netdocuments®

5 Steps to Implement a Zero-Trust Security Model

What is Zero-Trust Security?

Previous security models operated like a castle and moat: defend the perimeter to keep bad actors out and presume everything within the walls is safe and trustworthy. But cybercrime has evolved, and that model is no longer suited to meet the threats we now face. The zero-trust security model, on the other hand, presumes nothing can be trusted without authorization.

Of course, this is easier said than done. But here are five steps , derived from Forrester research, you can take to begin implementing zero-trust security at your law firm.

1 Identify your sensitive data.

To begin, you want to know what sensitive data you have and where it's stored, whether that's in the cloud, on a local network, etc. Your firm is likely dealing with an enormous quantity of sensitive documents and data, so while this may be a sizeable task, it's also of critical importance.

2 Map flows of sensitive data.

Security would be significantly easier if everything stayed in one place all the time, but it doesn't. Links get shared, files and folders get emailed, documents get downloaded to various user devices … it's nearly impossible to control where your data goes once it gets outside its "home."

This challenge is especially significant for law firms due to the many parties that need to access sensitive data or documents. Although it may get complicated, try to map out the usual paths your data takes between users and systems so you can better understand how its transferred and where any access points may be.

3 Employ granular perimeter enforcement and micro-segmentation.

In older security models, having the right password would be enough to grant access to sensitive data. But there are more questions you can and should be asking: Is the user coming from a known location? Are they using a familiar, secure device? Can we use multi-factor authentication to confirm their identity? There are a variety of security controls you can leverage to ensure the person trying to access your system is who they say they are.

Another question to ask is, *Should* this *user be gaining access to* this *part of the system?* Just because someone is authorized to access *some* sensitive data doesn't mean they should have access to *all* sensitive data. Privileged access management allows you to create access controls to limit certain users or groups of users within your systems

netdocuments®

5 Steps to Implement a Zero-Trust Security Model

4 Continuously monitor your systems.

This should be a no-brainer. Zero-trust means you don't even trust the system you set up to keep you secure! Stay aware of new security threats or trends and train your team if necessary. Look out for weak points in your system and respond as soon as you recognize one.

5 Embrace security automation and orchestration.

While some of these steps may sound daunting, the truth is that there are a variety of tools available that can help you manage your sensitive data safely and create a zero-trust environment for your firm that is effective and easy to use.

NetDocuments Can Help

Using a platform like NetDocuments can make it easier to implement a zero-trust security system. Within the platform you're able to manage document, workspace, and cabinet permissions. This enables you to set user access controls, including whether they have permission to view, edit, share, etc.

We also log every interaction with a file automatically—every open, download, edit, and upload—so you can always track down the source of an issue and resolve it quickly and easily.

Find out how NetDocuments can help you reach a true zero-trust security model.

netdocuments.com/demo