

Technology Spotlight

Advanced Managed Security in a New Era: Simple Steps to Rapid Response Advanced Managed Security

Sponsored by: GoSecure

Kevin Lonergan David Senf
February 2018

INTRODUCTION

In an emergency, paramedics claim that every second counts, from receiving the call, to arriving at the scene, to starting first aid. In IT security, IDC finds that too much time lapses between similar phases of breach, detection, and remediation. Many organizations are not alerted to a breach until it is too late, after the damage is done. And, as organizations extend applications and data further into the cloud and smartphones, the need to improve reaction time only increases. The good news is: reducing these time lags is not complicated.

In this IDC Technology Spotlight, we'll review basic and advanced security practices your organization should be implementing in order to improve its reaction time. Additionally, we'll present the services of an innovative Canadian-based security provider with presence in the U.S. and the U.K., – GoSecure.

If three practices are followed, shifting the odds of success away from an attacker and instead towards your own organization is relatively straightforward. By understanding your attack surface better (i.e., total number of points through which an attacker could try to enter, or extract data from your network), detecting threats faster, and keeping up with the basics of good security (i.e., patching systems and training employees), the risks of loss and disruption are greatly reduced. A primary goal of these practices is to reduce the time it takes your organization to find or even prevent an attack in the first place.

In a study of 200 security professionals from Canadian and U.S.-based organizations, IDC found that 83% reported a minor breach at their organization in the past year. This resulted in at least one employee being disrupted from getting their work done or other minor incidents. More strikingly, our research found that 49% reported a major security breach where funds were stolen, sensitive data exposed, or any number of other losses or downtime happened.

Because many organizations are not keeping up with basic security practices – and due to the incredible amount of exposed private data – governments around the world have passed stricter legislation to encourage improved security protections. Most U.S. states have passed mandatory breach notification laws similar to that put in place in California nearly 15 years ago. This is in addition to a myriad of industry-specific privacy regulations in health, finance, retail, and other verticals. Canada is just now enacting amendments to its federal privacy legislation in the Digital Privacy Act, triggering stiff fines for breach nondisclosure starting in 2018. The most stringent compliance requirements and fines on the planet, however, are contained in the new EU General Data Protection Regulation (GDPR), which comes into effect in May 2018. Any company doing business in Europe, in any capacity, or whose customers are EU citizens or residents, is subject to

significant penalties (i.e., up to 4% of revenue or a €20,000,000 fine) for not having adequate security safeguards to protect personally identifiable information (PII).

IDC finds the threat of stiffer penalties does result in increased security spend among organizations. However, increased spend usually means new technology purchases rather than effectively training staff or implementing better processes. Each security dollar needs to be allocated to the right controls. We explore this point further in the next section.


DIGITAL TRANSFORMATION RESHAPES RISK, OLD THREATS PERSIST, TAKE ACTION

New technology adoption is reshaping how organizations make products, deliver services, and interact with customers. The pace of change is so rapid that, at an organizational level, it is being called 'digital transformation', while, in a broader historical context, it's being labeled as the Fourth Industrial Revolution, according to the World Economic Forum. At the individual level, employees and customers are collecting, using, and storing far more data than ever on mobile devices and in the cloud. Despite the technological progress, and in part a consequence of it, many additional security challenges emerge.

All the old threats and vulnerabilities are still out there, while new ones (e.g., DDoS-for-hire, Internet-of-Things botnets, WannaCry) continually appear. On a positive note, mobile device manufacturers and cloud providers consider security from the ground up. They are far more hardened than the traditional PC or most organizations' server rooms ever were. The exponential growth in application usage and data collection – even with tighter security "out of the box" – leads to more vulnerabilities.

