WHITEPAPER

RAISING THE BAR - THREAT DECEPTION FOR THE LEGAL SECTOR

TABLE OF CONTENTS

THE STATE OF INFORMATION SECURITY IN THE LEGAL INDUSTRY

Malicious actors are continuously looking for inventive ways to steal sensitive information from organizations with highly-sensitive and high-value data. Many of these organizations have robust security infrastructures in place, making a successful breach challenging. As a result, cybercriminals have turned to third parties, such as organizations within the legal sector, to obtain the sensitive data, intellectual property, M&A information and trade secrets they are after.

In 2015, research concluded that the legal industry was far behind the curve in relation to cybersecurity preparedness and response. Challenges persisted, as attacks in this industry plagued some of the largest law firms representing numerous high-profile banks and corporations in 2016.[2] Due to the highly sensitive nature of the data housed by law firms, they will continue to be a key target for cybercriminals—and must continue to be diligent when it comes to protecting their confidential data and information.

> Deception can play a powerful role in demonstrating how the organization detects threats that bypass perimeter controls.

As one of the most widely used third-parties, legal organizations are responsible for the confidentiality and integrity of client data. From intellectual property and pending patents, to case strategy and confidential client data, to M&A details and fiduciary records, legal organizations are custodians of some of the most sensitive data to a person or organization. Safeguarding this information remains the highest priority, and should it be compromised, the organization faces many repercussions, from legal penalties to financial liabilities, to the loss of clients, including the ability to remain in business.An example that highlights the importance of having strong cybersecurity measures, especially in-network detection, for law firms is the infamous 2016 Panama Papers breach.[3] In what was called at the time "history's biggest data leak."[4], attackers stole over 2.6 terabytes of data and distributed 11 million documents from Panamanian law firm Mossack Fonseca. The documents revealed that many shell corporations were used for illegal purposes, such as fraud and tax evasion. The data covered nearly 40 years and named various world leaders and businesses. Data from more than 200,000 offshore organizations was released in the breach, and most of them had to deal with hefty financial, legal, and reputational repercussions from the incident.

2017 did not yield improvement and was a relentless year of cyberattacks in every sector, indicating an ever-present and dire need for change. Just a few of the many data breach news headlines from last year include, "Uber ousts in-house counsel who suppressed information about 2016 data breach," "Yahoo General Counsel Ron Bell Resigns Amid Data Breach Controversy", "Equifax looks to In-House Lawyer to 'Build a New Future' After Massive Breach," and "Ransomware Attack on DLA Piper Puts Law Firms, Clients on Red Alert."[5] The future success of the legal sector depends on their ability to keep their client's sensitive data protected and secure from advanced threats.

Not only is information security vital to the reputation and success of legal organizations, but executives and boards are looking toward the legal industry to aid in responding to security threats. This relationship results in a sharp upswing in responsibility when it comes to handling and having proficiency in security best practices. Failure to demonstrate a competent information security strategy can result in law firms being turned away by clients for cyber practices that are not up to snuff.

THE "SECURITY FIRST" APPROACH AND DECEPTION TECHNOLOGY

"Security first" is an approach that recognizes cybersecurity not only as an information technology requirement, but as a competitive asset to differentiate an organization from peer offerings. Those in the legal sector have a special opportunity to draw attention to their adoption of a holistic security infrastructure, while building their business on a "security first" ideology through the implementation of deception technology into their security stack.

Legal organizations are actively turning to deception technology as the preferred method for early and accurate detection of threats that have bypassed other security controls. Some are first-time deception technology adopters, drawn to the accuracy and efficiency of the solution, while others are migrating off homegrown deception solutions for additional accuracy, scale and operational efficiency.

Deception technology gives legal organizations the internal visibility often lacking in traditional security infrastructures. Most prevention and detection solutions, such as firewalls, intrusion detection/prevention systems, and data loss prevention technologies, focus on traffic and activity entering and leaving the perimeter, so-called "north-south" traffic. Few are designed to look at intra-network “east-west” traffic, activity between systems within the organization. While north-south solutions are a necessary part of any security infrastructure, without east-west visibility, there is little a legal organization can do to detect threats that target internal data stores from other systems on the network. With a deception technology solution, security teams gain the necessary visibility to detect such activity and can show prospective and existing clients that they have a solution to cover such a detection gap.

