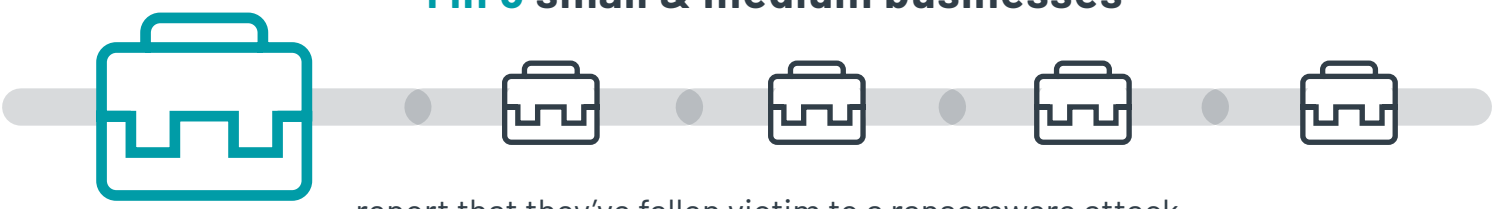
SysGen
experience IT

Managed Security

The cybersecurity landscape

Organizations spend more than ever dealing with the costs and consequences of increasingly sophisticated attacks

1 in 5 small & medium businesses



report that they've fallen victim to a ransomware attack.

Security breaches have increased by 11% since 2018 and 67% since 2014.

The average cost of downtime and recovery

for small businesses after an attack
is more than 23x the average ransom requested.

$9,000 ransom = $207,000 downtime cost

Leading causes of cyberattacks:

$30,000 is the average amount of money sent during a phishing attack.

SOURCES: DATTO'S GLOBAL RANSOMWARE REPORT & THE BUSINESS GUIDE TO RANSOMWARE; CSO ONLINE: *PHISHING STILL REMAINS ONE OF THE BIGGEST CYBER THREAT FOR ORGANISATIONS*

Obtain peace of mind with SysGen's comprehensive security offering

People | Policy | Technology

SysGen takes a three-pronged approach to a comprehensive cybersecurity strategy, emphasizing People, Policy, and Technology. If your business concentrates on one area but not the others, a gap will exist for a security breach to occur. It's like locking all the doors to your house but leaving the window open. Focusing on People, Policy and Technology is your **best defense** against a cybersecurity attack.

People

80% of data breaches are caused by human error. That's why SysGen provides educational tools including in-person training and online workshops for employees to understand how to identify and mitigate malicious attacks.

Policy

Policy creates the organizational framework for appropriate security processes within your company. SysGen provides templates and guidance for policy development, so that cybersecurity policies can be custom-built for your organization depending on your needs.

Technology

SysGen works with cutting edge organizations in the cybersecurity industry while continuously monitoring the security landscape as it evolves. While technology is not a silver bullet for your cybersecurity defense, it is an integral piece to your security strategy.

SysGen Managed Security suite of products

SysGen Managed Security offers three tiers of protection based on the needs of your organization: ESS, ESS+, and ESS+ Realtime.

Protection		ESS	ESS+	ESS+ Realtime
Technology	Anti-Virus	X	X	X
	Anti-Malware	X	X	X
	Anti-Spam	X	X	X
	Multi-Factor Authentication (MFA) *Requires O365/M365	X	X	X
	Forensics		X	X
	Intelligent Threat Protection		X	X
People	Training Platform	X	X	X
	In-Person Training	X	X	X
	Security Bulletins	X	X	X
	Mobile Device Protection		X	X
Policy	Policy Development	X	X	X
	Data Encryption		X	X
	Governance		X	X
	Real Time Monitoring			X

Your best defense against a cybersecurity attack

ESS	ESS+	ESS+ Realtime
A basic security package designed to reduce the chances of your technology or people being compromised.	An advanced security package designed to greatly reduce your security risks while developing corporate policies to manage security comprehensively.	The advanced security offering with the addition of real-time 24/7/365 monitoring, protection, and response.

ANTI-VIRUS: Software designed to detect and destroy computer viruses.

ANTI-MALWARE: Software used to scan, identify and eliminate malicious software (malware) on IT systems, as well as individual computing devices.

ANTI-SPAM: Software that prevents people from sending and receiving unwanted emails.

MULTI-FACTOR AUTHENTICATION*: a method of confirming a user's identity by utilizing something they know and a second factor such as something they have or something they are.
**Requires O365/M365*

FORENSICS: Should a cybersecurity event occur, forensics will provide a deep understanding of the who, what, where, when, why and how.

INTELLIGENT THREAT PROTECTION: A complete endpoint security solution offering a fleet of advanced endpoint threat prevention capabilities.

TRAINING PLATFORM: SysGen deploys mock-phishing attack to understand employee vulnerability in the organization. Users are assigned training based on their skills and knowledge.

IN-PERSON TRAINING: Engaging hands-on workshops for employees.

SECURITY BULLETINS: Instant updates on attempted or potential threats and attacks to your infrastructure.

MOBILE DEVICE PROTECTION: Software used to manage and secure employees' mobile devices, including mobile phones, laptops and tablets.

POLICY DEVELOPMENT: Support, guidelines and templates for developing internal cybersecurity policies.

DATA ENCRYPTION: A security method where information is encoded and can only be accessed or decrypted by a user with the correct encryption key or password.

GOVERNANCE: Roadmap for strategic direction to achieve cybersecurity objectives and safeguard high-risk assets.

REAL-TIME MONITORING: 24/7/365 scanning and monitoring of IT environment.

403.226.0994
info@sysgen.ca
www.sysgen.ca
Calgary, Edmonton, Red Deer, Vernon

SysGen
experience IT