VARS

Whitepaper

BREACH PROTECTION FOR LAW FIRMS

Powered by Cynet

Business Challenge

Law offices are built on information, which is now almost fully digitized. Sensitive personal and legal content is created, accessed and shared across a mix of devices including desktops, laptops, tablets and smartphones. Employees, outside contractors and clients can access the firm's systems at any time, from virtually anywhere. Increasingly, and especially since the Covid pandemic, much of the access comes from outside of the network perimeter, extending access to virtually anywhere in the world with a Wi-Fi connection.

Devices used to access content within law firms often double as personal devices, which decreases control and increases risks. And, because many devices can contain sensitive client data, they must be protected from threats whether on or off the corporate network. Fraudulent access to a single endpoint could result in a devastating loss of data, or worse, the entry point for access to the wider corporate environment.

Law firms have become very attractive targets for cybercriminals due to their highly valuable repository of sensitive legal, corporate, personal and financial information. Several law firms fell victim to ransomware attacks during 2020, such as the one perpetrated against Seyfarth Shaw in October. The ransomware was able to encrypt data on several systems and forced the company to shut down its email service and other systems. While the firm maintains that no confidential data was stolen, they did suffer from disruption and a potential reputational impact. Ransomware attacks that employ cryptolocking techniques can lead to lengthy recovery periods and loss of intellectual property.

Even the largest law firms tend to be supported by small cyber security teams that are sometimes also responsible for general IT support. With a primary responsibility of supporting data repositories and user systems, the staff focused on security often lack the time and expertise required to adequately protect the organization from cyberthreats. This is especially risky in a highly distributed, multi-office environment with an extensive collection of company, personal and third party devices remotely accessing the corporate network.

Top Security Challenges

Highly distributed remote access to corporate systems and intellectual property

Small security teams with limited cybersecurity technology budgets and expertise

Reliance on traditional antivirus and anti-malware software provides limited protection against newer threats like ransomware and cryptolocking

> “When the Covid pandemic hit, Cynet allowed us to extend protection to all personally owned endpoints at no extra cost. Cynet is a true partner.”
>
> CIO, Law Firm

> “It literally took us less than a week to deploy and become proficient using the Cynet platform. Protecting the company is no longer confusing and chaotic.”
>
> CISO, Law Firm

Key Cyber Security Challenges

Protecting a law firm environment is challenging given the highly distributed environment and unfettered access to corporate assets from outside the network perimeter. Protecting endpoints while outside of the corporate network is particularly complicated, especially given the pace of information exchange typical in the legal world. A single malicious file infiltrating a single laptop could lead to devastating corporate-wide consequences.

Limited visibility across environment

Many law firms rely on basic antivirus and anti-malware software, which can only detect a fraction of advanced attacks. This type of software provides limited protection against newer attack techniques like ransomware and is especially vulnerable to highly advanced targeted attacks. The bottom line is that even the best heuristic or behavior-based malware detection techniques cannot detect and prevent 100% of threats.

To extend protection beyond antivirus solutions, companies incorporate additional tools such as endpoint detection and response (EDR) and network detection and response (NDR). EDR solutions were borne out of the premise that because all endpoint threats cannot be prevented with antivirus software, these threats still need to be detected after they successfully infect an endpoint. EDR solutions continuously monitor endpoints to detect malicious activity and system behaviors that are indicative of compromise.

NDR solutions extend protection to the network to provide additional visibility across the environment. If an attack somehow bypasses both an antivirus and an EDR solution, the ability to detect lateral movement and other network traffic indicators could uncover a threat actor that has successfully infiltrated the environment.

Finally, protecting a variety of endpoint devices, interconnected systems and applications with a range of operating systems, updates and patch history is a challenge for the largest global companies. Small to mid-sized law firms face the same risks with a fraction of the resources.

Siloed security controls

While each of the security controls described above extend needed visibility across the environment, they are not without their problems. First, EDR and NDR solutions are notorious for false positive alerts. Security analysts either chase down these false flags or tend to ignore all but the highest risk alerts. In the first instance considerable time is wasted, in the second instance ignoring alerts is far from good security practices and opens the company to compromise.

