IDC ANALYZE THE FUTURE

CIO ASSOCIATION OF CANADA

ITAC INFORMATION TECHNOLOGY ASSOCIATION OF CANADA

ITWC The Content Experts

IT Security: Managing a New Reality

Kevin Lonergan

#IDCdirectionsTO

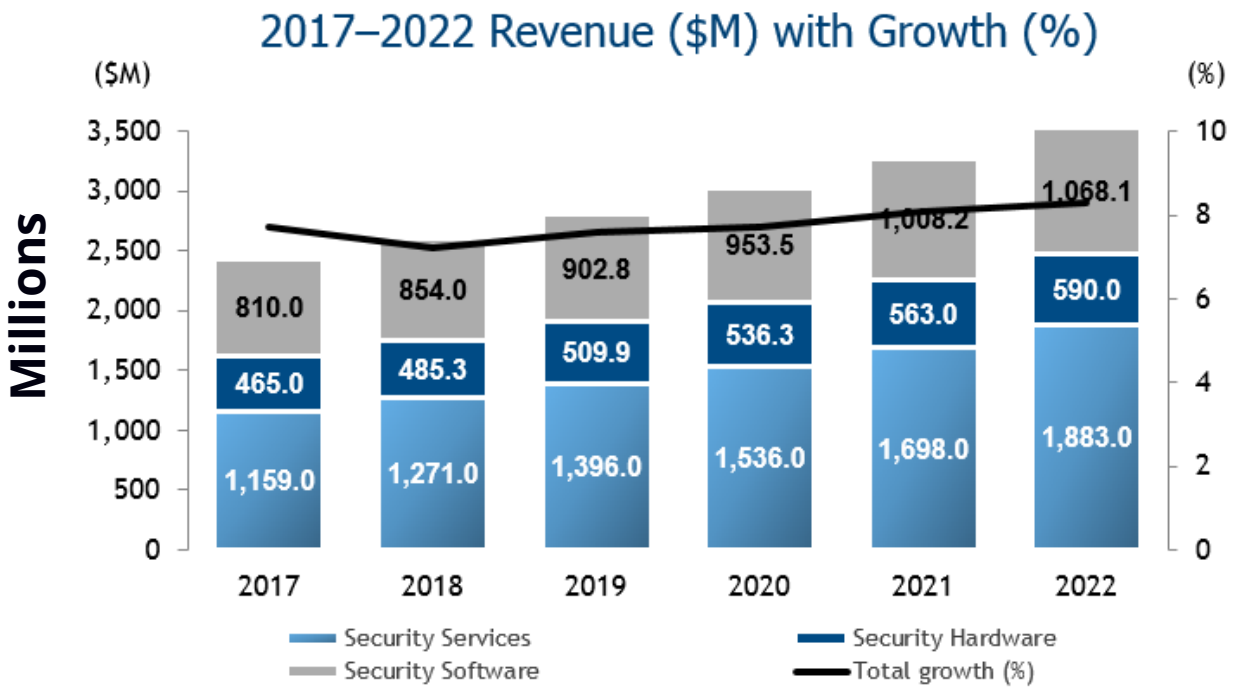
© IDC

You're Only as Strong as Your Weakest Link

Locks Only Work if you Know How to Use Them

© IDC

Canadian Security Market Forecast: 2017 - 2022



Selected Segment Growth Rate

- Security Services CAGR 10.2%
- Security Software CAGR 5.7%
- Security Hardware CAGR 4.9%

Total Market CAGR 7.8%

Key Trends

- Canadian organizations are currently spending 10% of their IT budget on security
- Cloud and DX reshaping market opportunities
- MSS leading growth of services as firms struggle with 24x7 monitoring and skills availability
- Subscription based solutions continue to evolve

