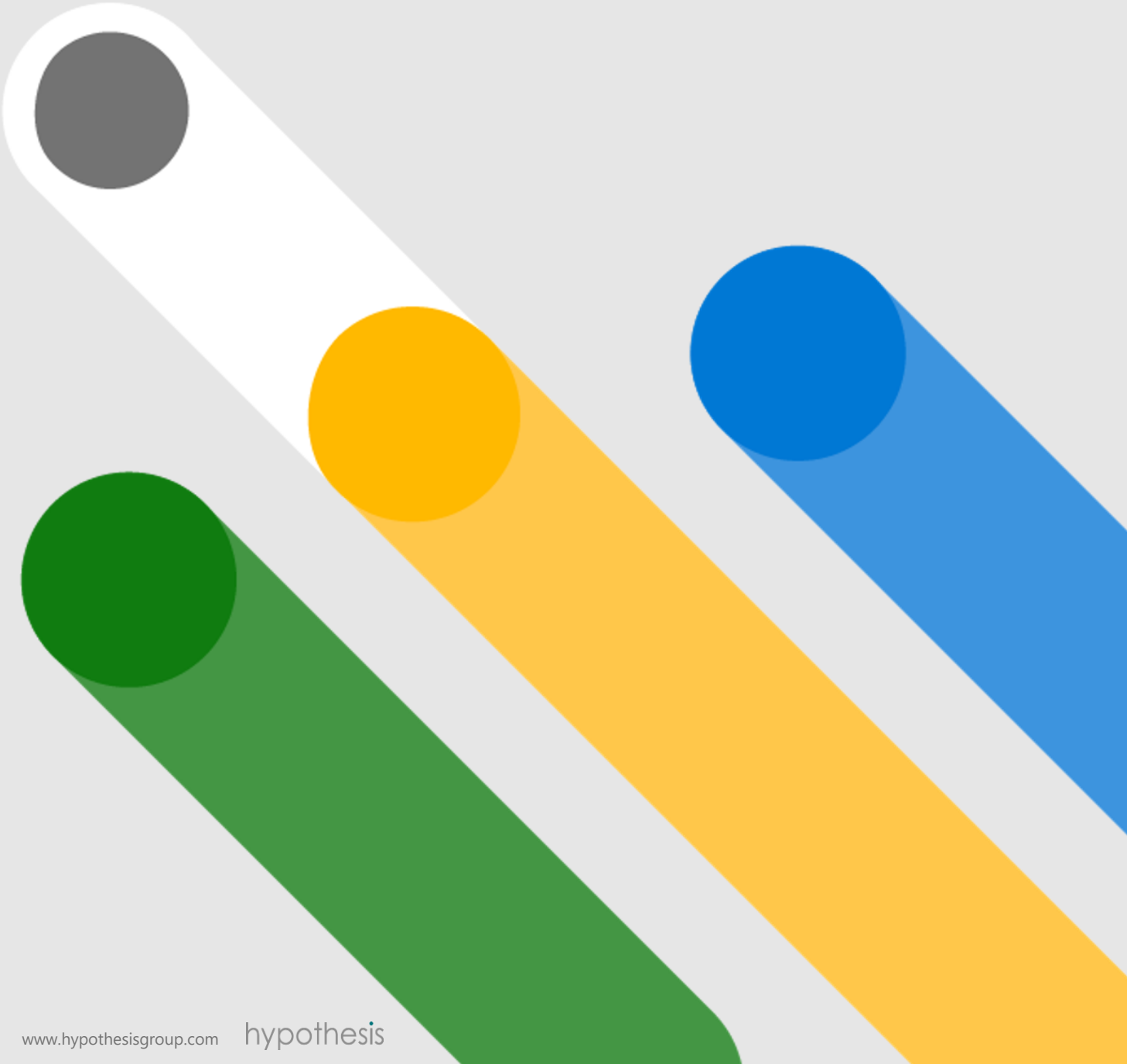
Microsoft Security

Security Signals Boost SDM Research Learnings

September 2021



Background

Following the release and successes of Microsoft Secured-core PCs, now is prime time to take another pulse of Security Signals, initially conducted in August 2020, and lend an ear to the consumer voice.

Objectives

01 Understand the current landscape of hardware, as well as current priorities and concerns among SDMs and consumers.

02 Explore security perceptions surrounding outdated hardware and other attributes among consumers surrounding device security.