Deception technology works by turning the network into a web of traps with misdirections that are designed to trick an attacker, whether human or automated threat actor, into engaging and revealing their presence. In a deception network, the attacker need make only one small engagement mistake to reveal their presence. By being present at the network and endpoint layers, deception technology blankets the network with lures and traps designed to attract and engage an attacker early in the attack lifecycle as they conduct reconnaissance or credential theft. Deception can also address client and regulatory requirements for safeguarding confidential client data, as it gives internal visibility into when insiders or unauthorized personnel attempt to access protected information.

> ”Security first” is an approach that recognizes cybersecurity not only as an information technology requirement, but as a competitive asset to differentiate an organization from peer offerings.

Unlike solutions that use behavioral or log analysis, a deception solution does not rely on learning the network baseline of activity, nor does it rely on pattern matching for signs of malicious activity. Instead, deception relies on creating confusion and misdirection, presenting decoy systems that masquerade as production assets to attract the attacker’s attention. When the attacker engages with the decoy, the system triggers a high-fidelity alert notifying security personnel of the activity. Decoy-based deception will alert on early reconnaissance and will scale across a wide variety of attack surfaces, giving security staff early warning and awareness that an attacker is in the environment

Deception technology uniquely addresses dwell time challenges legal organizations face for which there traditionally has been no easy solution. A deception solution provides immense value because it accurately and efficiently detects threats that are already inside the network and have bypassed perimeter controls.

Early attack detection can also be achieved through the detection of early credential theft. To reach sensitive client data, attackers will compromise systems to steal credentials that can then be used to move laterally within the network and escalate privileges to advance their attack. Breadcrumbs and lures at the endpoints further increase the likelihood that the attacker will engage with the decoy, as some of the credentials they steal will lead them to the deception environment. Having decoys and credential bait working hand in-hand has proven to be an extremely effective method for catching insiders, contractors, and suppliers who often can move around the network for long periods of time undetected.

> The ThreatDefend Platform's DecoyDocs solutions provides the ability to plant deception files that allow the organization to track documents that were exfiltrated.

Whether your organization is seeking detection in the cloud, in your network, for reconnaissance, phishing, insider threats, or ransomware, deception technology provides actionable alerts, visibility, and remediation capabilities that other security technology solutions do not match.

For those in the legal industry that excel at cybersecurity management, the advantages are clear: organizations that make cybersecurity a priority tend to have a competitive, technical, and economic advantage over those who do not make security a priority.

THINK DECEPTION IS DIFFICULT? THINK AGAIN.

The Attivo solution is designed to work for organizations in the legal sector of all sizes and with varying levels sophistication in terms of preexisting cybersecurity controls. Beliefs about deception technology being overly complex, having a high overhead, or requiring a large equip staff to deploy and manage the solution could not be further from reality. The Attivo solution is designed for ease of deception generation, deployment, and operations across an sizable set of attack surfaces at scale.

Attivo's Deception Makes it as Simple as 1,2,3.

1. Generate the Deceptions: Machine-learning is used to self-learn the unique behavior of differing networks, their applications, and their device profiles. For example, it is able to differentiate between specialty environments and an enterprise network as well as different credential naming conventions.
2. Intelligent and Agentless Deployment: As deception continuously learns the environment, the technology mimics network behavior, matches devices, and deploys deceptive credentials and assets that are indistinguishably authentic. Deception campaigns can be automatically deployed or can be reviewed and executed at the push of a button.
   a. The Attivo Networks agentless endpoint credential technology provides an extensive offering of deception breadcrumbs and non-invasive deploys without the need for additional CPU or traditional software infrastructure management.
   a. The company's ThreatDirect™ deception solution projects deception throughout the network without the need for additional hardware or infrastructure, making it extremely effective for deploying deception in cloud, remote office or micro-segmented networks.
3. Continuous Operation: Every aspect of the deception environment is monitored to determine when updates are required, credentials refreshed, and new deception decoys deployed. Additionally, deception can be automatically applied upon suspicion of foul play and following any attack, new deception is deployed to automatically refresh the deception environment. This prevents "fingerprinting" by attackers who would then know what to avoid.

