Zero Trust Architecture: An Imperative for Law Firms

by Sharon D. Nelson, Esq. and John W. Simek

The Good Old Days of Cybersecurity

Life really was simpler once, in the early days of cybersecurity. We had a clear network perimeter defined and knew we needed to protect all law firm data, users and devices inside the perimeter. Now we have employees working from home regularly, data in the cloud and vendors who have integrations with our networks and technology even including HVAC systems.

Law firms became accustomed to the network perimeter approach. They budgeted for tools to protect the perimeter and it became the norm for a very long time. Those days are now officially gone. To add to the misery of law firms, the cybercriminals are increasingly sophisticated – and successful in their attacks – causing a world of hurt in the form of data breaches which often become public, resulting in the loss of client confidence in the firm's ability to protect client data.

Sadly, law firms are a "one-stop shop" for cybercriminals. Break into a company and you will primarily get that company's data. Break into a law firm and you'll get the data of many clients. As an example, imagine breaking into a merger and acquisitions firm (among many other desirable law firm targets). Data is the new oil, right? You could hold the data for ransom, make a killing on Wall Street or use the data to infiltrate the law firm's clients. The nightmare scenarios are endless, as many law firms have discovered to their chagrin.

The Accelerating Ascension of Zero Trust Architecture

Zero Trust Architecture (ZTA) has been coming at us for a while and it is now officially here, championed by the U.S. government, leading technology firms and cybersecurity experts. In one portion of Deloitte's Tech Trends 2021 report, the title is "Zero trust: Never trust, always verify." The subhead is "Security in the age of the porous perimeter." On January 26, 2022, an Executive Order was released "requiring agencies to meet specific cybersecurity standards and objectives by the end of Fiscal Year (FY) 2024 in order to reinforce the Government's defenses against increasingly sophisticated and persistent threat campaigns."

We began to lecture to legal groups on Zero Trust several years ago. At first, we got blank stares from the lawyers. They had never heard of it, didn't know why it was needed, and were reluctant to embrace it. Our intent in the early days was to plant the seed of Zero Trust in the heads of those responsible for technology budgets. In other words, think about budgeting for Zero Trust even if you don't know what it is.

Things have changed over time, but we still have a long way to go. As we lecture these days, there is a small minority of lawyers who are aware of Zero Trust – and know that they will have to embrace it. But those lawyers are still a minority.

And even those lawyers are confused about Zero Trust. They ask us for a Zero Trust product recommendation. There is no such thing. It doesn't come in a box or bag. Zero Trust is an architecture, not a product. Pretty much, the legal world remains at sea when it comes to understanding Zero Trust and all its many changes to "old school" cybersecurity.

What is Zero Trust?

The obvious question is…what is zero trust? The concept of zero trust networks has been around for at least a decade, but cybersecurity events such as SolarWinds, Colonial Pipeline, Kaseya and attacks on Microsoft on-premise Exchange servers have brought renewed focus to the Zero Trust discussion.

The National Security Agency has stated, "The Zero Trust security model assumes that a breach is inevitable or has likely already occurred, so it constantly limits access to only what is needed and looks for anomalous or malicious activity. Zero Trust embeds comprehensive security monitoring; granular risk-based access controls; and system security automation in a coordinated manner throughout all aspects of the infrastructure in order to focus on protecting critical assets (data) in real-time within a dynamic threat environment. This data-centric security model allows the concept of least-privileged access to be applied for every access decision, allowing or denying access to resources based on the combination of several contextual factors."

In other words, trust nothing and constantly verify, even if access was previously authorized. Zero Trust gives new meaning to Ronald Reagan's words, "Trust, but verify."

In simpler times, when we had a security perimeter, once a device or person was trusted, that trust was not re-verified. This meant that if someone got access to a user's credentials, they were permitted to access the network and data no matter who they really were. Since users and devices regularly move from inside the network to outside, the Zero Trust approach means that a once-safe device cannot continuously be assumed to be safe. We know – it's enough to make your head hurt.

The 'trust nothing and constantly verify' means that every device, user, application, network traffic, etc. is untrusted. Every attempted access needs to be authenticated and explicitly authorized with the least amount of privilege. Multi-factor authentication (MFA) is a good first step to authenticate a user.

Unlike our current "flat" network, we'll need to segment the network into much smaller pieces that can be monitored and controlled. A user could be authorized for access to resources on one segment but denied access to resources on a different segment.

It's not just users either. Application access also needs to be authorized. In other words, if a piece of software wants to access data in a database, the application needs to be authenticated for access. The type of access is also verified and granted. Just because an application can access data in a database doesn't mean it can **change** the data. Perhaps only read or view access is granted. Next generation firewalls will monitor and control traffic between the various segments to assist in building the Zero Trust architecture.

As if we need additional challenges, migration to more cloud services increases the complexity of access. Hybrid cloud solutions require strict enforcement of least privileged access. Users and resources should have just enough privileges to get the job done and then expire. In other words, the trust factor is reset back to zero. If future access is needed, authorization must occur again. This is an exception to the "one and done" of cybersecurity.

Zero Trust Assumes a Breach

In a breach-ridden world, it is fundamental to cybersecurity that we assume you have been breached, meaning that an attacker has already compromised your network and remains present within the environment. This assumption explains the need for network segmentation. Compromising one segment

of the network won't allow complete access to all the firm's data or resources. This is critical to stop lateral movement within the environment.

