zscaler™

WHITE PAPER

How Much Cyber Loss Can Be Prevented By Using Zero Trust Solutions?

A Zscaler report based on research conducted by the Marsh McLennan Cyber Risk Intelligence Center

Executive Summary

Zscaler commissioned the Marsh McLennan Cyber Risk Intelligence Center to assess whether organizations have a reduced risk of cyber incidents when zero trust is deployed.

Zero trust is a framework with six core pillars of focus: identity, devices, networks, applications, data and operations. Zero Trust Secure Access Service Edge spans many of these pillars to enable least privileges through continuous verification of users, applications, and devices accessing an IT estate. In contrast to legacy networks, which trust all traffic inside the perimeter, zero trust operates on the principle of, “never trust, always verify.”

Marsh McLennan analyzed hundreds of thousands of reported cyber incidents from their historical incident datasets between 2017 and 2023. By estimating the proportion of losses that could have been avoided if the impacted organization had deployed a zero trust architecture before the incident, the researchers calculated the potential reduction in insured cyber losses.

Key findings

The results of this study suggest that broad deployment of zero trust architecture could have significant benefits for both insured organizations and cyber insurance providers. Organizations with properly implemented zero trust tend to have fewer cyber incidents, claims, and losses.

- The average company can reduce its risk of a cyber incident by deploying zero trust throughout its environment. If all organizations were to widely deploy zero trust, it is estimated that the number of insured cyber losses could be reduced by up to 31%.
- Companies with over U.S. $1 billion in revenue have the most to gain from deploying zero trust. In 2023, up to 60% of all incidents affecting companies with revenue over $100 billion were assessed as being zero trust mitigatable. (All dollar figures are U.S.)
- If zero trust architecture were widely adopted, average annual U.S. insured cyber losses could be reduced by up to an estimated $2.3 billion, in the aggregate. The annual total economic loss from cyber attacks could be decreased by an estimated $123 billion in the U.S. and up to $465 billion globally, based on Marsh McLennan's view of total cyber losses around the world.

Twenty-three percent of events in Marsh's dataset were determined to be not mitigatable by deploying zero trust and 46% were unknown, due to lack of sufficient details in the incident description.

Research Findings

While legacy networks trust all traffic and devices inside the perimeter, a zero trust architecture does not. Instead, it eliminates implicit trust from users, devices and applications, and instead requires continuous verification to determine whether a connection can be allowed based on business policies. One key benefit of a zero trust architecture is that it does not allow an attacker with access to a compromised device to move laterally within a network, therefore limiting the damage that can be done in the event of a breach.

With this in mind, Zscaler's hypothesis was that organizations that have a zero trust architecture would have fewer cyber incidents, and would make fewer claims. Zscaler commissioned the Marsh McLennan Cyber Risk Intelligence Center to assess whether that was the case.

Marsh McLennan researchers analyzed reported cyber incidents in its historical datasets between January 1, 2017 and October 31, 2023 to assess whether any could have been prevented had a zero trust architecture been deployed.

Three sets of keywords were used in the analysis:

- Search terms associated with attacks that zero trust would be expected to mitigate were used to identify avoidable incidents in the dataset.
- Two sets of keywords, one conservative and another liberal, to establish a minimum (lower bound) and maximum (upper bound) percentage of avoidable incidents.
- Parallel search terms for attacks that would not have been preventable with zero trust. Marsh McLennan also found incidents that did not fall into either category due to a lack of information.

Armed with the results of these searches, Marsh McLennan was able to estimate the proportion of historical incidents that would have been mitigatable with zero trust, and the resultant risk reduction.

Key results

On average across the seven year period, up to 31% of incidents analyzed were found to be potentially mitigatable by zero trust, also known as the 'upper bound' of the calculated range.

Ransomware incidents have significantly contributed to the rise in cybersecurity events. We identified attacks by some of the larger ransomware gangs as potentially mitigatable through Zero Trust solutions. These attacks often involve more sophisticated techniques and access to widely distributed infrastructures, which Zero Trust principles are designed to counter effectively.