Key Cyber Security Challenges

Cont'd

Siloed security controls

cont'd

Siloed controls also mean more "panes of glass" for the security team to monitor and access when investigating potential threats. Because each security tool has a separate management console and presents information differently, it is challenging for security analysts to make sense of all the information being presented and then link activities together between the various security controls to see the big picture. This is why stealthy attacks are able to bypass environments with multiple layers of controls.

Small security teams with limited bandwidth

Putting siloed controls aside, which do create significant manual overhead, most security tools require a meaningful human investment to operate. When threats are discovered, security analysts must investigate to determine the root cause and then uncover the full scope of the attack across the environment.

Once the root cause and scope are determined, all threat components must be fully remediated. This often involves access to multiple systems and can be a painstaking, time consuming process.

Small security teams with limited cybersecurity skills

With the threat landscape rapidly evolving even the largest, well funded security teams are vulnerable to threats. Look at any review of breaches against large companies and it's quick apparent that even the best cybersecurity experts with leading-edge tools are challenged to protect their organizations. For smaller security teams with limited technology budgets and cybersecurity expertise, the risk of breach is compounded exponentially.

The Cynet-VARS Approach

Cynet was built for smaller cyber security teams with limited bandwidth, cybersecurity expertise and technology budgets. Cynet XDR provides a single, unified platform to automatically prevent, detect, investigate and fully remediate the broad range of attack vectors faced by law firms. Visibility across endpoint, network and user activities, plus the power of deception provides the broadest and deepest protection against all threats.

Cynet XDR is the only solution that triggers an automated investigation following each endpoint, user, or network alert, fully disclosing its root cause and scope and applying all the required remediation activities to fully eliminate the threat. Cynet also provides a broad set of automated and highly customizable remediation actions to address threats according to your preferences. Moreover, Cynet provides an expert team of cybersecurity experts to augment and guide your team 24 hours a day, 7 days a week – included with the Cynet 360 platform.

Cynet Benefits for Law Firms

Easy to Deploy and Operate

The Cynet agent can be deployed to over 5,000 endpoints in less than an hour. While many solutions require months to deploy and become fully operational, Cynet is fully functional within 24 hours of deployment, providing all the insights and protections available in the platform. The Cynet console was built to be intuitive and effortless so smaller security teams do not need years of expertise to operate.

Full Visibility Out of the Box

Cynet XDR provides complete visibility and multiple points of telemetry leading to low false positives and early detection of stealthy threats. A single, unified Extended Detection and Response (XDR) platform that provides Next Generation Antivirus (NGAV), Endpoint Detection and Response (EDR), Network Detection and Response (NDR), User and Entity Behavior Analytics (UEBA) and Deception technology fully integrated and easily configurable with a single dashboard out of the box.

Cynet Benefits for Law Firms

Cont'd

Automated Protection

Cynet's Incident Engine automatically performs all required threat investigation and response actions, uncovering the root cause and full scope of high risk threats and taking appropriate actions to fully eradicate the threat across the environment. Cynet additionally provides an array of remediation playbooks that can be executed automatically in response to a detected threat for immediate response or can be triggered manually to provide more oversight and control. Cynet's autonomous response actions provide the comprehensive protection needed by smaller and overburdened security teams.

Include Managed Detection and Response Oversight

All Cynet clients are automatically protected by a comprehensive Managed Detection and Response (MDR) service, included with the Cynet platform at no extra cost. Small security teams at law firms rely on Cynet's MDR team (CyOps) to proactively monitor their environment 24x7 to ensure nothing is overlooked. They can contact VARS at any time for guidance in configuring the Cynet platform, providing attack investigation expertise and guiding them on all necessary response actions. CyOps becomes an extension of the law firm security team, adding resources and world-class cybersecurity expertise.

Summary

Protecting law firms from cyberattacks is beyond challenging, especially with a smaller, less experienced security team. With limited budgets, most small to mid-sized law firms cannot obtain, integrate and operate the required security controls to protect the organization from advanced threats. Law firms rely on Cynet's intuitive, comprehensive breach protection platform to solve their security challenges, knowing they always have a team of cybersecurity experts watching their backs.