WatchGuard®

UNLOCK ACCESS CONTROL WITH RISK POLICIES AND ZERO TRUST SECURITY

ccb TECHNOLOGY®

TABLE OF CONTENTS

Why You Need a Zero Trust Risk Framework 4

Multi-Factor Authentication and Risk Intelligence: Optimized User Management 6

Risk Policies Prevent Breaches 9

There Can't Be Zero Trust Without MFA 10

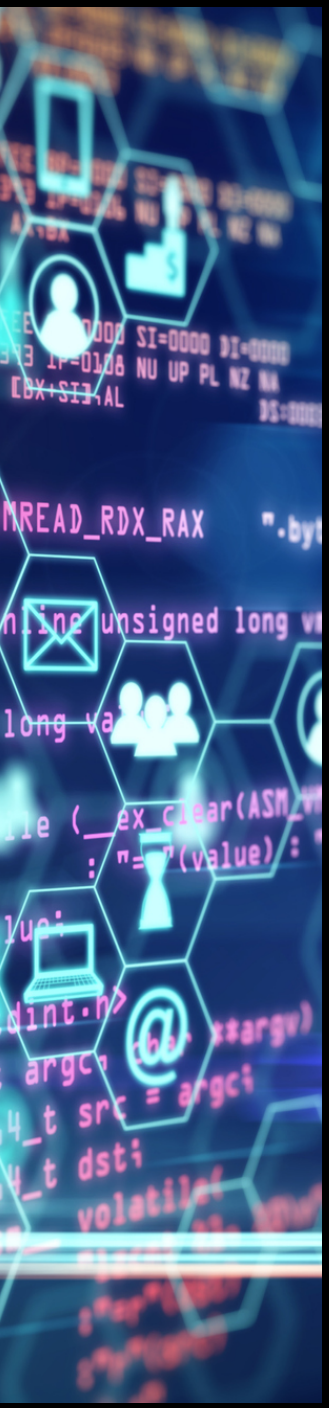
Using MFA and Risk Policies to Enable Zero Trust 12

Risk Assessment Guide 13

Forrester Research Inc. first coined the term "zero trust" in 2010. With businesses implementing hybrid multi-Cloud environments, identity and access management can no longer be considered optional. Extending VPN protection is not enough.

Enabling a zero trust risk framework enhances both security and user experience by allowing you to rank the resources you want to protect based on risk level and type of user. This gives you the power to create policies that are unique to the security structure in your organization, therefore enabling more flexibility and higher protection only when necessary.

In this eBook, we discuss the powerful connection between zero trust adoption and risk policies, and how multi-factor authentication sits at the core of these approaches by bringing the security solutions required to properly verify user identities.



Why You Need a Zero Trust Risk Framework

User Authentication

- Something you know (password, PIN)
- Something you have (token, mobile phone)
- Something you are (fingerprint, face)

User authentication is a static way to verify the identity of a user when trying to access a protected resource. You may authenticate using a single factor (weak), or multiple factors (strongly recommended).

In a dynamic world, where user mobility impacts security almost 100% of the time, multi-factor authentication has become imperative and key to enabling zero trust.

- Users are connecting to company resources from different, unprotected networks
- Working hours have become more flexible, so they could be working from early hours to late evenings
- Devices could have been shared with other family members
- The threat landscape is expanding at faster rate than hybrid work and Cloud adoption

User Authentication

Risk Factors

- **Which network are you connected to?**
- **Is your computer safe?**
- **Are your mobile devices safe?**
- **What is your current location?**
- **Are your device and computer located in the same place?**

Adopting a zero trust risk framework takes risk factors into account when performing an authentication decision. It goes beyond a static authentication, allowing administrators to create rules that can modify the authentication behavior, sometimes making it easier if the risk is low; or asking for additional steps to ensure this is the right user, and blocking the access if the risk is too high, even if the user provided a correct one-time password (OTP).

