WatchGuard AuthPoint Multi-Factor Authentication (MFA) Solution Competitive Validation Testing Summary Report

July 2022

SR220610D

Contents

1.0 Executive Summary

MFA (Multi-Factor Authentication) enhances how users verify their identity and assists in protecting sensitive information within the user accounts. It also guards against brute force attacks and stolen usernames and passwords. This is done by requiring one or more additional verification factors in combination with something the user knows (e.g. PIN number) and something the user has (e.g. mobile device). The most common ways that MFA can be implemented is through TOTP (Time-Based One-Time Passwords), Push Notifications, SMS, and email.

Customers are looking for a reasonably priced MFA solution with well-rounded functionality that is easy to use. WatchGuard engaged Miercom to validate its AuthPoint solution's simple deployment of MFA security – abundant in features that its competitors charge for with separate licenses and subscriptions. This MFA solution was tested competitively with two similar solutions: Cisco Duo and Azure MFA – for the following:
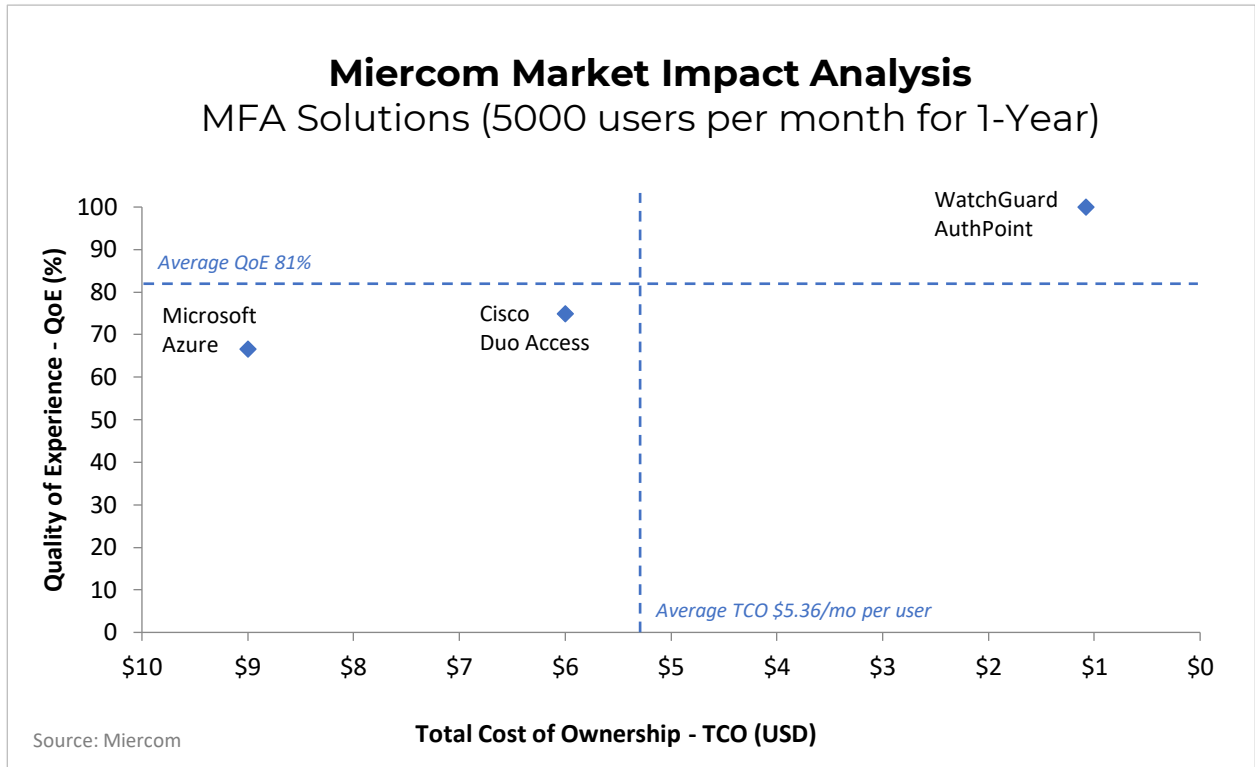
- Authentication Methods
- Provisioning and User Experience
- Deployment Efficacy
- Security and Risk-Based Authentication
- Total Cost of Ownership

WatchGuard proved its competitive edge as the most affordable solution that included exceptional MFA functionality with an easy-to-use interface – for both users and administrators. While its competition could sometimes offer the same functionality, it came at the cost of meticulous interfaces and documentation that made for a challenging first-time experience.