03 Strategize how Microsoft can position themselves as a leader in the space through their Windows 11 strategy.

Methodology

Quantitative Sample

10-minute online surveys
Mobile optimized

Fielded September 1–10, 2021

Security Signals Edition One occurred in August 2020, when a 20-minute online survey was conducted with 1,000 decision makers involved in security and threat protection decisions (SDMs) at enterprise companies from a range of industries across the US, UK, Germany, China, and Japan.

Key Subgroups	Base (N=)
Security Decision Makers	212
Financial Services & Banking SDMs	51
Consumers	203
Total	**415**

Screening Criteria

B2B (Security Decision Makers)

- US Only
- Age 18-64
- Security Decision Makers, with a range of job responsibilities and titles
- Work at Enterprise companies with 1,000+ employees
- Mix of industries, with a focus on financial services
- No sensitive industry or recent participation

B2C (Consumers)

- US Only
- Age 18-64
- Balance of gender, age, ethnicity, and region to census
- Natural fallout of income, education, and other key demos
- No sensitive industry or recent participation
- Own or are open to buying a personal computer in next 6 months

Key Findings for Security Decision Makers

Hybrid work is here to stay

On average, 60% of employees are working out of the office at least some of the time. SDMs express concern with hybrid working. 3-in-4 feel that the move to hybrid work leaves their organization more vulnerable to security threats. With remote work, 70% of SDMs are more worried about the risk of device theft.

Concerns surrounding outdated hardware are top of mind

When purchasing new computers, 42% of SDMs rank security as their top priority over performance, reliability, and compatibility. 86% of SDMs say that outdated hardware leaves organizations more open to attacks. Despite the concern, SDMs report that an average of 30% of hardware in their organization is outdated and only 45% upgrade employees' computers every 2 years.

Software isn't enough, modern hardware is the solution

80% of SDMs believe software alone is not enough protection from emerging threats, and 86% agree modern hardware would help protect against future threats. 82% of SDMs also recognized that a TPM (Trusted Platform Module) can bring greater security. Firmware attacks are also on the rise with server attacks most common. 87% experienced at least one firmware attack in the past two years, up from 83% in 2020.

With 60% of employees working at home, hybrid work is here to stay, but SDMs feel that leaves their organization even more vulnerable to security threats

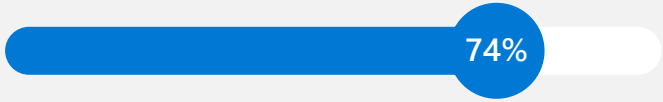
Hybrid Word Status

Base: B2B (n=212)

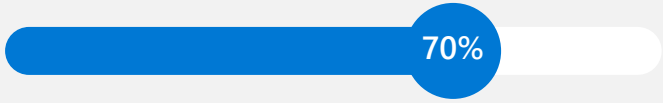
Hybrid Work Perceptions – Showing T2B

Base: B2B (n=212)

The move to hybrid work leaves my organization **more vulnerable to security threats**



I worry more about device theft than before, since users are working remotely

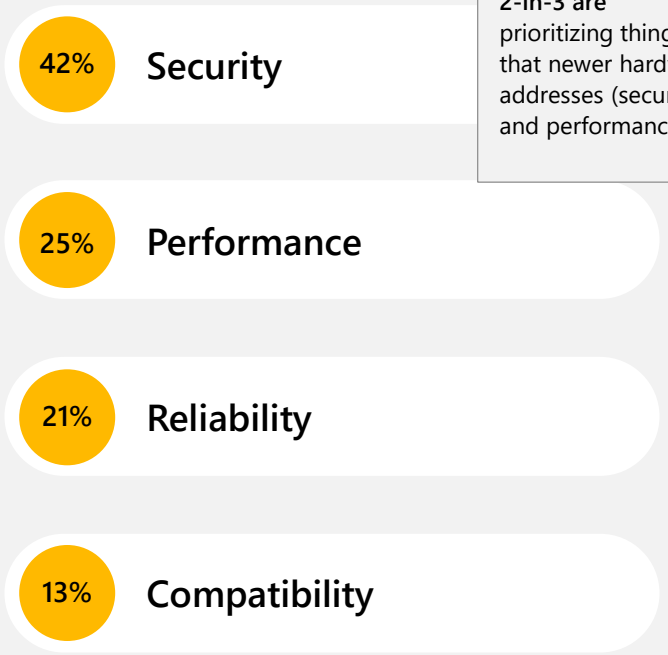


SDMs most frequently rank security as their #1 priority when purchasing new computers

