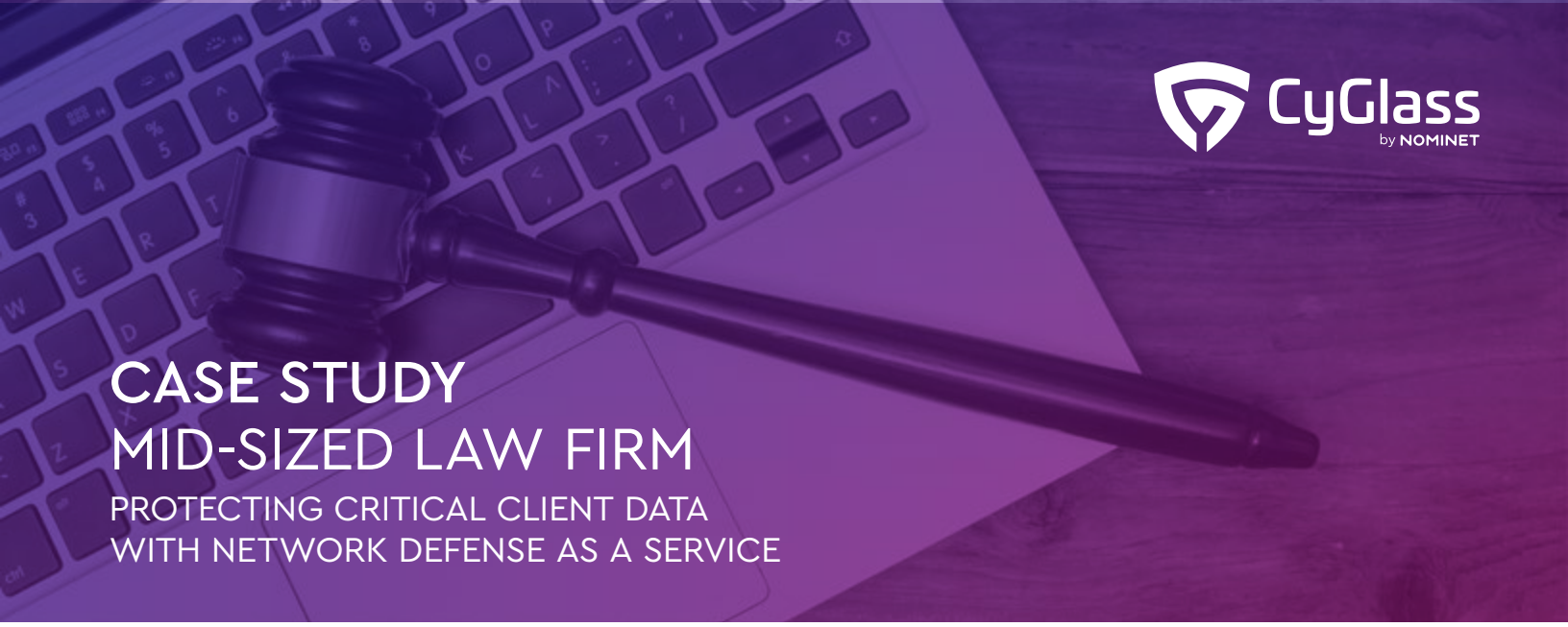

CASE STUDY
MID-SIZED LAW FIRM
PROTECTING CRITICAL CLIENT DATA WITH NETWORK DEFENSE AS A SERVICE

Founded in 1894 and growing rapidly over the past decade from six to 12 offices nationwide, this U.S. firm of 182 attorneys and 450 employees recognized the firm and its clients were under threat and took action to better protect its network and data from attack.

Like many law firms, the organization had invested in IT systems with extensive on-premise support. But its attention to cybersecurity lagged, leaving the firm open to attack.

FEBRUARY 17, 2020

The journey began with a conversation.

"Ransomware is potentially a real problem for us – did you see the Law.com article about Baker Wotring?" asked the Chief Information Officer.

The firm's head of Network Operations, who also wears the cybersecurity hat, responded, "Yes, I am not comfortable that we could detect or stop what happened to them. Would we pay?"

CIO: "Honestly, it depends on what they are able to lockup and steal. Paying would make our firm look weak, and I am sure the partners would have our jobs if it went there. And there is this: In the last leadership meeting we were briefed on this Coronavirus. They said it is real, it is growing, and it is coming here. We need to plan for it."

