Customer Spotlight

Yellow Pages: Better Security, Great User Experience

Sponsored by: GoSecure

Kevin Lonergan David Senf

February 2018

INTRODUCTION

Yellow Pages(YP) (www.yellowpages.ca) is a digital media and marketing solutions company in Canada, with 3400 employees across eight offices. Operating since 1908, YP has grown substantially, currently serving over 236,500 Canadian small businesses with over 464 million visits to its digital properties annually. Traded on the Toronto Stock Exchange, YP owns and operates multiple subsidiaries including YellowPages.ca, RedFlagDeals.com, and Canada411.ca.

As a public company, YP operates within several compliance frameworks such as PCI-DSS and C-Sox (bill 198). It is highly focused on strong security protection throughout the organization, and wants staff and providers to be proactive in identifying potential threats to the organization and its sensitive data. Application and web development are key operations for its business, and are accomplished by a team of over 400 in-house developers. Supporting the developers requires a substantial amount of IT infrastructure.

When CISO Eric Hebert joined YP in October 2016, the decision was made to outsource security monitoring for its 3,000 PC endpoints and 2,000 servers. This IDC Customer Spotlight describes YP's choice of GoSecure as its managed security service provider (MSSP) for endpoint detection and response (EDR), the onboarding process for the service, its experience during the proof of concept (POC), and future plans.

Solution Snapshot

Organization: Yellow Pages Limited (YP)

Operational challenge: Due to the large number and variety of PC, server, and smartphone endpoints deployed at YP, the organization was looking for help managing endpoint detection and response (EDR) security. YP's CISO, Eric Hebert, sought a security provider that offered high-touch customer service focused on threat mitigation rather than responding to simple automated alerts. He wanted human judgement and oversight to discern malicious activity on top of what the technology may or may not catch.

Solution: GoSecure's Advanced Adversary Protection (AAP) with Attack Stream Interrupter to provide EDR security and threat hunting.

Project duration: Ongoing. Completed four-month proof of concept and currently rolling out services to approximately 3,000 server and PC endpoints.

Benefits: Vastly improved detection rates and mitigation times over what YP was able to accomplish internally. GoSecure's AAP solution also includes a USB/external media monitoring component, which offers protection from insider threats. As part of AAP, YP has dedicated GoSecure analysts threat hunting and monitoring endpoints 24 x 7, and is provided with multiple reports and portals to view and manage suspicious events on its network. The GoSecure solution did not impact end-user experience, and offers good protection while remaining invisible to YP staff.

PROJECT OVERVIEW

YP's outsourcing of basic IT infrastructure led to a fundamentally different approach to security. YP decided to rebuild its in-house security protection from the ground up, from tightening perimeter security to addressing cloud vulnerabilities.

The first step in this process, tightening perimeter security, included finding a suitable provider for EDR. Proper patch management and antivirus can go a long way toward securing endpoint devices, but they cannot provide the insight, or put the pieces together of threat identification and mitigation in the way properly trained and experienced security analysts can. Despite the majority of organizations running corporate antivirus software, there has been an incredible increase in the number of endpoints infected with ransomware and malware over the last few years. YP sought active threat hunting and monitoring — the human element — to proactively detect vulnerabilities and attacks, rather than respond reactively after alerts have been sounded.

Antimalware and antivirus suites have been staples for securing PCs and other endpoints for decades, but their traditional detection and mitigation capabilities haven't kept up with the rate of change of new threats. Signature-based solutions are too slow to match the pace of ever-evolving malware, allowing attacks to go unidentified. To address the reality of this present-day threat landscape, newer algorithmic-based approaches have been developed. Commonly referred to as next-generation endpoint security, these solutions use machine-learning algorithms to create models capable of classifying malware by learning their traits and behavior, rather than comparing it to a static list of known threats. Although these solutions are far more powerful than they were only a few years ago, malware passed on by phishing and spoofing attacks continues to infect endpoints at an alarming rate.

With the rollout of GoSecure's Advanced Adversary Protection (AAP) near completion, YP's focus is shifting toward enhancing the security of its cloud-hosted environments. YP was an early adopter of cloud, and has migrated most of its externally facing assets to cloud environments.

VENDOR SELECTION

In previous roles, YP's CISO had dealt with some of the large vendors in the EDR space, but was never satisfied with the level of detection, speed of mitigation, and level of personalized service . YP's CISO was aware of GoSecure and its EDR offering, and decided to conduct a POC with the provider. When comparing EDR solutions, the following were key performance indicators for YP:

- **Low performance impact on endpoints.** Traditional antivirus and EDR clients have been known to affect endpoint performance considerably, specifically in terms of CPU cycles and hard-drive churning. With hundreds of developers programming and compiling code, YP couldn't afford, and knew staff wouldn't tolerate, a significant performance hit on their machines.
- **Competitive price at or below industry average.** YP was looking for an MSSP that could provide more value than the large vendors could at a similar price point.
- **Faster alerts and mitigation times.** YP was looking for the human element — Hebert wanted security analysts to alert and concurrently work with his team to address endpoint security issues, instead of a traditional alert fire-and-forget model. Alerting and mitigation had to be faster and more efficient than what had been done in-house.
- **Stable platform.** The underlying technology needed to be stable and require little-to-no maintenance from the customer side.
- **Breadth of capabilities.** YP supports multiple operating systems across its servers, PCs, and smartphones. Moreover, it has on-premise, hosted, and cloud environments that need to be secured across multiple deployment models. The solution chosen had to address all of the above.