"Zero trust mitigatable risk has been increasing over time, and is therefore very timely to be addressed and accounted for by cyber practitioners," said Scott Stransky, Managing Director and Head of the Marsh McLennan Cyber Risk Intelligence Center and leader of the study.

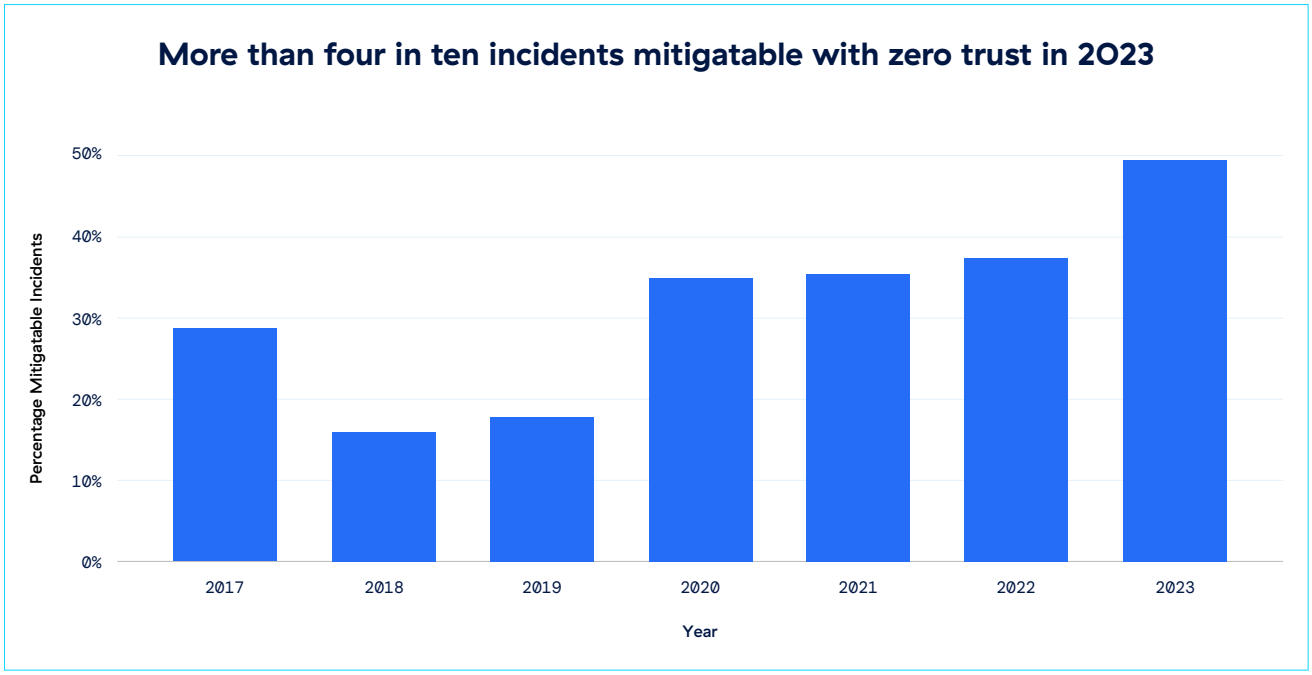

Figure 1: Upper bound of the range of the percentage of incidents mitigatable by zero trust for each year of the study. Note: available data for 2023 only covers the period until October 24 and—with Marsh McLennan's concurrence—has been linearly extrapolated in the chart above to cover the full year.

Revenue–based results

The largest companies in the study were found to have the most to gain from deploying zero trust. In 2023, up to 60% of all incidents affecting companies with revenue over U.S. $100 billion were assessed as being zero trust mitigatable. Companies with revenue less than U.S. $50 million recorded many more events, but a negligible percent of those were found to be mitigatable with zero trust.

