Akamai

WHITE PAPER

Securing the Modern Law Firm

Protection for critical applications and client data

Introduction

Legal professionals handle sensitive data every day. With that in mind, many firms are investing in more advanced security controls, and focusing their efforts on designing their IT systems and processes around the concept of Zero Trust, to secure their critical applications and control end user access.

The Zero Trust approach implements a model of least privilege, ensuring that authorized users, systems, and applications only have the access appropriate for their respective functions, while also protecting against lateral movement, ransomware, and unauthorized access. One of the most flexible and most secure ways to implement the Zero Trust approach is to use microsegmentation.

To understand why this is important, let's start by reviewing some history.

High-profile breaches: A wake-up call to the legal industry

For years, U.S. federal authorities have warned that big law firms are easy targets for cybercriminals because they are home to information-rich repositories of corporate data. The FBI began warning prominent law firms that they were being targeted by organized cybercriminals as early as 2009. In 2011, they went as far as inviting 200 of the largest law firms to discuss the rise in sophisticated cyberattacks targeting the sector.

> **One of the most flexible and most secure ways to implement the Zero Trust approach is to use microsegmentation.**

Since 2014, more than 100 law firms in 14 states have reported data breaches, according to Law.com. The American Bar Association's 2022 Legal Technology Survey Report, an annual survey exploring the use of technology in the legal industry, found that more than a quarter of law firms (of all sizes) experienced a security breach. The impact of breaches ranges from downtime, caused by ransomware, to lengthy legal disputes after client data surfaces on the internet.

In 2015, the legal sector appeared on Cisco's annual ranking of industries targeted by hackers for the first time. As a result, many financial institutions have started requiring law firms to undergo periodic audits of their cybersecurity practices when doing business together.

In particular, two massive breaches of international law firms Mossack Fonseca & Co and DLA Piper resulted in a wake-up call for the entire legal and financial industry. In a leak dubbed the "Panama Papers," more than 11 million documents, over four decades of records, were leaked from the offshore law firm Mossack Fonseca & Co. The breach exposed tax havens and the offshore accounts of global companies and influential world leaders, with severe consequences. In 2018, the firm announced it was shutting down, largely due to fallout from the breach. Law firms have an ethical and fiduciary responsibility to make all reasonable efforts to protect the information they hold. The "Panama Papers" data leak represents the largest breach thus far of confidentiality between a law firm and its clients and has contributed to a change in the industry's cybersecurity approach. However, despite the newfound focus on improving security posture, attackers show little signs of slowing down.

> **More than 1 in 4 law firms have experienced a security breach.**
>
> — American Bar Association Legal Technology Survey Report 2022

Almost simultaneously to Mossack Fonseca & Co's leak, DLA Piper, one of the world's most prominent law firms with a presence in over 40 countries, fell victim to a NotPetya malware attack. It cost the firm weeks of disruption, millions in lost business, recovery costs, and some very bad publicity.

More recently, after a ransomware attack, Grubman Shire Meiselas & Sacks lost 756 gigabytes of data about their high-profile clientele, including Lady Gaga, LeBron James, and Madonna. The law firm was reluctant to pay the ransom, which led the attackers to leak information on Lady Gaga and auction off what they claimed was data containing details on other clients.

Modern law firms: Time for modern cybersecurity solutions

The majority of the breaches outlined have involved advanced persistent threat (APT) attacks that included phishing, malware, and ransomware to steal sensitive client data, merger materials, intellectual property, and financial information. Lured by vast amounts of money, attackers are increasingly backed by organized crime groups making significant investments in attack tools and professional teams.

> **Firms that lack proper segmentation in their IT environment risk being denied coverage in the event of a data breach.**

More clients are now considering cybersecurity as a serious factor in deciding which law firm to do business with today. Firms that lack modern security controls are more likely to lose business to firms that have taken steps to improve their security posture and show their commitment to securing client data. Also, many cyber insurers are now requiring some form of segmentation for sensitive data and applications. Firms that lack proper segmentation in their IT environment risk being denied coverage in the event of a data breach.

What's missing:
Protecting the firm's critical applications

As you can see, law firms are no longer the safe repository of privileged information that they once were. Today, cybercriminals recognize law firms as vaults of proprietary, sensitive corporate data that are optimal targets for cybersecurity attacks.

In fact, law firms are often perceived as easier targets than most of their clients. That is why an attacker wanting specific data from a corporation will often try to get this data through its law firm first. The sensitive nature and the variety of information that law firms store, coupled with their generally weaker security controls, make them a lucrative target for attackers.

Attackers are incredibly interested in the information stored in the law firm's business-critical applications, most notably the document management system (DMS) and email. From an IT security perspective, a law firm's most critical business applications are its DMS and email applications. These applications hold the lion's share of the highly confidential, sensitive, and privileged client information, and in many cases they no longer reside only in on-premises data centers.

DMS applications offer a wide range of functions and features, including a centralized organization of files and folders, version management, email management, document editing, indexing and searching, permission management, and more. They are often deployed across heterogeneous IT environments with a mix of virtualized and bare-metal servers, and require integration with multiple other systems with varying levels of internal security. While these integrations can make a DMS more useful to a law firm, they can also make it less secure and drastically increase its attack surface.

