



# Zero

# Trust:

**Securing Your Business  
for Tomorrow**




security

## We talk a lot about trust at Salesforce.

In fact, it's our number one value. It's the bedrock of our company, written in the DNA of our culture, technology, and focus on customer success. Trust is having a culture that builds security into everything we do, so that our customers know that their data is safe, and theirs – to be accessed when, where, and how they intend. And we do that by adopting the latest technology and security best practices available.



An illustration of a woman with long dark hair, wearing a white top and blue pants, walking through a grocery store aisle. She is carrying a brown paper shopping bag. In the foreground, a small child in a brown bear costume is also carrying a shopping bag. The background shows shelves with green leaf-patterned items and a window with a view of the outdoors.

## The Next Evolution of That? Zero Trust.

Which might sound like a contradiction. But is actually how we're moving our trust-first culture forward – for our customers and ourselves.

So what is this latest practice all about? Zero Trust is a strategy. A framework. One that throws the idea of a trusted network out the window in favor of authorization at every step. Think about it like your home. Just because you let someone in the front door doesn't mean you want them to snoop through your medicine cabinet. Zero Trust is designed to protect the network from the inside, so that even if someone accesses one aspect of the network, they will not have the ability to move freely inside it.

## Perimeter Defense is No Longer an Option

In the last twenty years, cybersecurity best practices have gone through many iterations. Gone are the days when we all showed up to the same office, with heavy desktops all connected to the same network, did our jobs, and left it all there – the data, the devices, the work – to go home at the end of our shifts. And with that evolution, gone are the days of single passwords and simple cyber threats.



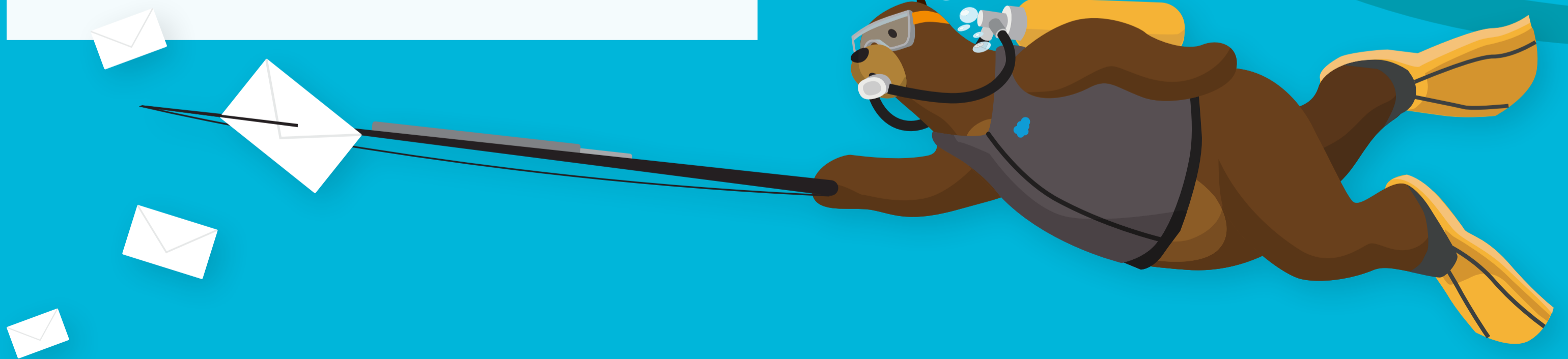
What used to be a comfortable perimeter for security teams to monitor is now a vast network of international offices, home work environments, public clouds, mobile devices, and of course, more coffee shops than we'd like to admit. 2020 only accelerated the work from anywhere revolution.

With more people working from home than ever before and more businesses adopting cloud technologies, attack surfaces have expanded and **malicious actors have found new vulnerabilities to exploit**. Overloaded corporate VPNs, shortcuts to get remote workers online, bypassing protocols to get information to both

colleagues and customers alike – the risk landscape has completely changed. While **nailing the basics** – patching vulnerabilities, detecting and mitigating threats, and educating employees on how to be defenders for security is still important, staying ahead of today's sophisticated threats requires raising the bar.



You've heard about them in the news: targeted malware and ransomware threats, countless phishing and vishing attempts, data breaches, and insider threats. These threats are not only a problem for the private sector – they deeply affect the public sector as well. So much so that **President Biden issued a May 2021 Executive Order** mandating Federal agencies to modernize their cybersecurity strategies and adopt multi-factor authentication (MFA), a key component of achieving Zero Trust.



## Verify First, Then Trust

Where traditional network security verifies permissions at the perimeter then allows users to have access to many components inside, Zero Trust is built on the **principle of least privilege**. This principle is a fundamental tenet of information security, and means only giving users, devices, applications, and systems the minimum privilege level they need to do their job.

In a traditional network environment, a privileged user will have a high level of access to data and systems. If this user is compromised by a malicious actor (a hacker), their access could be exploited

to perform unauthorized actions or access data – otherwise known as a breach. The possibilities are endless, and potentially extremely harmful to a company. With Zero Trust, a user only has access to specific things (applications, services, etc.) through a predefined pathway, thus preventing a hacker from doing a lot of damage in the unlikely event they are even able to gain access to the network.