The concept of deception is not new. However, the ability to do this accurately and at scale without human intervention has evolved and as such, has firmly earned Attivo Networks the business of organizations across all major verticals including the legal sector.

CHALLENGES

THE INTERNAL RISK

> Deception can play a powerful role in demonstrating how the organization detects threats that bypass perimeter controls.

When it comes to threats, the insider is the hardest for a security team to defend against. How does one protect their environment from disgruntled employees or those motivated by an opportunity for personal financial gain? How does one go about protecting the network from the employee who is unaware they are doing something potentially damaging? Insiders and suppliers have an inherent advantage in their attack because they already have access to the network. Detection of nefarious activities based on the behaviors of employees that are using valid credentials can be extremely difficult and often missed by security teams and traditional security tools.

There are three types of insider threats to be mindful of[6]: These threats also may not always appear in the form of an employee and often are through contractors or 3rd party suppliers. Regardless of the type, they can be extremely difficult for security teams to detect.

- The Accidental Insider. The Accidental insider is the most common threat to organizations in the legal sector. Security experts state that the most considerable cybersecurity risk stems from a firm's own well-intentioned employees. The accidental insider harms the company not with malicious intent, but simply because of poor decision making. They create weak passwords and reuse them across different services, click on links in emails or inserting random thumb drives, fall for social engineering attacks or simply don't keep their systems patched in a timely fashion.
- The Opportunistic Insider. An opportunistic insider is an employee who is familiar with the security controls in place and works to find a way around them. They may not initially set out to harm the company but may gain access to a valuable asset during regular business activities and benefit from compromising it, perhaps monetizing it through a sale or leaking it to enhance a social reputation.
- The Determined Insider. The determined insider seeks to do intentional damage. These employees may be disgruntled employees or even those spying for the competition.

DECEPTION FOR INSIDER THREATS

Because of the efficient way that deception technology detects threats already inside the network, it is effectively positioned to identify insiders before they can compromise client data, whether accidentally or intentionally.

1. The Accidental Insider. The accidental insider poses a threat to client data stemming from an inadvertent system compromise that leads to data theft or destruction, such as with a botnet, ransomware, or RAT infection that allows an external threat actor access to the system. When the attacker accesses the compromised system remotely, steals credentials, conducts reconnaissance and attempts to laterally move, the decoys, breadcrumbs and lures will serve to lead the attacker into the engagement environment and alert the security staff to his presence. With ransomware and malware infections, the decoys add the benefit of alerting upon compromise and providing the ability to isolate the infected system before damage can be completed.
2. The Opportunistic Insider. Usually, the presence of deception technology on the network is known only to a few within the organization, such as select members of the security and networking teams. An insider who chooses to bypass security controls generally does not have the access level or the knowledge of where all client data is. They will also not want to use their own credentials to log onto those systems to access data even if they do have access, as doing so will leave an audit trail that leads straight to them. They will thus attempt to steal credentials to gain access, hide their tracks, or conduct network reconnaissance to locate the specific data they are looking for. In either case, they will interact with deception decoys, breadcrumbs, and lures and alert the security staff to their activity. Today's deception technology is field-tested by numerous pen testers proving its ability to detected skilled intrusions in addition to those of optimistic insiders.
3. The Determined Insider. Like the opportunistic insider, the determined insider is seeking to bypass security controls, but the motivation is much more malicious. The malicious insider will also experience the same issues as the opportunistic insider: insufficient access, not knowing where the data is stored, not wanting to the activity to be traceable, etc. As with the opportunistic insider, determined insiders will conduct credential theft, reconnaissance, and lateral movement to find the data they want, and will be susceptible to the deception decoys, breadcrumbs, and lures a prepared organization has placed within the network.

TARGETED ATTACKS

> The Attivo solution is designed to work for organizations in the legal sector of all sizes and with varying levels sophistication in terms of preexisting cybersecurity controls.

Attackers who target specific victims typically have a high level of expertise and extensive resources at their disposal to conduct their schemes over a long period of time. They often have specific documents and files they are looking to obtain. They customize, adjust and refine their tactics to counter their victim's defenses, often leaving legal organizations without a solid security infrastructure in a precarious situation.