Key Findings

- **Remote Work Made Easy.** WatchGuard had the smoothest Single Sign-On (SSO) portal setup and usage, making remote work with secure login and access to applications effortless.
- **Seamless User Experience.** WatchGuard's hallmark differentiators from its competitors were its intuitive interface, helpful guides, and single-click setups – making it the top choice for first-time users.
- **Modern Authentication Methods.** WatchGuard had the most straightforward setup and use of risk-based authentication (RBA) and secure authentication contingency. RBA was very simple to set up, even while providing high granularity. Secure authentication contingency with WatchGuard provided a challenge/response process for higher security.
- **Mobile DNA for Secure Migration.** WatchGuard was the only vendor to offer a footprint-based migration through the cloud, for the highest level of security against hackers – across all platforms as soon as activation was complete.

- **High Value and ROI.** WatchGuard showed highest value with its quality of experience. Compared to other solutions, WatchGuard delivered a rich set of native features with its one-time purchase. Other solutions come with added complexity and cost by requiring extra subscriptions that are priced separately.

Miercom Market Impact Analysis
MFA Solutions (5000 users per month for 1-Year)

Quality of Experience - QoE (%) vs. Total Cost of Ownership - TCO (USD)

- WatchGuard AuthPoint: ~$1, 100%
- Average QoE 81%
- Microsoft Azure: ~$9, 67%
- Cisco Duo Access: ~$6, 75%
- Average TCO $5.36/mo per user

Source: Miercom

Quadrants are formed based off average values. WatchGuard was in the upper right quadrant, showing it had the highest QoE of competing vendors at the lowest cost. Cisco and Microsoft do not offer nearly the same amount of functionality, ease of use, or intuitive interface as WatchGuard.

Based on our findings, WatchGuard AuthPoint Multi-Factor Authentication Solution proved competitively superior in authentication, provisioning, deployment, and security testing, earning the ***Miercom Performance Verified*** certification in recognition of its high TCO value, user-friendly, and effective MFA capabilities.

Robert Smithers
CEO, Miercom

2.0 Test Summary

✅	⚠️	❌
Passed	Passed but with notable adverse behavior	Fail

WatchGuard AuthPoint	Cisco Duo	Microsoft Azure
5.1 Time-Based OTP (TOTP)		
✅	⚠️	✅
5.2 Offline Multi-Factor Authentication		
✅	✅	✅
5.3 Push-based Authentication		
✅	✅	✅
5.4 Pull Authentication		
✅	✅	✅
5.5 Secure Hardware Token		
✅	⚠️	⚠️
6.1 Token Provisioning		
✅	✅	✅
6.2 User Synchronization		
✅	✅	⚠️
6.3 Mobile Token Enrollment		
✅	✅	✅
6.4 Secure Migration		
✅	⚠️	⚠️
6.5 Mobile App Ease of Use		
✅	✅	✅
7.1 Ease of Deployment		
✅	✅	❌
7.2 Configuration Wizards		
✅	❌ *Product did not support this feature.*	⚠️
7.3 Single Sign-On (SSO)		
✅	✅	✅

7.4 SSO Client / SAML Support		
✅	✅	✅
7.5 Windows and macOS Login Protection		
✅	✅	⚠️
7.6 Remote Desktop Protocol (RDP) Login Protection		
✅	✅	⚠️
7.7 VPN Protection		
✅	✅	⚠️
7.8 Push Verification / Push Test / Helpdesk Tools		
✅	✅	❌ *Product only supported feature with a paid subscription.*
7.9 Time to Initially Deploy		
✅	✅	❌
7.10 Breadth of Supported Platforms		
✅	✅	✅
8.1 Risk-based Authentication (RBA)		
✅	⚠️	⚠️
8.2 Secure Authentication Contingency		
✅	✅	✅
8.3 Mobile DNA Addition		
✅	❌ *Product did not support this feature.*	❌ *Product did not support this feature.*
8.4 Audit Logs		
✅	✅	⚠️

3.0 Solutions Tested

**WatchGuard AuthPoint MFA &
Mobile Application**
version 1.16.1

AuthPoint is a cloud-based MFA solution offering powerful, user-friendly multi-factor authentication via mobile device DNA, matching the authorized user's phone when granting access to systems and applications.

Cisco Duo Access
version 4.4.0.0

Cisco Duo Access provides an easy-to-use, secure mobile authentication application for quick, push notification-based approval to verify user identity with hardware for devices, such as smartphone, smartwatch and U2F token support.

**Microsoft Azure Premium P2 &
Authenticator Application**
version 6.2112.8213

Microsoft Azure helps safeguard access to data and applications while maintaining simplicity for users. It provides additional security by requiring a second form of verification and delivers strong authentication through a range of easy-to-use validation methods.