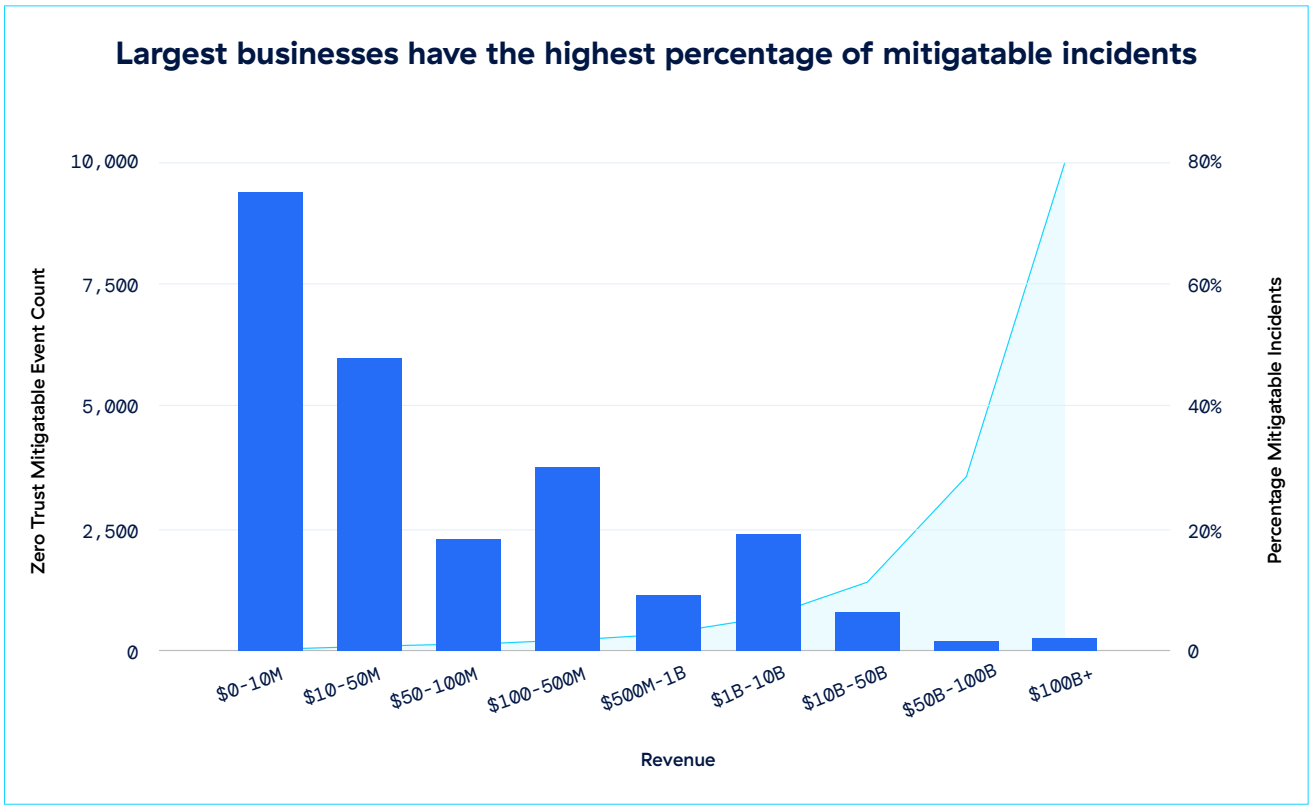

Figure 2: Upper bound of the number and percentage of incidents mitigatable by zero trust by revenue size.

Industry–leading cyber insurers like San Francisco–based Resilience view the research findings as compelling and have further positioned zero trust as a favorable trait among insured clients. Zscaler has pioneered a standards–based approach to zero trust, significantly enhancing cybersecurity hygiene. This is reflected in the lower incidence of losses observed among our shared clients. Through our ongoing engagement with clients to quantify and mitigate cyber risk, Resilience can affirm that adopting a zero trust architecture strengthens an organization's ability to withstand and recover from cyber incidents," said Tim Riley, SVP of Product at Resilience.