Targeted attacks often utilize similar tactics recognizable in typical online threats such as exploits, malicious or compromised sites, malware, and malicious emails. Targeted attacks vary from typical online threats in several ways:

- Targeted attacks typically target specific industries such as the legal sector, businesses, government agencies, or political groups. Cybercriminals usually have long-term goals in mind driving their attacks, with motives that include, but are not limited to, business data theft. political gain or financial profit.
- Targeted attacks are traditionally conducted as campaigns. APT activities are often conducted in campaigns—a series of failed and successful attempts over time to get deeper and deeper into a target's network—and are thus not isolated incidents.
- Attackers frequently customize and enhance their methods depending on the nature of their target sector and to outmaneuver any security measures that have been put in place to keep unwanted outsiders away from sensitive data.

DECEPTION AND TARGETED ATTACKS

The customized and specific nature of the methods used in a targeted attack make it difficult to defend against. From the authentic-looking emails purportedly sent from high-ranking officials in the organizations to custom-crafted malware that bypasses specific security solutions, the attackers have spent a great deal of effort to infiltrate and ensure a successful attack. They will often use unknown zero-day vulnerabilities or customized payloads. They usually have a greater level of expertise than the "average" attacker and can be state-sponsored or backed by sophisticated cybercrime organizations. Essentially, if an organization is targeted by a determined, patient, well-resourced, and technically proficient adversary, they have a strong likelihood of being compromised.

To protects against the theft of particularly important documents and files in the case of a targeted attack, Attivo Networks deception technology adopters can look to the platform's DecoyDocs solution. The ThreatDefend Platform's DecoyDocs solutions provides the ability to plant deception files that allow the organization to track documents that were exfiltrated. By embedding a tracking call-back function into a document, the DecoyDocs solution can provide data on what was stolen and beaconing to identify where an attacker opened the file. The DecoyDocs callback provides the externally facing IP address and geolocation of every system that opens the DecoyDoc and the name of the file stolen thereby providing data that can help with attribution, identification, and proactive security measures.

> The future success of the legal sector depends on their ability to keep their client's sensitive data protected and secure from advanced threats.

DecoyDocs are fast and easy to set up. Word, PowerPoint or PDF files are loaded into the BOTsink engagement servers where they are tagged for tracking and a notification email address set up. The Attivo Networks cloud security service will then alert via this email address any DecoyDoc notices arising from beaconing alerts.

Today's targeted attacker is making fewer and fewer mistakes, making a reactive defense less and less effective. With deception at the network, endpoint, data, and application layers, organizations have a detection mechanism to alert on attackers as they attempt to reuse stolen credentials, conduct reconnaissance, and laterally move from system to system. Additionally, by gathering early and detailed threat-, adversary-, and counter-intelligence, organizations can take a proactive posture to their organization's security and ultimately call checkmate on the attacker.

THE MALWARE CHALLENGE

While internal threat actors are a concern, the data a legal organization is responsible for also faces threats, particularly from malicious computer code in the form of malware or ransomware.

Remote access trojans and botnets have challenged information security teams within the legal sector for many years, with exceedingly high business impact. Remote access Trojans, or RATS, are pieces of malware that allow an attacker who has compromised a system to access it over the Internet regardless of any safeguards on the network or the endpoint. RATS provide administrative level access to the malware owner, who can then access any data on the system, or steal credentials delve further into the network to find valuable data to exfiltrate and monetize.

Botnets act as a force multiplier for cybercriminal groups, individual cybercriminals, and nation-states seeking to tamper with or break into their targets' systems. Botnets are a collection of any type of Internet-connected device that a malicious actor has compromised. Commonly used in DDoS attacks, botnets can leverage their collective computing power to distribute large amounts of spam, compromise credentials at scale, or spy on people and organizations.[7] A botnet infection suggests that an attacker has acquired partial to complete control of a system. While the unauthorized use of a legal organization's computing resources is a concern, more worrisome is the botnet malware's ability to grant system access to, and take commands from, the malicious actor who owns the botnet.

