SMB PULSE SURVEY

Findings Overview

Webroot and the small- to medium-sized business (SMB) focused research agency Bredin recently conducted a survey on the cybersecurity habits of small (1-19), medium (20-99), and large (100-500) companies. The results are a revealing look at the preparedness, approaches, and cybersecurity attitudes of these organizations. They range from concerning to impressive, and are invaluable for understanding how those outside of the industry conceive of their own digital security.

Some highlights:

An astounding 20 percent of respondents admit to not having, or not knowing if they have, endpoint protection in place within their organization.

Twenty percent of those surveyed said they were enticed to purchase their endpoint solution of choice based on a positive experience during a free trial.

Ease-of-use was cited as by far the most popular reason for adopting an endpoint security solution, but predictive threat intelligence came in as the second most cited reason.

A full quarter (26 percent) buy into a layered security approach, deploying endpoint, DNS, and user training as security solutions.

Companies and our threat researchers largely agree that phishing and ransomware attacks represent the most significant threats to their cybersecurity.

Eighty-one percent of respondents say their companies have "strong password" policies in place.

A Note on Company Size

The findings of this survey confirm that size has a strong bearing on a company's approach to cybersecurity. For instance, medium (39 percent) and larger-sized (48 percent) companies are far more interested in AI and machine learning capabilities than are their smaller counterpoints (21 percent).

Only 12 percent of small businesses have dedicated IT security teams in-house, a fact that is perhaps not surprising but certainly has an effect on the rest of the survey results. Eighty-seven percent of large companies have some sort of employee IT security training program in place, a number that drops to 13 percent for smaller companies. These disparities are no doubt resource-driven, but nevertheless say a lot about the cybersecurity shortcomings of small and medium-sized business.
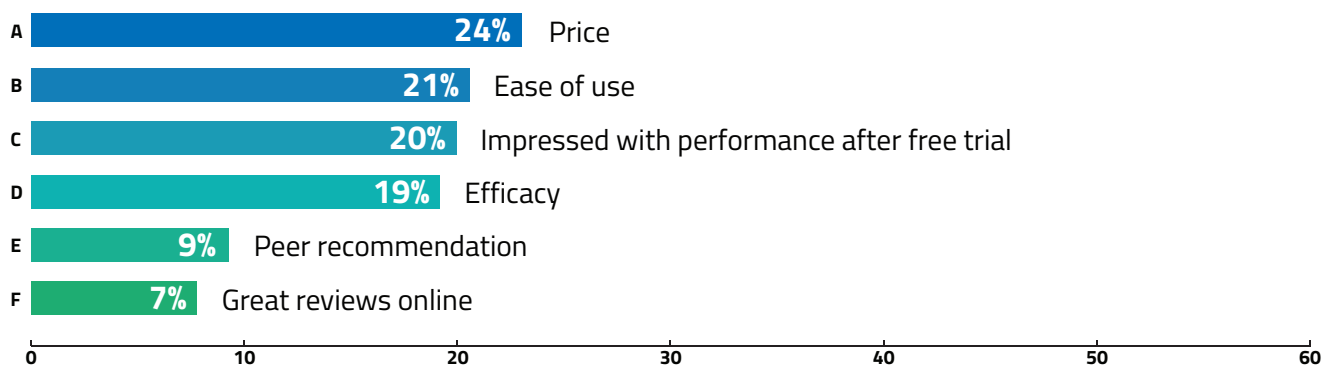
You can find a more detailed excerpt of the survey findings below.