4.0 How We Did It

Miercom engineers simulated a test environment to represent a real-world scenario, where mobile devices have the client component of the MFA solution applied and enabled. All three tested solutions included the minimum license needed, and the main elements of each environment were as follows: Central cloud MFA management, three (3) added test users with a corresponding individual mobile device, One (1) hardware token, Two (2) endpoints, and a Windows Server (for specific use cases).

Each user's mobile device had all three MFA solutions downloaded.

4.1 Product Setup

WatchGuard AuthPoint was setup by downloading the application via PlayStore or AppStore and activating via a generated QRcode. **Cisco Duo Access** was remotely accessed; licensing was not performed by Miercom. All other testing was performed as a remote validation on an existing account. **Microsoft Azure** was set up using a cloud account via a required Microsoft account, a downloaded Microsoft Authenticator Application via PlayStore or AppStore, and third-party hardware tokens – as well as multiple subscription and licenses to perform different activities.

4.2 Test Bed Overview

Source: WatchGuard 2022
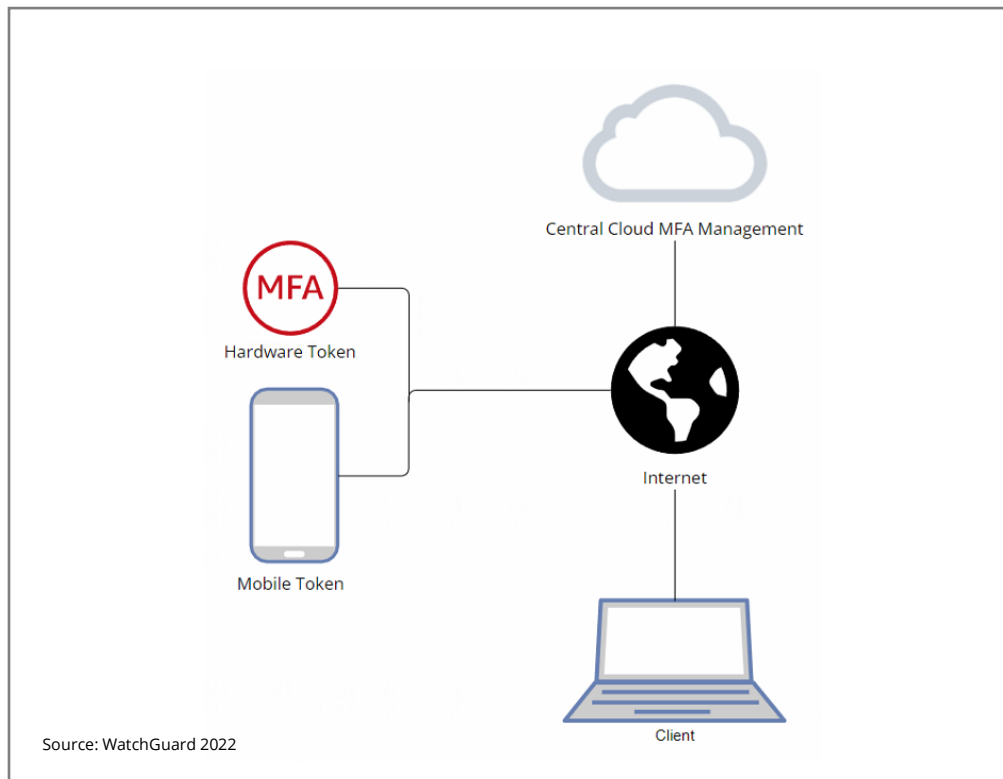
A general topology of testing an MFA solution is shown above. This topology was used for all three tested solutions. Each solution was deployed with a hardware token, a mobile device, and an endpoint – all managed through the cloud. Additional individually configured servers, and their gateways/proxies, were added to the cloud management.

5.0 Authentication

5.1 Time-Based One-Time Password (TOTP)

TOTP is a uniquely generated, single-use passcode that is valid for a limited duration that expires. Tokens change, or expire, every 30 seconds.

WatchGuard AuthPoint	Cisco Duo	Microsoft Azure
✅	⚠️	✅

The TOTP method was supported by **WatchGuard** and **Microsoft** only. **Cisco** provides event-based OTP, which doesn't expire and is therefore less secure.

> **WatchGuard AuthPoint and Microsoft Azure were
> the only vendors to natively support TOTP.**

5.2 Offline Multi-Factor Authentication

Offline multi-factor authentication is useful for working machines where Internet access may not be available.