© IDC

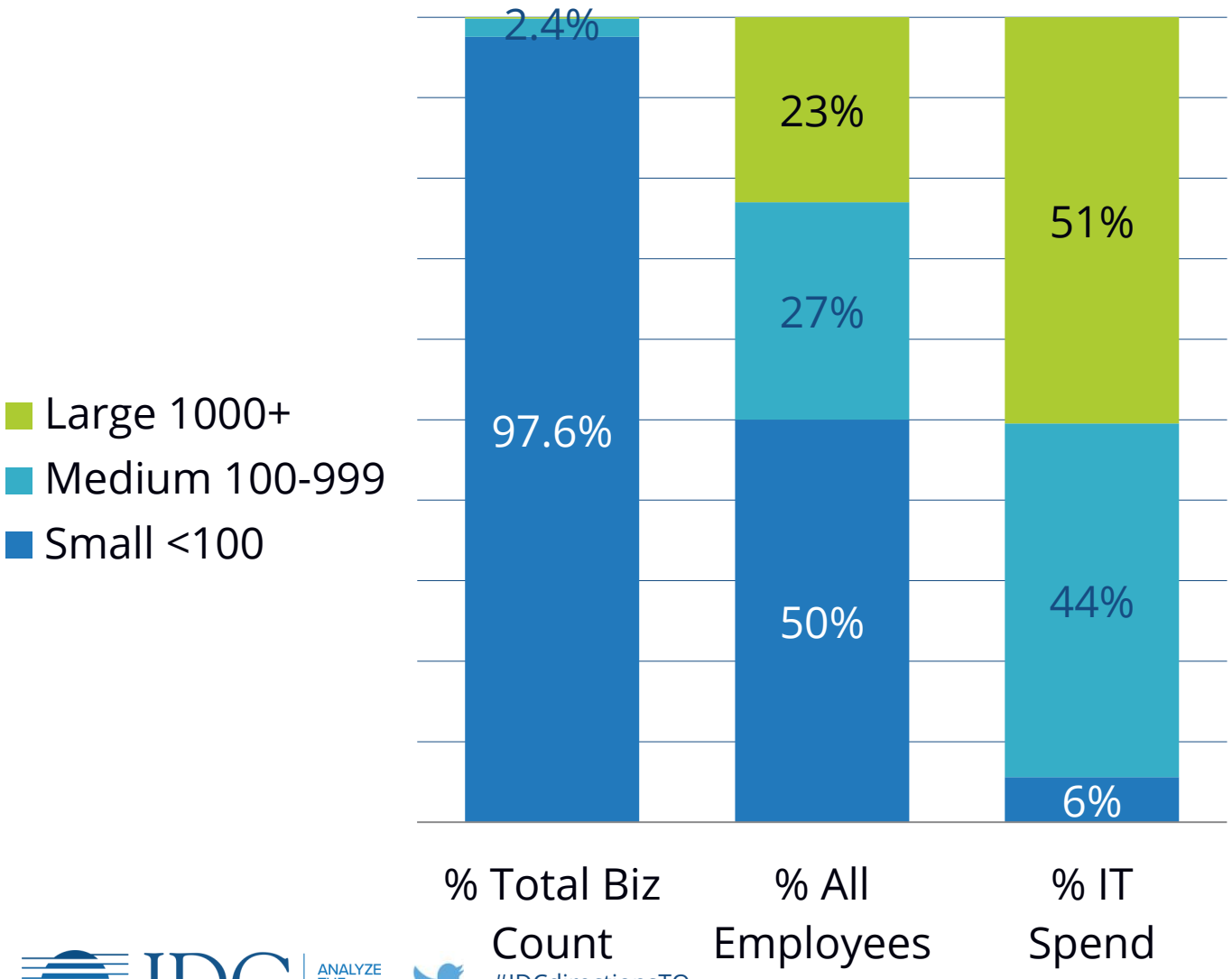
Big Cybersecurity Numbers Across Canada

Attacks (known)	83,000,000 nationwide
Breaches (known)	2,600,000 nationwide
Days of downtime	813,000 nationwide
Records exposed	100,000,000 nationwide
Average attacks per year	455 / organization
Average cost per breach	$3,700,000 / organization

Mega breaches – exposing millions of records – make headlines. But attackers will settle for dozens of records, from a breach of smaller organization.

© IDC

The Truth About the Canadian SMB



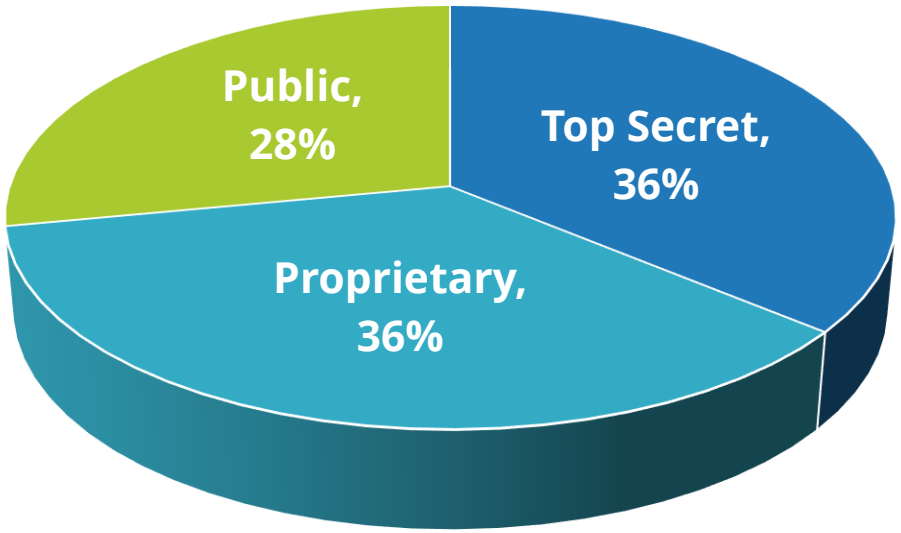
Market Breakdown

- The 1800 enterprise organizations make up over 50% of IT spend.
- Midmarket organizations represent 2.4% of the market and represent 44% of IT spend
- The vast majority of Canadian organizations have less than 100 employees. 97.6% of organizations fall into this category, employing 50% of the Canadian workforce, but only generating 6% of overall IT spend