> Because of the efficient way that deception technology detects threats already inside the network, it is effectively positioned to identify insiders before they can compromise client data, whether accidentally or intentionally.

Remote access Trojans and botnet malware both provide unfettered access through existing security controls, allowing the malware owner to steal information and access confidential data, thereby compromising the confidentiality of the data or alternatively ransomware to lock or erase files for financial gain or malicious destruction.

Ransomware poses a different type of threat to critical client information, targeting the integrity and availability of the data. The threat of catastrophic data loss due to a ransomware infection is a risk no legal organization takes lightly, as illustrated by the DLA Piper Petya incident. Petya is a family of encryption ransomware discovered in 2016, targeting Window-based systems, encrypting data and demanding a ransom payment to recover it. DLA Piper is one of the largest law firms in the world, with over 3600 lawyers and a presence across over 40 countries. In July of 2017, DLA Piper suffered a Petya infection that crippled operations for weeks, costing millions in lost business and recovery efforts. The Petya variant that infected DLA Piper wasn't designed for extortion, but for destruction. As a result, with no way to pay a ransom to get the data back, the firm spent considerable time recovering what data they could while trying to limit the infection.[8] With the reputational and business impact to their operations, DLA Piper lost millions.

Although malware is seen as preventable by many organizations, the easy repackaging of malware can bypass security controls and leave an organization exposed. As DLA Piper and others have found out, anti-virus and perimeter defenses are not always enough to prevent this form of attack.

DECEPTION FOR MALWARE

Network-enabled malware, such as botnets, RATs, and ransomware, try to propagate to systems connected to the compromised endpoint. Whether it is co-opting network and computing resources as part of a botnet, allowing outsiders access to steal passwords and data, or encrypting data for ransom or destruction, these infections use their network connectivity to rapidly spread throughout the environment. Deception technology will accurately and quickly detect such activity.

Deception technology can better prepare organizations for GDPR Article 33 – the notification of a personal data breach to the supervisory authority – by providing powerful security controls not only detect attacks before they become full blown data breaches, but by gathering forensic information to assist in meeting the regulatory reporting requirements.

An attacker who successfully compromises a system with botnet malware will often try to spread the infection to others on the network, either manually or as part of the botnet propagation code. The attacker or malware will conduct discovery activity to find other hosts to infect, and in doing so will interact with a network decoy, generating an alert. Should the attacker or malware connect to the decoy and infect it, the security team now has visibility into the botnet malware activity, capturing the infection vector and any communications traffic originating from within the engagement environment. This early detection and notification is often all the organization needs to prevent a botnet from gaining a significant foothold and potentially compromising privileged client information.

CYBERSECURITY REQUIREMENTS FROM CLIENTS

Success in the legal industry is rooted in an unparalleled level of trust between lawyers and their clients. Clients engage with lawyers in the open manner they do because of the promise of client confidentiality. When that confidence is compromised, the lawyer's most essential asset can no longer be of use to them. Firms are increasingly realizing that clients are measuring them not just by the services they provide, but on how well they can secure their clients' data.

> Deception technology uniquely addresses dwell time challenges legal organizations face for which there traditionally has been no easy solution.

Clients often place requirements a firm must meet before even considering hiring them. If the legal organization initially meet these requirements, they face the added challenge of demonstrating their ability to adequately protect client data and mitigate potential threats. According to ALM Intelligence Legal Compass, 82% of law firms indicate that clients require them to upgrade their cybersecurity capabilities upon commencing business.[9]

As malicious actors become increasingly sophisticated in their attack methods and vectors it is critical for those in the legal sector to continuously assess the reliability of their security infrastructure and adapt to the modern threat landscape. A modern adaptation will include a balance of prevention, detection, and incident response and not rely on perimeter-based measures alone.

DECEPTION TECHNOLOGY TO MEET CLIENT REQUIREMENTS

> This early detection and notification is often all the organization needs to prevent a botnet from gaining a significant foothold and potentially compromising privileged client information.

