

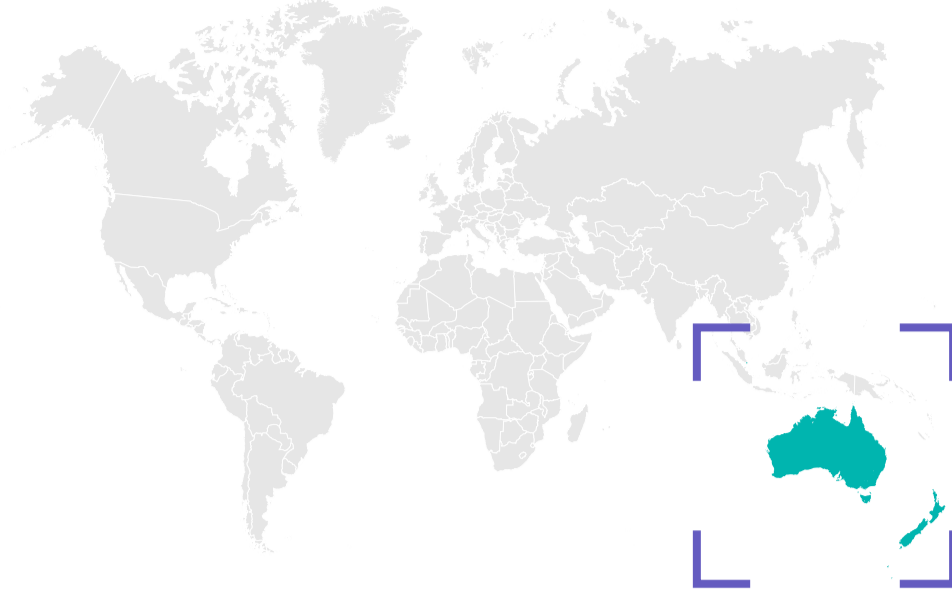
# Zscaler™ Cloud Threat Insights

► Australia, New Zealand, and Singapore

## A regional look at Zscaler cloud detections

Cyberattacks have become a normal part of everyday business in today's digital landscape. With remote employees, branch locations, and the majority of your traffic bound for the internet, cybercriminals have a myriad of attack methods.

The Zscaler cloud blocks such attacks as it processes **120B+ transactions** every day. But what does that look like from a regional perspective? Let's take a peek at the security issues faced by organizations in **Australia**, **New Zealand**, and **Singapore**.



## Policy and security blocks

Policy and security blocks are fundamental categories within the Zscaler security cloud.

While threat blocks are critical, **implementing access control** to sanctioned and unsanctioned sites for proper internet use and compliance is just as important.



A **policy block** is an action that controls where and what users are allowed to access on the internet.



A **security block** is protection of a user from a threat (such as malware, botnets, or zero-day attacks).

On average per week, Australia, New Zealand, and Singapore saw:

More than  
**21 million**  
policy blocks a week

About  
**2 million**  
security blocks a week

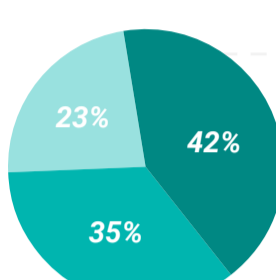


## Malware detections across the region

This dangerous internet content includes known malicious files or content hiding in websites and scripts. How dangerous is the region?

More than  
**1.5 million**  
pieces of malware

a week were blocked across Australia, New Zealand, and Singapore.



But which region is the most active with malware? Of all the malware blocked in the region:



**42%**  
targeted organizations in Australia



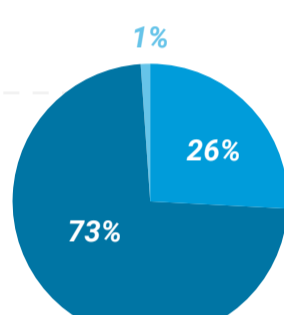
**35%**  
targeted organizations in Singapore



**23%**  
targeted organizations in New Zealand

Singapore by far leads the pack with the majority of botnets detected.

Of all botnets blocked in the region:



**73%**  
targeted organizations in Singapore



**26%**  
targeted organizations in Australia



**1%**  
targeted organizations in New Zealand



## Botnet detections per region

A botnet operates in stealth on your network, quietly working to exfiltrate data or further propagate itself across the organization.



Almost  
**150,000**  
botnets

were detected a week across the region.

## Sandboxing suspicious content

Some files are so suspicious they require full sandboxing analysis. After all, it only takes one bad file to immobilize an organization.

● unknown suspicious file

● malicious file

\*1 file = 1,000 files



More than

**46GB**

of unknown suspicious content was analyzed (comprising 34,000 files).



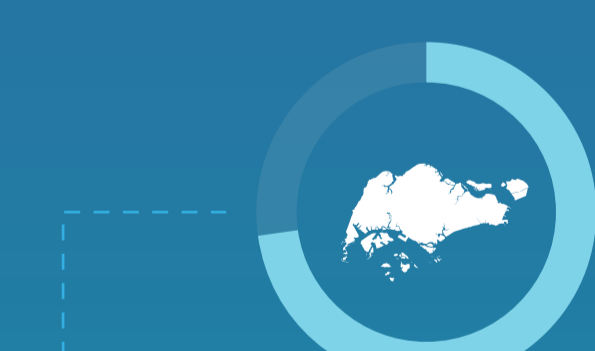
Sandboxing analysis



Of that content,

**7%**

of files were found to be malicious.



**73%**  
of Singapore organizations are inspecting SSL traffic.



**72%**  
of Australia organizations are inspecting SSL traffic.



**70%**  
of New Zealand organizations are inspecting SSL traffic.

## SSL inspection

With more than 90% of all internet traffic now encrypted, inspecting as much SSL traffic as you can is paramount to good security hygiene.

While some SSL traffic can't be inspected due to compliance reasons, how is the region doing inspecting SSL traffic?

## Protection where it counts

Organizations in the Australia, New Zealand, and Singapore region face their fair share of cyberthreats. But, they face them confidently knowing that the Zscaler cloud blocks more than **100 million threats** per day globally.

And, as cybercriminals develop new, more sophisticated attack methods, the Zscaler cloud will be there with more than **175K unique security updates** each day to help keep your organization safe.

The Zscaler cloud blocks more than

**100 million**

threats per day globally.

## Does your organization need this type of security?

Learn what the Zscaler Cloud Security Platform can do for you.