Industry-based results

The types of threats and threat actors industries face vary substantially, based on a number of factors including the value of the data an industry typically holds and its perceived ability to protect that data. Some industries therefore see a far greater potential for mitigatable events than others.

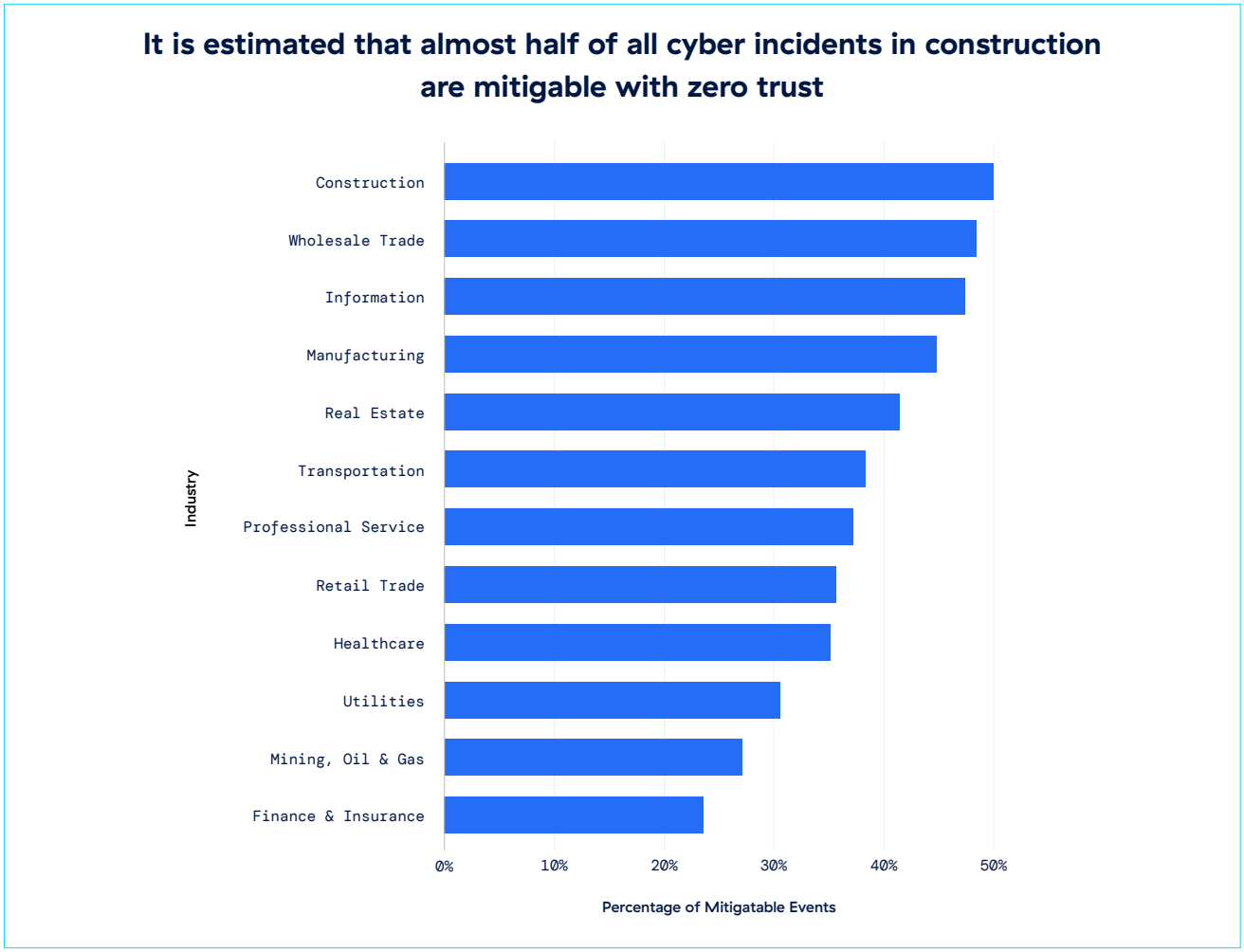

Figure 3: Upper bound of the percentage of zero trust mitigatable events for selected Industries.

