Menlo Security

BRIEF

Secure Critical Infrastructure with the Menlo Cloud Security Platform

Eliminate threats and protect productivity with a Zero Trust approach powered by isolation.

Benefits:

- Secure government work by eliminating online threats
- Enable fast, secure user access to the tools needed to keep the government running
- Deliver critical government services to citizens without disruption

Government Departments and Agencies are a Tempting Target.

The Australian government is the target of more than 400 cyberattacks per year—more than a third of all documented cyberattacks in Australia. A cyberattack that succeeds in shutting down or overwhelming key government services could impact Australia's ability to respond to an emergency or cripple the country's social safety net. Studies show that a four-week disruption to the country's Internet would cost AU$30 billion and result in a loss of more than 163,000 jobs.

Cybersecurity is a matter of national security, but government agencies lack the tools and resources to adequately protect users from web-based threats.

Traditional Cybersecurity Approaches Fall Short.

Government departments and agencies need to migrate away from traditional detect-and-respond security practices in favour of a more proactive threat protection strategy that protects against increasingly sophisticated malware threats such as zero days, watering-hole attacks and drive-by downloads. Government organisations also need to prevent spearphishing and other credential theft attempts and enforce security updates. And they need to do this while reducing security complexity and the time spent on manual security tasks.

However, accomplishing this goal by using legacy security solutions is impossible. A detect-and-respond approach works only if the attack is a known threat. Once the threat is exposed, however, attackers simply tweak some code just enough to prevent detection and they relaunch the attack. Government security teams then need to react again, starting the process all over. This puts security professionals on the defensive, reacting to emerging threats in order to mitigate the damage resulting from the inevitable successful attack.

Instead, government organisations need a way to prevent all attacks before they gain a foothold on end users' devices.

A Modern Approach to Securing Government Organisations: Zero Trust Powered by Isolation.

Zero Trust means that no traffic should be trusted, even packets that originate from inside the organisation. Instead, all browser-based Internet traffic should be treated as malicious, and web traffic should be isolated from endpoint devices. This isolation approach is comprehensive and removes the flaws associated with detection-based security.

Zero Trust powered by isolation allows government organisations to completely outsmart malware and other web-based threats.

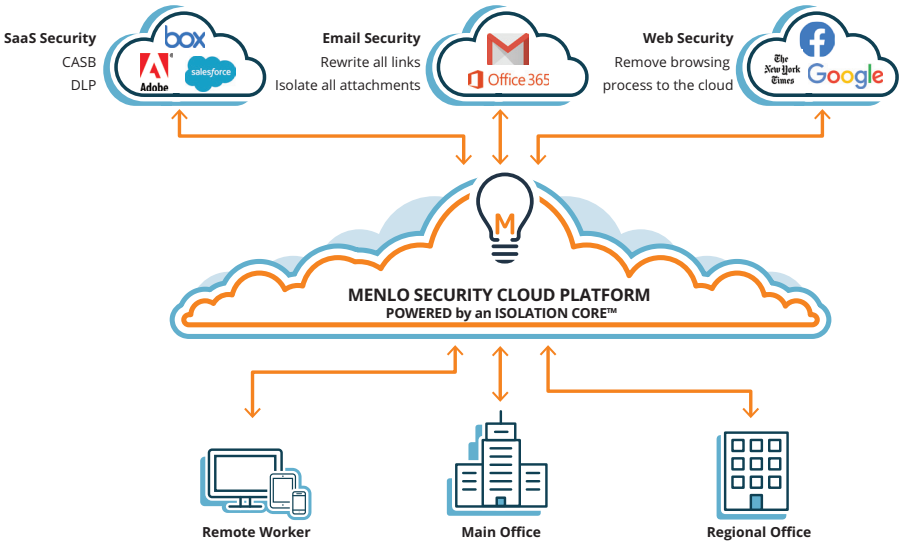
Zero Trust powered by isolation allows government organisations to completely outsmart malware and other web-based threats, giving public servants worry-free, secure access to the tools and information they need to keep the government running.

The Menlo Security Isolation-Powered Cloud Security Platform Enables Zero Trust.

Menlo keeps government systems, users and data safe from web-based threats. Our solution works by routing all web traffic through a cloud-based remote browser before delivering only safe content to the endpoint. It doesn't matter if the web content is good or bad, categorized or uncategorized, because our isolation-powered platform assumes that all content is malicious and treats it accordingly.

Based in the cloud, Menlo's Cloud Security Platform is incredibly agile—scaling to be as large as the government's cloud while accommodating fluctuating workforces, citizen needs or traffic volume without requiring complex configuration or clients deployed on endpoint devices.

Zero Trust Internet Architecture



Traditional security architectures and philosophies don't work anymore; cybercrime is still growing despite the huge number of security tools in an organisation's stack. Why is this the case? How can we stop it?

Completely Eliminate Malware and Other Web-Based Threats.

Today's political climate makes government IT systems a tempting target. Unfortunately, traditional detect-and-respond approaches to cybersecurity are ill equipped to deal with the increasing volume and sophistication of today's attacks. Instead, Australia's government organisations should take a modern approach to securing government work. Menlo's Zero Trust approach powered by isolation prevents malware and other web-based attacks from accessing the endpoint without hindering application access or productivity. No attacks. No breaches. No worries.

To find out how Menlo Security can provide your organisation with protection against cyberattacks while giving secure Internet access worldwide, visit menlosecurity.com or contact us at ask@menlosecurity.com.

About Menlo Security

Menlo Security enables organisations to outsmart threats by completely eliminating attacks and fully protecting productivity with a one-of-a-kind, isolation-powered cloud security platform. It's the only solution to deliver on the promise of cloud security—by providing the most secure Zero Trust approach to preventing malicious attacks, by making security invisible to end users while they work online and by removing the operational burden for security teams. Now organisations can offer a safe online experience, empowering users to work without worry while they keep the business moving forward.

© 2021 Menlo Security, All Rights Reserved.

Contact us
menlosecurity.com
(+61) 2 401 494 641
ask@menlosecurity.com