Multi-Factor Authentication and Risk Intelligence: Optimized User Management

Risk-based policies enhances both security and user experience by allowing you to rank the resources you want to protect based on risk level and type of user. This gives you the power to create rules that are unique to the security structure in your organization, therefore enabling more flexibility and higher protection only when necessary.

For example, you could decide to allow users to authenticate with just username and password when directly connected to a local, corporate network, but use MFA if working from a separate network. And this is the definition of advanced user management.

Common risk factors can be addressed with authentication policies

NETWORK LOCATION

A corporate network might have all border security measures, such as firewall, secure Wi-Fi, threat detection, etc. Therefore, someone physically connected to that network would pose less risk than someone in a remote office with less security measures, or someone connected through the home office.

MOBILE DEVICE RISK

A user's device that has been compromised poses a security risk to a company. One way a device can be easily compromised is when a user jailbreaks an iOS device or roots an Android operating system, circumventing the operating system security measures. A vulnerable device increases the overall risk and should be blocked most of the time.

ENDPOINT / COMPUTER RISK

Like mobile device risk, endpoint or computer risk can also be used to assess what measures should be taken. A user with their own laptop, with all protections, would pose a low risk. The same user trying to connect later in the day, with an unknown computer – maybe a Linux machine with a Tor browser – and the risk would greatly increase.

TIME POLICIES

Date and time can be used for different purposes. Let's say a corporate application usually goes through backup and maintenance every day, from 1am to 3am. Time policies could be used to block access to that application during this period of time. In terms of risk, if a user is trying to access an application on a weekend, or maybe in the middle of the night, this could raise the risk dramatically, since this could be a hacker performing an attack while the IT team is resting, so additional measures could be taken.

Common risk factors that could potentially be added to authentication policies

GEOFENCING

Physical location could be used to prevent access from specific countries or geolocations, thus mitigating chances of attacks. A company with offices and activities only in the USA could potentially block any access outside the country. Access to a specific application could be also limited to an area around a company office.

GEO-CORRELATION

It's expected that a user connecting to a company service has a mobile phone in their hands. A connection initiated from a computer located in Sao Paulo, Brazil, with the mobile phone registering its current location in Virginia, USA could show that a hacker is trying to connect to a service, while using social engineering to convince a user to approve the MFA authentication.

While some geolocations are not very precise – some carriers will route the connection to a different location, and some Android devices can have its GPS location manipulated – this can be another way to dismiss potential attacks.

GEO KINETICS

Another form of using GPS or geolocation factors for a risk decision is geo kinetics or authentication velocity. A user authenticating from Seattle at 9:05 am cannot authenticate 25 minutes after from San Diego, 1,300 miles away. Most likely, the second authentication attempt is trying to reuse the first authentication.

Risk Policies Prevent Breaches

Without risk policies in place, your company would need to enable the most secure authentication method at all times, for all users, potentially causing user friction for some segments. Risk authentication is a way to modernize your strategy by using the precise amount of security with customized risk protection that improves your ability to detect and respond to threats.

The following scenarios show cases of potential data breach that can be prevented if risk policies are enabled.

A

USING STOLEN CREDENTIALS

User authenticates regularly with username, password, and an OTP. An attacker was able to get the user credentials through the dark web or phishing attack, but the token could not be hacked or cloned.

- **Attack:** Using social engineering, attacker calls the user, and convinces user to give away an OTP. Attacker enters credentials and types in the time-based OTP, getting access to the protected resource.

- **Risk Policy Prevention:**

  Computer risk policies could show the computer being used is not the user's personal one.

  Geo kinetics policies would possibly show the user is trying to authenticate from a location where the transition is impossible between two authentications.

B

iOS JAILBREAKING

User authenticates with username, password, and push. The iPhone was jailbroken by the user, and malware ended up being installed by an attacker, giving them full control. Push is not protected by a PIN or biometric.

- **Attack:** The attacker, from a different country, would use stolen credentials to authenticate, while monitoring the user's phone. When the push arrives on the user phone, the attacker will use the Remote Access Tool (RAT) to approve the push, and get access to the resource.