It's not only the growing count of "more" – more smartphones, more cloud, more IoT sensors, etc. – that's contributing to security issues. Unfortunately, attackers are going unnoticed, watching and retrieving customer, employee, and other sensitive data from organizations for months at a time before being detected. In Canada, for example, a recent survey highlighted that, in 6 out of 10 organizations, attackers operate undetected within their networks for months or even years, before being discovered. This inability to detect an attack is common in the U.S., the U.K., and other regions around the world as well. With so many publicized breaches dragged through the media on an ongoing basis, why is there such fertile ground for attackers to roam?

There are three main reasons why so many attacks are successful:

Top Challenge	Description	Take Action
 <p>Risk isn't well understood</p>	<p>Organizations do not fully understand their attack surface and its vulnerabilities – and therefore they aren't clear where to deploy security solutions to best effect.</p>	<p>Understand risk. Conduct regular risk assessments by rating: a) the likelihood that damage may occur, and; b) the extent of the loss if a given device, application, system, or employee knowledge were compromised.</p>
 <p>Detection and remediation isn't fast enough</p>	<p>Organizations are unaware that attackers are watching their devices and systems for months at a time. Faster detection and response is required.</p>	<p>Continuously monitor, always. Leverage your risk plan to identify where to put security solutions to best detect attackers and start the process of remediation. Monitor your network and devices 24 x 7 for changing attacks.</p>
 <p>Security basics aren't routinely done</p>	<p>Attacks are often successful because basic patching of systems, employee training, and other simple yet effective tasks haven't been completed.</p>	<p>Do the basics. Train employees on security basics. Patch and update systems. Have an executive take a leadership role to ensure good security practices are understood.</p>

IDC expands on how to begin handling these three areas of security weakness below.

1. Understand Risk

Know your attack surface, make a risk plan. Implement threat modelling to improve the management of your security risks by understanding where and how attackers might access sensitive data or otherwise disrupt your organization (e.g., social engineering, denial of service, ransomware, etc.).

Take a step back and list out the most valuable data, critical applications, and devices employees work on within your organization.

Make a list of the assets an attacker might use to compromise your data, applications, or work (e.g., employees, email, PCs, smartphones, cloud, Web app, servers, wireless/wired network, etc.).

List the various ways these assets across your attack surface are vulnerable to an attack, such as an employee being phished, cloud credentials being left open after an employee leaves, or the web app server is not patched/up-to-date.

Sort these lists from most important to least important. To apply basic risk principles, apply two numbers to each item on each list to sort them – the likelihood it could get attacked and the damage that would occur if it was attacked. Use a simple 1-4 rating scale where 1 is lowest risk and 4 is highest risk.

Prioritize your investments/decisions regarding which security solutions to put in place, and where, based on the highest rankings.

Have a response plan as well. No matter how much has been spent on security (and the IDC rule of thumb is 10% of IT budget) an attacker will eventually be successful. By following through on putting a risk plan in place, your organization already knows what might be exposed. Develop an incident response plan, as well, to reduce the likelihood and severity of a breach. The most important areas to focus on are: detection of an intruder, and; responding quickly in the aftermath of an attack. Create an incident response plan to know what to do when a ransomware attack happens, your web server is compromised, a cloud instance is exposed, or any other number of breaches that might happen. For more detail on incident response planning please visit:

<https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901>

2. Continuously Monitor, Always

Attackers are ping-ponging and otherwise trying to find holes in every single internet-connected device. Putting security technology in place to protect against and detect an attack is just the start to preventing a breach. Many organizations take a "set it and forget it" approach to security controls; they deploy technology and hope that it will stop the "bad guys." No matter how much the technology costs, if it's not monitored 24 x 7, its value is greatly diminished. Attackers continually adapt their approach and opt for new ways of entry into an organization's network and other devices. Have your team (or outside provider) continuously watch for and defend against attacks.

3. Do the Basics

Once you have a basic risk plan in hand and monitoring is set up across your attack surface, ensure your organization keeps up with the security basics. Areas to focus on include:

- Patching systems
- Revoking old access credentials
- System scanning/monitoring
- Network segmentation
- Practice minimal data retention for sensitive elements (e.g., PII or PCI DSS data)
- Least privileges (e.g., give access to the fewest people and only provide them access to what they absolutely need)

When IDC asks chief information security officers, security pros, and other leaders in the industry "what is their one piece of advice to help organizations stay secure?", the most popular response is "do the basics." The second most popular response, along the same lines, is "train employees on the essentials of IT security and privacy".