Information security, security control and brand trust also lead more nuanced device selection priorities

Computer Purchase Considerations
Pillar Level – % Ranked 1ST

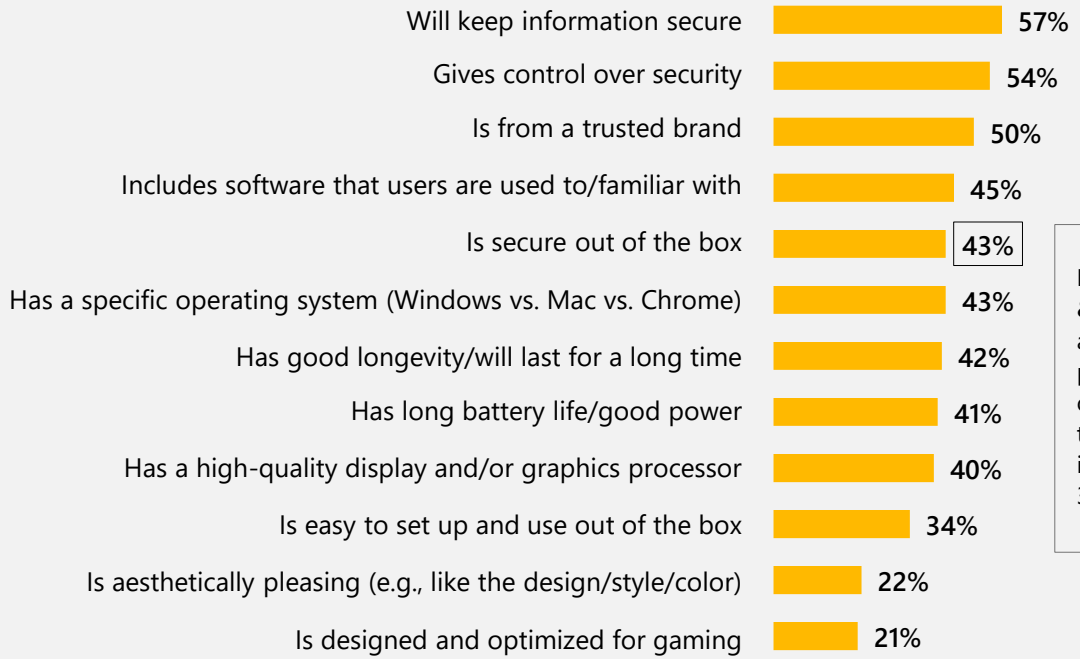
Base: B2B (n=212)



2-in-3 are prioritizing things that newer hardware addresses (security and performance)

Computer Purchase Considerations
Attribute Level – % Ranked Top 5

Base: B2B (n=212)