SURVEY RESULTS

1. Does your business have antivirus software or endpoint protection?

- **A** | **80%** Yes
- **B** | **20%** No/Don't know

(scale: 0, 20, 40, 60, 80, 100)
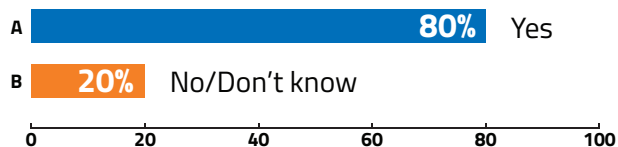
1a. Please rank these reasons for purchasing your current business antivirus product or endpoint protection from most important (top) to least important (bottom):
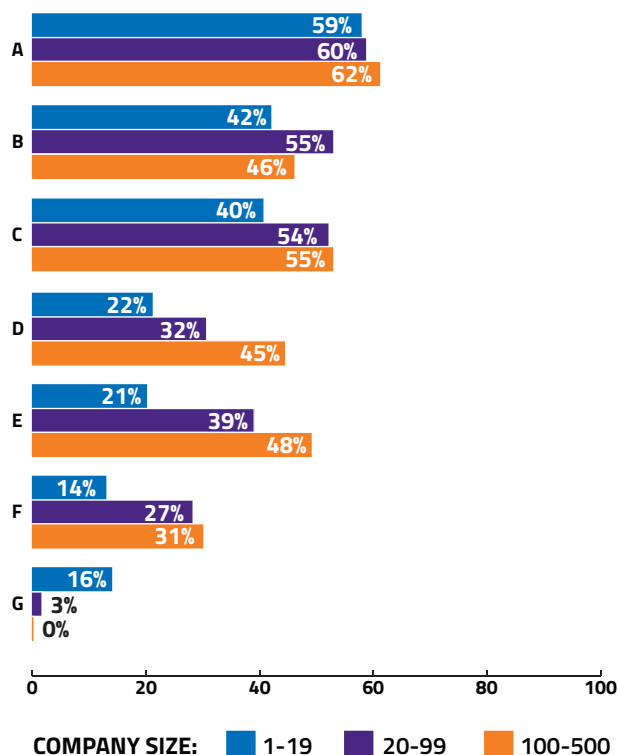
- **A** | **24%** Price
- **B** | **21%** Ease of use
- **C** | **20%** Impressed with performance after free trial
- **D** | **19%** Efficacy
- **E** | **9%** Peer recommendation
- **F** | **7%** Great reviews online

(scale: 0, 10, 20, 30, 40, 50, 60)

2. What makes a business cybersecurity product superior? (Select all that apply.)
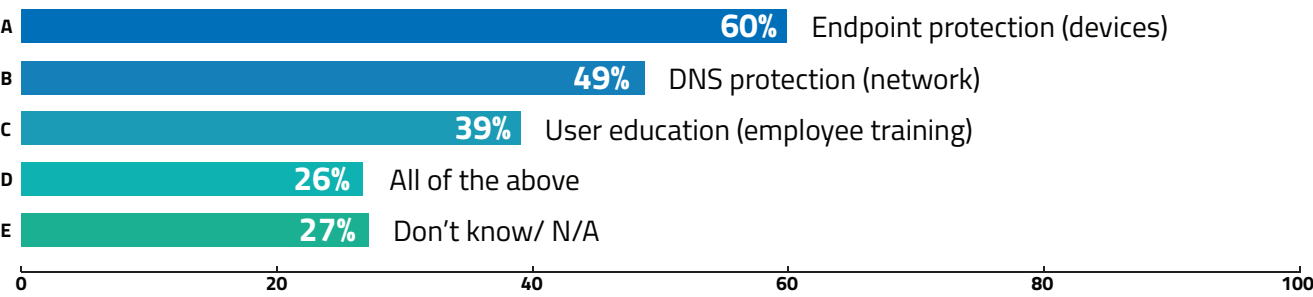
OVERALL RESULTS
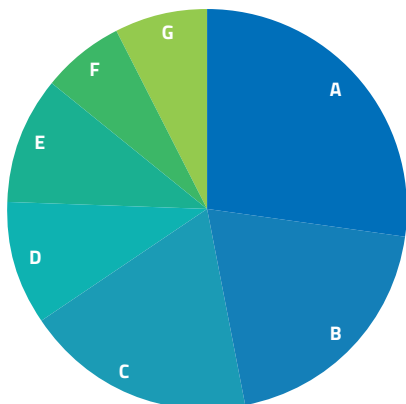
- **A** **59%** Ease of use/management
- **B** **42%** Predictive threat intelligence
- **C** **40%** Integrations with other products I use
- **D** **22%** Cloud architecture
- **E** **22%** AI/Machine-learning capabilities
- **F** **14%** Robust, connected product portfolio
- **G** **16%** Don't know / N/A

RESULTS BY COMPANY SIZE

	1-19	20-99	100-500
A	59%	60%	62%
B	42%	55%	46%
C	40%	54%	55%
D	22%	32%	45%
E	21%	39%	48%
F	14%	27%	31%
G	16%	3%	0%

(scale: 0, 20, 40, 60, 80, 100)

COMPANY SIZE: 1-19, 20-99, 100-500

3. Which of the following security protection layers have you implemented?

- **A** — 60% Endpoint protection (devices)
- **B** — 49% DNS protection (network)
- **C** — 39% User education (employee training)
- **D** — 26% All of the above
- **E** — 27% Don't know/ N/A

4. What do you think is the #1 cybersecurity threat to your network? (Select one.)

OVERALL RESULTS

- **A** 24% Phishing Scam
- **B** 19% Ransomware
- **C** 14% Employee naiveté
- **D** 9% DDoS attack
- **E** 7% Mobile attack
- **F** 3% Other
- **G** 24% Don't know / N/A

