CISCO DUO for...

Cyber Liability Insurance

Starting with multi-factor authentication, Duo helps you build a strong proactive security foundation.

THE CHALLENGE:

Securing Against the Unknown

Modern challenges like phishing, ransomware, remote workforces, and personal devices demand increasingly sophisticated cybersecurity practices. Organizations must secure against the unknown and advancing threats while striking a balance between proactive and reactive measures.

Multi-factor authentication (MFA) has proven to be a strong preventative strategy against stolen credentials and brute-force attacks, making it a top criterion requested by cyber insurance companies. However, proactive security means more than an extra step at log-in.

Cyber liability insurance acts as a general line of coverage designed to mitigate losses and costs from a variety of cyber incidents, including data breaches, network damage, and the resulting business interruption.

Factors that impact premium prices may include:

- Size of business, in terms of revenue and number of employees
- Type of business, nature of data accessed, and who is accessing it
- Quantity of sensitive information requiring coverage
- Past insurance claims and existing cybersecurity measures in place

THE SOLUTION:

Duo's Secure & Trusted Access

Duo helps you secure all users, devices, and applications, preventing potentially compromised devices from accessing valuable resources and data. Duo can verify users' identities while ensuring that devices are compliant, up-to-date, and safe before granting access to applications.

01

Easy to Deploy and Use

As a cloud-based solution, Duo integrates with your infrastructure and can roll out enterprise-wide in a few hours.

Duo's login process is designed to be simple for all users without compromising productivity. Flexible authentication methods such as push notifications, tokens, biometrics and more allows users to choose the best fit for their workflow.

Based in the cloud, Duo integrates easily with your existing technology. Admins have access to Duo's support teams and deployment resources and can benefit from Duo's native integrations, easy cloud-based setup, and low-maintenance solution.

02

Build Strong Security Habits

Strong security practices are vital at every level of an organization, from contractors to executives. Along with MFA, security awareness and behaviors across the workforce can help mitigate risk.

Duo Mobile acts as a second authentication factor for users and helps them self-remediate security concerns, while giving admins an overview of device security hygiene. For laptops and desktops, the Duo Health App checks for firewall, encryption, and up-to-date operating systems.

With Duo, admins also gain access controls and complete visibility into endpoint security across all devices, whether personal or corporate-owned. They can check if a device is registered or managed before allowing access.

03

Broad Coverage that Grows

Offering more than 200 out-of-the-box integrations, Duo protects access to both on-premises and cloud-based applications like Office 365, Dropbox, and Cisco VPN.

Duo also scales to meet companies at their security needs, providing offline MFA, compliance-friendly reporting and logs, and the ability to add users and devices at any time.

MFA can pair with single sign-on to create a consistent login workflow across all applications and sync with directories to ensure policies stay current even as the user base changes. No headaches, no interruptions – it just works.

Duo Editions

Feature	Benefit	Duo Essentials	Duo Advantage	Duo Premier
MFA	Protect against stolen credentials and account take over with Duo MFA	✓	✓	✓
Push Phishing Protection	Prevent attackers from bypassing MFA using phishing-resistant FIDO2 authenticators or Verified Duo Push	✓	✓	✓
Single Sign-On	Log in only once to access multiple applications with Duo SSO	✓	✓	✓
Passwordless	Securely log in without a password using Duo Mobile or FIDO2 authenticators	✓	✓	✓
Trusted Endpoints	Check if device is registered or managed before allowing access	✓	✓	✓
Device Health	Check device security posture before granting access. Provide visibility into security health of devices trying to gain access.		✓	✓
Risk-Based Authentication	Dynamically adjusts authentication requirements in real time based on risk signals		✓	✓
Threat Detection	Detect potential on-going attack attempts using machine learning-based Duo Trust Monitor		✓	✓
Remote Access	Securely access private resources without VPN using Duo Network Gateway			✓

CISCO DUO for Cyber Liability Insurance

CONCLUSION

Where Is Cybersecurity Trending?

From ransomware concerns and government mandates to the prevalence of cyber insurance, security is moving toward adoption of a preventative zero trust model – one where security extends beyond the perimeter and into the operations of modern-day hybrid workforces. Zero trust allows you to mitigate, detect and respond to issues across your environment, helping protect against identity-based and other access security risks.

While MFA may seem like an item on an insurance requirement checklist, it has potential to set foundations for a security strategy that's proactive, not reactive. Duo can grow and scale alongside any organization's needs, offering a wide range of workforce cybersecurity solutions that prepares for the risks and regulations of today and tomorrow. In an uncertain world, Duo can help any organization set a precedent of best practices.

"Duo was the first vendor that put the zero trust model into practice with multi-factor authentication. It not only looks after MFA, it sees who the user is, what device they're using, whether it's a trusted device. Duo ties it all together in one product, especially for MSPs, and it makes it easy to manage customers of different sizes"

Ian O'Connell
Security Operations Center Team Lead, CommSec

© 2023 Cisco Systems, Inc. and/or its affiliates. All rights reserved.