NATILIK

Protect sensitive data at scale with Duo

Secure access starts with zero trust

Why Zero Trust?

The rise of a cloud-connected, mobile and remote workforce has put the visibility and control of users and devices outside your organization's physical walls. The security perimeter has expanded, making it more difficult for IT teams to verify user identities, and the trustworthiness of their devices, before granting both access to enterprise applications and data.

Compromised user credentials are a prime security risk, allowing cyber attackers to easily access systems through phishing, brute force and other password attacks.

Duo's 2018 Trusted Access Report found that 63% of phishing attacks successfully captured user credentials.

Zero trust treats every access attempt as if it originates from an untrusted network to ensure your data stays secure.

Every user and device is authenticated before access is granted to any application.

5 Steps to Zero Trust

1.

Establish user trust

Multi-Factor Authentication (MFA) is a scalable solution to establish user trust, protecting against compromised credentials, phishing and other password based attacks.

2.

Gain visibility into user devices

The ability to identify every device that accesses your applications allows you to see which may be introducing risks such as out-of-date software.

3.

Establish device trust

At the time of login, check the trustworthiness of all user devices accessing your applications, whether corporate or personally-owned devices.

4.

Enforce adaptive policies

Enforce contextual access policies that assess risk based on factors like location, user role, device type, etc., to gain dynamic control and allow only the minimum amount of access required for a user to do their job.

5.

Enable secure acces to all apps

Implement MFA and device insight to enable secure access to all different types of applications, services and platforms. This combination makes it harder for unauthorised users to login into your applications.

Duo security zero trust model for the workforce

Establish user trust
Verify the identity of your users with strong MFA that provides flexible, broad coverage for every type of user.

Full visibility
Get a single view of overall security status and detailed endpoint visibility of all your users' devices.

Enforce adpative policies
Duo gives you the control to limit access from risky endpoints and comply with local data privacy laws based on conditional risk.

Enable secure access to all apps
Duo provides easy set up with out-of-the-box integrations with all types of apps – from legacy to modern to custom tools.

Establish device trust
Duo provides administrators with visibility into user and device risks and provides the ability to apply controls that prevent threats and risky devices from gaining access to sensitive applications and data.

Why Natilik?

Capability
Expertise in all IT and Communication technologies, with a deep understanding of the interconnection of security across the whole network.

Consistency
Leading by example: Natilik utilise Duo Security in house and have installed and enabled the platform in their ISO 27001 Accreditation.

Coverage
London HQ and offices in Sydney and New York with 24/7 follow the sun support team to provide a consistent experience globally.

Possible **together.**

Get in touch to find out more about how you can get a free 30 day trial.

London
+44 203 597 8000
hello@natilik.com

New York
+1 646 766 8600
hello@natilik.com

Sydney
+61 282 945 500
hello@natilik.com

www.natilik.com