WatchGuard AuthPoint	Cisco Duo	Microsoft Azure
✅	✅	✅

> **All MFA solutions supported offline sign-in, despite having no Internet connection.
> Some solutions also support a challenge/response feature in addition to OTP, which
> provides better security against social engineering. An encrypted QRcode (readable
> only from the user device) is one example of a more secure offline authentication
> method that not a lot of MFA solutions offer.**

5.3 Push-Based Authentication

Push-based authentication verifies users by securely sending a notification. The user verifies their identity by responding to a presented challenge to access the service.

WatchGuard AuthPoint	Cisco Duo	Microsoft Azure
✅	✅	✅

WatchGuard showed the most competent push authentication – displaying user, timestamp, and geolocation. **Cisco** proved inconsistent and **Microsoft** was extremely limited.

WatchGuard Competitive Advantage

WatchGuard AuthPoint showed the most competent approach – displaying the users, timestamp, and geolocation information.

All MFA solutions supported push notifications.

5.4 Pull Authentication

Pull authentication allows users to check for pending notifications (e.g. if notifications are delayed).

WatchGuard AuthPoint	Cisco Duo	Microsoft Azure
✅	✅	✅

All MFA solutions supported pull notifications.

5.5 Secure Hardware Token

Secure hardware token is a physical device used to authorize access.

WatchGuard AuthPoint	Cisco Duo	Microsoft Azure
✅	⚠️	⚠️

WatchGuard successfully activated a new hardware token in less than one minute. Its tokens are highly secure – never revealing any secrets as most vendors do, leaving tokens easily cloned. **Cisco** did not provide certain TOTP features (e.g. syncing, valid passcode generation) but does support import of token data. **Microsoft** preview feature supported input of purchased OATH-TOTP SHA-1 tokens. However, this feature has not officially launched, as shown in this document.

WatchGuard Competitive Advantage

WatchGuard AuthPoint provided their own hardware token, where the seeds were never exposed. It also supports third-party hardware tokens, imported only in PSKC format, with a transport key. This ensures tokens secrets are never exposed – different from other MFA solutions, where seeds are completely open and easily cloned.

Additionally, WatchGuard easily activated a new hardware token under a minute – the fastest of all vendors. Its steps were the simplest to follow, especially helpful to first-time users.

6.0 Provisioning and User Experience

6.1 Token Provisioning

Token provisioning is the process of enabling a mobile device to process token transactions.

WatchGuard AuthPoint	Cisco Duo	Microsoft Azure
✅	✅	✅

While all vendors supported token provisioning, **WatchGuard** was the only vendor to provide automated emails with instructions, QRcode, and prompt for token activation. **Cisco** required admins

to manually send an activation link or SMS to new user. **Microsoft** required users to navigate to their Azure AD for authentication method options.

WatchGuard Competitive Advantage

WatchGuard was the only vendor to support automated emails with instructions, QRcode, and prompt for intuitive token activation.

6.2 User Synchronization

User synchronization ensures accurate, secure, and compliant user data congruence between source and endpoints. All data is checked for errors and duplication before being used.

WatchGuard AuthPoint	Cisco Duo	Microsoft Azure
✅	✅	⚠️

All vendors supported **user synchronization**. WatchGuard used LDAP external identities and AuthPoint Gateway. Cisco imported Duo users and identity information to an on-premises OpenLDAP directory. Microsoft supported this feature but only on a Windows 2016 server or higher.

WatchGuard Competitive Advantage

- Supported user sync on all Windows server versions
- Easy to understand setup and use
- Provided straightforward help documentation
- Connects with other directory services

6.3 Mobile Token Enrollment

Mobile token enrollment securely onboards users via an enrollment method (e.g. email, QRcode). The user opens this on compatible mobile device to follow further instructions.

WatchGuard AuthPoint	Cisco Duo	Microsoft Azure
✅	✅	✅

All MFA solutions proved easy and secure activation of mobile tokens via QRcodes.

6.4 Secure Migration

Secure migration ensures proper migration of a token from one device to another, without compromising users or their data.

WatchGuard AuthPoint	Cisco Duo	Microsoft Azure
✅	⚠️	⚠️

WatchGuard was the only vendor to offer secure migration. It successfully scanned the QRcode to activate a new mobile device, which was not usable again for another device. **Cisco** and **Microsoft** only do backup/restore, which is copied from their cloud account. Cisco Duo Restore backed up accounts via Google Drive. Microsoft Authenticator Application cloud backed up account credentials via a Microsoft or iCloud account.

WatchGuard Competitive Advantage

Migration was easy to use
Supports the easiest secure migration via a scanned QRcode to activate the mobile device, usable only once.

Migration vs Backups
- Relies on token migration, as opposed to backups, because it is more secure. Backup/Restore can trigger threats.
- Minimizes risk of token cloning.
- Minimizes risk of breached password seen in backup processes.
- No cloud backup needed.

