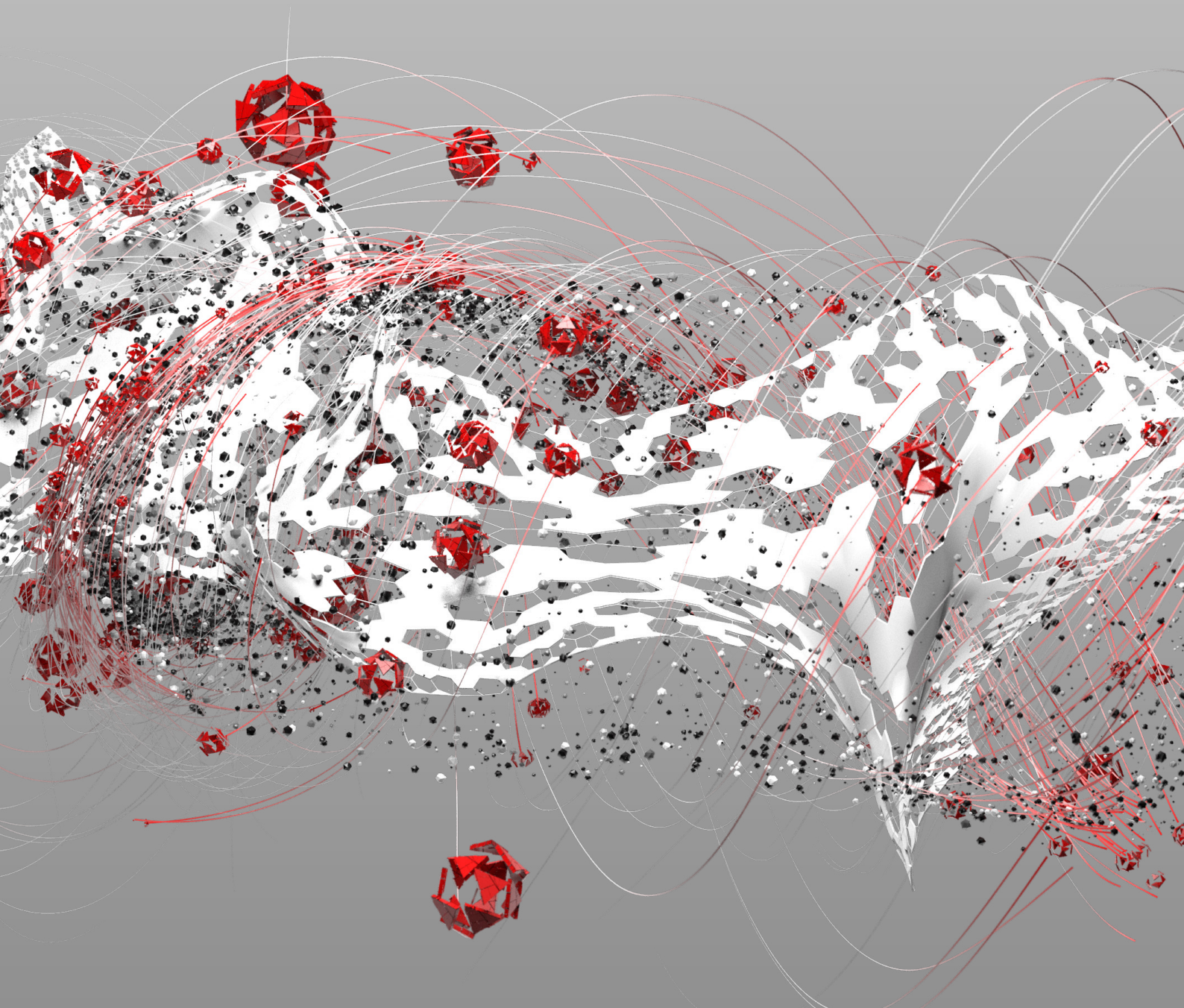
TREND MICRO™

A global study

MANAGING THE SECOPS TOOL SPRAWL CHALLENGE



Over half of Security Operation Centers are overrun with redundant security tools

The cybersecurity market has been flooded in recent years with security monitoring tools. They can cover every inch of the IT environment—from endpoints and servers to networks, email and cloud infrastructure. They are increasingly necessary given the advent of hybrid working, and the growing corporate attack surface which has emerged from digital investments during the pandemic. However, when organisations have too many tools, and are unable to integrate, trust or use them, it becomes a problem.

As new research* from Trend Micro reveals, the challenge of tool sprawl has now become critical—putting organisations' security operations (SecOps) at risk.

2,303
IT security decision makers

21
countries

85% includes leaders who run SOC teams

15% manage SecOps from within their IT security team

250+
employee companies

The scale of the challenge

Our global research reveals that organisations have on average 29 security monitoring solutions in place, rising to 46 for companies with more than 10,000 employees. Why have security solution sets become so bloated? For some organisations it may be the result of mergers and acquisitions over the years. For others it may simply be that point solutions were bought over time to fix specific problems, without any overarching strategy to guide these purchases. The security industry is also culpable to an extent—promoting silver bullet solutions to each new breaking threat.

Whatever the cause, tool sprawl is here. And it comes with a long list of negative consequences. These include:

- Extra overheads associated with managing each tool separately
- Security and detection gaps that exist between tools
- Wasted effort where tools overlap
- Extra licensing costs
- Extra costs linked to training SecOps teams how to use each tool
- Alert overload

Tool sprawl means alert overload

Of all of the challenges related to too sprawl, alert overload is one of the most critical. It can overwhelm SecOps analysts with data, making it impossible for them to prioritise. And if they're unable to prioritise alerts, they may spend hours chasing dead ends while serious breaches go undetected. That's not to mention the potentially severe impact on mental health that alert overload can have on SecOps.