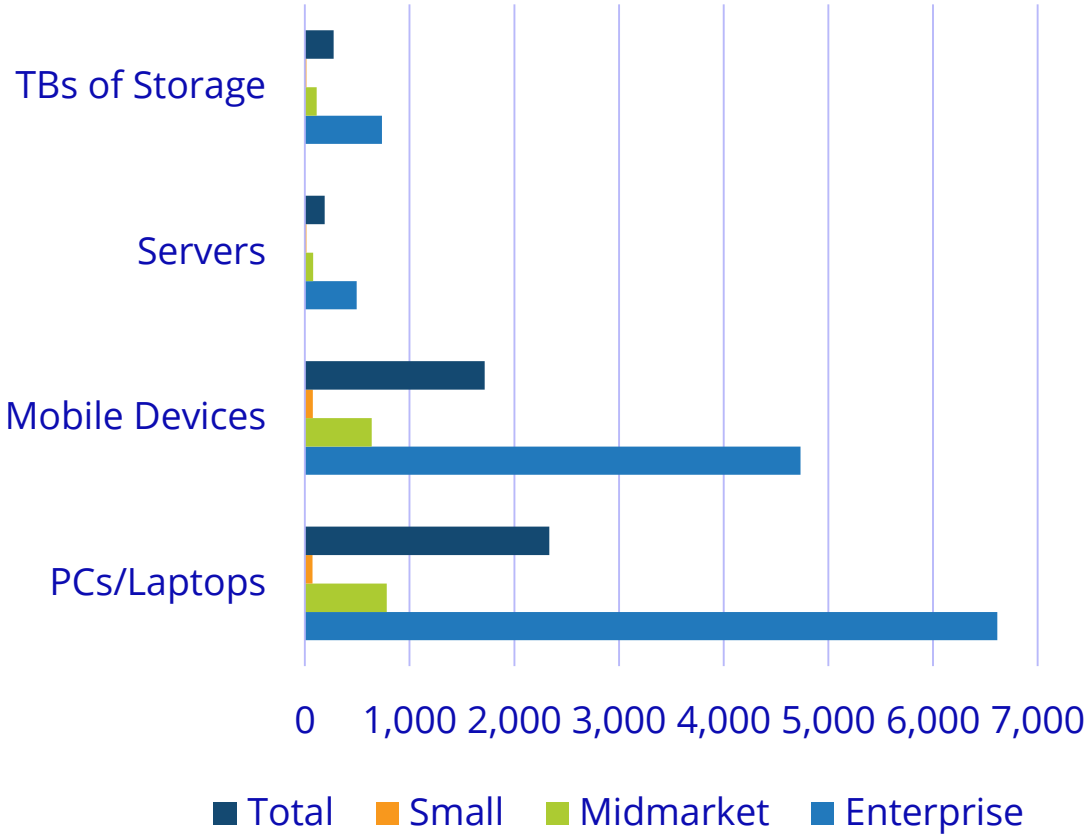
© IDC

What Are We Protecting?

Data Classification



IT Assets by Organization Size



Average Number of Breaches per Year

- Small: 8 breaches
- Midmarket: 9 breaches
- Enterprise: 11 breaches

Results from the 2018 Scalar Study conducted by IDC Canada

© IDC

How Long Before Knowing a Breach Happened

Length of time security consultants and vendors say it takes the average Canadian organization to detect a breach

Within hours	Within a week	Within a month	Within a year	A year or more
5%	34%	18%	31%	12%

