Guardicore

SECURING THE MODERN LAW FIRM

PROTECTION FOR CRITICAL APPLICATIONS AND CLIENT DATA

WHITE PAPER

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 around a Zero Trust approach to secure critical applications and control end user access.

The easiest, most flexible, and most secure way to implement a Zero Trust model is to use micro-segmentation.

The Zero Trust approach implements a least privilege model, 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. The easiest, most flexible, and most secure way to implement a Zero Trust model is to use micro-segmentation.

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

HIGH PROFILES BREACHES: A WAKE UP CALL TO THE LEGAL INDUSTRY

For years US 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.

Since 2014, more than 100 law firms in 14 states have reported data breaches, according to Law.com. The American Bar Association's 2019 Legal Tech Report, an annual survey exploring the use of technology in the legal industry, found that over one in four law firms has experienced a security breach. These breaches have impacted law firms of all sizes, including large firms such as DLA Piper and smaller firms such as Warden Grier. 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.

1 in 4

law firms have experienced a security breach.

American Bar Association
TechReport 2019

In particular, two mega breaches of the 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 of confidentiality between a law firm and its clients to yet occur 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.

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. So far, the law firm has been reluctant to pay the ransom, which has led the attackers to leak information on Lady Gaga and auction off what they claim is 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.

More and more clients are now considering cybersecurity as a serious factor in deciding which law firm to do business with today. Firms who 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.

Clients are now considering cybersecurity as a serious factor in deciding which law firm to do business with today.

WHAT'S MISSING: PROTECTING THE FIRM'S CRITICAL APPLICATIONS

As you can see, law firms are no longer the safe repository of client privileged information, such as merger plans and high-profile deals, 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 clients. That is why an attacker that wants to get data from a corporation will often try to get this data through its law firm first. The sensitive nature and variety of information law firms store, coupled with weaker security controls, make firms a lucrative target for attackers.

Attackers are incredibly interested in the information stored in law firms' business-critical applications, most notably the DMS and email. A law firm's most critical business applications are its Document Management System (DMS) and email application. These applications hold the lion's share of the highly confidential, sensitive, and privileged client information. They also increasingly 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 environments such as 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, it also makes it less secure and drastically increases 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 and endpoint-based solutions. 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 bad actor accesses the network.

Given all of these challenges, many law firms are now beginning to invest in a new generation of cybersecurity solutions capable of addressing the unique and changing needs of the modern law firm. Micro-segmentation solutions provide a more granular and effective security posture, allowing only authorized users and systems to access critical applications.

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 insecure 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 Guardicore 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 micro-segment 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.

To better protect client data, many law firms are turning towards micro-segmentation solutions to implement a more granular and effective security posture, allowing only authorized users and systems to access critical applications.

UNIFIED PROTECTION WITH GUARDICORE CENTRA

The Guardicore Centra Security Platform offers the industry's most comprehensive micro-segmentation solution for protecting business-critical applications. It dramatically accelerates the implementation of segmentation, simplifies ongoing maintenance, and is ultimately more effective in mitigating threats.

Guardicore provides a visual map of all applications in the data center and their dependencies. Security operators can then create and enforce network and individual process-level security policies to isolate and segment critical applications and assets. This software-defined overlay approach is independent of the underlying infrastructure and protects workloads that span across on-premise legacy systems, VMs, containers, and clouds.

Policies can be created around individual or logically grouped applications, regardless of where they reside in the data center. These policies dictate which can and cannot communicate with each other, creating the foundation for a Zero Trust framework.

Another important capability included in Guardicore Centra is breach detection and integrated response, which reduces the complexity of managing multiple dedicated tools. Breach detection and response are required to comply with the new 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.

GUARDICORE CENTRA: 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 ring-fencing 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. Ring-fencing 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 bad actors before ransomware or another threat brings business to a standstill.
- **Reduce risk by limiting lateral movement:** Set internal boundaries and ring-fence 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

Guardicore 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 micro-segmentation to implement a Zero Trust approach.

Guardicore Centra provides the widest security coverage for a law firm's critical applications across hybrid environments, residing on both virtualized and bare-metal machines, and across on-premises or IaaS or PaaS. Centra provides visibility into application dependencies and flows, segmentation policy enforcement, and integrated 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 Guardicore Centra can better understand their environment, secure their critical applications, and drastically reduce the impact and response time in the event of a breach. Moreover, Centra's software-based segmentation capabilities are significantly more cost effective, less time consuming, more flexible, and more effective than traditional firewalls. All in all, Guardicore is the right solution for the unique and changing needs of the modern law firm.

DISCOVER HOW YOU CAN SAFEGUARD YOUR CLIENTS' VALUABLE DATA

Learn more about the Zero Trust security model:

www.guardicore.com/zero-trust-security

About Guardicore

Guardicore is the segmentation company disrupting the legacy firewall market. Our software-only approach is decoupled from the physical network, providing a faster alternative to firewalls. Built for the agile enterprise, Guardicore offers greater security and visibility in the cloud, data-center, and endpoint. For more information, visit www.guardicore.com or follow us on Twitter or LinkedIn.

Guardicore