PROOF OF CONCEPT WITH GOSECURE

During the POC, YP quickly realized the value that GoSecure's AAP service could deliver. The first alert YP received was a call directly to the IT team informing them that an employee had installed a suspicious piece of software. GoSecure wanted to confirm that this was acceptable policy, and the total time from detection to response was approximately 20 minutes, a vast improvement over what YP had experienced in the past.

As the POC progressed, YP became more comfortable with AAP and decided to utilize more features of the service. This included GoSecure's Attack Stream Interrupter and quarantine service, allowing GoSecure's Active Response Center (ARC) team to disconnect and reset network connections that may be malicious in nature, as well as quarantine files. With the full portfolio of AAP services enabled, YP had a partner in endpoint detection and response, but also real-time mitigation and threat hunting.

SELECTED GOSECURE SOLUTIONS

After a four-month POC with GoSecure, YP signed on for its AAP services.

GoSecure: AAP

GoSecure's AAP service combines best-of-breed technology, custom IP, and tier 3 analysts to proactively monitor, detect, and mitigate attacks. AAP is conducted out of GoSecure's Active Response Center (ARC) in Dartmouth, Canada. This SOC2 Type II facility is manned 24 x 7 x 365 and supported by two tier 4 datacentres that host the proprietary system that combines threat intelligence feeds, machine learning, and custom-built antimalware tools to support the ARC team in threat hunting and incident mitigation. The ARC team consists of SANS certified analysts and engineers who are exclusively dedicated to incidence response and threat hunting. With AAP, the ARC team proactively hunts for threats on your network under the assumption that there is always a vulnerability on it, rather than wait for an alert from an EDR, SIEM, or device to appear. AAP runs under three key concepts:

24 x 7 threat hunting

Proactively search the network for advanced attacks that evade traditional security solutions. Using machine learning, threat intelligence, and malware analysis tools, tier 3 security analysts continuously hunt the network for vulnerabilities and signs of attack. The threat hunting team works under the assumption that there is always malicious activity on the network.

Full transparency

Allow customers to have full visibility into the actions and results of the ARC team. Transparency allows customers to see the value they are being provided, and helps them to follow up on any events or inquiries. AAP customers have 24 x 7 access to analysts in the ARC.

Data residency control

To properly monitor and secure a customer's environment, full network packet capture, sandboxing attachments and executables, and access to physical memory are just some of the requirements that MSSPs require. GoSecure accomplishes all of this without AAP subscriber data ever leaving their datacentres and sensitive data stays on-premise.

CHALLENGES

As with any major IT rollout, care has to be taken to ensure that the transition is smooth and workflows aren't interrupted. For YP, this meant spending a considerable amount of time upfront, creating escalation trees, testing the GoSecure log collectors, and conducting a POC study before deploying EDR across all of its endpoints. In the end, this conservative approach paid off and YP has been able to install and run the EDR client on endpoints seamlessly without user intervention.

BENEFITS

YP reported that the four-month POC study was a tremendous success, and roll out of GoSecure's AAP service has been extended across all endpoints. Coupled with GoSecure's AAP service, YP has experienced the following benefits:

- Improved **detection times** over legacy solutions
- Direct access to GoSecure staff for **rapid incident mitigation**
- Low **performance** impact on endpoints compared with other EDR solutions
- USB/external media **port monitoring** to protect against insider threats
- Customized reports
- No customer-side **maintenance** required for EDR solutions
- No **data residency** concerns – all data stays on customer's premises
- The **scalability** of the EDR solution allows YP to remain agile and increase its number of endpoints while remaining protected
- No impact on **user experience** – maintaining protection while not getting in the way of productivity
- GoSecure's web-based customer portal provides real-time **asset tracking** data on endpoints connected to the network

IT SECURITY ADVICE FROM YP'S CISO

Eric Hebert is actively involved within the security community and has more than two decades in the security industry. He offered the following advice to security professionals:

- **Process and people are more important than the technology sitting behind it.** "Optimizing people and processes is key to rapid mitigation. Technology should support both. Not the other way around. Get the basics right. Get your patch management and antivirus up to date, everywhere, and monitored. If you can't get these done in your organization, you are not mature enough to implement more security technologies. No amount of security technology will protect your organization if you don't have the basics down."
- **If you're in IT security, stop being scared of business stakeholders – engage with them.** "Engage with the LOB and put forward a risk dialogue, not security or IT. Stay away from statistics and keep it simple. Pick one or two urgent risks that need to be fixed, explain the real-world impacts, the cost and time requirements, and stay away from diving into specific risk levels."
- **Shop around and negotiate**. "Always test any service you are considering with a POC to make sure you see it performing in a real-world situation. A service is about more than technology – it must include a human element. Without it, you likely won't get what you pay for."

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC Canada

33 Yonge St., Suite 420
Toronto, Ontario Canada, M5E 1G4
Twitter: @IDC
idc-community.com
www.idc.com