RESULTS BY COMPANY SIZE

- **A** — 24% / 22% / 22%
- **B** — 20% / 11% / 22%
- **C** — 13% / 28% / 30%
- **D** — 9% / 17% / 10%
- **E** — 7% / 15% / 14%
- **F** — 3% / 0% / 0%
- **G** — 24% / 6% / 2%

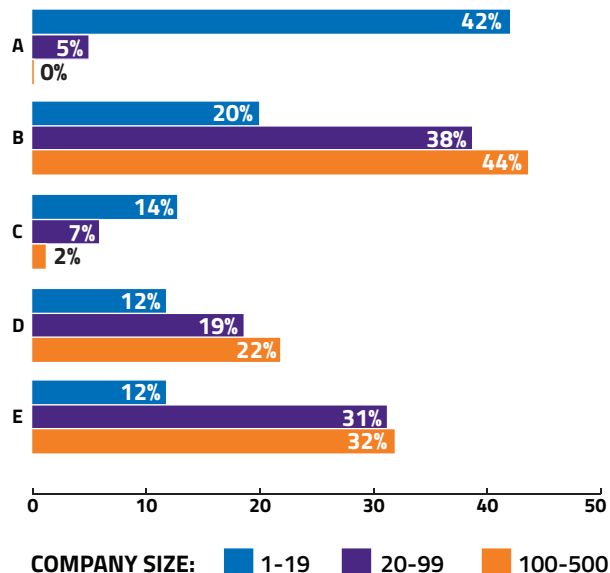**COMPANY SIZE:** 1-19 | 20-99 | 100-500
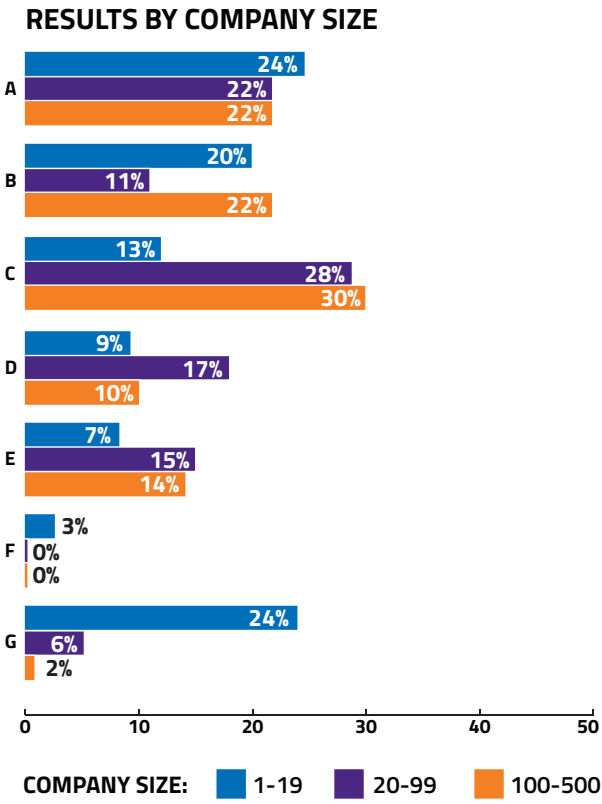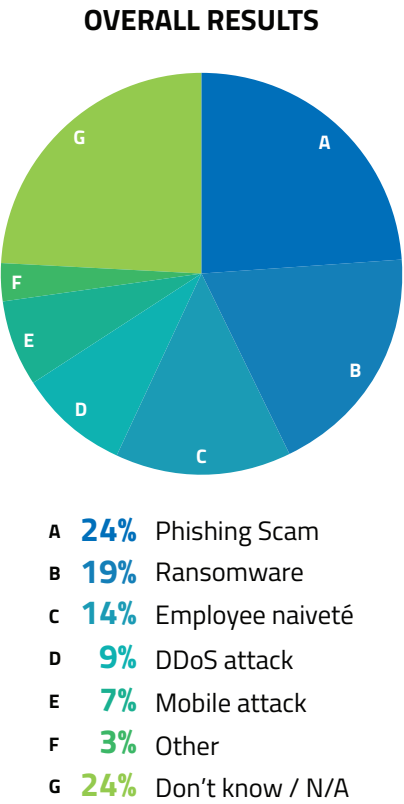
5. Which of the following best describes how your business currently manages IT security? (Select one.)
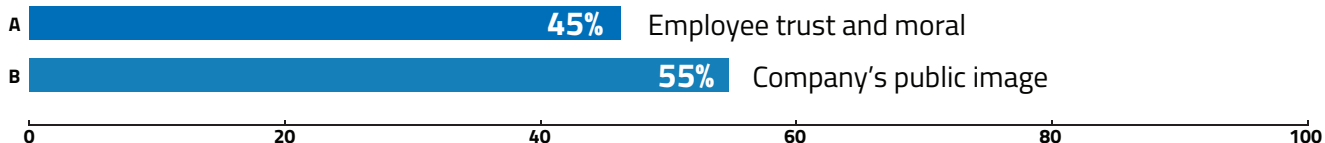
OVERALL RESULTS
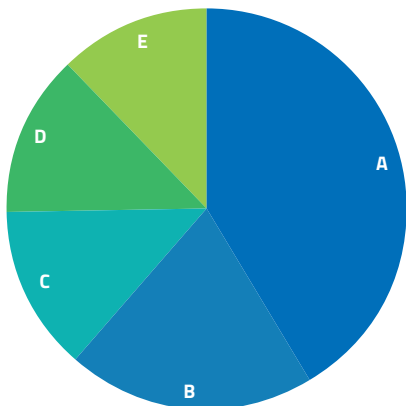
- A **41%** We do not have IT security-specific resources
- B **20%** A mix of in-house and outsourced IT security
- C **13%** Outsourced IT security support through a third-party managed service provider
- D **13%** In-house IT employees who handle IT security among other responsibilities
- E **12%** Dedicated in-house security professional or team
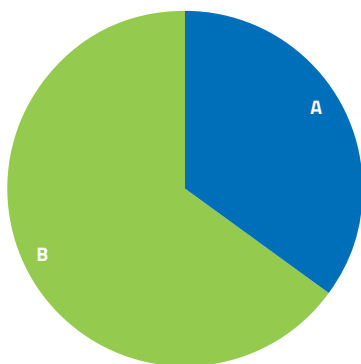
RESULTS BY COMPANY SIZE

