

Achieving Zero Trust with Cisco Duo MFA

A Comprehensive Guide to Strengthening Your Security



Sorry to Disappoint You.

Your Business is Not Immune to Cyberattacks.

The ruthless cyberattacks have not spared even the planet's biggest corporations, including the big tech poster boys.

The stakes have never been higher. In this unforgiving digital battleground, only the vigilant survive. With every device connected to this or that network, businesses must strengthen their security at every turn to survive the onslaught.

PASSWORDS are PASTWORDS.

Insert all your dollars, and hashtags, make it alphanumeric, and use upper-lower cases, they are still fallible.

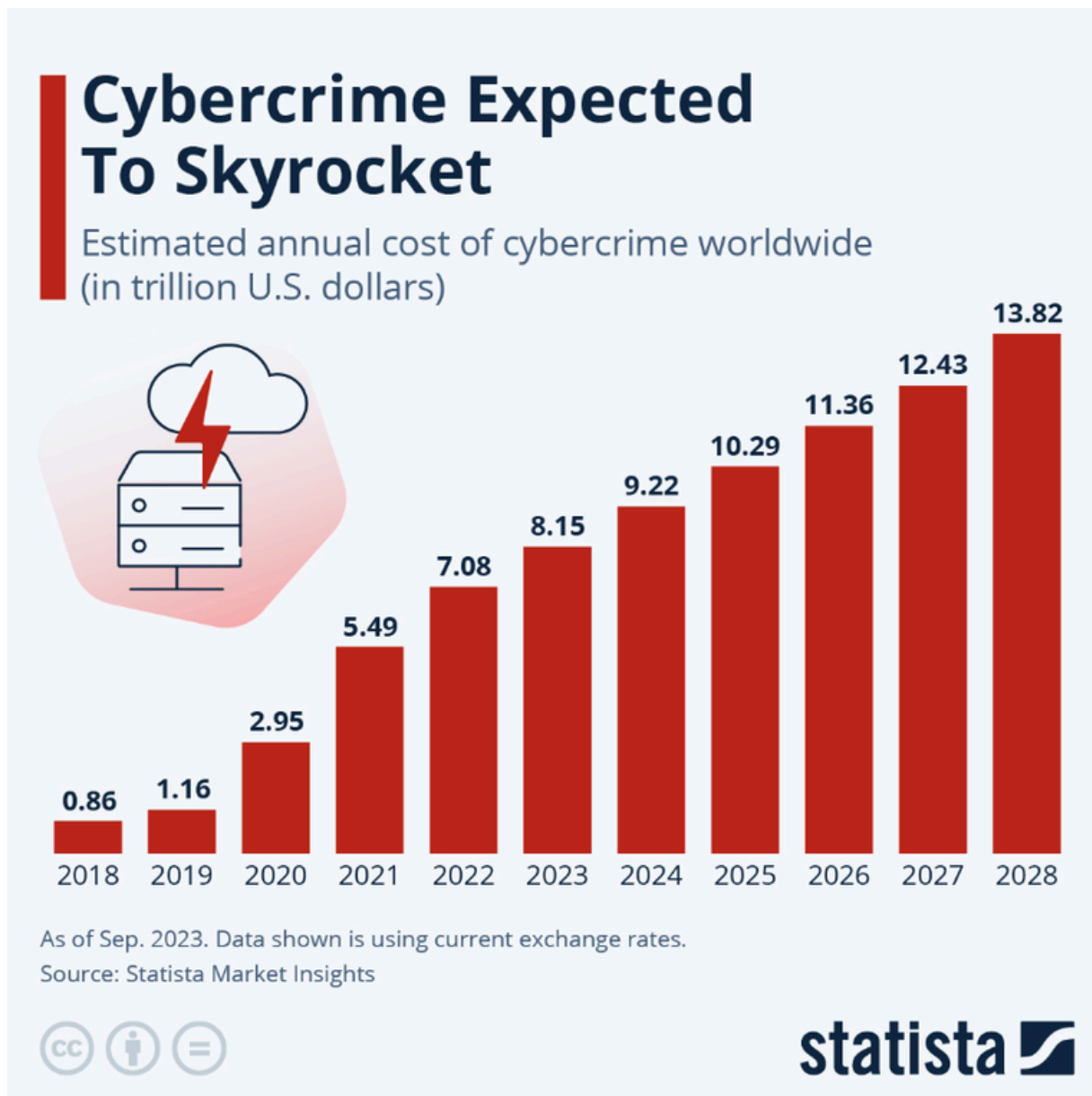
This is where Multi-Factor Authentication (MFA) comes into play