- **Risk Policy Prevention:**

  Device Risk policies would detect the user's mobile device is not reliable and deny authentications from it.

  Geo-correlation policies would check that the computer is located in a different location than the mobile device, blocking the connection as well.

MFA is the cornerstone for zero trust implementation in that it provides the security structure for user and identity management and continuous authentication for any user to any resource.

There Can't Be Zero Trust Without MFA

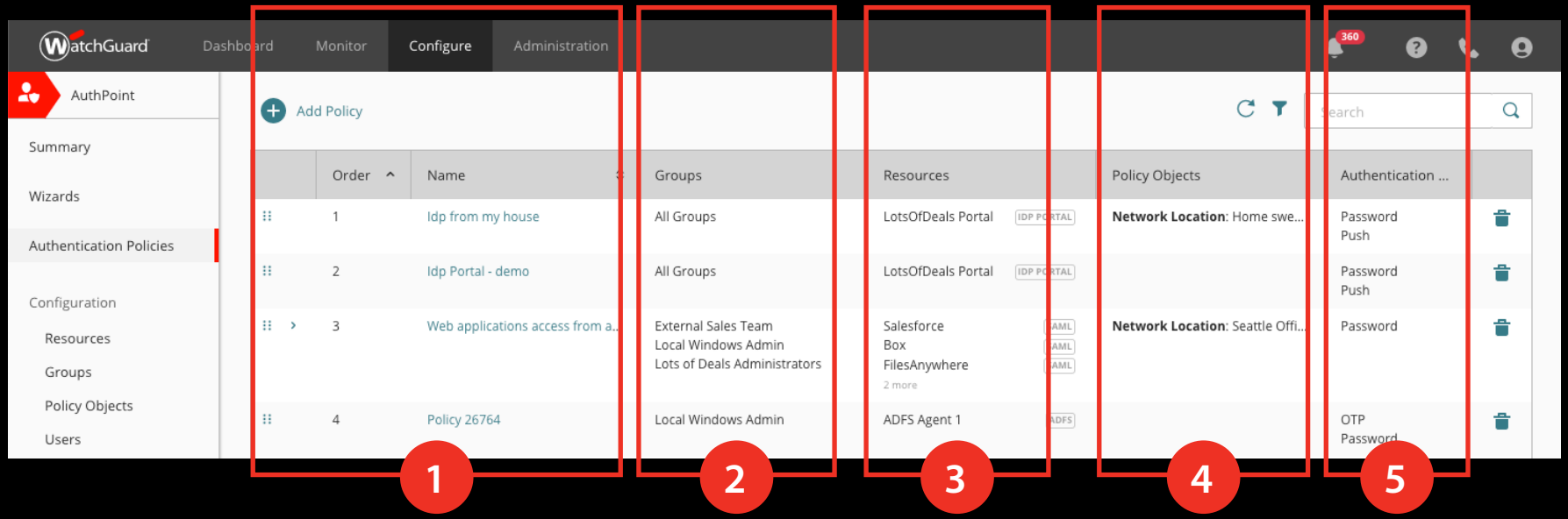
Identity and access management can no longer be considered optional. Businesses need to focus on a strong user protection and management strategy, which are core areas that MFA and risk authentication govern. This will give you the opportunity to truly roll out access control capabilities on your company network, endpoints, and Cloud applications without compromising user experience.

Whereas a traditional network is built around the idea of inherent trust, a zero Ttust framework assumes that every device and user, on-network or off, represents a security risk. The "never trust, always verify" approach uses multiple levels of protection to prevent threats, block lateral movement and enforce granular user-access controls.