It goes without saying that a serious breach could cost the organisation dear in financial and reputational damage. Respondents say that, on average, their company stands to lose over $235,000 if they fall foul of the GDPR due to an incident. However, some ransomware attacks have cost victim organisations tens of millions in lost revenue, operational charges and IT overtime.

Next steps for SecOps

Organisations therefore need the right detection and response platforms to arm their SecOps teams. They should be predicated on the idea of connected threat defence—sharing information across layers (email, endpoint, server, cloud, networks) and then applying intelligent algorithms to correlate and prioritise alerts. Some IT buyers may want to outsource this function completely, which is another worthwhile option, freeing up in-house staff to focus on higher value tasks. Some 92% of respondents tell us they've considered managed services to for threat detection and response.

Trend Micro Vision One™ offers both options. This purpose-built threat detection platform goes beyond typical XDR to offer a prioritised view of threats across the enterprise—allowing teams to provide accelerated response.

It offers:

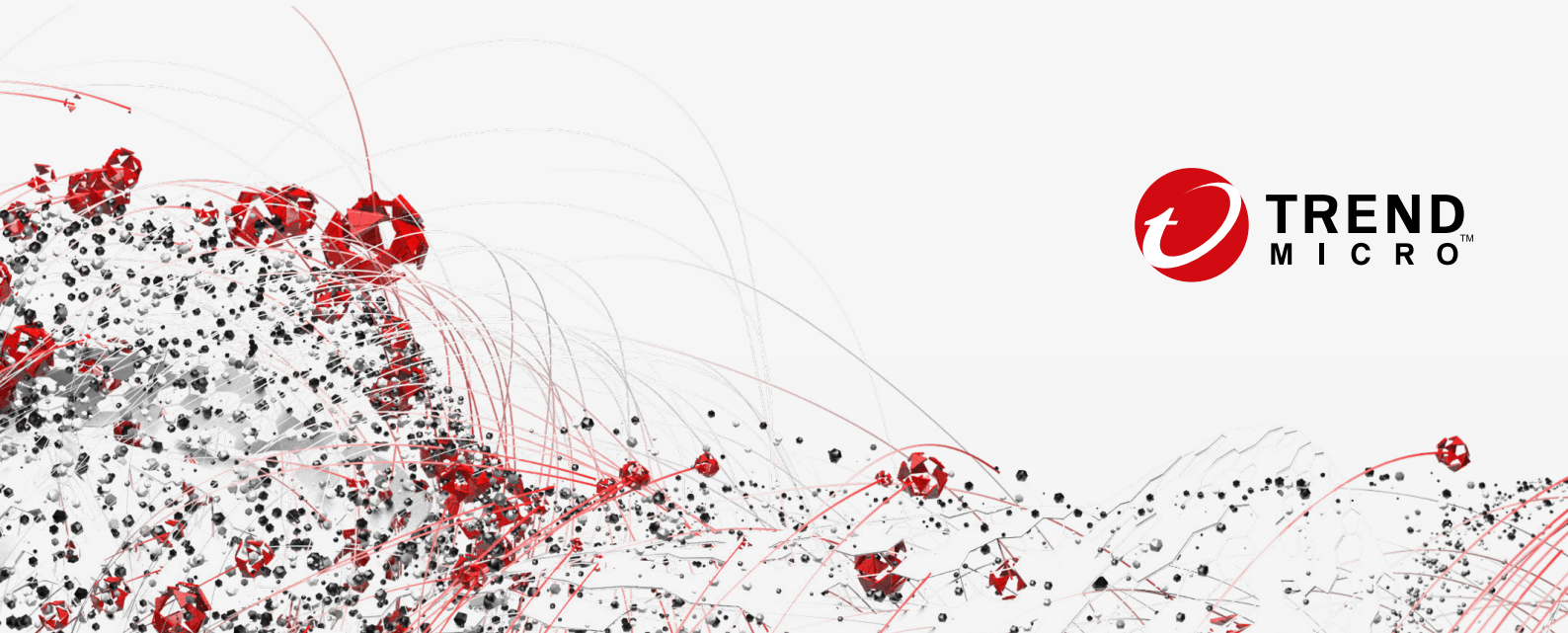
- Faster time-to-detection and response, thanks to fewer, prioritised alerts flagged for action
- Comprehensive protection via web reputation, application control, IPS and more to automatically block attacks
- Automated remediation to remove malware and free-up analyst time
- A centralised source of alerts, investigations and containment, to support faster response with fewer resources
- Improved SOC analyst productivity
- Reduced exposure to financial and reputational risk
- Happier SecOps teams

Whatever approach organisations take, the risks stemming from tool sprawl are very real. IT leaders should revisit threat detection and response with some urgency, to consolidate on fewer suppliers and give analysts the ability to prioritise alert data. In this way, security can finally be a strategic enabler of business growth, as well as a mitigator of risk.

To find out more, please read the accompanying report, Security Operations on the Backfoot: How poor tooling is taking its toll on security analysts.

***Research methodology**

The study was based on interviews with 2,303 IT security decision makers in 21 countries. This includes leaders who run SOC teams (85%) and those who manage SecOps from within their IT security team (15%). All respondents came from 250+ employee companies.



TREND MICRO™