Zero Trust Segmentation Helps Organizations Avoid Cybersecurity Disasters

ESG, in partnership with Illumio, conducted a research study to understand the impact of Zero Trust and how Zero Trust Segmentation helps organizations prevent security incidents from becoming disasters. The findings are based on a global survey of 1,000 information security and IT professionals knowledgeable about their organization's security priorities, technologies, and strategies.
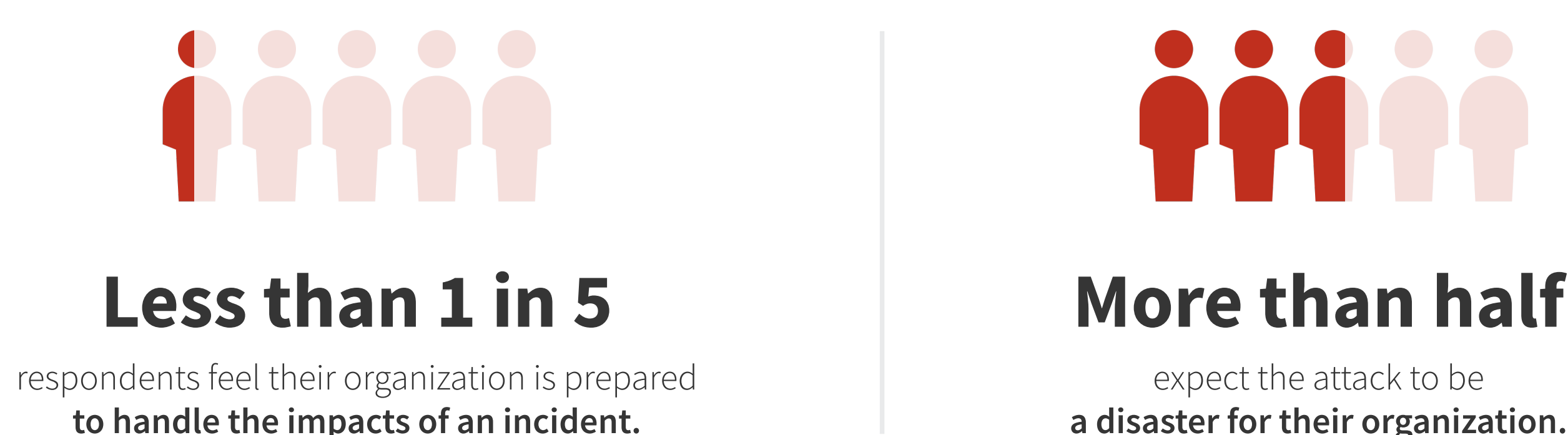
Severity and Frequency of Attacks Are on the Rise

Security teams are grappling with a steady stream of cyberattacks—and many are not ready:

43%
suffer from **unplanned downtime** due to a cyberattack at least monthly.

66%
have experienced **at least one supply chain attack** over the past 24 months.

76%
of organizations have **encountered a ransomware attack** over the same timeframe.

Many Organizations Default to a "Strategy" of Hoping for the Best

Despite the constant attacks organizations must weather, **47% of organizations do not operate with an "assume breach" mindset**—the guiding principle of Zero Trust security.

Less than 1 in 5
respondents feel their organization is prepared **to handle the impacts of an incident.**