Oh, Canada

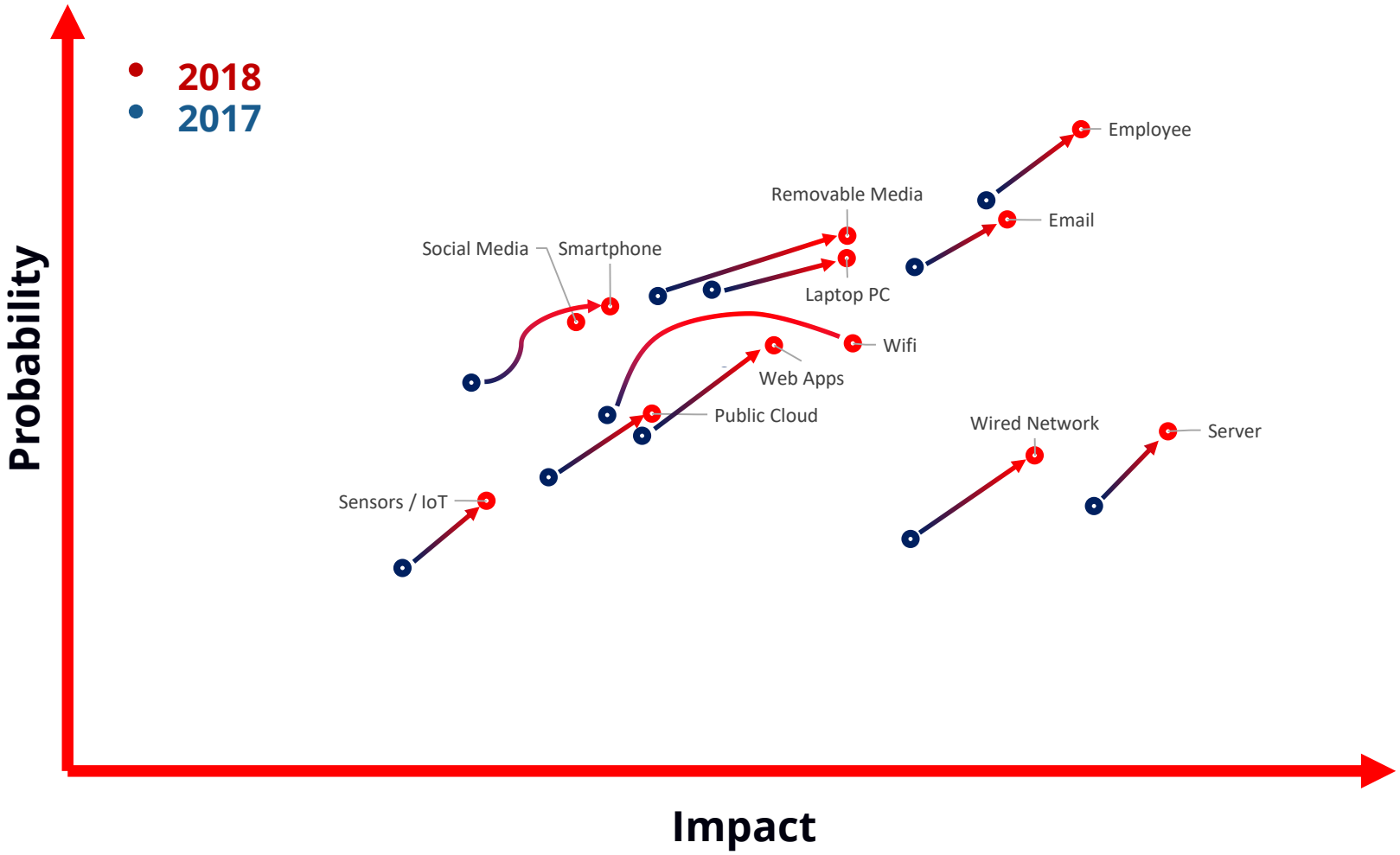
© IDC

10 Key Areas to Protect:

Target	Scalar Study Finding	Comments
Employee	26% trained to identify attacks / 59% learn care for sensitive data	Train employees on tools, attacks, updating, care of data…
PC	30% left exposed for weeks after patch release	Keep 'm updated
Smartphone	28% concerned about mobile threats	Doing an OK job, but increase awareness of new threats
Sensor / IoT	37% concerned w/ IoT security	This will get worse
Messaging	58% see high value in email security solutions	Lots of focus has paid off
Web	89% admit slow patching/updating	Horrible! At least patch/update
Server	86% admit slow patching/updating	Importance of pen tests/vuln assessment
Network	61% finding good satisfaction with NGFW	Don't rely on basic tech, Upgrade to better analytics
IaaS/PaaS	66% left exposed for MONTHS	This will get worse too. Treat cloud like on-prem
Partners	26% have comprehensive knowledge of partner security	Try to learn more about your partners' security posture

© IDC

How Canadian Organizations View Their Attack Surfaces



© IDC

Critical Roadblocks to Improving Security

Rank	Top 5 Security Roadblocks
1	Budget
2	Employee knowledge
3	New and changing threats
4	Lack leadership
5	Lack policy