That discussion kicked off a series of actions that would lead the firm quickly down the path of increased remote working, digitalized business processes, and virtual meetings. For this firm, it was the early recognition of the potential for ransomware attacks to grow exponentially, together with an understanding of the risks created by rapid digitalization and remote working, that drove a risk mitigation strategy which has ultimately protected the firm and their clients' data.

DEFINING RISK IN A RAPIDLY CHANGING ENVIRONMENT

Visibility became the goal for the entire IT team as they tried to plan and execute the rapid changes to their business processes that would keep the firm prospering during the pandemic. The pressure for rapid change was intense, since the firm was working multiple high stakes cases where any slowdowns were unacceptable.

The IT team assigned security of the rapidly growing remote workforce as priority one. The initial plan expanded VPN usage to on-premise systems and storage. At first, this plan was effective, but the team quickly ran into issues around connectivity and complaints by clients and then partners grew. Simultaneously, the team read about VPNs as a growing attack vector for ransomware attacks and realized an alternative path must be found.

MOVING TO THE CLOUD

Like many law firms, Skype was a oft-used collaboration tool, but with Microsoft discontinuing Skype for Business and the firm already using Active Directory, the logical move was to Teams, Azure, and Office 365. The long-term plan was to increase VPN usage to cover the firm's legal content management system, while rolling out MS Teams, along with Azure and Office 365.

VISIBILITY, VISIBILITY, VISIBILITY

As plans for remote working and dealing with the pandemic continued, the threat of ransomware and other cyberattacks resurfaced. The IT team evaluated their defensive posture and process based on the DoppelPaymer and Ryuk ransomware attacks headlining in March of 2020.

The results showed alarming gaps in the firms visibility into devices on its network, as well remote VPN usage and network communication inside and moving across its firewalls. These were all areas critical to monitor for protection against both ransomware attacks. The audit also found that network and cloud firewall coverage was solid with multiple Fortigate firewalls in place, policies current, and operating properly. The firm also had Sentinel One endpoint protection working effectively, but the lack of a 24X7 security operations center meant that nighttime and weekends were uncovered. Operating a SOC or deploying a security incident management system were determined to be beyond the resources of the firm.

Further evaluation found risks with the move to more broad usage of Office 365 and Teams. Multi-factor Authentication needed to be widely deployed. Better access control over Azure accounts was required, and policies were needed to ensure that sensitive case and client data was not leaked or shared in Teams or in cloud file systems like SharePoint.

BANG FOR THE BUCK

The company looked at different tools to help mitigate their risk, including traditional on-premise network detection and response (NDR) solutions, and Cloud Access Security Brokers (CASBs) but found that these systems were overly complex, required dedicated staff, and were universally expensive. It was obvious that enterprise cybersecurity tools operated by large companies could not be deployed with the resources available.

Ideally, the firm needed threat visibility to network and cloud systems that was affordable and deployable by a mid-size law firm.

NETWORK DEFENSE AS A SERVICE

The company came across CyGlass while attending a cybersecurity seminar. CyGlass presented its network monitoring, threat detection and response tool that was cloud-native, operationally simple, and affordable. Most relevant, it was being successfully run by two other law firms of roughly the same size.

Information was collected about the solution with t the first call made to CyGlass' existing legal customers. The CIO remembered the conversation.

"I had met this firm's CIO at an ISSA meeting a few years back and so I reached out to ask about their CyGlass deployment," the CIO recalled.

What the CIO heard gave him hope. He learned CyGlass had been deployed five months earlier and provided 24X7 monitoring of the company's north/south and east/west traffic. The product was a SaaS service, meaning all the maintenance work, patching, etc. was done by CyGlass. No new headcount was needed, the product had great reporting, and was simple to operate. CyGlass did not overload the small team with alerts, while the alerts they did get were risk-scored in order of priority and offered guidance on how to mitigate the risks and threats discovered. The product even included automated remediation through their firewall when needed. Most importantly, CyGlass was currently beta testing a version that included coverage for Azure and Office 365. The firm was participating in the beta and was impressed with the early results. Then came the question of price, and the surprising answer was, "The service is less expensive to operate than our firewalls or EDR tool!"