The primary security hole organizations identify is employee lack of knowledge. Surprisingly then, few organizations follow through with training their employees on good security practices. Far less expensive than an antimalware solution or a firewall – and yet likely more effective – are a series of "lunch and learns" with employees to help them with security awareness. Depending on the type of sensitive data your organization collects and uses, the compliance requirements, and the type of systems being used, its training program content will vary. However, there are fundamentals that apply to all organizations, including:

- How to use a password manager

- Understanding the basics of social engineering – don't trust, verify
- How to identify a phishing/spear-phishing attack – which links and attachments to click on
- What PII is and how to manage it
- Ensuring smartphone and PC backups are happening daily

In addition to the security challenges listed above, IDC research identifies the following challenges:

- **Not enough budget.** Typically, how an organization spends its limited security budget is more important than the actual dollar amount. There is roughly a quarter of the market where its budget is indeed too small, however. For the rest, follow a basic risk plan to better sort out how to effectively distribute your security spend for more effectiveness.
- **Threats are changing rapidly.** Historically most successful breaches occur based on poor info sec practices – that is, attacks against systems that are unpatched. Do the three recommended actions from the table above to stay ahead of threats, old and new.
- **"We don't have enough security staff."** This is a big issue. Organizations that perform optimally – those with the fewest security breaches – are the ones that constantly train their IT, security, and end-user staff. Also, IDC sees healthy growth in managed security services (MSS) as organizations outsource more of their security requirements to offset the lack of available skilled security professionals for hire.

THE RISE OF MANAGED SECURITY SERVICES

Several trend lines are converging to drive high growth in managed security services adoption. The most notable trends are: a heightened familiarity with outsourcing because of cloud; discovery that managed security services can be less costly (and sometimes more effective) than in-house security operations; a tight labour supply for security talent, and; difficulty determining what is a real threat.

- **Cloud.** Cloud adoption is sparking increased interest in managed security services as organizations experience the benefits of outsourcing multiple layers of their IT stack. Most organizations will never be able to completely migrate from on-premise infrastructure, but they can outsource some if not all of their security operations.
- **Cost.** For the first time in 2017, IDC survey results show that a top reason for organizations migrating to the managed security services model is because they believe it will be less expensive than running a comparable in-house security operation.
- **Staffing.** Organizations increasingly do not have enough time or qualified staff to defend themselves against a growing list of threats, leading them to seek out help from third-party providers. This is a top challenge and will persist for years to come, as there are not enough trained security professionals in the market.
- **Signal-to-noise.** Related to the point above about staffing issues, organizations are looking to managed security services providers to reduce their struggle with the sheer number of false positives they get from various network devices and other security solutions. This prevents them from detecting when an actual attack occurs.

As attacker methods become more advanced – and as organizations realize they require a wider array of security solutions – the role of managed security service providers (MSSPs) is expanding. Today, management and advanced analytics capabilities have been added to basic monitoring services to include distributed denial of service (DDoS) protection, vulnerability scanning, security information and event management (SIEM) for wider field of visibility and defence, threat intelligence (e.g., live feeds that update signatures addressing new attacks), and enterprise mobile management (e.g., to keep devices up-to-date and configured properly).

The need for an increasingly long list of security products provided by multiple vendors can be overwhelming for organizations attempting to run their own security operations, especially when

implementing a best-of-breed policy. Due to these factors, IDC forecasts that worldwide managed security services spend will outpace the growth of all other IT security product and services markets, hitting \$34 billion by 2021.