The industries with the most to gain from implementing zero-trust architectures include construction, information, real estate and transportation, each of which can potentially eliminate up to half of all cyber incidents and the costs, time, and resources of remediating and recovering from them. Over one-third of incidents experienced by healthcare companies, and just under one quarter of incidents experienced by financial services and insurance companies, were found to be potentially mitigatable with zero trust.

“We now have validated data indicating that prioritizing investments in zero trust offers significant benefits for security practitioners,” said Darren Hurd, EVP and Chief Information Security Officer, Guaranteed Rate, a mortgage company. “The study confirms what security practitioners have suspected for a while, companies that prioritize zero trust investments gain a significant edge as cyber defenders.

Geographical results

North America experienced up to nearly 25,000 incidents that were deemed potentially mitigatable by zero trust according to the Marsh analysis, almost four times the number of incidents seen in Europe and eight times the number in Asia — noting that incident data does tend to be biased towards North America in general. This reflects a far greater number of potentially zero trust mitigatable events occurring in North America than in other regions of the world.

However, the percentage of mitigatable incidents in each continent tells a slightly different story, as figure 4 illustrates. North America has more total companies than other regions. While up to 42% of events in Oceania and up to 41% of events in Europe were determined to be potentially mitigatable with zero trust, 31% is where the upper bound lands in North America. Up to 35% events in both South America and Africa were found to be potentially mitigatable, with the figure for Asia slightly lower at up to 19%.

Figures renormalized paint a different picture for zero trust mitigation opportunities