It's a strategy that can help mitigate threats such as malware, ransomware, and phishing, along with minimizing the risk of insider threats, DNS data exfiltration, and advanced zero-day attacks. While unwinding legacy security processes and changing strategies isn't an easy task and the ongoing administration of a Zero Trust model can impact productivity, the benefits can outweigh the challenges.

#### POTENTIAL BENEFITS OF ZERO TRUST:

- Increased compliance and agility
- Faster threat detection and remediation
- Simplifying analytics
- Fewer accidental high-privilege actions
- Prevention of lateral network movement





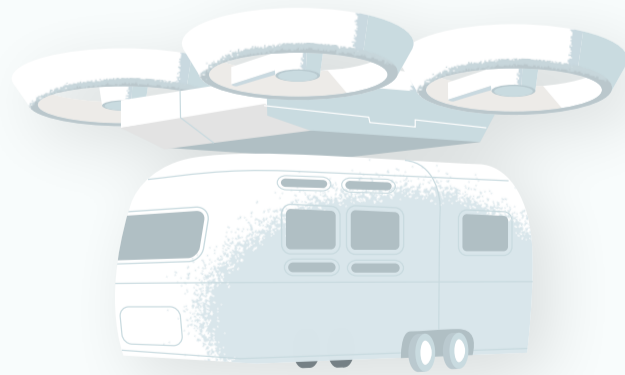
# Our Approach to Zero Trust

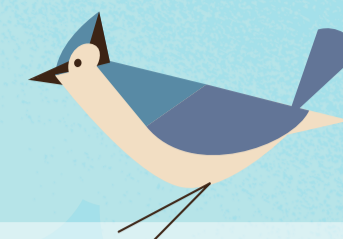
At Salesforce, we recognize that the attacks and attackers are getting more sophisticated every day, and our team continuously innovates to stay ahead of tomorrow's threat landscape. We build defense-in-depth into all of our systems – another way of saying we try to limit the possibility of any single point of failure by building in a layered approach of technology, process and people.

This is all part of our vision for a work from anywhere employee experience that includes seamless access to corporate resources while also uplifting our overall security posture. As more of us move to public cloud and remote work, it's important that all

access decisions be made dynamically, accounting for policy as well as context about the current state of the user and device making each request.

And we practice what we preach – we don't ask our customers to do the things we wouldn't ask our own employees to do. This includes using multi-factor authentication, one of the key components to achieving Zero Trust.





## A FEW OF OUR ZERO TRUST BEST PRACTICES:

- Device credentials should be hardware-backed or hardware-isolated on a system
- All connections use strong, approved encryption
- Authentication and authorization are done before allowing access to services and resources
- Connections are monitored and closed if they have exceeded authorization
- Location is not a proxy for device or sole authorizing attribute
- Maintain dynamic inventory of devices and authorizations
- Implementation of multi-factor authentication (MFA)



## Multi-Factor Authentication and Zero Trust

As threats that compromise user credentials grow more common, usernames and passwords are no longer sufficient safeguards against unauthorized account access.

**Multi-factor authentication (or MFA)** adds an extra layer of protection against common threats like phishing attacks, credential stuffing, and account takeovers by requiring additional factors to prove the identity of a user. That means even if a bad actor steals a username and password, they won't make it past an additional security check to access critical data.



**How does it work?** MFA requires a user to validate their identity with two or more forms of evidence – or factors – when they log in. One factor is something the user knows, such as their username and password combination. Other factors are verification methods that the user has in their possession. While there's a risk that a password may be compromised, it's highly unlikely that a bad actor can also gain access to a strong verification method like a security key or authentication app.

Not only is implementing multi-factor authentication (MFA) one of the most effective ways your company can increase its security posture, but it's a critical component of a larger Zero Trust strategy. It's so effective, in fact, that, as of February 1, 2022, **we're requiring all customers to use MFA to access Salesforce products.**



Not to worry, though. Salesforce offers simple, innovative tools and training to help you be successful – and secure. This includes extensive resources to assist in implementing MFA, including:

- [Salesforce Multi-Factor Authentication FAQ](#)
- [User Authentication Module](#)
- [MFA Quick Guide for Admins](#)
- And join us on the trail in the [MFA - Getting Started Trailblazer Community](#)

Ultimately, the goal of adopting a Zero Trust security posture goes beyond simply reducing your attack surface. Going borderless is vital to organizations with global workforces and remote employees.

It can also help accelerate integration of acquisitions, enable improved platform integrations, and provide a better end user experience.



To learn more about the security features and resources available to help your organization work smarter, faster, from anywhere, explore the [Salesforce Security Guide](#) or visit [security.salesforce.com](https://security.salesforce.com).

© Copyright 2000–2021 salesforce.com, inc. All rights reserved. Salesforce.com is a registered trademark of salesforce.com, inc., as are other names and marks. Other marks appearing herein may be trademarks of their respective owners.