Rank	Who Needs the Most Training?
1	IT Staff
2	Operations Staff
3	Sales Staff

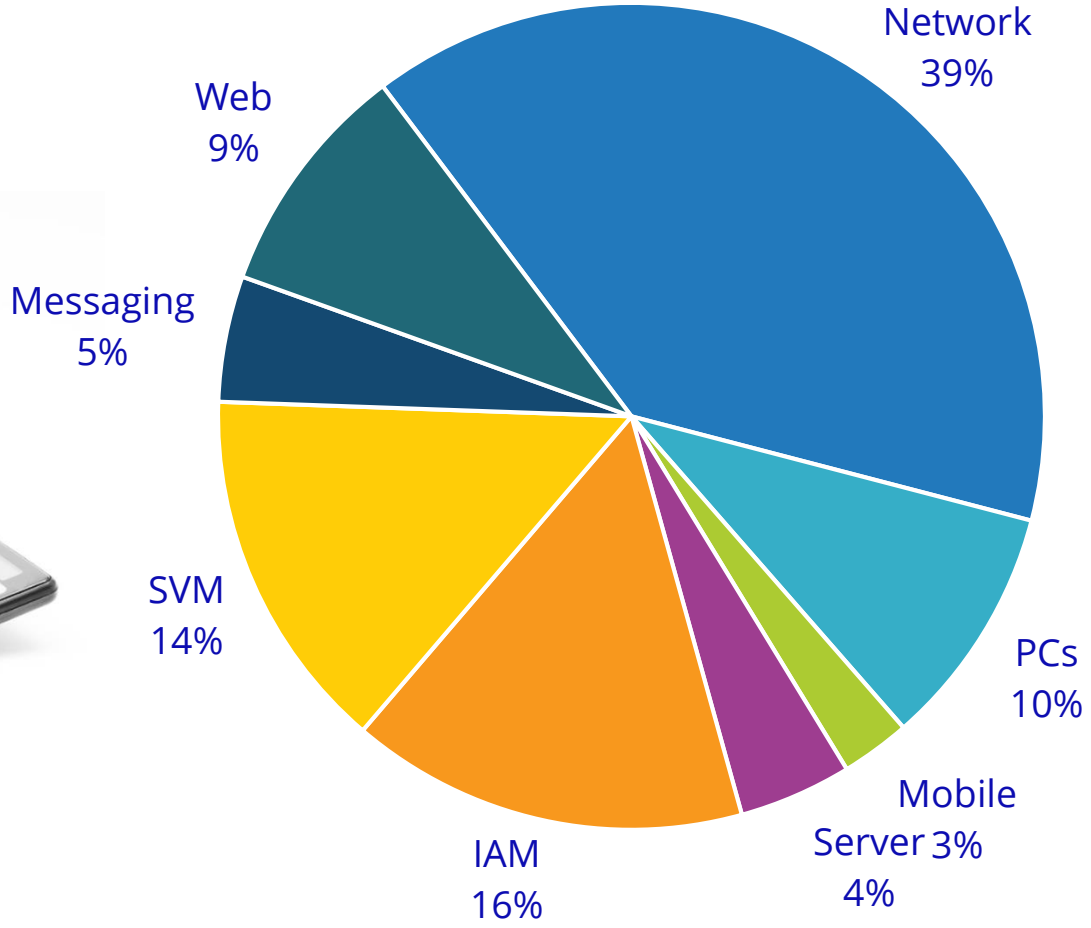
% employees trained in email and web security in the last 12 months:

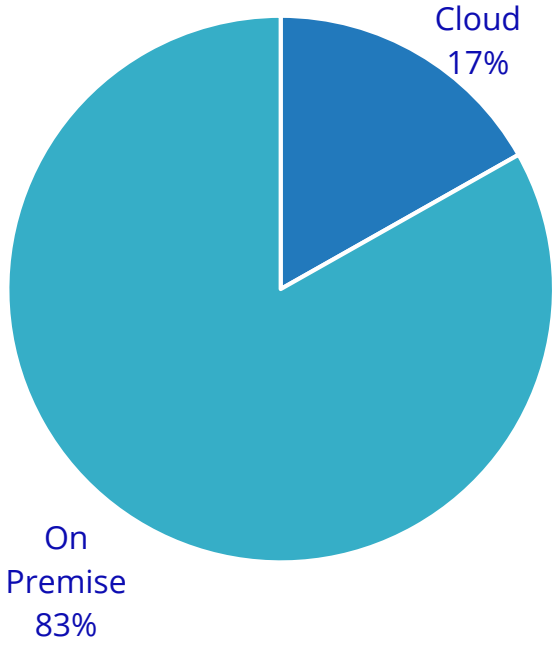
<25%	25%-49%	50%-74%	>75%
54%	8%	10%	23%

- Employees' lack of knowledge regarding security is a top roadblock cited by Canadian firms, yet there is limited training happening! Majority of workers receive little to no training.
- Half of Canadian organizations admit that their IT security habits need improvement, including training