If a password is the seatbelt, MFA is the airbag. MFA adds an extra layer of defence, ensuring only verified users and devices can access your systems. MFA integrates seamlessly with a Zero Trust architecture, verifies identities and secures every access point - no matter where the user or device is located.

In this white paper, we will explore how Cisco Duo MFA plays a critical role in implementing Zero Trust security. We'll understand the principles of Zero Trust, the challenges of traditional security models, and how MFA offers superior protection.

The Hard Numbers

According to Statista Market Insights data, the financial impact of cybercrime increased by over 847% from \$0.86 trillion in 2018 to \$8.15 trillion in 2023. What lies ahead is no less alarming. The report predicts this number to go up by a whopping 70%, reaching \$13.82 trillion by 2028.



Infographic Source: Statista

 Unlock Our Exclusive
White Paper

Achieving Zero Trust with
Cisco Duo MFA

What is the ‘Cost of Cybercrime’?

It's not only about money. The cost of cybercrime refers to the total impact caused by malicious cyber activities on businesses, governments, and individuals, including direct and indirect expenses:

- **Financial Losses:** Theft of money, intellectual property, or data through hacking, phishing, quishing, ransomware attacks, or other forms of cybercrime.
- **Operational Disruption:** Downtime, infrastructural damage, and halted operations.
- **Legal and Regulatory Fines:** Costs incurred from non-compliance with data protection regulations after a breach, such as fines under the General Data Protection Regulation (GDPR) or other privacy laws.
- **Incident Response Costs:** Expenses related to identifying, investigating, and mitigating cyberattacks, including forensics and cybersecurity services.
- **Reputational Damage:** Loss of customer trust and brand image.
- **Lost Business Opportunities:** Long-term effects, such as lost revenue from customers who no longer trust the organisation after a breach.
- **Insurance Premiums:** The rising cost of cyber insurance coverage due to the increasing threat of cybercrime.



Understanding Zero Trust Architecture

The Zero Trust model is founded on the idea that trust should never be implicit, regardless of where a request originates. This stands in stark contrast to traditional perimeter-based security models, where any user or device inside the network is automatically trusted.

With the rise of sophisticated cyberattacks, insider threats, and the increased fluidity of modern workplaces, organisations can no longer afford to make such assumptions. The Zero Trust approach emphasizes strict identity verification, device validation, and access controls before granting permission to any part of the network.

The Zero Trust Approach Guilty Till Proven Innocent!

As remote work and cloud adoption increase, traditional security methods are not enough to protect digital assets. The security approach that once focused on keeping external threats out is redundant because internal networks are now just as vulnerable.

In the wild world of cybersecurity, the Zero Trust approach works like a seasoned sheriff. It doesn't take any network for granted, treating every device and user as a person of interest. Every request - whether internal or external - is treated with suspicion until it proves its innocence. No one gets a free pass.



Zero Trust has emerged as a paradigm shift in how organisations approach cybersecurity. There is no such thing as a secure perimeter. Not anymore. The "trust but verify" model has failed us.

The new and improved model is:
never trust, always verify.

IDC on Zero Trust Adoption: According to IDC, organizations that adopt Zero Trust architectures can reduce their security incidents by up to 50%. This is achieved through enhanced visibility, strict access controls, and continuous monitoring, which are core components of the Zero Trust model.

Here's a simple breakdown of Zero Trust architecture:

No Assumptions

It doesn't assume anyone, or anything is safe, even if they're inside the network

Verify Everything

Every device and user must prove they are trustworthy before they can access anything

Constant Vigilance

It continuously checks and rechecks credentials to ensure nothing suspicious slips through

Think of it like a bouncer at a club who checks everyone's ID, even if they are regulars. No one gets in without proving they belong there!