GOSECURE

Founded in 2002, GoSecure offers a wide range of managed security services (CORE), via its Montreal, Canada-based security operations centre (SOC), which are supported by 40 security analysts and engineers operating out of this facility. Additionally, its premier service, Advanced Adversary Protection (AAP), is run out of its Active Response Centre (ARC) based in Dartmouth, Canada, where a team of 25 tier 3 analysts provides threat hunting and mitigation services. Additional services include Advanced Persistent Threats (APTs) and Endpoint Security Lifecycle (ESL). Outside of its service offerings, GoSecure has a highly active research and development team that publishes peer reviewed studies and creates antimalware tools. In the cybersecurity community, GoSecure is seen as a corporate citizen, hosting and sponsoring multiple conferences and events each year that educate and connect security professionals across Canada. GoSecure has an extensive list of certifications, including PCI, ISO 27001, and SOC 2.0, allowing it to provide services across multiple industries such as finance, public sector, and business services.

Reasons Customers Choose GoSecure to Protect Their Organization

As some of the more recent mega breaches have taught us, relying on technology alone to protect your network from attack can leave an organization vulnerable. A simple hardware misconfiguration, too many false positives, or a zero-day vulnerability can quickly compromise security leading to an incident or breach. What is missing – and what organizations struggle to provide internally – is the human element. Even with the most advanced software and hardware solutions available today, there is still no substitute for a certified and experienced IT security professional. As a pure-play security services provider, GoSecure combines best-of-breed solutions, custom IP, and highly trained analysts together to monitor, detect, and mitigate any attacks on your network.

A central operating principle for GoSecure is that it does not collect or store customers' PII or other sensitive data as part of its managing, monitoring, or threat hunting services. Customer data remains on-premise within its control. Not only does this improve customers' information security by reducing the number of copies available, it allows GoSecure to offer flexible consumption models for its services (i.e., customers can terminate a contract at any point without concern regarding the retention or disposal of their data by GoSecure). Due to GoSecure's breadth of service, tiered service model, and flexible contract length, it claims an exceptional customer retention rate of 94.7% over the past 12 years for its managed cybersecurity services.

GoSecure Services

GoSecure offers a comprehensive portfolio of security services, packaged into easily consumable offerings, as shown below.

FIGURE 1

GoSecure Services



Source: GoSecure, 2018

Endpoint Security Lifecycle (ESL)

Patching and updating endpoints is a critical step toward securing your business, but it isn't without its challenges. The wide range of endpoint devices, operating systems, and applications can make patching and updating cycles into a full-time job. GoSecure's Endpoint Security Lifecycle (ESL) service ensures that all of your endpoints are patched with the latest operating systems and application versions, significantly reducing the potential attack vectors available to malicious actors. Built around industry-leading systems management software, ESL integrates asset discovery, continuous state-based awareness, software distribution, patching, and configuration management via a lightweight endpoint client to ensure compliance and simplify audits for all major mobile and desktop operating systems. Included in the service, ESL's web-based customer portal provides real-time information on the status of assets on your network and creates custom reports reducing the time and complexity of audits. ESL can lower operational costs while freeing up IT resources to focus on other more pressing tasks.

CORE: Managed Security Operations

CORE services allow customers to outsource all cybersecurity operations to GoSecure, and span across perimeter and application defence, endpoint protection, and security monitoring. This includes total life-cycle management for hardware and software solutions from leading vendors. Security operations are supported by a team of over 40 security analysts operating out of GoSecure's Montreal SOC who monitor customers' networks 24 x 7 x 365 for alerts and malicious activity while eliminating false positives. In terms of monitoring, GoSecure can support all major SIEM platforms on the market, but, for customers that don't want to make the investment in on-premise infrastructure or software licensing, GoSecure offers a cloud-based SIEM as well. The NetWitness Logs and Packets solution allows customers to have fully outsourced SOC 2.0 SIEM operations in an easily consumable model. The full portfolio of CORE services is outlined in Figure 2.