© IDC

Proportion of Security Spend by Product Type





© IDC

Security Technology Growth, 2018

Functional Market	Sub-Market	2018	2018 Growth	Share
Vulnerability Management	SIEM	$72	9.8%	39.8%
	Policy and compliance	$46	8.9%	25.4%
	Vulnerability assessment tools	$37	11.2%	20.4%
	Forensics and incidence investigation	$21	14.3%	11.6%
	Secure device systems management	$5	1.8%	2.8%
Identity and Access Management	Single sign on	$80	7.9%	42.1%
	Advanced authentication	$61	6.7%	32.1%
	User provisioning	$34	3.3%	17.9%
	Priveledged access management	$10	17.4%	5.3%
	Legacy authentication	$5	-3.0%	2.6%
Network Security	UTM	$298	9.2%	62.7%
	Firewall	$89	0.0%	18.7%
	IDP	$81	1.0%	17.1%
	VPN	$7	0.1%	1.5%
Content Management	Web	$109	2.8%	65.7%
	Messaging	$57	0.3%	34.3%
Endpoint Security	Enterprise	$176	6.4%	58.9%
	Consumer	$123	-3.9%	41.1%
Total		$1,311.3	7.2%	100%

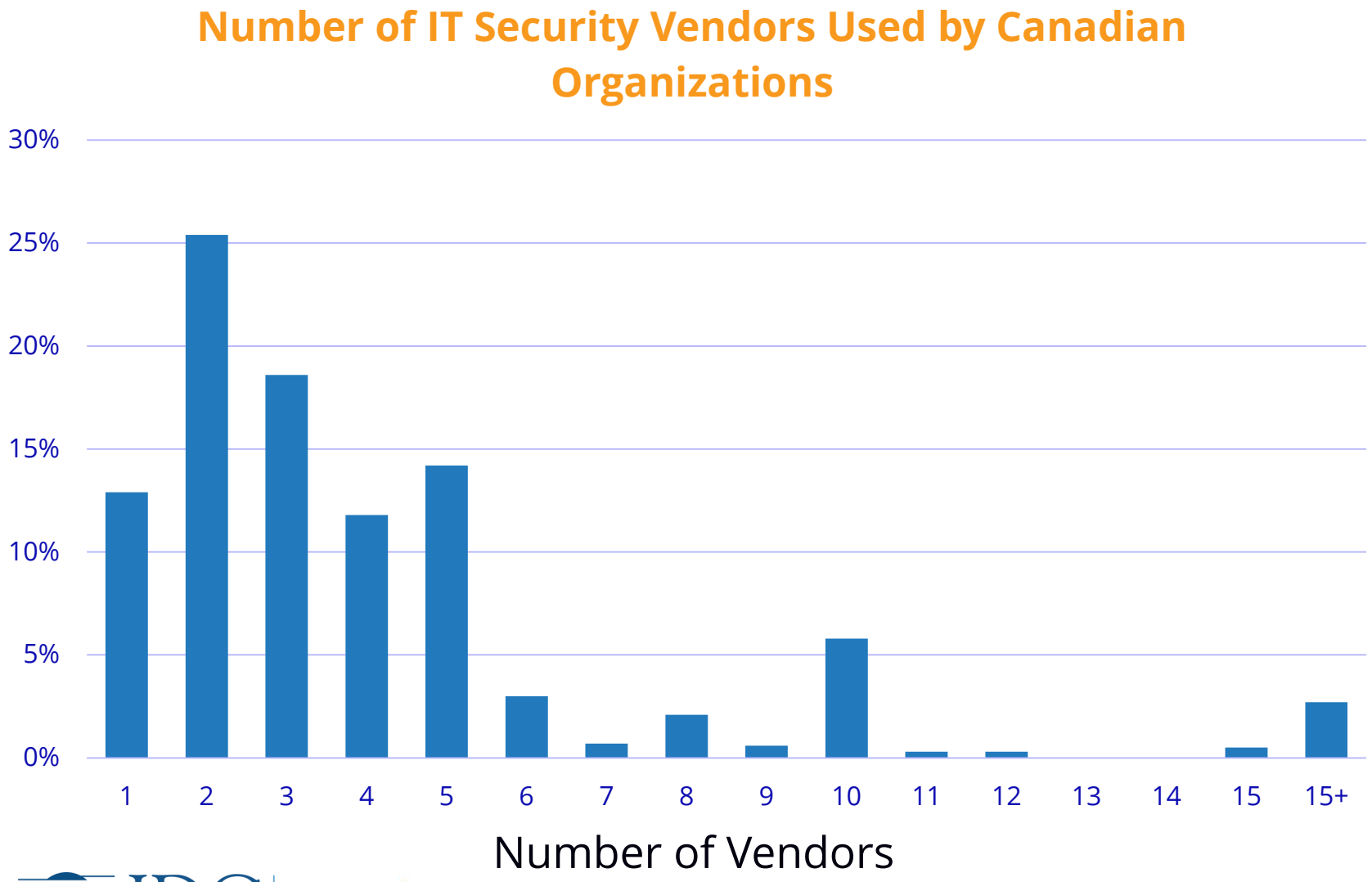
© IDC

Canadian Cybersecurity Focus, 2018

	Identify	Protect	Detect	Respond / Recover
Size	$418M	$2.1B	$300M	$47M
Growth	9.2%	7.1%	16.3%	18.9%
	weaknesses & priorities	*data & uptime*	*attacks & breaches*	*thoroughly & quickly*
Canadian Market Trends	**Focus on risk mgmt., grows as attack surfaces expands across digital.** **DPA and GDPR drive spend in 2018.**	**Analytics, integrated edge, securing IaaS / PaaS is evolving the market** **Majority of spend is still on traditional perimeter security.**	**ML/AI improving threat intel. MSSPs differentiated by maturity level.** **Critical: attackers on Cdn networks for months before detection.**	**Larger/targeted attacks drive planning and recovery spend.** **Shared responsibility w/ cloud providers adds complexity and activity.**