No third-party tokens
- Third-party tokens do not carry same security measures as AuthPoint, but it can do backups for third-party tokens using cloud accounts.

6.5 Mobile App Ease of Use

Ease of use is an important metric for user experience with the mobile application version of the MFA solution.

WatchGuard AuthPoint	Cisco Duo	Microsoft Azure
✅	✅	✅

All vendors showed **easy mobile applications** that were simple and straightforward for users to activate tokens on their own. However, Microsoft had many settings to configure, with one being a possible security concern if the user was not properly trained.

WatchGuard Competitive Advantage

- Easy mobile app use for users to active tokens on their own
- Straightforward configuration settings with no potential security flaws

7.0 Deployment Efficacy

7.1 Ease of Deployment

Ease of deployment helps users build trust with the product and vendor. A reliable, intuitive interface ensures customers are more willing to work with the solution, and its entire platform, for other practices.

WatchGuard AuthPoint	Cisco Duo	Microsoft Azure
✅	✅	❌

WatchGuard ease of deployment was superior. Activation, license setup, and configuration were completed in under an hour. **Cisco** Duo was remotely accessed for testing; Miercom did not set up license activation. **Microsoft** deployment included delays, had confusing and complex navigation, and required multiple subscriptions to access basic features.

<div style="background-color:#e2efda; padding:10px;">

WatchGuard Competitive Advantage

- Quickest deployment of all vendors
- Quick Start setup guide gave simple instructions for a smooth user experience

</div>

7.2 Configuration Wizards

Configuration wizards explains the solution and guides users for an accurate setup that minimizes misconfiguration.

WatchGuard AuthPoint	Cisco Duo	Microsoft Azure
✅	❌ *Product did not support this feature.*	⚠️

WatchGuard offers a configuration wizard that is extremely easy for first-time users that minimizes configuration errors. **Cisco** Duo does not offer configuration wizards. **Microsoft** provides two wizards, but they are more situation-specific and difficult for the first-time user.

<div style="background-color:#e2efda; padding:10px;">

WatchGuard Competitive Advantage

- Offers a configuration wizard that require no additional installation steps
- Extremely easy to use, especially for first-time users
- Shows actual configuration setup, as opposed to a summarized view, to avoid missing configuration nuances

</div>

<div style="background-color:#e2efda; padding:10px;">

Microsoft Competitive Advantage

The QuickStart Center, located in the Azure Portal, provided courses and guides to common projects.

</div>

7.3 Single Sign-On (SSO) Portal

Single Sign-On (SSO) allows users to use one set of login credentials across multiple applications for easy access management.

WatchGuard AuthPoint	Cisco Duo	Microsoft Azure
✅	✅	✅

Setting up the **WatchGuard** IDP single sign-on portal took only seconds to set up and was immediately ready for use. **Cisco** IdP Portal was easy to navigate, but setup proved complicated for first-time users – despite help documentation. **Microsoft** Office Portal was easy to navigate and supported Microsoft Office and SAML applications.

WatchGuard Competitive Advantage

- Had easiest SSO portal setup and usage
- SSO portal was ready within minutes
- Makes remote work with secure login and application use effortlessly accessible

7.4 SSO Client / SAML Support

SSO Client and SAML support is part of the SSO Portal experience, allowing users to configure and implement SSO for a SAML client application.

WatchGuard AuthPoint	Cisco Duo	Microsoft Azure
✅	✅	✅

WatchGuard provided numerous in-depth integration guides to support all application types involved with SSO Client / SAML support. **Cisco** Duo Central was used to configure/enable SSO and implement features (e.g. 2FA), globally or for specific users. **Microsoft** used a five-step method, where users could view and manage applications to integrate SAML.

All MFA solutions easily supported SSO Client / SAML Support.

7.5 Windows and macOS Login Protection

Windows and macOS login protection enables required authentication when users log in to a computer or server. This includes protection for RDP and RD Gateway.

WatchGuard AuthPoint	Cisco Duo	Microsoft Azure
✅	✅	⚠️

WatchGuard successfully installed the Logon App for Windows and macOS login protection. **Cisco** provided device insight, but this requires Duo Access or Duo Beyond Edition to have this feature. **Microsoft** Azure does not support MFA computer login but offers Windows Hello biometric authentication technology. However, Windows Hello is only supported for Windows 10 or higher on-premises deployments. This process also proved difficult for macOS devices.

7.6 Remote Desktop Protocol (RDP) Login Protection

RDP login protection enables required authentication when users log in to a computer or server using RDP connections.