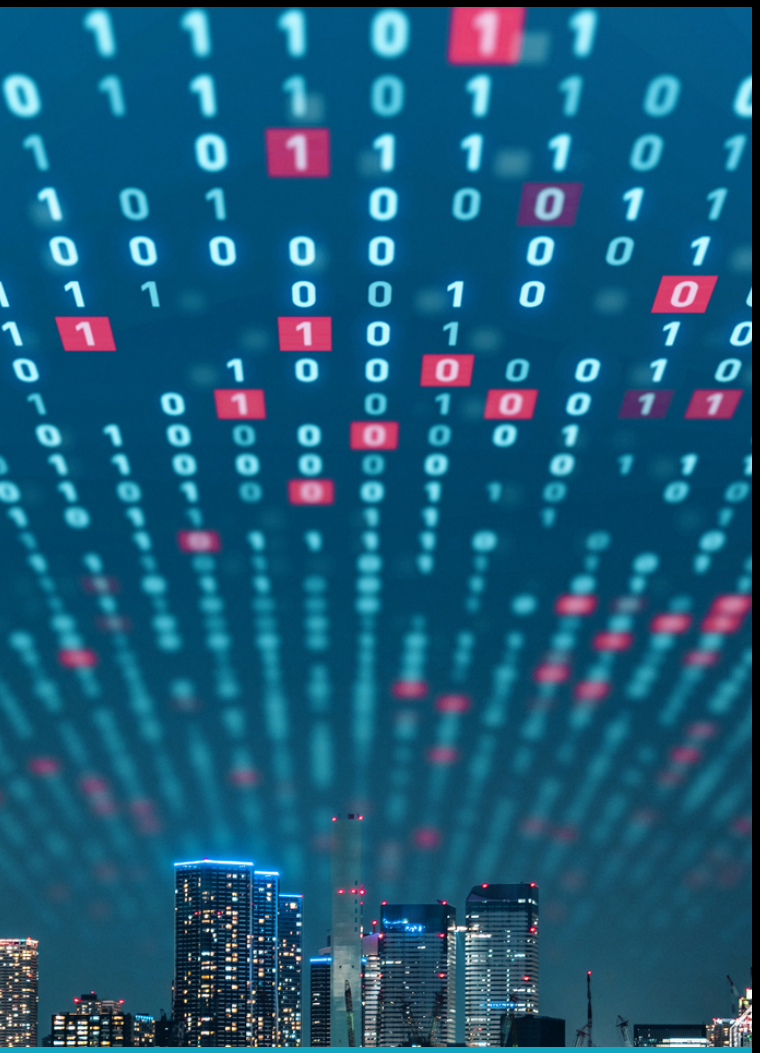
Under the premise that nothing can be completely trusted, the zero trust approach focuses on three principles:

Verify Explicitly	Restrict Access	Assume Breach
To maintain data security, risk policies are necessary to ensure that only authorized users can access information. Authentication plays a crucial role in this process. It is recommended to use a multi-factor authentication method to enhance security and verify user access explicitly. This helps grant necessary privileges based on their role.	Limit access to business-critical systems and applications to only those devices that have explicit permission to access them. In the zero trust framework, the goal of access management is to provide a means to centrally manage access across all common IT systems, while limiting that access to only specific users, devices, or applications. Single sign-on (SSO) technologies, combined with MFA, can improve access security and minimize the password burden on users.	By restricting access and applying continuous monitoring, you can improve threat detection and create a better line of defense against potential attacks. With this approach, there is no assumed trust between users or machines, and access is granted only when necessary and verified. This provides a much-needed level of visibility into your network, applications, and data.

Example of enabled risk policies that meet zero trust approach:



1. The policy name would represent a zero trust micro-segment and can be organized in priority and/or importance order.
2. Groups of users, synchronized or not with Active Directory, represents those who should be allowed – and only them – to the protected resource.
3. The micro-segment application(s). Could be a single application, could be multiple, in case the applications have exactly the same policy.
4. Policy objects, or risk policies, that can determine specific restrictions, based on network, time, geolocation, etc.
5. Refers to the authentication methods that should be allowed, if any, or just have authentication denied, based on a risk factor.



Risk policies can be used to define more granular rules based on dynamic situations, which better fits the current remote access trends and hybrid work models that businesses are experiencing.