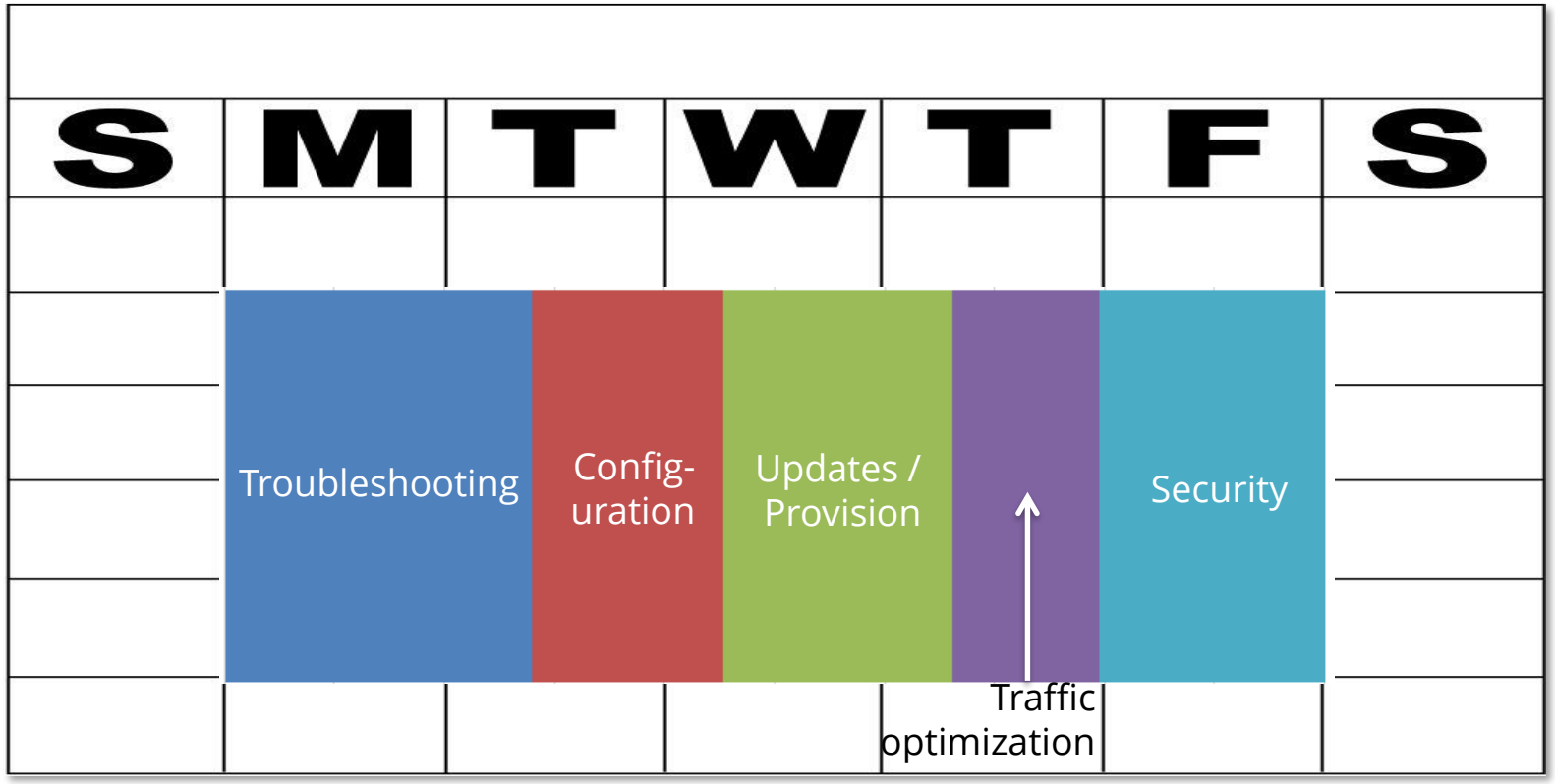
NIST: https://www.nist.gov/cyberframework

Security Product Market Remains Fragmented



- The security product market remains fragmented with organizations implementing point solutions for different vendors
- Almost 1/3 of organizations state using different vendors for all security products.

A Network Admin's Typical Work Week



Network admins are spending more time on security than they were a few years ago.