FIGURE 2

GoSecure CORE Services



Source: GoSecure, 2018

CORE services are built to be highly customizable, and GoSecure offers a variety of service options and extensions to meet the unique needs of customers. This includes additional consulting services such as SIEM use case design, computer and network forensics, and integration with a client's helpdesk, to name a few. GoSecure CORE customers have access to detailed security reporting through an on-demand web portal.

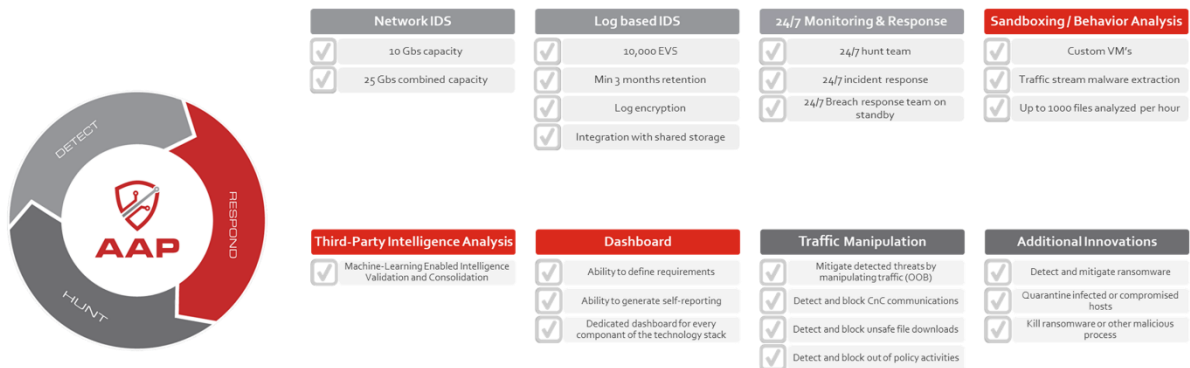
Advanced Adversary Protection

GoSecure's premier service, AAP, is conducted out of the ARC located in Dartmouth, Nova Scotia, on the Canadian east coast. This SOC2 Type II facility is manned 24 x 7 x 365 and supported by two tier 4 datacentres. 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 malicious activity, rather than wait for an alert from a SIEM or device to appear.

IDC was granted a behind-the-scenes tour of the ARC and the ability to meet its analysts in person. We found the team to be highly engaged, thorough, and well trained. More importantly, our one-on-one meetings revealed how many side projects GoSecure allows team members to invest in to deepen their ability to protect customers. Such projects include advanced machine learning to automate processes, open source project contributions, and uniform resource identifier, to name a few.

FIGURE 3

AAP Operating Concepts and Capabilities



Source: GoSecure, 2018

ARC Differentiation



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.

GoSecure has gone to considerable lengths to simplify SLAs for AAP. A standard service operation package is available which incorporates monitoring, incident management, updates, and vulnerability scanning services. GoSecure offers a standard and premium service package, with standard service guaranteeing incident response in an hour or less, and the premium service level dropping response time to 30 minutes.

CHALLENGES AND OPPORTUNITIES

GoSecure operates within a growing but highly competitive market offering managed security services to customers in Canada, the U.S., and the UK. There are low-cost providers and high-touch providers that are closing in from opposite ends of the market. Moreover, these providers have expanding sales footprints, channel partners, and expansive digital marketing against which GoSecure needs to position itself.

In a noisy market, GoSecure has taken a subtle approach to marketing by creating, leading, and being a part of security communities (e.g., HASK), organizations (e.g., ISACA, IAA, Public Safety Canada), information sharing (e.g., OWASP, SERENE-RISC), and conferences (e.g., NorthSec, ATLSECCON, GoSec, BSides).

Based on the size and knowledge of the GoSecure team, and its focus on advanced services such as AAP, IDC believes GoSecure is well placed to protect customers and grow its business. We are impressed by its attention to customer satisfaction above the desire to rapidly scale its business. This customer-centric approach allows it to continue to provide rapid detection and response when attacks occur.