The Four Key principles of Zero Trust include:

1. Continuous Verification

Every access request, regardless of origin, must undergo verification. This is done through constant monitoring and re-authentication

2. Least Privilege Access

Users and devices are only given the minimum level of access necessary to perform their tasks, limiting the scope of potential breaches

3. Micro-Segmentation

The network is divided into smaller zones with tight access controls, preventing lateral movement within the network in the event of a breach

4. End-to-End Encryption

All data moving between devices, applications, and the cloud should be encrypted to ensure privacy and integrity

In a Jan 2024 article, Forrester emphasises that Zero Trust is the de facto security strategy for modern organisations. It requires continuous, contextual, risk-based verification across users and their associated devices to prevent unauthorised access.

Challenges with Traditional Perimeter-Based Security Models

Perimeter-based, legacy security models guard the borders of a network from outside threats. But once something gets inside, it's trusted forever without further checks, leading to significant vulnerabilities. Some major challenges of perimeter-based security models include:

Trust Assumptions

Users and devices inside the perimeter are automatically trusted, even if they have been compromised. This creates a blind spot for insider threats

Complex Environments

Modern organisations use cloud, remote access, and third-party integrations, which makes it difficult to define a clear network perimeter

No Granular Control

Traditional models often do not provide granular controls to monitor and restrict user actions once they are inside the network. If a bad actor gains access, it can move laterally across the network easily

Increased Attack Surface

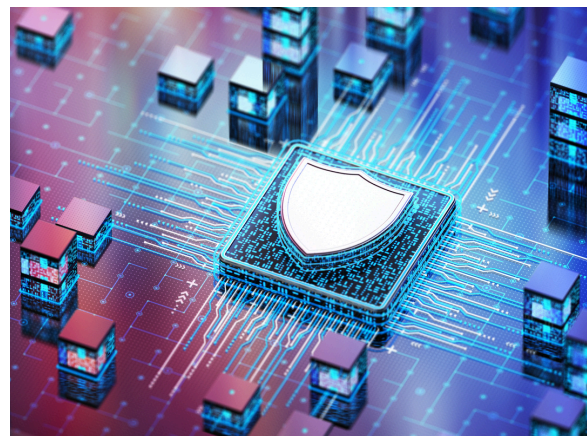
With mobile devices, remote work, and cloud adoption, organisations have a growing attack surface that is difficult to defend through a perimeter-based approach

Role of Multi-Factor Authentication (MFA) in Zero Trust

A key part of Zero Trust is the concept of strong authentication. Just a username and password aren't enough. MFA requires users to verify their identity in multiple ways before accessing network resources, every single time. This helps prevent unauthorised access, even if the passwords are compromised.

Why Authentication is Critical to Zero Trust

In a zero-trust model, the authenticity of every user and device must be continuously verified. Traditional single-factor authentication methods, such as passwords, are easily compromised, especially when the attacks are becoming more sophisticated by the day. Attackers frequently exploit stolen or weak passwords, making additional layers of authentication critical.



MFA addresses these vulnerabilities by adding additional layers of security that require users to present at least two of the following:

Something they know

A password or PIN

Something they have

A physical token, smartphone, or a security key to deliver a unique code or a one-time password (OTP)

Something they are

Biometrics, like a fingerprint or facial recognition

This additional layer significantly reduces the likelihood of unauthorised access, even if one factor (such as a password) is compromised.

How MFA Fits into the Zero Trust Framework

Besides repeated checks, MFA uses risk-based authentication. This means the level of access or verification steps can change based on how risky a request appears. In practice, MFA ensures:

- **Secure Access for Remote Workers:** Employees can securely access network resources from any location, without increasing security risks.
- **Protection Against Credential Theft:** Even if credentials are compromised, unauthorised access is prevented because attackers would need access to additional factors, like a code delivered on a phone or security token, or biometric data.
- **Device Trust and Health Verification:** MFA can be combined with device health checks to verify not only the user but also the security posture of the device being used for access.

Cisco Duo MFA as a Key Component of Zero Trust

Cisco Duo MFA aligns perfectly with Zero Trust principles by ensuring that only verified users and trusted devices can access important resources. It's a strong solution for securing remote workers, protecting cloud apps, and defending against advanced cyber threats.