Using MFA and Risk Policies for Zero Trust Deployment

As we know, zero trust implementation starts with the assumption nothing can be trusted. By defining micro-segments and applying policies that are tailored to your organization's security needs, you are creating a trusted environment. This starts by identifying the user that will access those applications and services.

A micro-segment could be a Cloud-based customer relationship management (CRM) application. For example, sales and technical support teams might need access to that CRM. Engineering? Possibly not, so they won't be included. In the case of the technical support team, all employees are in the same city and they work only during business hours, which means maybe the access for this group should be geographically and time limited. And due to the sensitivity of the data within the CRM, MFA should always be used.

If we put that into the authentication context and risk factors, there are two rules that will define the risk policy associated with this micro-segment:

RULE 1 NAME
CRM FOR SALES TEAM

Who can Access: Sales

Application: Cloud CRM

Risk restrictions: Low Mobile Device Risk, Low Geo-Correlation Risk

Authentication: Password + Push-Based Authentication

RULE 2 NAME
CRM FOR TECHNICAL SUPPORT TEAM

Who can Access: Technical Support

Application: Cloud CRM

Risk Restrictions: Low Mobile Device Risk, Business Hours, USA only, Low Geo-Correlation Risk

Authentication: Password + Push-Based Authentication

Business Risk Assessment Guide

Assessing the risk in your organization by looking at your potential risk scenarios can greatly enhance those deployments by adding dynamic facts and analysis to the decision.

CREATE A RISK QUESTIONNAIRE

Common business use cases that can help identify the right risk policies for you:

- On-site: Are your employees accessing company data and platforms from the office?
- Remote home office: Do you have a lot of employees working from home?
- Remote coffee shop, shared office: Do you expect your remote employees do access company networks from locations such as coffee shops?
- Traveling users: Do you have employees who travel and may access work platforms while on the go?
- Vertical: Is the service your company offers associated with specific business hours? For example, healthcare offices
- Third-party providers: Do you provide company access to contractors or third-party providers?
- Device: Do you expect employees to access work information using their own devices?

TRY MICRO-SEGMENTATION

A micro-segmentation exercise will also give you better visibility over your assets and users. Below, a simple table template that could be used for this exercise – at least the first part, which deals with identity.

Micro-Segment Example: Use this template as a starting point to create your micro-segments and expand it based on your own security needs to create more specific access policies.

Zero Trust Micro-Segment

Cloud CRM

Group of Users	Scenario	Network Location	Geo Location	Time Restrictions	Device Risk	Computer Risk	Authentication
Sales	Working from the office	Office network			Low risk	Business laptop	Password
Technical Support Finance	Traveling for work	Any			Low risk	Business laptop	Push MFA QR code MFA
3rd Party Group	Working only from the office	Office network		Business hours	Low risk	Business computer	Password
	Working through VPN	Company VPN		Business hours	Low risk	Business computer	Push MFA
IT - CRM	CRM Consultants	Any	USA only	Business hours			Push MFA
	CRM Support	Any	USA only		Low risk		Push MFA

Business Risk Assessment Guide continued

RISK ASSESSMENT GUIDE	Risk Factor		MFA	Risk Attributes		
	Username	Password	OTP, QR Code or Push	Network Location	Authntication Result	Risk Level
SCENARIO 1 Company employee connects from home to a corporate resource	✓	✓	✓	✗	Allow	Pass
SCENARIO 2 Company employee connects from the Seattle, WA office location to a corporate resource	✓	✓	MFA Not Required	✓	Allow	Pass
SCENARIO 3 User attempts to log in to access corporate data from an unknown location	✓	✓	✗ MFA Not Allowed	✗	Deny	Deny

ccb TECHNOLOGY®

Interested in learning more about Zero Trust, or Multifactor Authentication?

Contact **CCB Technology for all your security needs!** Since 1991 we've provided affordable Products, Services, Licensing and IT Projects to Nonprofits and SMBs.

Call 1-800-342-4222 or
visit ccbtechnology.com to learn more!

WatchGuard®