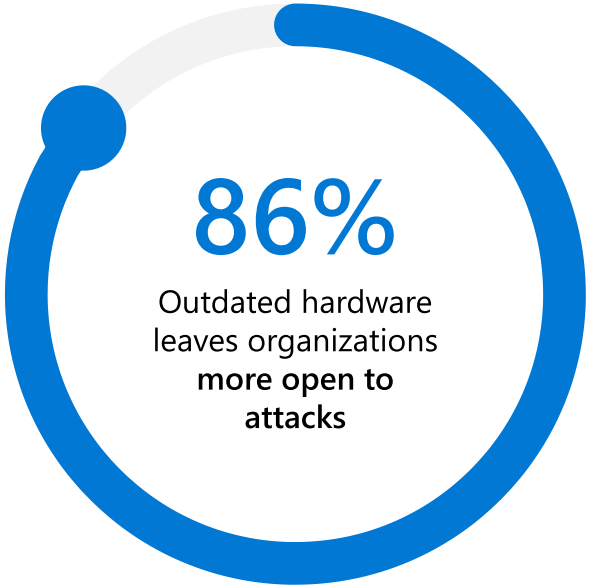


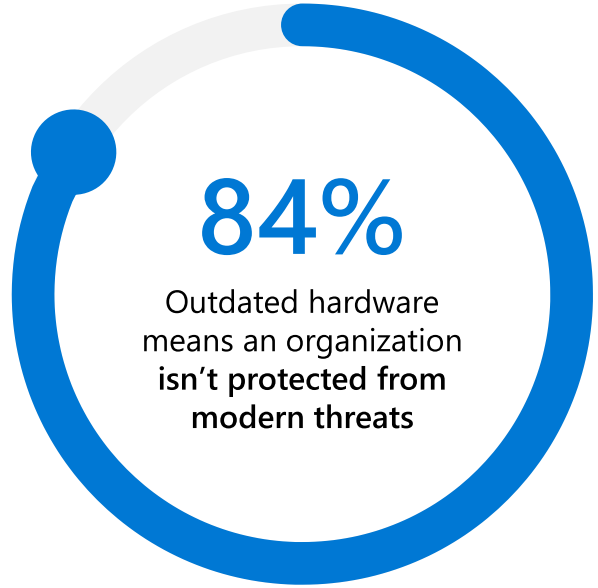
Financial Services & Banking SDMs are more likely to prioritize "Is secure out of the box" than those in other industries (55% vs 39% respectively)

SDMs thoroughly agree that outdated hardware leaves organizations vulnerable

Security Perceptions – Showing T2B

Base: B2B (n=212)





An average of 30% of devices are outdated at SDMs' orgs, and less than half upgrade employee's computer every 2 years

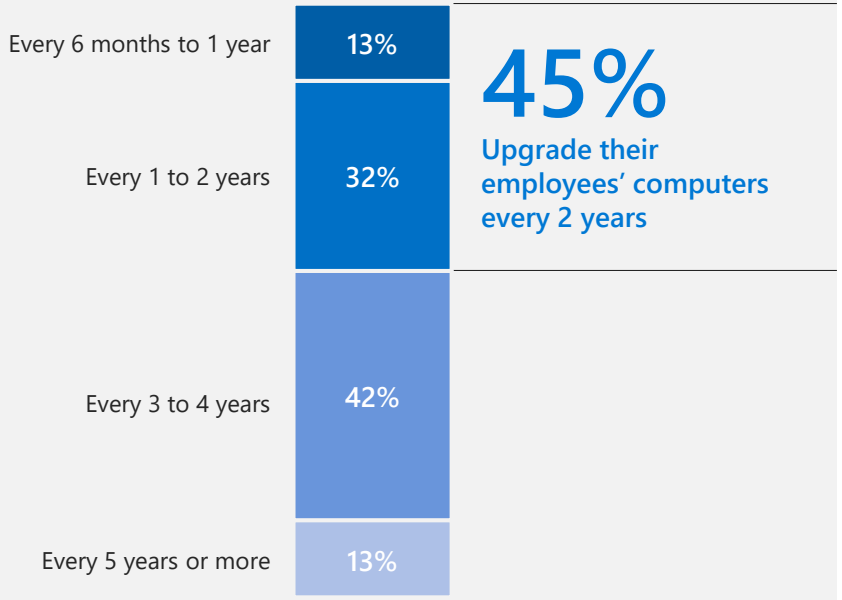
Outdated Hardware

Base: B2B (n=212)

Financial Services & Banking SDMs are less likely to claim their org has outdated hardware than those in other industries (25% vs 35% respectively)

Frequency of Computer Replacement

Base: Total (n=212)