WatchGuard AuthPoint	Cisco Duo	Microsoft Azure
✅	✅	⚠️

WatchGuard provided simple configuration for RDP login protection with the TeamViewer application. **Cisco** offered RDP protection via Duo Authentication. **Microsoft** offered remote desktop services via RD Web proxy, but it could be easily bypassed and, therefore, offered no protection to Windows Servers.

WatchGuard Competitive Advantages

- One of only two vendors to support RDP login protection
- Simple setup, with step-by-step instructions for secure protection of a specific application

Cisco Competitive Advantages

- One of only two vendors to support RDP login protection
- Simple setup

7.7 VPN Protection

Virtual Private Network (VPN) protection requires authentication for VPN encrypted connections.

WatchGuard AuthPoint	Cisco Duo	Microsoft Azure
✅	✅	⚠️

WatchGuard successfully supported VPN protection with a certificate-based VPN via the AuthPoint Gateway. **Cisco** offered different VPN options, easily installed with a wizard and Duo Security Authentication Proxy. **Microsoft** VPN protection proved very confusing despite given help

documentation. (Documentation for setting up MFA authentication for VPN can be found at: https://docs.microsoft.com/en-us/azure/vpn-gateway/openvpn-azure-ad-mfa.)

WatchGuard Competitive Advantages

- Setup Wizard made creation of RADIUS server/client, VPN encryption and connection easy
- Push notification feature appeared for successful certificate-based VPN authentication

Cisco Competitive Advantages

- Offers integration with different VPNs
- Setup wizard made VPN setup and authentication easy

7.8 Push Verification / Push Test / Helpdesk Tools

Push verification tools are useful for ensuring push notifications work properly for specific users or guaranteeing a helpdesk person is speaking with the correct user.

WatchGuard AuthPoint	Cisco Duo	Microsoft Azure
✅	✅	❌ *Product only supported feature with a paid subscription.*

WatchGuard and **Cisco** both offered native push verification that was simple and easy to use. **Microsoft** supported this feature but required purchase of the Notification Hubs subscription which is not a part of Azure MFA. For more information on how to Activate Notification Hubs, visit: https://docs.microsoft.com/en-us/azure/notification-hubs/create-notification-hub-portal.

WatchGuard Competitive Advantages

- One of two vendors to offer native support of push verification, without requiring an additional subscription
- Push verification was simple and quick to use

7.9 Time to Initially Deploy

Initial deployment time is how fast, or slow, it is to set up a solution; namely, the MFA solution.

WatchGuard AuthPoint	Cisco Duo	Microsoft Azure
✅	✅	❌

WatchGuard's initial deployment time was quick, under 30 minutes, and easy because of its simple user interface (UI). Cisco deployment was not fully tested, but adding a user took less than five minutes because of its straightforward UI. **Cisco** also provides instructions for complex concepts. **Microsoft** was confusing and difficult; features always required subscriptions. Navigation and configuration were also not easy, and instructions were not always helpful.

WatchGuard Competitive Advantages

- Under 30-minute setup
- Simple UI made process quick and easy for first-time users

Cisco Competitive Advantages

- User setup was less than 5 minutes
- Straightforward UI made navigation easy for first-time users
- Offered step-by-step instructions more difficult concepts

7.10 Breadth of Supported Platforms

Supported platforms can make integration of the MFA solution expansive within its environment of deployment.

WatchGuard AuthPoint	Cisco Duo	Microsoft Azure
✅	✅	✅

WatchGuard had a wide breadth of supported platforms with over 150 implementation guides that made deployment an easy, straightforward process. **Cisco** supported about 180 applications with step-by-step integration documentation. **Microsoft** supported over 2,000 applications, but it is unclear how many are actually usable by Azure MFA.

WatchGuard Competitive Advantages

- Provides over 150 platforms
- Offers over 140 integration guides

Cisco Competitive Advantages

- Provides 180 platforms
- Offers step-by-step integration documentation

8.0 Security and Risk-Based Authentication

8.1 Risk-based Authentication (RBA)

Risk-based authentication is an adaptive security measure for dynamic system behavior, evaluating user and device risk. As risk level increases, the authentication process becomes more refined and restrictive.

WatchGuard AuthPoint	Cisco Duo	Microsoft Azure
✅	⚠️	⚠️

WatchGuard was the only vendor to include risk-based authentication (RBA) in its solution without the need for an additional costly license. Policy creation was straightforward for first-time users. **Cisco** RBA policy granularity depends on the Duo plan chosen; Duo Beyond requires an additional license but offered the most granularity, with built-in global policies for applications and users. **Microsoft** also required an additional license for RBA but offered many risk-based services, such as Conditional

Access, for sign-in risk detection. However, setup was meticulous and potentially overwhelming for the first-time user.

