CyberEdge Group’s eighth annual Cyberthreat Defense Report reveals key IT security professionals’ perceptions of the security posture of their organizations, the challenges they face in establishing effective cyberthreat defenses, and the plans they have to overcome those challenges. Here’s to being on better footing for the year to come.

BAD GUYS ARE MORE ACTIVE THAN EVER

Percentage of organizations...

- Facing challenges: 88%
- Not facing challenges: 12%

BARRIERS TO ESTABLISHING EFFECTIVE DEFENSES

The most serious obstacles to adequate defense against cyberattacks include...

- Lack of contextual information from security tools
- Poor integration between security solutions
- Too much data to analyze
- Insufficient automation of threat detection and response processes

DECRYPTION CHALLENGES

Almost everyone faces serious challenges decrypting and inspecting SSL/TLS traffic.

- COMMON ISSUES:
  - Decryption decreases security tool performance
  - Compliance standards prevent decryption of some network traffic
  - Many of our security tools can’t decrypt SSL/TLS traffic

AN UNDERLYING PROBLEM

Adding numerous parallel layers of security tools over the years has led to an ad-hoc security architecture. Besides contributing to the flood of security data, such designs suffer from...

- Unreliable access to network traffic
- Inability to efficiently process encrypted traffic
- Increased hybrid security stack complexity and cost
- Recurring false positives and alerts
- Poor support for testing new security tools

A SOLUTION THAT WORKS

Overcoming these challenges requires a solution that provides pervasive visibility, even in hybrid cloud environments, yet eliminates redundant distribution and processing of source data and resulting security events. It’s all about getting the right intelligence and insight to your tools and teams, without overwhelming them, by:

- Centralizing and offloading resource intensive processes (e.g., decryption)
- Accelerating deployment and integration of new security tools
- Enabling orchestration and automation (to enhance operational efficiency)

The most serious inhibitors to adequate defense against cyberattacks include...

- Lack of contextual information from security tools
- Poor integration between security solutions
- Too much data to analyze
- Insufficient automation of threat detection and response processes