Endpoints have also become so mobile and dynamic that traditional security solutions often fail at protecting them, since like many organizations, law firms have primarily focused their security tool investments on the perimeter. These solutions no longer provide the level of protection law firms need to secure critical applications. Additionally, the reality is that many law firms still lack the controls necessary to detect or prevent an attacker from moving laterally and accessing sensitive data systems once a threat actor accesses the network via a compromised endpoint.

Given all of these challenges, many modern law firms are now beginning to invest in a new generation of cybersecurity solutions capable of addressing their unique and changing needs. Software-based segmentation, specifically microsegmentation, supports a Zero Trust approach to securing critical applications and data by providing a more granular approach to controlling communications within the network, allowing only those authorized users and systems to communicate with critical applications. This makes it much more difficult for an attacker to move laterally throughout your network, limiting the scope of a potential breach.

COVID-19 made things even more challenging:

- Many law firms transitioned to remote work
- Because of this, employees no longer connected to the network from their corporate office, but instead, from unsecure home networks
- The increased use of VPN and VDI solutions made implementing security policies and attributing network traffic to authorized users even more challenging

Four ways Akamai helps law firms protect client data

Complete visibility

Gain comprehensive workload visibility to understand all open connections to applications that house sensitive data.

User access control

Implement policies that control access to applications and data regardless of where it resides: on-premises or in the cloud.

Software-based segmentation

Quickly and flexibly microsegment critical applications such as DMS and email to limit exposure in the event of a breach.

Threat detection and prevention

Combine dynamic segmentation and deception features to detect and contain active breaches and protect client data.

Unified protection with Akamai Guardicore Segmentation

Akamai Guardicore Segmentation offers the industry's most comprehensive microsegmentation solution for protecting business-critical applications. It dramatically accelerates the implementation of segmentation policies, simplifies ongoing maintenance, and is ultimately more effective in mitigating threats that rely on lateral movement to succeed.

> **To better protect client data, many law firms are turning toward solutions like microsegmentation to implement a more granular approach to controlling communications within the network, allowing only those authorized users and systems to communicate with critical applications.**

Our solution provides a visual map of all applications and other assets in your data center, along with their dependencies. Security operators can then quickly and intuitively create and enforce network and process-level security policies to isolate and segment their critical applications and assets. This software-defined approach to segmentation is independent of the underlying infrastructure, allowing it to consistently protect workloads that span on-premises systems (both legacy and modern), VMs, containers, clouds, and devices.

Policies can be created around individual or logically grouped applications, regardless of where they reside in the data center. These policies dictate which applications can and cannot communicate with one another, supporting a Zero Trust approach. Another important capability exclusive to Akamai Guardicore Segmentation is our integrated breach detection and response, which reduces the complexity of managing multiple dedicated tools. Breach detection and response are required to comply with regulations from the New York State Department of Financial Services (DFS), other industry mandates such as PCI DSS, and increasingly by high-profile customers auditing their law firms.

Akamai Guardicore Segmentation: Comprehensive protection for critical applications

Protect client data: Create the foundation for a Zero Trust framework, and enforce network security hygiene and best practices, in increasingly complex and interconnected environments.

Isolate critical applications from the broader IT infrastructure: Segment high-value assets — such as a DMS or email application — with ringfencing policies, reducing exposure to threats from both inside and outside of a law firm.

Adopt the cloud securely and quickly: Map workloads and take inventory of all critical applications and their dependencies before migration. Ringfencing policies use these maps as a foundation for consistent security that follows workloads throughout the migration process. This approach enables faster and more secure migration of workloads into the cloud, keeping the same security controls in place.

Ensure business continuity with efficient breach mitigation: Use granular visibility into east-west traffic, and breach indicators set to alert on abnormal movement, to stop threat actors before ransomware or another threat brings business to a standstill.

Reduce risk by limiting lateral movement: Set internal boundaries and ringfence business-critical applications and systems to reduce the attack surface. This effectively protects against the lateral spread of attacks, limiting damage in the event of a breach.

Conclusion

Akamai Guardicore Segmentation provides law firms with a solution that allows them to visualize and understand the open connections that could be used in an attack. Moreover, the solution enables firms to secure those connections using microsegmentation.

Our solution provides the comprehensive security coverage for a law firm's critical applications across hybrid IT environments, residing on both virtualized and bare-metal machines, and across on-premises or IaaS or PaaS. It provides visibility into application dependencies and flows, granular segmentation policy enforcement, and integrated breach detection and response. These capabilities are crucial to preventing data loss and business downtime scenarios that may disrupt a law firm's business.

Law firms using Akamai Guardicore Segmentation can better understand their environment, secure their critical applications, and drastically reduce the impact and response time in the event of a breach. Moreover, the software-based segmentation capabilities provided are significantly more cost-effective, less time-consuming, more flexible, and more effective than those from many other segmentation solutions, such as traditional firewalls. Overall, Akamai Guardicore Segmentation is an industry-leading security solution that is well equipped to meet the security challenges of the modern law firm.

Discover how you can safeguard your clients' valuable data. Learn more about us at akamai.com/guardicore.