	1-19	20-99	100-500
A	42%	5%	0%
B	20%	38%	44%
C	14%	7%	2%
D	12%	19%	22%
E	12%	31%	32%

COMPANY SIZE: ■ 1-19 ■ 20-99 ■ 100-500

---

6. If your business suffered a cyberattack in 2018, which of the following would be harder to restore?

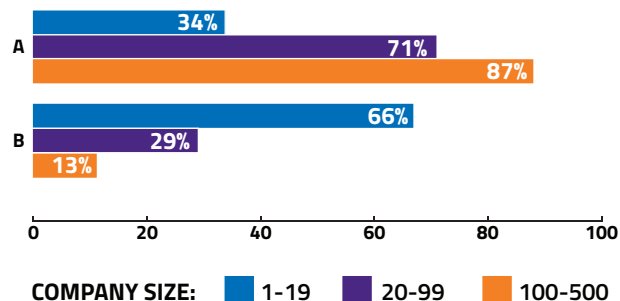|		
A	45%	Employee trust and moral
B	55%	Company's public image

---

7. Do you currently do any employee training on cybersecurity best practices?

OVERALL RESULTS

- A **35%** Yes
- B **65%** No

RESULTS BY COMPANY SIZE
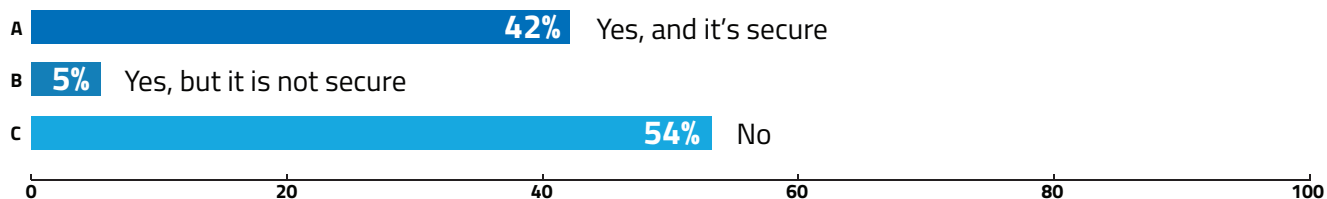
	1-19	20-99	100-500
A	34%	71%	87%
B	66%	29%	13%

COMPANY SIZE: ■ 1-19 ■ 20-99 ■ 100-500

8. Do you enforce a "strong password" policy at your company?

A **81%** Yes
B **19%** No

| 0 | 20 | 40 | 60 | 80 | 100 |

9. Do you have a guest WiFi network at your office and, if so, do you feel confident that it is secure? (Select one.)

A **42%** Yes, and it's secure
B **5%** Yes, but it is not secure
C **54%** No

| 0 | 20 | 40 | 60 | 80 | 100 |

Methodology:

The 2018 Webroot SMB Pulse Report is based on research administered by Bredin, a research firm specializing in small and midsized businesses. The survey was conducted online from April 17-24, 2018, and polled 500 principals of U.S. companies with up to 500 employees. It has a margin of error of +/-4%.

WEBROOT®
Smarter Cybersecurity™