ESG Executive Summary

Zero Trust Impact Report: Key Findings for Small and Midsize Enterprises

Date: August 2022 **Author:** John Grady, Senior Analyst; and Adam DeMattia, Custom Research Director

An Expanding Attack Surface Drives Interest in Zero Trust

The hyperconnectivity created by digital transformation between users, applications, data, and things massively expands the attack surface and increases risk. Seeking to exploit these trends, attackers use a variety of methods to compromise targets, often causing significant business disruption. To address these issues, many businesses have begun to implement Zero Trust architectures in order to modernize their cybersecurity programs and limit the impact of these attacks. To gain deeper insights into where businesses stand with Zero Trust broadly, and how segmentation specifically fits into their strategy, Illumio commissioned the Enterprise Strategy Group (ESG) to conduct a global research survey of 1,000 businesses located in North America, Europe, and Asia Pacific and Japan. Some of the key findings among the small enterprise (500-2,499 employees) and midsize enterprise (2,500-4,999 employees) segment respondents include:

- Only 17% of small enterprise respondents feel their business is prepared to handle a breach, with 57% believing a breach is likely to become a disaster. By comparison, 21% of midsize enterprise respondents felt prepared to handle a breach.
- This may be due to past experiences, since 85% of small and midsize enterprises that have had data and systems held hostage by a ransomware attack were forced to pay the ransom, either directly or through a cyber insurance provider. The average ransom paid by small enterprises was more than $333,000, while the average among midsize enterprises was more than $513,000.
- Small and midsize enterprises are prioritizing Zero Trust, with 92% of small enterprise respondents and 90% of midsize enterprise respondents indicating that it is a top-3 cybersecurity priority.
- Despite the prevalence of Zero Trust and the resulting likelihood of suffering an attack, 41% of midsize enterprises do not operate under the assumption that they will be breached. Though this was slightly better than small enterprise respondents (44%) fared, it still points to a glaring disconnect between what businesses say they are doing and how they are actually operating.

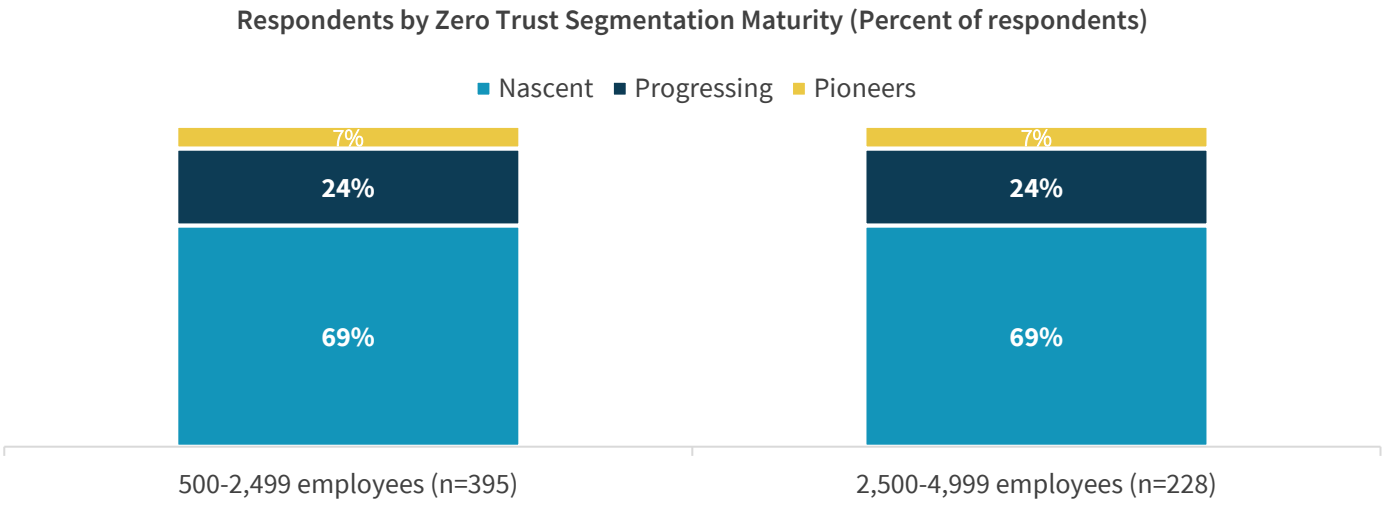
Zero Trust Segmentation Maturity

As part of the research, ESG assessed where respondents fell with regard to their progress toward Zero Trust Segmentation. Zero Trust Segmentation is a modern approach to stop breaches from spreading across hybrid IT, from the data center to the cloud. It includes gaining comprehensive visibility across all application types, locations, and endpoints; quickly and

effectively containing attacks that do occur; properly segmenting different parts of the environment (such as IT from OT and development from production); and finally, expanding these capabilities across the entire environment to ring-fence high-priority resources and ensure proper segmentation across all applications to prevent lateral movement everywhere in the environment.

Research respondents were grouped into three categories based on their responses to five key questions assessing their segmentation technology and practices relative to integrations with SIEM and SOAR solutions, environmental separation, ability to contain infections, and consistent visibility and enforcement across the environment. Those in the Nascent group reported very good capabilities in 0-2 areas, Progressing in 3-4 areas, and Pioneers across all 5 areas. Only 7% of small and midsize enterprises were included in the Pioneers category, meaning that, although many recognize the importance of Zero Trust, there is still a long way to go with the implementation of segmentation to support an "assume breach" mentality.

Figure 1. Zero Trust Segmentation Maturity in the Small and Midsize Enterprise



Source: ESG, a division of TechTarget, Inc.

Why are these groupings important? Businesses identified as Pioneers saw significant security and business advantages compared to their peers. Among global respondents, Zero Trust Segmentation Pioneers reported:

- Better visibility. Pioneers were 4.3 times more likely to have comprehensive visibility into traffic across their environment and five times more likely to have comprehensive visibility across all types of application architectures.
- Lower annual downtime costs. Pioneers were twice as likely to have avoided a critical outage due to an attack and boasted a 68% faster mean time to recover (MTTR). By avoiding outages and recovering more quickly when attacks do occur, these businesses enjoy a $20.1 million advantage in the annual cost of downtime.
- Faster digital transformation. Pioneers will move 14 production applications to the cloud over the next year that they otherwise would not due to a lack of security confidence, which freed up an average of 39 person-hours per week.
- Confidence in preventing cyber disasters. Pioneers were more than twice as likely to feel prepared to handle cyberattacks and reported preventing five cyber disasters annually.

To find out more about the success Zero Trust Segmentation Pioneers are seeing and what they are doing to achieve these results, explore the full report.

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188