

Zero Trust Security Model for Small and Medium Businesses

The Zero Trust security model matters for small and medium businesses (SMBs) alarmed by the prospect of how to protect their company and customers' data. Trust is important in business—between service providers, investors, partners, employees, and customers.

If you're unfamiliar with 'zero trust', you could be forgiven for assuming skepticism and suspicion. But many of the largest companies in the world have long adopted the zero trust (ZT) security model to establish an assured approach to securing their company and customers' data.

In this blog post, we explain what the zero trust security model is and why it matters. We outline its core principles and provide some simple steps for how your SMB can adopt the Zero Trust security model to confidently reinforce your security posture.

What Is the Zero Trust Security Model?

The traditional view of cybersecurity treats access like the primary safeguards on a medieval, European castle. Everything inside your network security measures and corporate firewall was completely safe—like villagers behind a moat, high walls, and a heavy, iron drawbridge. Meanwhile, everyone on the inside roamed free without challenge. Once you passed through the wall's gate house, you had access to everything.

The ZT outlook from our secure fortifications is a little different, and for good reason.

- Malicious actors continue to find new ways to hack through our security measures, pillage the unprepared, and carry off their spoils.
- Meanwhile, the borders between home and work (inside and outside) have become fuzzy. Employees, partners and customers increasingly require remote and freelance access to our systems, across locations, networks and wifi connections with unknown security measures.

Zero trust is a framework for keeping your online activities and data safe. It requires strict identity verification for every user or device that attempts to access your network's parameter *and, crucially, at every point within it*. There is no implied trust based on network location, IP address, or even employment status.

Why Does the Zero Trust Security Model Matter?

The rise of remote working, accelerated due to government mandates that restricted individuals' movement throughout the COVID-19 pandemic of 2020-2022, has [increased security risks](#). SMBs require a different approach to [security practices](#). The traditional 'castle-and-moat' model of trusting devices and users within your corporate parameter has become increasingly inadequate.

Instead, the ZT approach is designed to create 'parameterless security' that:

- Verifies the identity and integrity of devices and users without regard to location
- Provides minimal access to applications and services based on authenticated users and devices

Zero Trust Principles

Zero trust is summed up in the phrase: *never trust, always verify*. There are three core principles for modern networks:

1. Verify explicitly
2. Use least-privilege access
3. Assume breach

What do they mean?

Verify Explicitly

Users or devices should not be trusted by default under the ZT model—even if they were previously verified or are currently connected to a permissioned network.

To *verify explicitly* means that:

- User access should only be granted to explicitly authorized data that is necessary for them to complete a set task
- You must always require continuous verification at every stage for who is accessing and using your company data—while denying access to everyone else

Verification may be required on:

- Computer networks and systems
- Cloud services and infrastructure
- User and email accounts
- Databases
- Devices like laptops, tablets, and smartphones
- Platforms and software packages
- Web services and applications

Examples include:

- Insisting on strong user identity and device verification prior to granting access
- Assigning relevant identity types, verification methods, access roles or levels, and custom permissions

The custom nature of this access also helps comply with various country, state legislation around data security, and similar industry standards and benchmarks.

Use Least-Privilege Access

Adopting a ZT stance requires that you grant the least number of privileges needed to anyone who accesses or uses data by way of access controls.

To *use least-privilege access* means that you:

- Give access to user only to the resources they need to perform their job
- Explicitly prevent users from accessing anything else

This is sometimes called the Principle of Least Privilege (POLP) or the least privilege access model.

Examples include:

- External users, such as clients or suppliers, who log on to your website application, portal or platform to gain access to their account
- An HR partner who requires access to some employee records on appraisals and performance, but not to information about salaries and pensions

Assume Breach

ZT puts you on guard.

If you *assume a breach*, this means that:

- You should configure constant monitoring of all activity across your network, systems, platforms, devices, and websites applications
- You should establish a system for acting on these alerts and reports—not only after something has gone wrong or when you need to demonstrate compliance

Examples include:

- Using activity logs and other software to record every single system and user action networks, software and devices
- Configuring logs to send SMS or email alerts to system administrators following unusual behavior such as repeated or failed login attempts, file uploads, or a higher payload than usual on your network

Executive Order on Improving the Nation's Cybersecurity

The White House's [Executive Order on Improving the Nation's Cybersecurity](#), mentions Zero Trust Architecture (ZTA) as one of the "security best practices" in the context of cloud technology. (Standards and guidance to achieve this plan have been outlined by the National Institute of Standards and Technology.)