<div style="background-color:#e8f0d8; padding:1em;">

WatchGuard Competitive Advantage

Only vendor to not require additional licenses or costs to enable or use this RBA feature

</div>

8.2 Secure Authentication Contingency

Secure authentication contingency having a contingency plan, when the main authentication method is not available, provides secure alternatives to mitigate issues related to losing access to protected resources. It should be developed following a security protocol to prevent hackers from easily bypassing the original authentication method.

WatchGuard AuthPoint	Cisco Duo	Microsoft Azure
✅	✅	✅

WatchGuard security authentication contingency used a challenge/response process with a time session for more security. **Cisco** used alternative authentication methods that posed a security concern to known attacks. **Microsoft** had multiple authentication methods – some being passwordless or single factor only.

<div style="background-color:#e8f0d8; padding:1em;">

WatchGuard Competitive Advantage

- Superior administrative control
- Challenge/response process includes a time session to provide more security

</div>

<div style="background-color:#e8f0d8; padding:1em;">

Microsoft Competitive Advantage

- Offers multiple options for contingency authentication
- Includes bot checking to protect against brute force attacks

</div>

8.3 Mobile DNA Addition

Mobile DNA is a proprietary WatchGuard MFA feature of its AuthPoint solution. This feature ensures only the authorized user can access online accounts and assets from their mobile device – as it is completely unique. Mobile DNA is not replicable by a hacker using an entirely different mobile device or emulator DNA.

WatchGuard AuthPoint	Cisco Duo	Microsoft Azure
✅	❌ *Product did not support this feature.*	❌ *Product did not support this feature.*

WatchGuard was the only vendor to support the unique Mobile DNA feature, which acquired information during activation, stored in the cloud for use across all platforms, to prevent hackers posing as users. **Cisco** and **Microsoft** did not support this feature.

WatchGuard Competitive Advantage

Only vendor to support the unique concept of the mobile DNA footprint feature to prevent hackers from impersonating users for a highly secure migration.

8.4 Audit Logs

WatchGuard AuthPoint	Cisco Duo	Microsoft Azure
✅	✅	⚠️

WatchGuard audit logs were filterable by data and exportable to a .csv file. The **Cisco** Duo Authentication log provided reports, divided by category, that were exportable if needed. **Microsoft** Azure Audit Logs were thorough with significant delay for updates, proving problematic when troubleshooting.

All vendors offered detailed, filterable, and exportable audit logs.

9.0 Total Cost of Ownership (TCO)

9.1 Support Quality and Effectiveness

We evaluated how useful and timely product support was to find a resolution for real-world issues.

WatchGuard provides an extensive Help Center (equipped with integration guides, deployment guides, quick start guides, troubleshooting, and tips) through the WatchGuard Cloud. All support level packages come with 24/7 support. WatchGuard AuthPoint comes ready with the Gold Support Level, by default. This includes 24x7 support, for anywhere in the world. Additional support services include priority response upgrades for your business needs. **Cisco** provides helpful documentation (e.g. step-by-step guides) and user assistance links. However, 24/7 support is only available with the Cisco Duo Premium Care Support. Users have the option of sending an email for support or opening a support ticket. **Microsoft** offers Virtual Assistance for support but not 24/7 technical support without purchasing the Azure Standard Support or higher tier package.

WatchGuard Competitive Advantages

- Offers many specific types of support
- WatchGuard Help Center gives in-depth documentation and assistance with an easy search feature
- By default, AuthPoint comes with Gold Support, giving global 24x7 support

9.2 TCO Analysis

WatchGuard AuthPoint is a mid-market application that provides security for varying business sizes. For WatchGuard and its competitors, we performed cost-benefit analysis – looking at its price point as well as holistically at its simplicity, security, scalability, and ease of use.

The following chart details the annual cost-benefit of the WatchGuard AuthPoint MFA solution with respect to similar vendors in its industry; namely, Cisco Duo Access and Microsoft Azure Premium P2.

Miercom's Market Impact Analysis (MIA) for the tested MFA solutions investigated value based on quality of functionality and use, as well as the average cost for first- year deployment.

Quality of Experience, also called **QoE** (vertical axis), summarizes security efficacy, functionality, ease of use, service setup and utilization, and support.