Clients rightfully expect their legal counsel to protect any information they provide within the confidentiality of attorney-client privilege. Whether it is the fear of a patent application being stolen and having a product knockoff showing up in the market, the secret workings of a business acquisition being leaked to the press, or trial strategy being stolen and made public, clients are requiring more stringent assurances that the information they provide remains confidential. With high profile breaches like the Panama Papers fresh in the news, legal organizations must show their clients that they are meeting these expectations with security measures sufficient to the task. Deception can play a powerful role in demonstrating how the organization detects threats that bypass perimeter controls. The solution can also be used to demonstrate advanced measures for detecting insider threat activity.

GDPR AND SIMILAR REGULATIONS

The General Data Protection Regulation (GDPR) will radically change the global data usage and protection landscape when it becomes effective in May of 2018. This European legal framework will hold any organization collecting, controlling, or processing EU personal data accountable to safeguard it. This means that those in the legal sector that fail to adequately comply will risk facing potentially crippling penalties of up to $28 million or 4 percent of their annual revenue.

Legal organizations handle a great deal of private personal information, so GDPR and similar regulations affect them greatly. Of particular importance to GDPR compliance is the reporting requirements to notify the supervisory authority of a personal data breach within 72 hours. To maintain their viability within the EU, legal organizations must adjust processes and technology to become and remain compliant.

DECEPTION FOR EFFECTIVE SECURITY AND COMPLIANCE REQUIREMENTS

For a regulation such as GDPR, the intent is to give control back to individuals over their personal data and to set a bar for organizations to demonstrate compliance with protective measures. In today's criminal underground economy, personal data is the digital currency. Cybercriminals steal personal data to sell it in illicit websites to other criminals who use it to commit various acts of fraud. Among other things, GDPR and similar regulations are written to ensure that organizations who suffer a data breach are forced to notify the people whose data is affected or else suffer extensive monetary penalties.[10] While stipulations such as pseudonymisation and encrypting data at rest protect information should it be stolen, there is nothing that adds additional security to actually prevent the data theft in the first place. The organization is still saddled with onerous reporting requirements that force disclosure within 72 hours. Traditional information security systems have repeatedly demonstrated that they can be compromised, and existing security controls are unreliable in detecting threats that have bypassed preventative defenses. These gaps in detection and inability to quickly and accurately disclose a breach leave these organizations exposed to substantial violations.

In readying for GDPR organizations have re-evaluated their technology and processes to assess their ability to detect, audit, and report breaches to ensure GDPR compliance. Many are rapidly adopting new solutions that are designed to detect attacks early, accurately, and provide a detailed analysis that can explain the magnitude of the breach, as well as the corrective actions to contain it. This is an area where deception technology can help.

> Although malware is seen as preventable by many organizations, the easy repackaging of malware can bypass security controls and leave an organization exposed.

Deception technology can better prepare organizations for GDPR Article 33 – the notification of a personal data breach to the supervisory authority – by providing powerful security controls not only detect attacks before they become full blown data breaches, but by gathering forensic information to assist in meeting the regulatory reporting requirements.

THE ATTIVO SOLUTION

The Attivo ThreatDefend™ Deception and Response Platform has created a new class of deception-based threat detection that levels the playing field against attackers. The ThreatDefend platform is recognized for its comprehensive network and endpoint-based deception, which turns user networks, data centers, cloud, remote offices, and even specialty environments such as IOT, ICS-SCADA, point-of-sale, telecom, and network infrastructure systems into traps that will quickly confuse, misdirect, and reveal the presence of attackers. This "hall of mirrors" creates an environment where the attacker is lured into making a mistake, reducing their dwell time within the network.

The Attivo solution is designed for the utmost of authenticity and its camouflage deception techniques and campaigns, lure the attacker by running real operating systems and production golden images. These capabilities fool attackers by customizing decoy engagement servers to be indistinguishable from production assets, luring attackers away from production systems.

> Deception technology uniquely addresses dwell time challenges legal organizations face for which there traditionally has been no easy solution.

Additionally, the solution uses machine learning to create Adaptive Deception Campaigns. These self-learning deception campaigns enable automatic credential and decoy refresh based on a schedule or suspicion of an attack that may be underway. Deceptions can be set to automatically rebuild and re-spin after attacker engagement to avoid fingerprinting.