SELECTION CRITERIA FOR A MANAGED SECURITY PROVIDER

When considering a managed security services provider, there are several key factors to keep in mind:


- **Comprehensive SLAs.** Compare pricing and hold providers to an appropriate SLA. There is a wide range of pricing in the marketplace for given service levels. Whether it's basic firewall management or full SIEM monitoring, you should compare providers to make a decision. There are many variables that you will consider (e.g., quality of their analysts, usefulness of their interface/portal, and solutions supported). However, we recommend simplifying your selection to: a) speed of resolving an incident (i.e., within what span of time), and b) proactiveness when alerting your organization to new threats.
- **Proactive service.** Understand what the provider is doing "behind the scenes" to protect your organization. Many MSSPs will advertise a list of threat intelligence services that they subscribe to, how many analysts they have, or that they follow the sun in SOC activity and so forth. Ask them about what their staff are doing on your behalf. In other words, how often are their analysts reactive (e.g., calling you when an alert appears on their screen) versus hunting for problems in order to get ahead of an alert – and to know if it is a false positive or a real incident.
- **Relationship building.** Know the people your team will work with. Having a good working relationship with a provider is important for bidirectional knowledge transfer (e.g., gaining some of your MSSP's knowledge, while continuing to update them about changes that may impact security).
- **Technical depth.** Ensure the provider is familiar with your particular technology and setup. If your organization relies on certain security technologies, ensure that your MSSP is well versed in them rather than merely having a base level familiarity with them.
- **Roadmap alignment.** As your organization extends into cloud, IoT sensors or other technologies unique to your industry, make sure that your choice of MSSP will understand and be able to secure your business as your attack surface changes.

BRINGING IT ALL TOGETHER

Throughout this paper we've described the landscape of security challenges and how successful organizations are starting to address them. These challenges will impact your organization in very

different ways, depending on your current state of IT security, culture, compliance requirements, and size of attack surface. Try to determine where your organization is today – and plan for how it might improve over time.

To assist, IDC classifies organizations into four groups based on their approach to IT security. Consider which persona best matches your own organization. The groups form around how many breaches they suffer, what their security budgets are, their security maturity, and the kinds of defences they put in place.

	Summary	Action
 Defeatist	<p>These organizations suffer the most breaches and vastly underspend on security. IT has given up trying to get security leadership and investment from their executives. This is the second largest group of organizations and accounts for one out of four organizations.</p>	<p>Join security communities in your area or online to build back your confidence, learn best practices, and be among peers who face similar issues.</p>
 Denialist	<p>These organizations suffer more breaches than average and may overspend on IT security. They invest in technology – and can boast about having the latest solutions in place. However, they do not do enough assessment of risk (e.g., they are likely spending too much in some places and too little on others, without considering where they are most vulnerable). They don't do enough to teach employees the basics of good security practices.</p>	<p>Maintain your technical depth, but add security risk management into the mix.</p>
 Realist	<p>These organizations suffer fewer breaches than average and spend an appropriate amount on IT security. Their greatest strength is their focus on assessing risk. They know where to invest each security dollar. Their failing is that they don't do enough employee training.</p>	<p>Increase your attention on security staff training and on end-user employee security training.</p>
 Egoist	<p>These organizations suffer the fewest breaches and spend an appropriate amount on security. They are a small group comprising only one out of six organizations. They buy the right technologies, they monitor their security, they do risk assessments well, AND they train employees. In other words, they are much like the Realists, but add in a focus on employee training.</p>	<p>Try not to miss new risks by being overconfident in your abilities (this is one side effect IDC notes with this category).</p>

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

Copyright and Restrictions

Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. For permission requests contact the Custom Solutions information line at 508-988-7610 or permissions@idc.com. Translation and/or localization of this document require an additional license from IDC. For more information on IDC visit www.idc.com. For more information on IDC Custom Solutions, visit http://www.idc.com/prodserv/custom_solutions/index.jsp.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015
www.idc.com.