The **Total Cost of Ownership**, or **TCO** (horizontal axis), is the sum of costs calculated per a specified device count for a first-year deployment. This cost is subject to change, based on current discounts or negotiations made between vendor and customer. But this cost is used to best reflect the cost of training and related expenses, product upgrades, support, licensing, and legal restrictions.
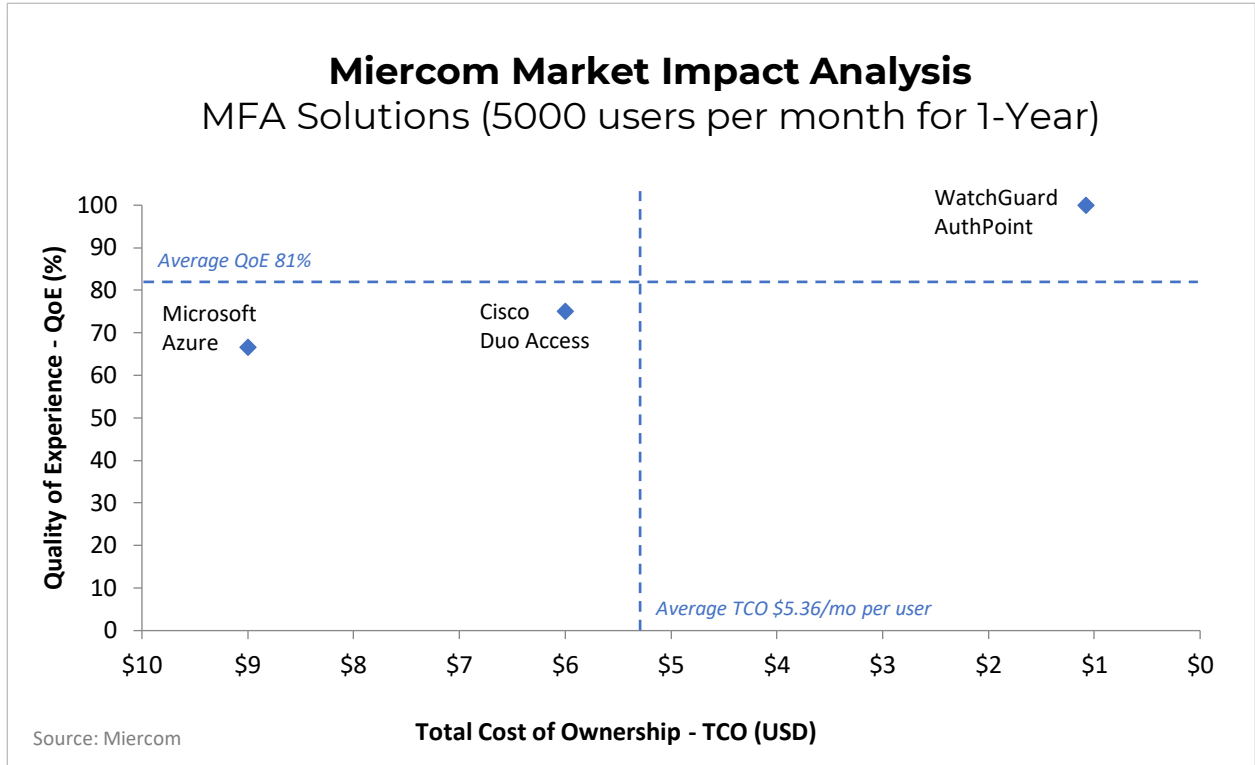
Miercom Market Impact Analysis
MFA Solutions (5000 users per month for 1-Year)

Quadrants are formed based off average values. WatchGuard was in the upper right quadrant, showing it had the highest QoE of competing vendors at the lowest cost. Cisco and Microsoft do not offer nearly the same amount of functionality, ease of use, or intuitive interface as WatchGuard.

WatchGuard Competitive Advantage

- WatchGuard AuthPoint MFA solution had the highest Market Impact Analysis value
- AuthPoint offered above average Quality of Experience for a below average cost

About Miercom

Miercom has published hundreds of network product analyses in leading trade periodicals and other publications. Miercom's reputation as the leading, independent product test center is undisputed. Private test services available from Miercom include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Interoperable, Certified Reliable, Certified Secure and Certified Green. Products may also be evaluated under the Performance Verified program, the industry's most thorough and trusted assessment for product usability and performance.

Customer Use and Evaluation

We encourage customers to do their own product trials, as tests are based on the average environment and do not reflect every possible deployment scenario. We offer consulting services and engineering assistance for any customer who wishes to perform an on-site evaluation.

Use of This Report

Every effort was made to ensure the accuracy of the data contained in this report but errors and/or oversights can occur. The information documented in this report may also rely on various test tools, the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the vendors that were reasonably verified by Miercom but beyond our control to verify to 100 percent certainty.

This document is provided "as is," by Miercom and gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness, or suitability of any information contained in this report.

All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading, or deceptive or in a manner that disparages us or our information, projects, or developments.

By downloading, circulating, or using this report in any way you agree to Miercom's Terms of Use. For full disclosure of Miercom's terms, visit: https://miercom.com/tou.