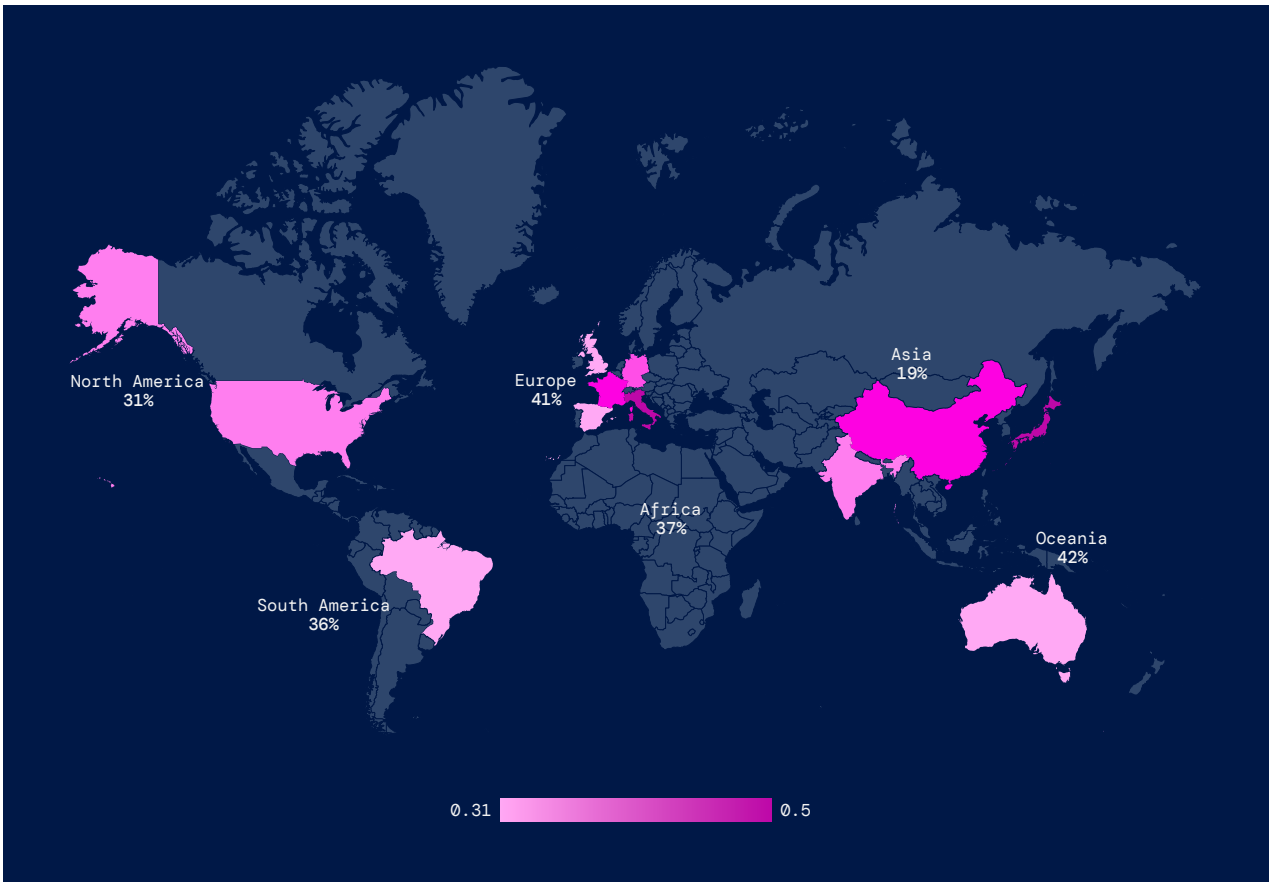

Figure 4: Upper bound of the percentage of zero-trust mitigatable incidents by continent and select countries.