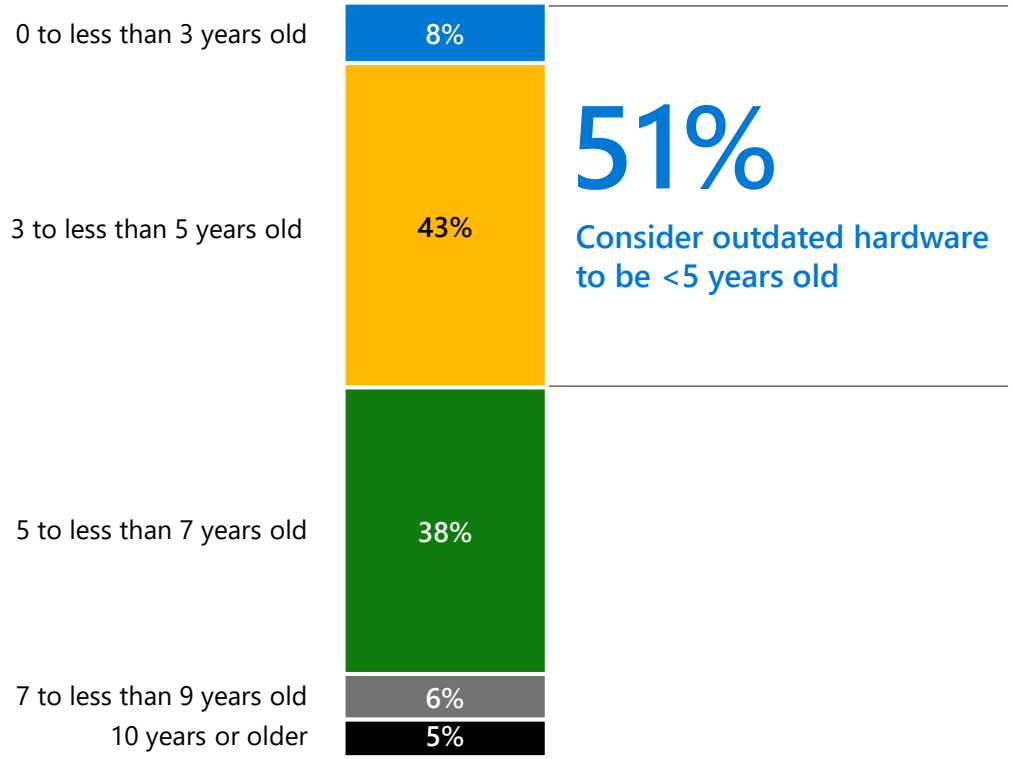


63% of SDMs' organization's oldest devices are older than 5 years old.

Only half of SDMs are aligned on the industry standard of a current vs. “outdated” device

Outdated Hardware Classification

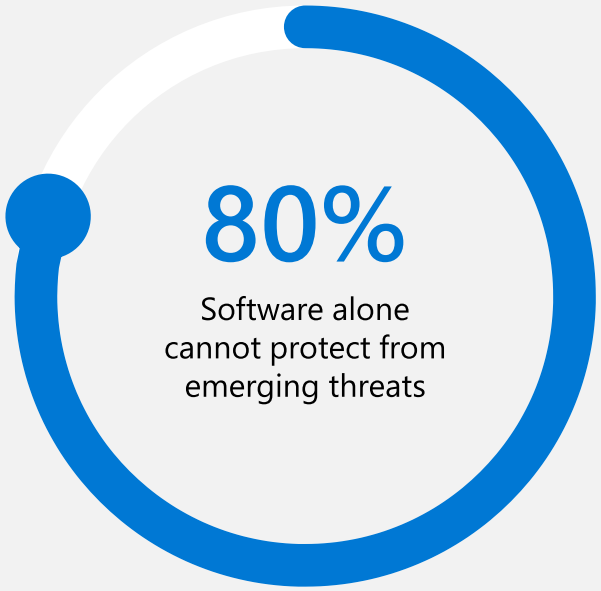
Base: B2B (n=212)



Software isn't enough to protect from emerging threats – not just meeting but raising industry standards to more modern hardware may best protect within the new "attack frontier"

Security Perceptions – Showing T2B

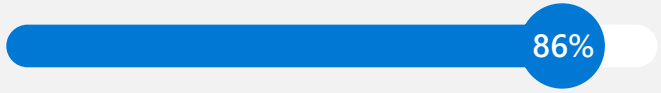
Base: B2B (n=212)



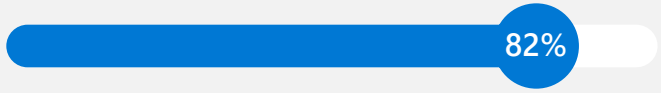
Security Perceptions – Showing T2B

Base: B2B (n=212)

More modern hardware would help protect organizations against future threats



A TPM (Trusted Platform Module) can bring greater security



SDMs report experiencing at least one security attack in the P2Y (up from Aug ‘20)

