Starting the conversation

Introducing ISA endpoint protection and vulnerability management services.

Nobody can be truly safe from cyberattacks, but the ability to detect a potential threat early is critical for protecting any organization. But many IT departments simply don't have the time, resources or even skillsets to investigate and mitigate constantly evolving security threats, nor to implement increasingly complex security applications. Cloud-based services hosted by ISA offer a great alternative, where ISA does the heavy lifting. With ISA's SOC-as-a-Service, your client doesn't have to invest in or manage security infrastructure. Instead, they can focus on their core business. ISA Infinity Partners can offer services like **PROTECT EDR** and **RADAR** to their clients:

PROTECT EDR

Through deployment of a single agent, multiple layers of protection are provided to all endpoints in the network. **PROTECT EDR** detects unusual activity and your client can trust ISA's team of specialists to take proactive action

RADAR

A virtual scanner performs periodic non-invasive scans that uncover vulnerabilities and allows audit of patch management processes. If severe issues are found, the client is notified immediately.

Straightforward and predictable licensing.

Most managed cybersecurity services are complex and often their licensing is complex too, not to mention very costly. ISA's SOC-as-a-Service model makes things easy! **PROTECT EDR** and **RADAR** are licensed per endpoint, per month. Through the ISA Infinity Partner Program, you have the option to sign up your client for cost-effective 3-year subscriptions or choose a flexible consumption-based* model. The fee for the services decreases as the client signs up more endpoints.

*consumption-based licensing requires an on-boarding fee.

Conversation starters and scoping questions:

CEO, CIO, and CISO:

+ How do you currently manage the risk and impact of cyber threats on your business?
+ Has your organization adopted cloud-based services to increase business productivity?
+ Are you confident you have the staff in place to detect and respond to cyber threats?
+ Are you interested in cybersecurity solutions delivered as a service?

IT Director:

+ What are your major cybersecurity concerns; do you have a plan in place in the event of an incident?
+ Does your team have the expertise to detect and respond to threats? How much of their time is spent managing the security tools?
+ Do your existing cybersecurity tools help you achieve your goals?
+ What industry regulations do you need to comply with? How do you report on your cybersecurity posture?
+ What vulnerability management solution do you have in place? Have you been able to keep it up to date?
+ How many remote sites do you haven and how are users connecting to the network?

IT Specialist:

+ What are the cybersecurity responsibilities of your team?
+ Do you have visibility in all the internal and external endpoints connecting to the network?
+ How do you currently detect internal and external threats?
+ What security products/tools do you use to detect and respond to cyberthreats?
+ What tools do you use to report on your cybersecurity posture?
+ Is your vulnerability management solution currently scanning internal and external assets?

Objection handlers

Cyberattacks? Our company is too small to be a target!

+ All companies that have digital assets and handle or store client data are under threat of cyberattacks.
+ In Canada, SMB's are becoming targets, often to penetrate the supply chain of a larger organization.

We'll hire a security engineer, we don't outsource!

+ Security analysts are more expensive and harder to find than you may expect there's a global shortage of cybersecurity specialists.
+ You may require multiple engineers for ongoing security and the ability to handle employee churn.

PC's have free Anti-Virus, why pay for a service?

+ Pre-installed Anti-Virus protects individual devices from known threats, not professional endpoints, part of shared environments.
+ **PROTECT EDR** comes with many features, including signature-based Anti-Virus , that proactively manages all your endpoints.

We've done a positive assessment, we are compliant!

+ Security assessments are helpful and detailed snapshots of an environment; ISA performs many for their clients.
+ After an assessment, it only takes one user making a change, to create a potential threat. **RADAR** will catch this in the next scan.

Our network and endpoint security tools are sufficient!

+ Can you continuously monitor alerts these tools generate and identify break-ins and advanced attacks?
+ If you haven't detected at least an attempted attack in the past month, you've missed something.

New security tools to manage? I'll get lost in reporting!

+ You won't have to worry about management: after on-boarding, the ISA team will manage your Cybersecurity Service for you
+ All the insights and reporting for ISA services come together in one easy to understand portal with dynamic dashboards.

We already have robust Patch Management in place!

+ A Vulnerability Management service will audit your patching trends and management to see if necessary, fixes were applied properly.
+ It's good practice to validate fixes separately to avoid conflict of interest.

I manage cybersecurity, if we sign up, I may lose my job!

+ Many vulnerabilities come from human error; let cybersecurity specialists worry about potentially complex cybersecurity solutions.
+ You and your teams will have the time to focus on supporting your company's core business.

Here are 6 reasons why Canadians are choosing ISA services:

IDC MarketScape©: "ISA is a Major Player in Canadian Security Services."‡

ISA is Canada's largest pure-play Managed Security Services Provider

ISA has offices across Canada and guarantees Canadian Data Residency

ISA has a culture built on quality, commitment and integrity*

ISA's state-of-the-art CIOC is SOC 2 Type 2 certified by AICPA

ISA is recognized as a top partner by industry leading technology vendors°

‡https://www.idc.com/getdoc.jsp?containerId=prCA45450419 *Articulated as such by the ISA Client Advisory Council. °Visit the ISA website for partnership details.