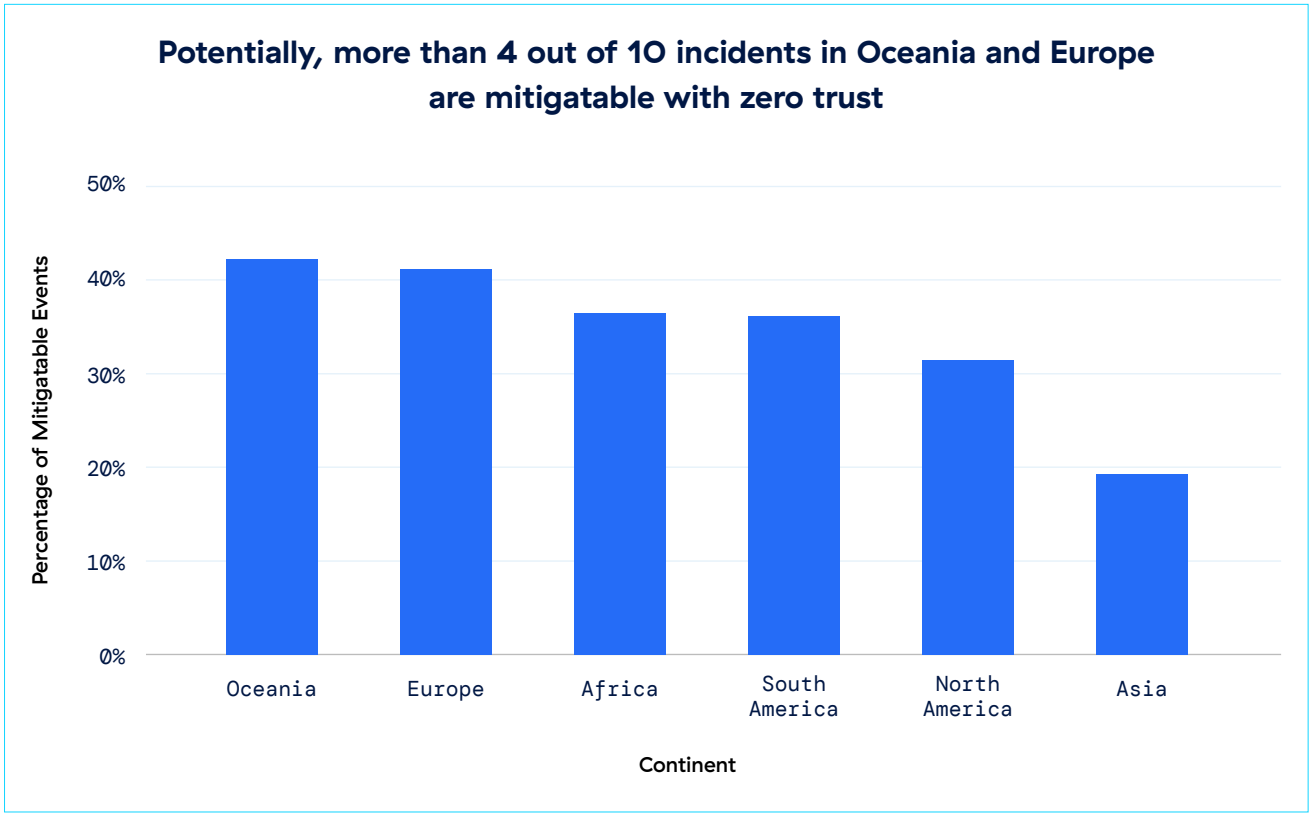

Figure 5: Upper bound of the percentage of zero-trust mitigatable incidents by geography.

Potential cost savings

The exact savings any company can realize through deployment of zero trust will vary depending on factors like the cyber risks they face, the types of incidents they regularly experience, and the amount of legacy infrastructure displaced. This will vary by business.

However, Marsh McLennan researchers used their findings to calculate how insured losses due to cyber attacks could be reduced on average if zero trust was widely deployed. Based on the assessment of $7.5 billion of insured cyber losses annually, it is estimated that zero trust could drive as much as a 31% reduction in losses, equating to a potential reduction of up to $2.3 billion in insured losses annually.

Further, the U.S. annual total economic loss from cyber incidents, estimated by Marsh McLennan to be around $400 billion, could be reduced by an average of up to $123 billion each year. Applying that same logic, the global annual total economic loss from cyber incidents, which Marsh McLennan estimates to be approximately $1.5 trillion, could be reduced by up to $465 billion each year.

> “The large cost associated with the lack of zero trust reveals its true value to companies and the cyber world,” says Scott Stransky, Head of the Marsh McLennan Cyber Risk Intelligence Center and leader of the study.

Conclusion

This study found that widespread zero trust deployment could have significant benefits for organizations: Organizations with properly implemented zero trust and other proper cyber hygiene controls would be exposed to fewer cyber incidents, claims, and losses.

Those organizations that may have previously struggled to qualify for insurance now have a path towards insurability. Those that have seen premiums rapidly rise can take actions to help them access lower premiums and improved coverage terms.

“Zscaler customers are receiving more favorable policies and better premiums, when partnering with their cyber insurance underwriters, clearly explaining their controls and sharing evidence through observability,” says Stephen Singh, Global Vice President, M&A/Divestiture, Private Equity and Cyber Risk Zscaler.

The findings in this report can help you make a case for zero trust architecture or communicate the maturity of your organization’s overall cyber security posture to cyber insurers. Reach out to Zscaler for additional resources and guidance. Zscaler is deployed at eight of the eleven leading insurers, a further sign of the industry’s confidence in the positive benefits of zero trust.

About the Marsh McLennan Cyber Risk Intelligence Center
The Marsh McLennan Cyber Risk Intelligence Center (Center) is Marsh McLennan’s enterprise-wide cyber data, analytics, and modelling center of excellence. The Center was founded in 2021 with a mission to advance how businesses and their communities quantitatively and economically anticipate, measure, and manage cyber risk. By leveraging advanced analytical and modeling techniques, the Center brings together Marsh McLennan’s expansive proprietary data and models across its Marsh, Guy Carpenter, and Oliver Wyman businesses with complementary leading external sources, to develop a robust suite of cyber quantification tools. The Center’s tools power cyber modeling exercises, cyber analytics, and thought leadership insights for Marsh McLennan clients around the world, including cybersecurity technology organizations, insurance and reinsurance providers, and others.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com