HOSTED SECURITY SERVICES

A PROVEN STRATEGY FOR PROTECTING CRITICAL IT INFRASTRUCTURE AND DEVICES

Being always-on, always-connected might be good for business, but it creates an ideal climate for cybercriminal activity. Cybercriminals keep pushing the bar with new ways to steal data, extort money, bring businesses to a halt — or simply wreak havoc, seemingly just for the fun of it. All of this comes at a cost that’s often in the millions of dollars!

It’s no longer enough to put up a fortress, hoping it will keep the bad guys out. These days, employees are mobile, using personal devices for work and business outside the workplace. They use applications that may not be authorized by the IT department, leading to shadow IT. And the emergence of the Internet of Things (IoT) means there may be thousands of end points in a single organization that can serve as an entry point (or back door) to cybercriminals.

Cybercriminals are always on the lookout for inventive new ways to exploit vulnerabilities, from malware attachments and distributed denial-of-service (DDoS) attacks, to ransomware, keyloggers and screen grabbers — not to mention social engineering tactics such as phishing, that trick employees into exposing or simply giving away their usernames and passwords.
THE THREAT LANDSCAPE IS BOOMING AND EVOLVING

The boom in cybercriminal activity is now costing people and businesses around the world almost $600 billion, according to The Economic Impact of Cybercrime: No Slowing Down, a report from McAfee and the Center for Strategic and International Studies (CSIS). The report also shows that new incidences of malware are propagating at the rate of 300,000 per ‘day’. Of all the threats, ransomware is the fastest growing, and today there are more than 6,000 online criminal marketplaces actively selling ransomware products and services.

Security breaches can cause damage that takes months or even years to resolve. And the malware is evolving to maintain its effectiveness, as cybercriminals adapt their techniques at a faster pace than organizations are able to defend. Malware is also being weaponized, and exploits are being launched with increasing frequency and magnitude. In fact, according to Cisco’s 2018 Security Capabilities Benchmark Study, threat actors have taken ransomware to a new level, with worm-like functionality that causes even more widespread damage.

The Cisco report asks, "When adversaries inevitably strike their organizations, will defenders be prepared, and how quickly can they recover? That depends largely on the steps they’re taking today to strengthen their security posture.”

WHY BUSINESSES ARE STRUGGLING WITH IT SECURITY

As the threat landscape grows and evolves, IT departments need to step up their efforts. Not only are they dealing with an increase in the sheer volume of attacks, but they’re also faced with increasingly complex, sophisticated attack methods. Attacks are being launched on all fronts, including mobile devices and the public cloud, while user behaviour remains an ongoing challenge. At the same time, the cost of security incidents is rising incrementally.

Even in the face of all this, many IT Security Professionals remain focused on just keeping the lights on, rather than improving security operations. In the Cisco report, security professionals cited budget, interoperability and personnel as the key reasons for this approach — and a lack of skilled talent topped the list of obstacles. But even those dedicated to security often spend an inordinate amount of time responding to alerts and putting out fires, leaving inadequate time and resources to take a pro-active approach by updating policies, upgrading software and implementing strategic security initiatives.

The solution? More and more organizations are turning to Hosted Services as an integral part of their corporate security strategy.
HOSTED SERVICES ADDRESS THE CHALLENGES OF TODAY’S THREAT LANDSCAPE

No network or device can be truly impervious to attack, but the ability to detect a potential security threat early — before it becomes an issue — is a critical strategy for protecting your organization. But many IT departments simply don’t have the time, resources or even skillsets to investigate and mitigate the constantly evolving security threats, nor to implement increasingly complex security applications.

Hosted Services offer a great alternative, where a third-party security solutions provider does the heavy lifting for you. With hosted services, you don’t have to invest in or manage security infrastructure – instead you can focus on IT initiatives that are more strategic to the business.