Section 10:(k) of the order refers to how ZTA achieves this by:

- Eliminating implicit trust ("in any one element, node or service")

- Requiring continuous verification ("of the operational picture via real-time information from multiple sources to determine access and other system responses")
- Allowing users full but bare minimum access (only what "they need to perform their jobs")
- Assuming a breach is inevitable ("or has likely already occurred")
- Constantly looking "for anonymous or malicious activity"

Let's look at three SMB case studies.

Case Study 1—Zero Trust Access in a Ambitious Financial Consultancy

Imagine you are a successful financial consultancy of 150 staff offering a range of financial planning services, portfolio management, pension consulting, and private fund managers. Your team uses multiple software platforms and your experts often work remotely.

What Zero Trust strategies can I use so that all platforms and customer data is secure and protected from malicious hackers, regardless of who is connecting or from where—and without password fatigue?

In this example, we will use the *verify explicitly* ZT principle.

One answer for your consultancy is to invest in [identity and access management](#) (IAM) solutions. Only login requests from recognized and specific sources will be authenticated. IAM solutions include:

- Single sign-on (SSO)—This authentication method enables users to log in to multiple, software systems securely using a single ID. You can configure other systems to 'trust' the same user based on the original ID.
- Multi-factor authentication (MFA)—This authentication method grants users access to website applications or networks only after providing two or more proofs of ID. Users can use an authenticator application on their smartphone, or via an SMS or email, to gain access to their user accounts on your finance portal.
- Password manager—This is a software tool that helps users prevent [hacked passwords](#) or [passphrases](#), store and manage them securely, across multiple website applications. Features include automatic logins, changing passwords regularly ([When's the Last Time You Changed Your Passwords?](#)), and tracking whether the login credentials have been detected on the dark web. They also help to reduce password frustration.

Case Study 2—Zero Trust Policy Across Critical Applications in a Medical Services Clinic

In this scenario, your SMB provides medical services within the private sector. Records contain lots of sensitive information about patients.

How can those in charge of the IT systems and databases ensure that only the right people have access to the patient information that's appropriate for their task?

Compliance with data protection laws such as the CCPA (California Consumer Privacy Act) or the EU's GDPR go without saying. But is there anything more specific for guiding your policy writing?

In this example, we will use the *least-privilege access* ZT principle.

This answer lies in written access policies such as:

- Just In Time (JIT)—This policy states that any personal data must only be accessible to users at the point of need (not before or after). A doctor should not be able to access the medical details of a patient before that patient has consented or come under the remit of their care.
- Just Enough Access (JEA)—This policy states that personal data must only be accessible by users with the appropriate level of authorisation. A finance administrator should be able to gain access to just enough of patients' medical reports and bank details in order to process a patient's bill.

Case Study 3—Zero Trust Solutions for a Specialist Law Firm

If you run a law firm, you'll have amassed a substantial amount of documentation, some stored on paper, online, or even on individual computers.

How do I modernize my inefficient and insecure client file storage to minimize information spills?

Larger enterprises use Security Information and Event Management (SIEM) solutions to recognize threats and address vulnerabilities before they can disrupt operations.

In this example, we will use the *assume breach* ZT principle.

- Cloud storage and [document management](#)—Storing all your business data and files on an off-site or online would help your firm manage and control access. If your offices, harddrives, or servers suffered physical damage or a cyberattack, your data would still be secure.
- [Endpoint detection and response](#) (EDR)—This technology helps you monitor the networks and devices that are subject to potential cyber threats. For example, EDR software can continuously monitor all your network endpoints for vulnerabilities, detect suspicious behavior, and launch preventative actions to halt further access.
- Outsourced IT security management—It makes sense for a SMB to procure the services of an information security management specialist. For example, you could commission cybersecurity assessments or [penetration tests](#) to stress test your network and connections for vulnerabilities.

Start Your Zero Trust Journey With A Business Security Assessment

The zero trust security model is designed to assist organizations like your adopt policies, practices and habits that reassure you and your customers that data is held securely. Not only that, the right people have access to your company and customer data at the right time. Finally, measures are in place to alert you of potential breaches, so you can act quickly to defend against intruders and you retain your customers' ultimate trust.

Contact us today to book a [business security assessment](#) to begin your zero trust journey to a security posture of confidence.