© IDC

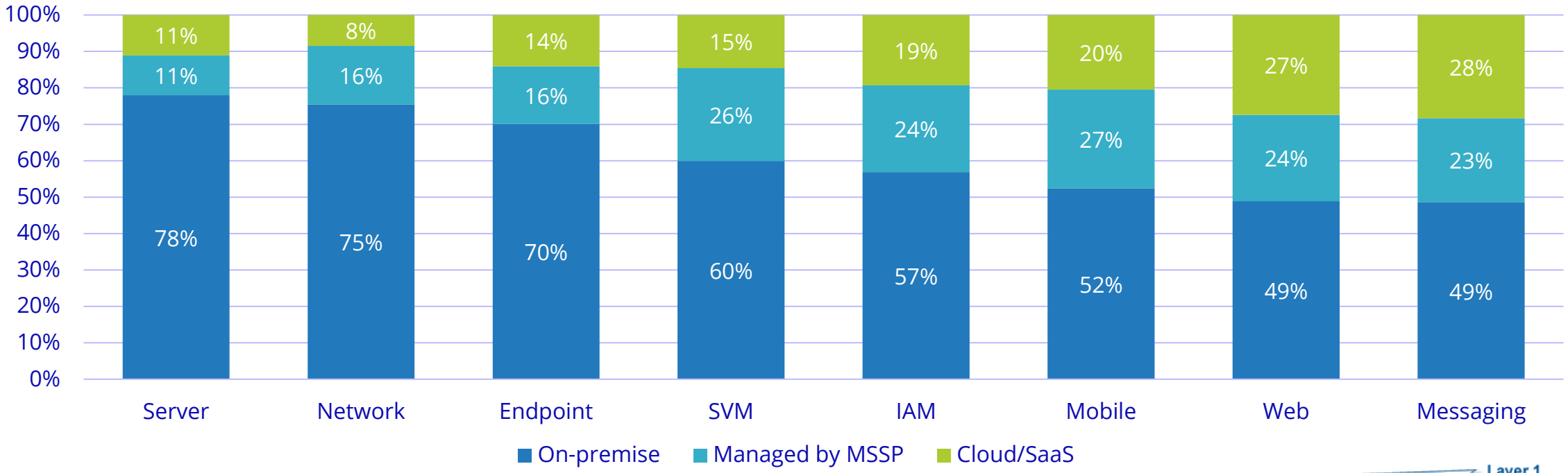
Reasons for Migrating to Managed Security Services

Sample Size = 211
QMS02: Why is/would your organization select managed security services?

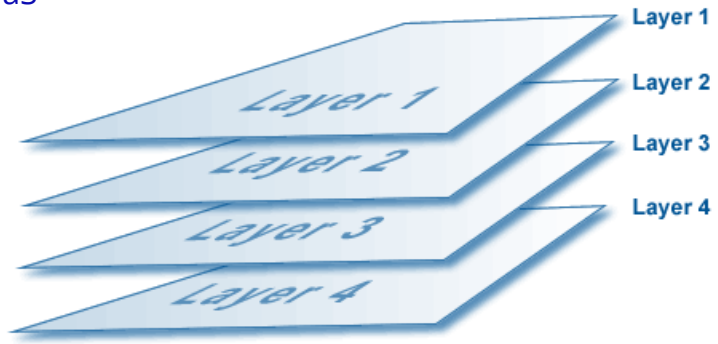
Staffing concerns are top drivers for MSS adoption in 2018. Organizations struggle to find qualified professionals for 24x7 monitoring and management

© IDC

The Growing Desire in Canada for 3rd Party to Take on Security – Next 3 Years



The move is on to bring in outside help to shore up defenses across the attack surface. Firms layer inside resources with external providers



© IDC

IDC Recommendations

1	**Be a leader.** A lack of leadership is a top 5 roadblock for improving cyber security. Organizations with strong leadership experience 25% less breaches
2	**Have a risk plan.** Spend the time to create a cyber security risk plan. Organizations with a risk plan experience a significant reduction in security breaches
3	**Revisit BYOD.** Make sure you have proper policies in place to secure BYOD devices. Telcos and MSSPs can't enforce security policies on personal devices without written consent from the employee. As a general rule personal devices shouldn't have access to the enterprise network, use guest instead
4	**Do the basics.** Train Staff and patch faster. Canadian organizations are still slow to patch their infrastructure and endpoints. No one wants to be the next Equifax
5	**Have an incident response plan.** Your organization will experience a breach. Having a incident response plan allows you to act quicker saving time and money

© IDC

For More Information…

Kevin Lonergan
klonergan@idccanada.com

Twitter
https://twitter.com/@IDCCanada

LinkedIn
https://www.linkedin.com/company/idc-canada

www.idc.com/ca

IDC Directions 2018

© IDC

Thank you!

© IDC