Hosted Services from leading security provider ISA, for example, are designed to respond to evolving security threats, and provide organizations with the tools to truly protect networks and devices. ISA’s Hosted Services minimize outbreaks and breaches with 24×7×365 monitoring and remediation, carried out by a dedicated team of highly-trained malware and forensic analysis specialists. The Hosted Services ensure strict adherence to daily and weekly endpoint security enforcement and validation tasks.

Just as important, ISA has a state-of-the-art Cybersecurity Intelligence and Operations Centre (CIOC) that is designed with unparalleled physical security capabilities, and a multi-tenant cloud offering powered by industry-leading SIEM technology. The CIOC ensures ISA can quickly detect and head off threats, as well as meet policy and regulatory compliance requirements, all focused on minimizing risks to mission-critical services, data and assets. The CIOC is the front line for monitoring and managing an organization’s security infrastructure.

When adversaries inevitably strike organizations, will defenders be prepared, and how quickly can they recover? That depends largely on the steps they’re taking today to strengthen their security posture.

2018 Cisco Security Capabilities Benchmark Study
ISA Hosted Services are designed to help organizations effectively manage their security operations and protect intellectual property. A proven outcome-based approach ensures malware signatures and trends are always fully up-to-date, and policy changes and security best practices are applied on demand. Plus, ISA provides important security intelligence, helping customers understand the impact of threats on their organization with real-time insight into their current security posture.

Organizations can choose from a menu of ISA Hosted Services:

**Hosted Endpoint Security Platform:** A cloud-based, centralized, professionally managed suite of industry-recognized endpoint security technologies designed to detect and protect organizations from the most advanced threats.

**Security Monitoring Service:** A 24×7×365 security monitoring service with built-in management, threat intelligence, triage and incident investigation services. Security experts provide guidance, context, support and recommendations.

**Vulnerability Management Service:** An integrated vulnerability management platform that identifies critical flaws and provides solutions for remediation. This service also helps organizations maintain compliance with regulatory requirements, and mitigate risk by ensuring they have a holistic view of their environment and the weaknesses they need to address.

**Security Awareness Program:** User-based risk assessment and deployment of security awareness training programs that can identify vulnerable users, and provide detailed reporting on the progress of training programs within the organization. This helps organizations evaluate their current security awareness landscape with insights to help understand their capacity to handle threats.

**RELIABLE SECURITY DEPENDS ON A TRUSTED PARTNER**

Canada's largest security-focused solutions provider, ISA has more than 25 years of experience helping organizations of all sizes solve complex IT security challenges. How are we different? Our state-of-the-art CIOC is based on Gartner Magic Quadrant technology. We have nurtured a mature framework for improving correlation rules as new threats and techniques are developed. And we provide our customers with advanced threat intelligence and contextualization.

**SECURITY IS WHAT WE DO – AROUND THE CLOCK.**

For more information about ISA:

[www.e-isa.com](http://www.e-isa.com)  1-877-591-6711  info@e-isa.com
ISA is a security-focused technology firm, with over 20 years of experience helping organizations across Canada solve complex challenges relating to IT security. We act as trusted advisors to help our clients define, implement and manage strategies to minimize IT security risks, and provide a secure business environment for employees and customers. Visit e-isa.com.


CONTACT US
For more information, contact us at:

1-877-591-6711
info@e-isa.com

TORONTO (Head Office)
3280 Bloor Street West, Suite 1100
Centre Tower, 11th Floor
Toronto, ON M8X 2X3
Tel: 416-591-6711
Fax: 416-352-7512
Email: info@e-isa.com

CALGARY
144 - 4th Avenue South West
Suite 1600
Calgary, AB T2P 3N4
Tel: 403-695-1790
Fax: 403-716-3637
Email: info@e-isa.com

OTTAWA
1 Rideau Street
Suite 700
Ottawa, ON K1N 8S7
Tel: 613-670-5741
Fax: 613-670-5701
Email: info@e-isa.com

Visit us online at www.e-isa.com