Beyond strong authentication, Cisco Duo offers better visibility into device security and adaptable security policies, making it a comprehensive tool for modern cybersecurity needs.



Why Cisco Duo MFA?

With over a billion monthly user authentications, Cisco Duo is One of the world's most trusted MFA solutions. With its robust functionality focused on verifying user identity and device health, Duo enhances security across distributed networks, helping organisations establish a more resilient security posture.

Introduction to Cisco Duo's Features

Cisco Duo MFA offers a variety of features that make it an essential tool for Zero Trust security. Key features include:



Two-Factor Authentication (2FA)

Duo supports multiple methods of two-factor authentication, including push notifications, security keys, one-time passwords (OTPs), and biometrics.



Device Trust

Cisco Duo ensures that only devices meeting predefined security criteria (e.g., updated operating systems, and security patches) can access applications.



Adaptive Authentication

Based on the context of the access request (location, device, user behaviour), Cisco Duo can dynamically adjust authentication requirements, making security both flexible and effective.



Single Sign-On (SSO)

Cisco Duo MFA integrates with a wide variety of platforms and services, allowing users to securely access multiple applications with a single login.



User and Device Visibility

Duo provides detailed insights into user authentication and device health, allowing IT teams to quickly identify and respond to security risks.



How Cisco Duo Ensures Secure Access in a Zero-Trust Environment

In a Zero Trust environment, every access request is subject to strict verification. Cisco Duo MFA enhances this process by offering granular control over who and what is allowed into the network. Here's how Cisco Duo ensures secure access:

User Identity Verification

Duo verifies that the person attempting to access resources is who they claim to be, using multiple authentication factors

Device Health Verification

Duo checks that the device being used meets security standards (e.g., is free of malware, has encryption enabled, etc.) before granting access

Adaptive Policies

Cisco Duo allows security teams to create context-aware access policies that adjust the security requirements based on factors such as user location or risk level

The Role of Adaptive Authentication and Device Trust

Cisco Duo's adaptive authentication goes beyond basic multi-factor authentication by adjusting security requirements based on factors like user behaviour, location, and device security. This keeps the process secure and smooth for legitimate users.

Additionally, device trust features ensure only healthy, trusted devices can access important resources, blocking compromised or untrusted devices from causing security issues.

Implementing Zero Trust with Cisco Duo

Implementing Zero Trust with Cisco Duo is more than just adding MFA. It needs careful planning to integrate Duo's features into the organisation's security setup. Companies must evaluate their current security, identify key assets, and use Duo at all access points to ensure strong security and compliance with Zero Trust principles.

Integrating Cisco Duo MFA into a Zero Trust Model A Step-by-Step Guide

1. Start with an Assessment

The first step is to take a close look at your current security setup and make a priority list. Find out where the biggest risks are, like remote access points or cloud apps, and identify the most critical assets that need protection.

2. Deploy Duo MFA to Key Systems

Once you know what's at stake, start integrating Duo MFA into the most sensitive applications. Whether it's your SaaS tools, VPNs, or internal systems, Cisco Duo works with almost everything, so getting it set up across these areas is seamless.

3. Enforce Device Trust

Duo's device health checks help ensure that only trusted devices can access your network. Create policies to block any compromised devices that could put your system in jeopardy.

4. Customise Security Policies

1. Cisco Duo's adaptive security lets you tailor authentication requirements based on the situation. If someone tries to log in from a new or risky location, you can add extra steps to confirm their identity.

5. Monitor and Adjust

Duo's reporting tools give you real-time insight into user and device behaviour. Keep an eye on what's happening, fine-tune your policies as needed, and make sure your security strategy evolves with emerging threats.



Best Practices for Using Cisco Duo MFA



Start with Privileged Accounts

First things first - apply MFA to the accounts that hold the most power, like those of admins and top brass. These are prime targets for attackers, so securing them should be the top priority.



Educate Your Team

Regular security training is key. Make sure employees understand why MFA is important and how to use Duo correctly to protect their accounts and the company.