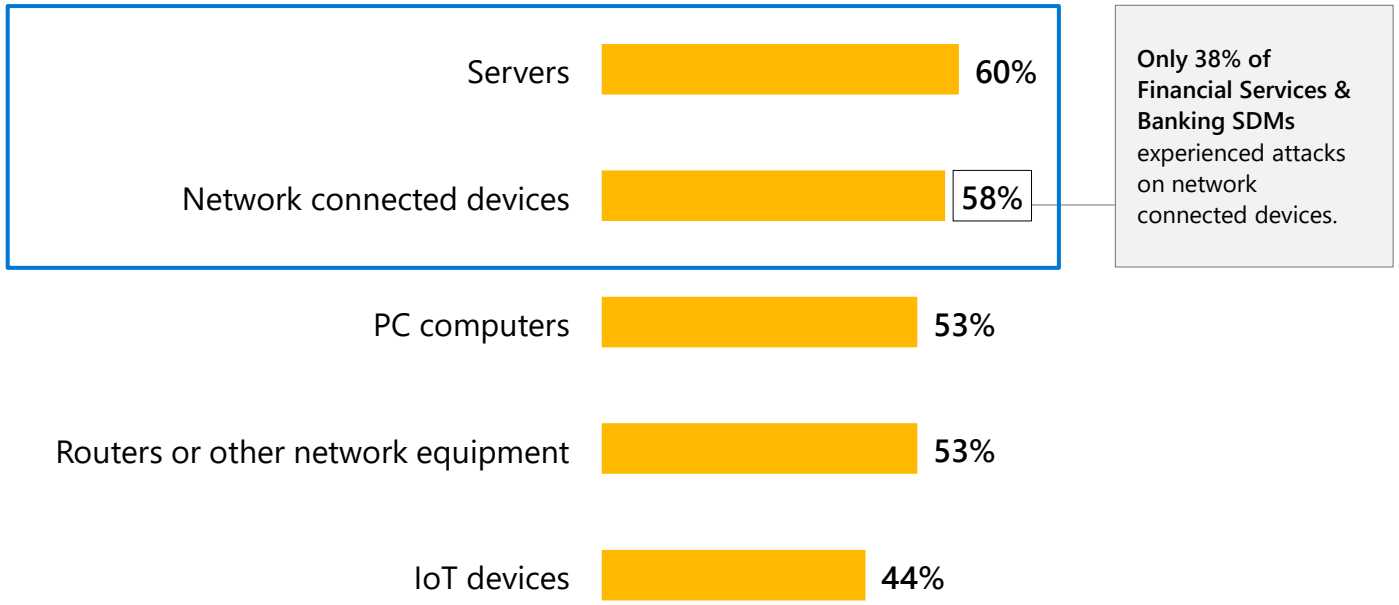
Attackers most frequently exploit servers and hardware like network connected devices, PCs and routers