ThreatStrike™ deceptive credentials can be placed throughout the network on endpoint and server devices for credential theft detection, deceiving the attacker into believing that he is harvesting valuable user credentials. Instead, the attacker's use of a stolen credential will have served only to lead him into a deception trap within the BOTsink engagement server. ThreatStrike deceptive credential deployment and operational management is simple given the solution is agentless, does not require endpoint software updates or device-level software, and is easily scalable and customizable, even for large global deployments.

The Attivo solution is designed for an active defense, which starts with deception-based detection of in-network threats and adds in automated attack analysis, forensic reporting, and a threat intelligence dashboard for a centralized view of all alerts and actionable drill downs. The ThreatOps solution provides the ability to create repeatable incident response playbooks to accelerate incident response (block, isolate, threat hunt) through 3rd-party integrations with firewall, NAC, end-point, and SIEM vendors.

The Attivo solution is designed for an active defense, which starts with deception-based detection of in-network threats and adds in automated attack analysis, forensic reporting, and a threat intelligence dashboard for a centralized view of all alerts and actionable drill downs.

Visibility tools empower organizations to proactively strengthen overall security defenses by showing exposed attack paths and attacker movement in a time-lapsed replay. The ThreatPath solution provides visibility into insider, contractor, supplier, and partner 3rd-party threats as they conduct reconnaissance and move laterally through networks. The ThreatDefend Platform also gives network visibility for device adds, changes, and location of deception assets. It can show attacks in a time-lapsed replay for understanding attacks and strengthening defenses. These tools can identify and graphically show misconfigured, misused, or orphaned credentials to shut down credential-based attack path vulnerabilities.

The ThreatDefend Platform detects attacks that are difficult for other solutions to detect. The ThreatStrike Endpoint Suite gives organizations detection capabilities for stolen credential attacks. The deceptions can incorporate with Windows Active Directory (AD) infrastructures, increasing their authenticity, giving visibility to attacker activities that query the AD for information while providing misinformation. The BOTsink solution provides decoys that detect network-based attacker activity, such as Man-in-the-Middle attacks that harvest credentials and other data traversing the network, or reconnaissance and lateral movement. The network decoys also provide a full engagement environment to keep the attackers occupied while offering deceptive network services, application, and data to deceive them further.

The ThreatDefend Deception and Response Platform is comprised of Attivo BOTsink™ engagement servers, decoys, deceptions, the ThreatStrike™ endpoint deception suite, the ThreatPath™ attack path visibility tool, the ThreatDirect™ virtual deception solution, and ThreatOps™ Incident Response playbooks. Together, the product suite creates a comprehensive early detection and continuous threat management defense against today's advanced threat actors. Lastly, ThreatDefend is a solution that can be easily installed and operated without the need for dedicated security staff and delivering value the day it's installed. For more information about The Attivo ThreatDefend Deception and Response Solution, visit https://www.attivonetworks.com or email marketing@attivonetworks.com

ABOUT ATTIVO NETWORKS

Attivo Networks® is the leader in dynamic deception technology for real-time detection, analysis, and accelerated response to advanced, credential, Active Directory, insider, and ransomware cyber-attacks. The Attivo ThreatDefend Deception and Response Platform accurately detects advanced in-network threats and provides scalable continuous threat management for user networks, data centers, cloud, IoT, ICS-SCADA, and POS environments.

www.attivonetworks.com

[1] Bitsight Insights: Exploring Data Security in the Legal Sector and Beyond
[2] Attackers Breach Law Firms, Including Cravath and Weil Gotshal", Nicole Hong and Robin Sidel, The Wall Street Journal, March 29, 2016
[3] https://www.bitsighttech.com/blog/recent-data-breach-panama-papers
[4] What are the Panama Papers? A guide to history's biggest data leak, The Guardian
[5] Bitsight Insights: Exploring Data Security in the Legal Sector and Beyond
[6] https://www.innovativecomp.com/blog/protecting-your-law-firm-from-inside-security-threats
[7] https://www.csoonline.com/article/3240364/hacking/what-is-a-botnet-and-why-they-arent-going-away-anytime-soon.html
[8] https://blog.barkly.com/dla-piper-petya-ransomware-attack
[9] http://www.almlegalintel.com
[10] https://en.wikipedia.org/wiki/General_Data_Protection_Regulation