Keep Policies Up-to-Date

Zero Trust isn't a one-and-done strategy. Regularly review and tweak your Duo policies to stay ahead of new security threats and changes in your organisation.



Use Phishing-Resistant Methods

Go beyond basic authentication. Opt for methods like security keys or biometrics that are much harder for attackers to bypass using phishing or social engineering tactics.

Benefits of Zero Trust and MFA

Adopting a Zero Trust security model with Cisco Duo MFA delivers both immediate and long-term protection. It reduces unauthorised access, prevents threats from spreading, and ensures every access request is fully vetted. By doing so, organisations significantly improve their security posture.

Key benefits include:

- **Reduced Attack Surface:** By micro-segmenting networks and limiting access to only what's necessary (least-privilege access), you drastically minimise potential entry points for attackers. This ensures that fewer systems are vulnerable.
- **Protection Against Credential Theft:** Even if attackers manage to steal login credentials, Duo's MFA stops them in their tracks. Without the required additional authentication steps, those credentials are practically useless to them.
- **Continuous Monitoring and Enforcement:** With Cisco Duo and Zero Trust, you get real-time insights into user and device activity. This enables faster detection of suspicious behaviour and allows immediate response to any potential threats.
- **Minimised Insider Threat Risks:** Insider threats are among the hardest to detect. Zero Trust enforces constant re-verification, even for internal users, significantly reducing the risk of an insider attack. Duo's MFA adds an extra layer of security, even if insider credentials are compromised.
- **Protection from Lateral Movement:** Once attackers breach a network, they often move sideways to access critical systems. Zero Trust, combined with Cisco Duo MFA, prevents this lateral movement through strict access controls and micro-segmentation, blocking them from gaining more ground.
- **Compliance with Regulatory Standards:** Many regulatory frameworks, such as GDPR, HIPAA, and PCI-DSS, require MFA and strong access control. By using Cisco Duo within a Zero Trust framework, organisations can easily meet these requirements, reducing regulatory risks and enhancing data protection.

Conclusion

In an era of ever-evolving cyber threats, the old ways of protecting your business just don't cut it anymore. This is where Cisco Duo MFA shines, fitting perfectly into a Zero Trust model. By verifying every user and device at every access point, Duo MFA strengthens your security from all angles, ensuring no one gets in without proving they belong.

With remote work on the rise, cloud apps becoming the norm, and cyberattacks getting more sophisticated, securing your business means locking down every access point. Zero Trust gives you the power to do that, safeguarding your systems and data from both internal and external threats.

Waiting to adopt Zero Trust is no longer an option. Cyber risks aren't going away, and companies that don't act now are leaving themselves open to future attacks. Cisco Duo MFA is your key to a stronger, more resilient security strategy that will protect your business now and in the future.

Start your Zero Trust and MFA journey with Proactive Data Systems today and build the security foundation your business needs to grow confidently.

The Proactive Partnership: Building Your Digital Future in India

Proactive Data Systems is an enterprise IT infrastructure and services company. For more than three decades, the company has designed, deployed, and operated the technology foundations behind some of India's most demanding enterprise environments, from regulated industries to large distributed operations.

Founded in 1991, Proactive serves more than 1,500 customers, from fast-growing businesses to Fortune 500 enterprises, across banking and financial services, manufacturing, healthcare, public sector, IT and ITES, retail, education, and global capability centres. Our work spans enterprise networking, cybersecurity, cloud and AI-ready data centres, collaboration platforms, structured cabling, and managed services.

A Cisco Preferred Partner under the Cisco 360 Partner Program, Proactive is recognised across the Networking, Security, Collaboration, Cloud & AI, and Services portfolios, and is a Cisco Advanced Customer Experience Specialised Partner. The company is ISO 9001:2015 and ISO/IEC 27001 certified, and engineers solutions in partnership with Dell, Nutanix, NetApp, Palo Alto Networks, Fortinet, VMware, Veeam, and CommScope.

Headquartered in Delhi NCR, with offices in Mumbai, Bengaluru, Pune, Hyderabad, Indore, and Singapore.

To learn more about our solutions, write to us at pro@proactive.co.in

 www.proactive.co.in

PROACTIVE[™]
Enhancing Digital Experience