Firmware Malware Attempts

Base: B2B (n=212)

Type of Firmware Malware Attempts

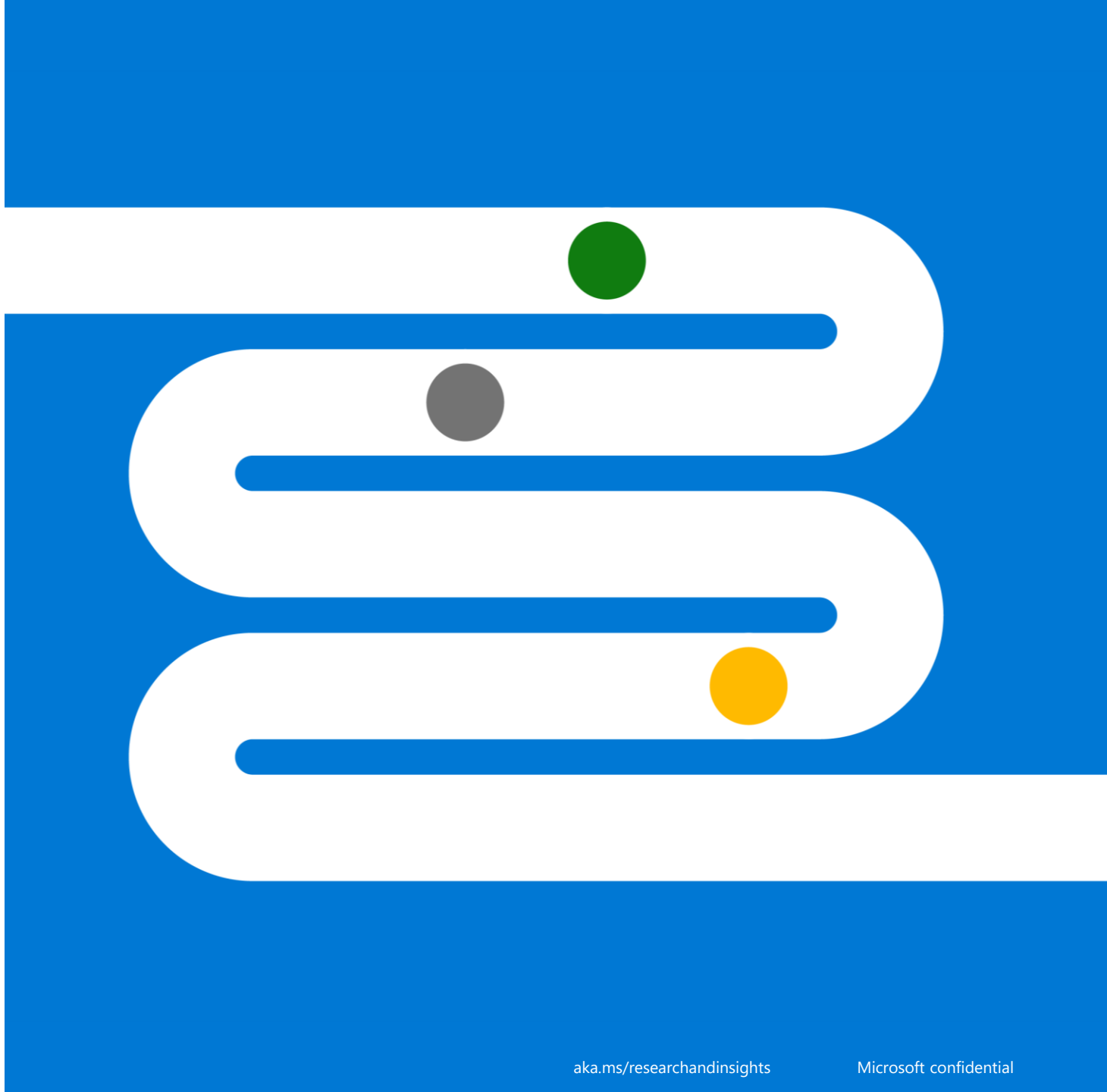
Base: B2B who experienced attacks (n=171)



