Cloud Made Simple

The Zero Trust Security Model

Can you afford to take the risk?

1300 30 4047
cloudmadesimple.com.au

Commercial in Confidence

Australia • New Zealand • United Kingdom • United States

Protect your business from Cybercrime

Cloud applications and the mobile workforce have redefined the security perimeter. Employees are bringing their own devices and working remotely. Data is being accessed outside the business network and shared with external collaborators such as partners and vendors. Business applications and data are moving from on-premises to hybrid and cloud environments.

The new perimeter isn't defined by the physical location(s) of the organization—it now extends to every access point that hosts, stores, or accesses corporate resources and services. Interactions with corporate resources and services now often bypass on-premises perimeter-based security models that rely on network firewalls and VPNs. Organizations which rely solely on on-premises firewalls and VPNs lack the visibility, solution integration and agility to deliver timely, end-to-end security coverage.

Today, organizations need a new security model that more effectively adapts to the complexity of the modern environment, embraces the mobile workforce, and protects people, devices, applications, and data wherever they are located. This is the core of Zero Trust.

The Cloud Made Simple Zero Trust approach is designed as an integrated security philosophy and end-to-end strategy.

Zero Trust Overview

Instead of believing everything behind the business firewall is safe, the Zero Trust model assumes breach and verifies each request as though it originates from an uncontrolled network. Regardless of where the request originates or what resource it accesses, Zero Trust teaches us to "never trust, always verify."

In a Zero Trust model, every access request is strongly authenticated, authorized within policy constraints and inspected for anomalies before granting access. Everything from the user's identity to the application's hosting environment is used to prevent breach. We apply micro-segmentation and least privileged access principles to minimize lateral movement. Finally, rich intelligence and analytics helps us identify what happened, what was compromised, and how to prevent it from happening again.

Building Zero Trust into your Business

The Cloud Made Simple Zero Trust approach extends throughout the entire digital estate and serves as an integrated security philosophy and end-to-end strategy. This is done by implementing Zero Trust controls and technologies across six foundational elements: identities, devices, applications, data, infrastructure, and networks. Each of these six foundational elements is a source of signal, a control plane for enforcement, and a critical resource to be defended. This makes each an important area to focus investments.

Identities

Identities – whether they represent people, services, or IOT devices – define the Zero Trust control plane. When an identity attempts to access a resource, we need to verify that identity with strong authentication, ensure access is compliant and typical for that identity, and follows least privilege access principles.

Devices

Once an identity has been granted access to a resource, data can flow to a variety of different devices—from IoT devices to smartphones, BYOD to partner managed devices, and on-premises workloads to cloud hosted servers. This diversity creates a massive attack surface area, requiring we monitor and enforce device health and compliance for secure access.

Applications

Applications and APIs provide the interface by which data is consumed. They may be legacy on-premises, lift-and-shifted to cloud workloads, or modern SaaS applications. Controls and technologies should be applied to discover Shadow IT, ensure appropriate in-app permissions, gate access based on real-time analytics, monitor for abnormal behavior, control of user actions, and validate secure configuration options.

Data

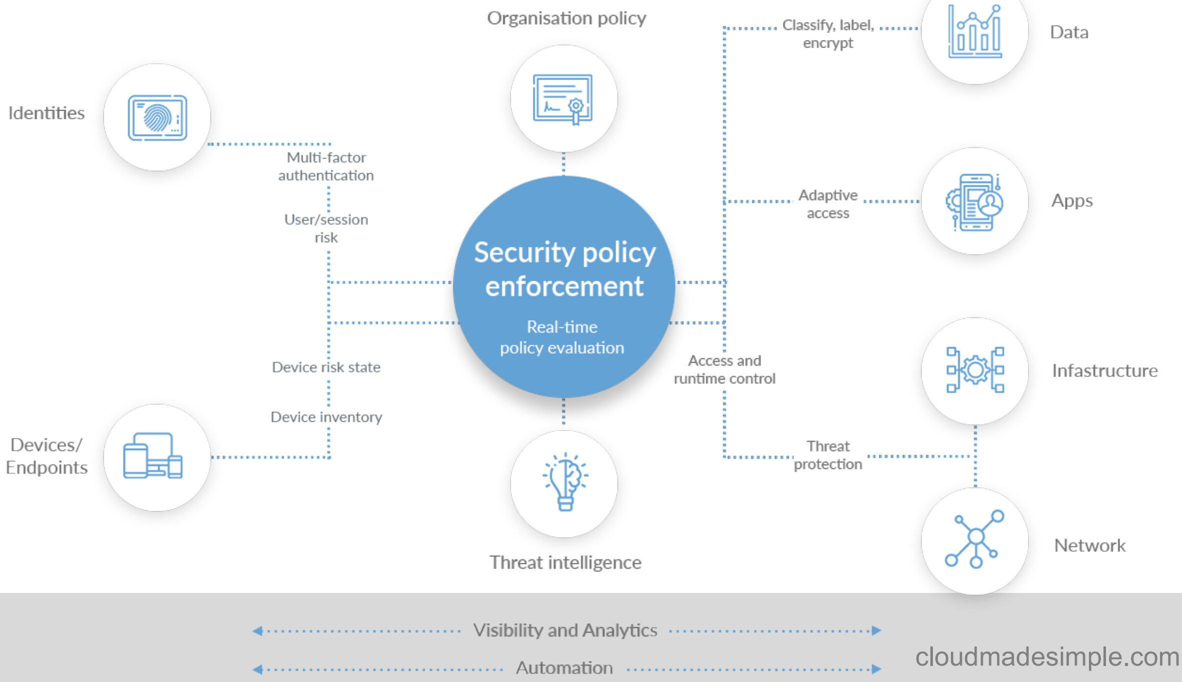
Ultimately, security teams are focused on protecting data. Where possible, data should remain safe even if it leaves the devices, apps, infrastructure, and networks the organization controls. Data should be classified, labeled, and encrypted, and access restricted based on those attributes.

Infrastructure

Infrastructure (whether on-premises servers, cloud-based VMs, containers, or micro-services) represents a critical threat vector. Assess for version, configuration, and JIT access to harden defense, use telemetry to detect attacks and anomalies, and automatically block and flag risky behavior and take protective actions.

Networks

All data is ultimately accessed over network infrastructure. Networking controls can provide critical “in pipe” controls to enhance visibility and help prevent attackers from moving laterally across the network. Networks should be segmented (including deeper in-network micro segmentation) and real-time threat protection, end-to-end encryption, monitoring, and analytics should be employed.



CMS
LOOKING AFTER YOU

Microsoft
Gold Partner

Get in Touch

For more information about how Cloud Made Simple can implement your Zero Trust Security Plan, please reach out to us:

support@cloudmadesimple.com

www.cloudmadesimple.com

Australia 1300 304047

New Zealand 0800 968748

United Kingdom 0161 706 0352