Assuming a breach means all access should be denied by default. Harsh, but necessary. It also means that we need to have a way to continuously monitor access to all resources, monitor any configuration changes and certainly monitor all network traffic for suspicious activity.

Where Do You Start?

The strange answer is 'it depends'. For endpoints, apps, network, data and automation, there doesn't seem to be a clear starting point. Security pros vary a great deal in which components they feel are top priority.

That said, strong authentication is usually prioritized for identities. Another priority is threat detection tools. Beyond that, paths deviate depending on the needs of the entity.

Once you embark on implementing Zero Trust, you should realize the following benefits:

- Increased security and better compliance
- Increased speed of threat detection and remediation
- More tightly protected client data
- More simple security analytics
- Containment of security breaches
- More secure remote work force

These are just a few of the many benefits. As a rule, once Zero Trust is implemented, everyone is on board and grateful for the substantially increased security.

What Will Zero Trust Implementation Cost?

The short answer is that most law firms don't know – yet. We expect that, by now, the reader understands the complexities of Zero Trust. Implementing it will not be cheap – or easy. Selling it to law firm management may be difficult. Management is not likely to find this wholesale change in security appealing, both because of the monies and time expended, but also because you cannot "set it and forget it" when it comes to Zero Trust.

In fact, it is likely that most firms will continually review their ZTA to determine what changes are needed, at least annually and perhaps more often in large firms. It seems likely that many mistakes will be made along the way, necessitating corrective measures as cybercriminals continually school us in the variety of ways that they can exploit our networks. Make no mistake about it, though – Zero Trust is going to make breaking into networks a much more complicated endeavor.

Microsoft Security: Zero Trust Adoption Report

There is perhaps no single technology vendor with the influence that Microsoft has on law firms. So, it was noteworthy that Microsoft issued a "Zero Trust Adoption Report" (https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWGWha) in July of 2021.

In the report, Microsoft surveyed more than 1,200 security decision-makers over a 12-month timeframe about their Zero Trust adoption. Here are some of the highlights:

- Zero Trust is taking off. 96% of security decision-makers said that Zero Trust is critical to their organization's success.
- The top reasons for Zero Trust adoption are increased security and compliance agility, along with quick detection of threats and remediation as well as simplicity and security analytics.
- Bearing in mind that the folks surveyed are likely from large organizations, it is not surprising that 90 percent of those surveyed are familiar with Zero Trust and 76 percent are in the process of implementation—a mammoth increase from the 2020 report of 20 percent familiar with Zero Trust and 6 percent in the process of implementing it, respectively.
- 35% now describe Zero Trust as fully implemented.
- Hybrid work, as we noted above, is driving adoption. 81 percent of the organizations have already begun the move toward a permanent hybrid workplace. Zero Trust will be critical to ensure security given the IT complexity that comes with hybrid work.
- More than half of respondents expect the importance of their Zero Trust strategy to increase by 2023. Unsurprisingly, 73 percent expect that their Zero Trust budget will increase.

Quite apart from the report, it is noteworthy that Microsoft says in the report, "We not only recommend this approach with our customers and partners, we embrace it in our approach to global security and software development here at Microsoft." It has been our observation that, as Microsoft goes down major paths of advancement, so do the law firms which are very dependent on Microsoft.

The NSA on Embracing Zero Trust

In February of 2021, the National Security Agency (NSA) issued "Embracing a Zero Trust Security Model" which law firms will certainly want to read, especially since it is only seven pages long – and designed to give readers a 10,000 foot view of Zero Trust.

Consistent with assumptions from cybersecurity professionals, the document stresses that Zero Trust assumes a breach is inevitable or has already occurred, so it limits access to what is needed and constantly scans for anomalous (very important to know why there is unusual activity) or malicious activity. The NSA is monitoring technologies that contribute to Zero Trust solutions, so keeping up with its guidance may be very useful. We are really seeing the federal government "upping" its cybersecurity posture and knowledge.

Practically speaking, we agree with the NSA's advice that everyone must be committed to a Zero Trust mindset – for our purposes in the legal sector, that means a law firm's managing partners, IT/Security providers, attorneys and staff.

Looking to a Future with Zero Trust

2022 will bring even more focus to Zero Trust. In a Forester survey, two-thirds of those surveyed stated expansion of their zero trust budgets for 2022, "allocating 36 percent of their total spend to micro-segmentation projects." As we've previously mentioned, network segmentation is key to tightening control of data access and minimizing potential lateral movement of a cyber attacker.

The corporate world is already embracing Zero Trust as the statistics above demonstrate. Law firms? The AmLaw 200 perhaps, but not most of the mid-size and smaller firms. But without question, clients and insurance companies are going to pressure law firms to adopted Zero Trust sooner rather than later. Expect to see the major players in law adopt Zero Trust in 2022 and 2023. Even mid-sized firms are likely

to implement Zero Trust in 2022 and 2023. The government's own requirement for Zero Trust adoption by 2024 is setting the "gold standard" for everyone. This is a train that is rapidly pulling out of the station – it's time to get aboard!

Sharon D. Nelson, Esq. is a practicing attorney and the president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA. snelson@senseient.com.

John W. Simek is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional, Certified Ethical Hacker and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity and digital forensics services from their Fairfax, Virginia firm. jsimek@senseient.com.