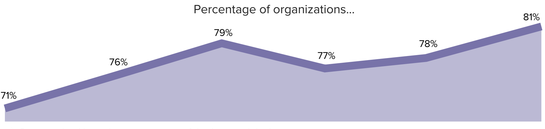
Gigamon®

2020 CYBERTHREAT DEFENSE REPORT

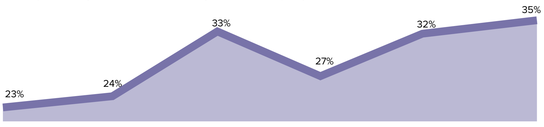
CyberEdge Group's seventh annual Cyberthreat Defense Report reveals how IT security professionals perceive the security posture of their organizations, the challenges they face in establishing effective cyberthreat defenses, and the plans they have to overcome those challenges. Read on to learn about some of the key findings from this year's report.

BAD GUYS ARE MORE ACTIVE THAN EVER

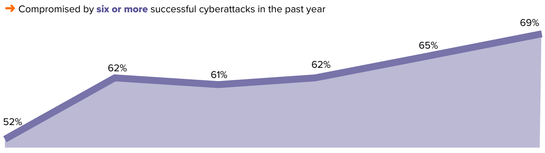
Percentage of organizations...



➜ Compromised by **at least one** successful cyberattack in the past year



➜ Compromised by **six or more** successful cyberattacks in the past year



➜ **Likely to be compromised** by a successful cyberattack in the next year

BARRIERS TO ESTABLISHING EFFECTIVE DEFENSES

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

Too much data to analyze

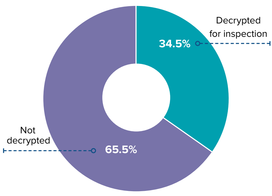
Insufficient automation of threat detection and response processes

Lack of contextual information from security tools

Poor integration between security solutions

A CAUSE FOR CONCERN

Two-thirds of SSL/TLS web traffic is never decrypted for inspection.



TOP PRIORITIES FOR 2020

Top priorities for IT security include...

SECURITY ANALYTICS

Widely used for detecting insider threats, investigating incidents, analyzing network traffic, and hunting for cyberthreats

SSL/TLS DECRYPTION

Currently in use in 56% of organizations

DENIAL OF SERVICE PREVENTION

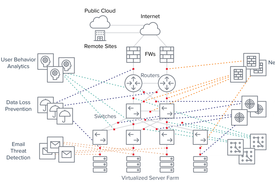
Planned for acquisition by 33% of organizations

SOLUTIONS FOR ZERO TRUST NETWORK ARCHITECTURES

67% of organizations that don't have a zero trust architecture are planning to implement one

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 inspect encrypted traffic
- Increased 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 yet minimizes 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:

1. Delivering optimized traffic to tools (from physical, virtual, and cloud environments)
2. Centralizing and offloading resource intensive processes (e.g., decryption)
3. Accelerating deployment and integration of new security tools
4. Enabling orchestration and automation (to enhance operational efficiency)

DOWNLOAD THE FULL REPORT AT:
www.gigamon.com/cdr2020

CYBEREDGE GROUP