▲ Directional increase from 2020 findings - 83% experienced at least one firmware attack

Security Decision Makers

Additional Learnings

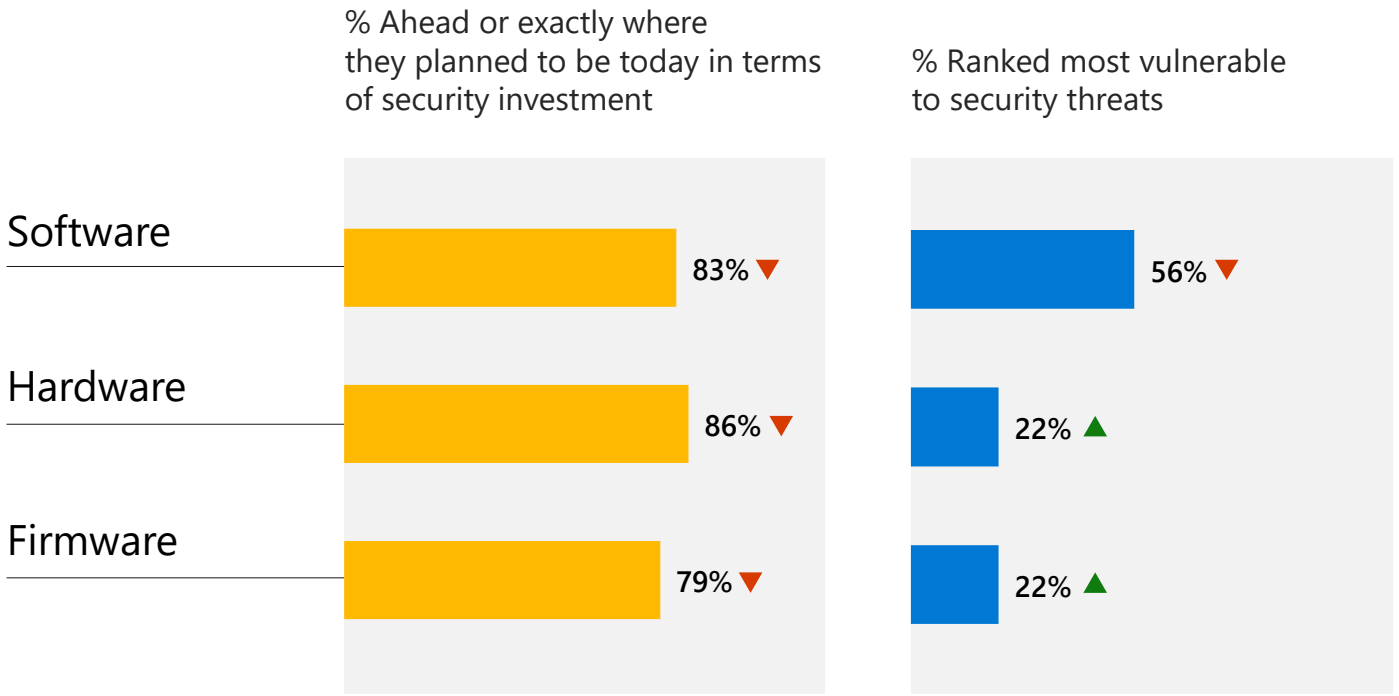


SDMs maintain that their organization is either ahead or exactly where they should be in terms of security investment, though there is a downward YoY movement

YoY movement also shows a perceived increase in hardware and firmware vulnerabilities

Security Project Execution and Greatest Security Exposure – % Ranked 1st

Base: B2B (n=212)



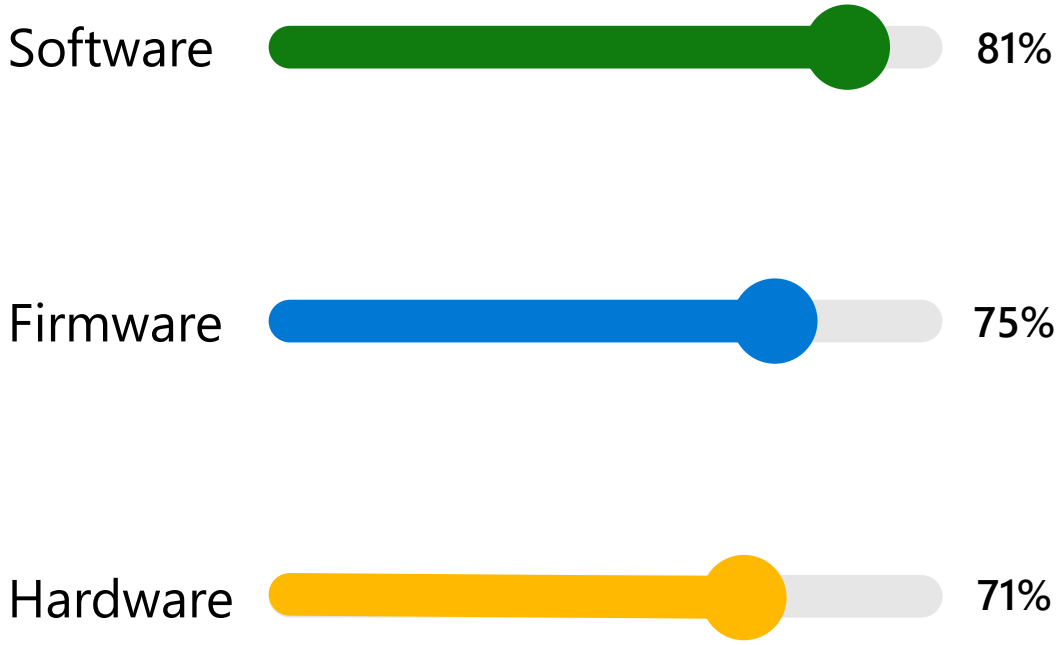
▲▼ Indicates directional increase/decrease vs. 2020 pulse

Please see speakers notes for data

The majority of SDMs view firmware and hardware as growing areas of concern

Future Attack Areas of Concern – Showing T2B

Base: B2B (n=212)



SDMs strive to inform themselves on device security throughout the purchase journey

SDMs invest several days or more into device security research, primarily leveraging tech specifications and industry standards to inform their selection

Device Purchase Research – Time Spent

Base: B2B (n=212)

Device Security Evaluation

Base: B2B (n=212)

Top 5 Security Evaluation Criteria		
1	Tech specifications	55%
2	Is up to industry standards/regulations	55%
3	Based on past experiences with brand/similar devices	53%
4	Complies with organizational requirements	51%
5	Rely on CISO/corporate security function	48%

Knowing about vulnerabilities helps SDMs feel more, not less secure

Product Publish Vulnerabilities

Base: Total (n=212)