DEPLOYING NDAAS

That was all it took to convince the firm to give CyGlass NDaaS a try. After talking to CyGlass, the system was set up and collecting Netflow data from the Fortigate firewall in under 20 minutes. Over the next month, the firm expanded the deployment to include its smart routers so that north/south and east/west traffic were covered. As promised, NDaaS' unique blend of AI and policy controls kept alerts down to a handful, and the guidance on remediation was helpful. The product was simple to operate and the reporting even included a "scorecard" report to track progress.

24X7 MONITORING & RANSOMWARE DEFENSE

The firm reported that the greatest value by far came in the 24X7 automated ransomware prevention controls. Included were 40 pre-built policies that look for risks and vulnerabilities across ransomware's common attack vectors. AI watched and correlated ransomware attack anomalies against threat intelligence and alerts when multiple stages of a potential attack are correlated. The firm now had a set of eyes watching for and alerting on ransomware attacks around the clock.

Within a week of deployment, the team had CyGlass NDaaS ingesting network traffic from their firewalls, VPNs, and from a set of internal network routers. After two weeks, the AI models had aligned and the team had visibility into the devices, networks and subnets. Two immediate risks were surfaced that shocked the team.

The first was a wide open FTP server. The team did not know who was responsible and why the file transfer was required. After reaching out to its ISP, the team found that the service provider had used the server to patch some of their backend systems and then forgot to shut down the server – three months earlier. The problem was quickly resolved along with an apology from their ISP.

The second issue involved 14 devices on the network that were not in the firm's inventory, and, upon investigation, were not properly protected. Three of the devices were IoT security camera's that a builder of one of their new offices had put in place for physical security. The local service provider had hooked them into the network, but had never complete the proper paperwork for IT to identify and track them. One of the devices had regular traffic going to Belarus, yet the company had no clients or cases related to Belarus. The other devices were identified as new end user devices that had been purchased locally and never properly checked in with IT. All of these devices were missing proper endpoint security and backup systems. These issues were also quickly remediated.

EXPANDING COVERAGE TO OFFICE 365

With the initial deployment for ransomware protection complete, the team looked to cover the Office 365 and Azure deployments. Challenges with these environments had developed rapidly as the deployment grew. Perhaps the most critical challenge was getting multifactor authentication in place for all employees. This became a much bigger challenge than anticipated. The company firm was able to about 85% of users authenticated, but the remaining 15% were surprisingly difficult. A mix of technical issues with end-user devices, limited internet connectivity based on geography, and technological usage challenges by some of the firms more senior people stymied efforts to achieve 100% MFA. The team also realized that for many of their clients and partners, the same challenge would exist.

It was ultimately decided that 100% MFA would not to be achievable for some time, so the team focused CyGlass on monitoring for authentication based on attacks against passwords.

The next challenge was dealing with alerts. Just four months into the Office 365 deployment, utilizing the E3 license, the team was already experiencing hundreds of alerts a day – way more than it could handle. Alerts covered everything from authentication and access issues to file movement and location risks.

The team needed a way to regain control of Office 365 security and needed it quickly. A team member recalled that CyGlass had an O365/Azure protection system in beta. They reached out to CyGlass and found out that O365/Azure was generally available and they could try it for 30 days. CyGlass connected and began capturing Office 365 and Azure usage logs within a few hours, and the project was up and running.

O365/AZURE RISK BASED ALERT TRIAGE

CyGlass AI models cover anomalous or high risk authentication events, user access events, file access and file share events, and user administrative rights as well as anomalous file and communications from the network to the cloud. As the models normalized, they detailed a risk-based view of where the Office 365 deployment should focus. Correlation of events allowed the IT team to understand where to start and what to focus on. The reports delivered by NDaaS became an Office 365 triage systems. Each day, the five or six alerts detailed a misconfiguration or process issue to fix or change. The team went from feeling scattered and frustrated to making progress every day and having it reflected in lowering risk score. The Office 365 rollout and the challenge to get to 100% MFA continues, but the team has confidence in its risk visibility and threat detection to both the cloud and the network.

FUTURE EXPANSION

The next steps for the firm are to deploy internal east/west visibility to have a better handle on threats inside the network. The team wants to focus on building zero trust into their network using CyGlass's identity and micro-segmentation capabilities to further protect critical case and client data. The firm looks forward to increasing the value of the NDaaS platform across the organization.