More than half
expect the attack to be **a disaster for their organization.**

This indicates that most organizations have neglected to build enough cyber resilience to deal with the inevitability of a cyberattack.
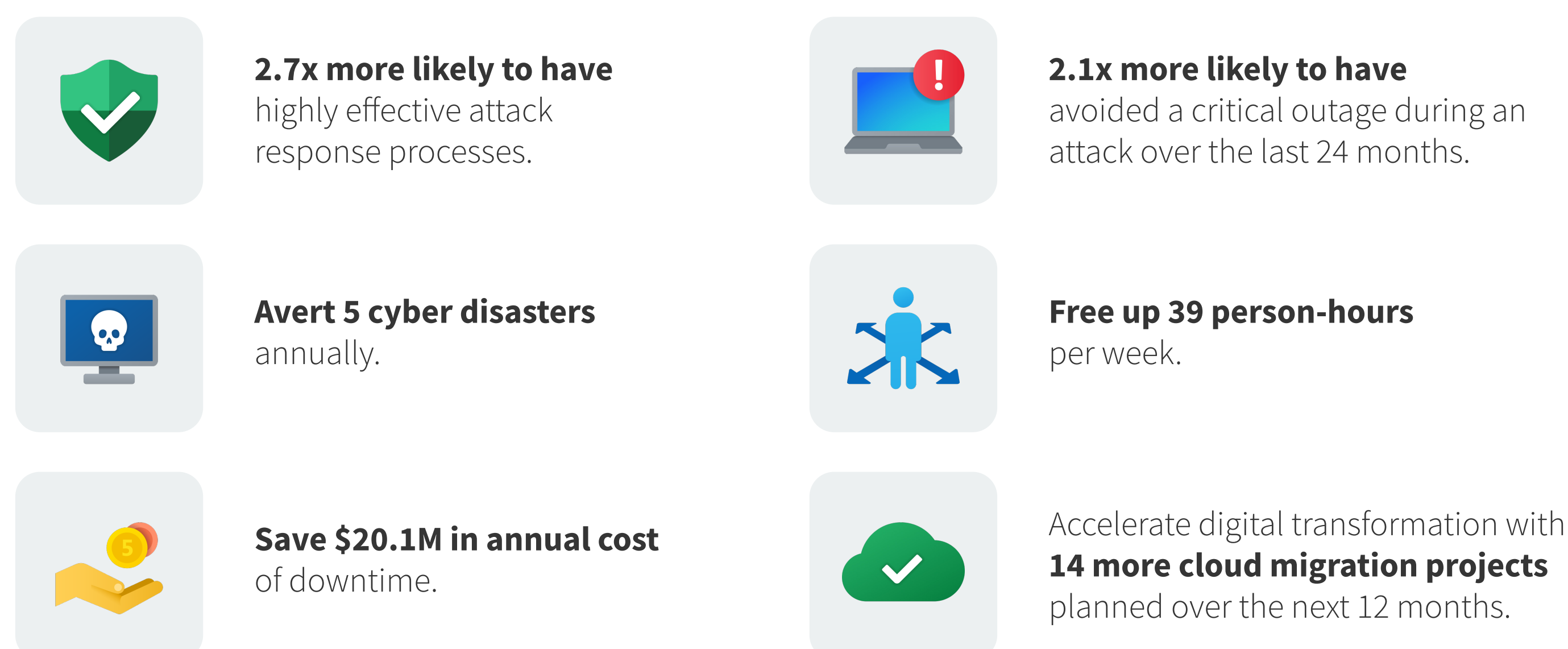
Zero Trust Segmentation: A Proven Solution to a Difficult Problem

Zero Trust Segmentation is foundational to progressing Zero Trust and improving cyber resilience. Proper segmentation of resources helps organizations drive security efficacy across hybrid multi-cloud environments.

THE STAGES OF ZERO TRUST SEGMENTATION

VISIBILITY
Comprehensive visualization across all applications, locations, and endpoints.

PROTECTION
Segmenting environments and assets so attackers cannot access high-value targets.

CONTAINMENT
Preventing attackers from moving laterally to infect and disrupt systems.

Zero Trust Segmentation Brings Significant Advantages

Users who have progressed further down the path of Zero Trust Segmentation experience a host of business and security benefits:

2.7x more likely to have highly effective attack response processes.

2.1x more likely to have avoided a critical outage during an attack over the last 24 months.

Avert 5 cyber disasters annually.

Free up 39 person-hours per week.

Save $20.1M in annual cost of downtime.

Accelerate digital transformation with **14 more cloud migration projects** planned over the next 12 months.

The Bigger Truth

ESG's research shows that advanced Zero Trust Segmentation users are faring much better across a multitude of security and business metrics. These organizations have more confidence, are more agile, and are more resilient in the face of adversity.

For more information, **read the full report**.

[GET THE REPORT]

illumio