Navigating Your Security Journey: A Guide for SMBs

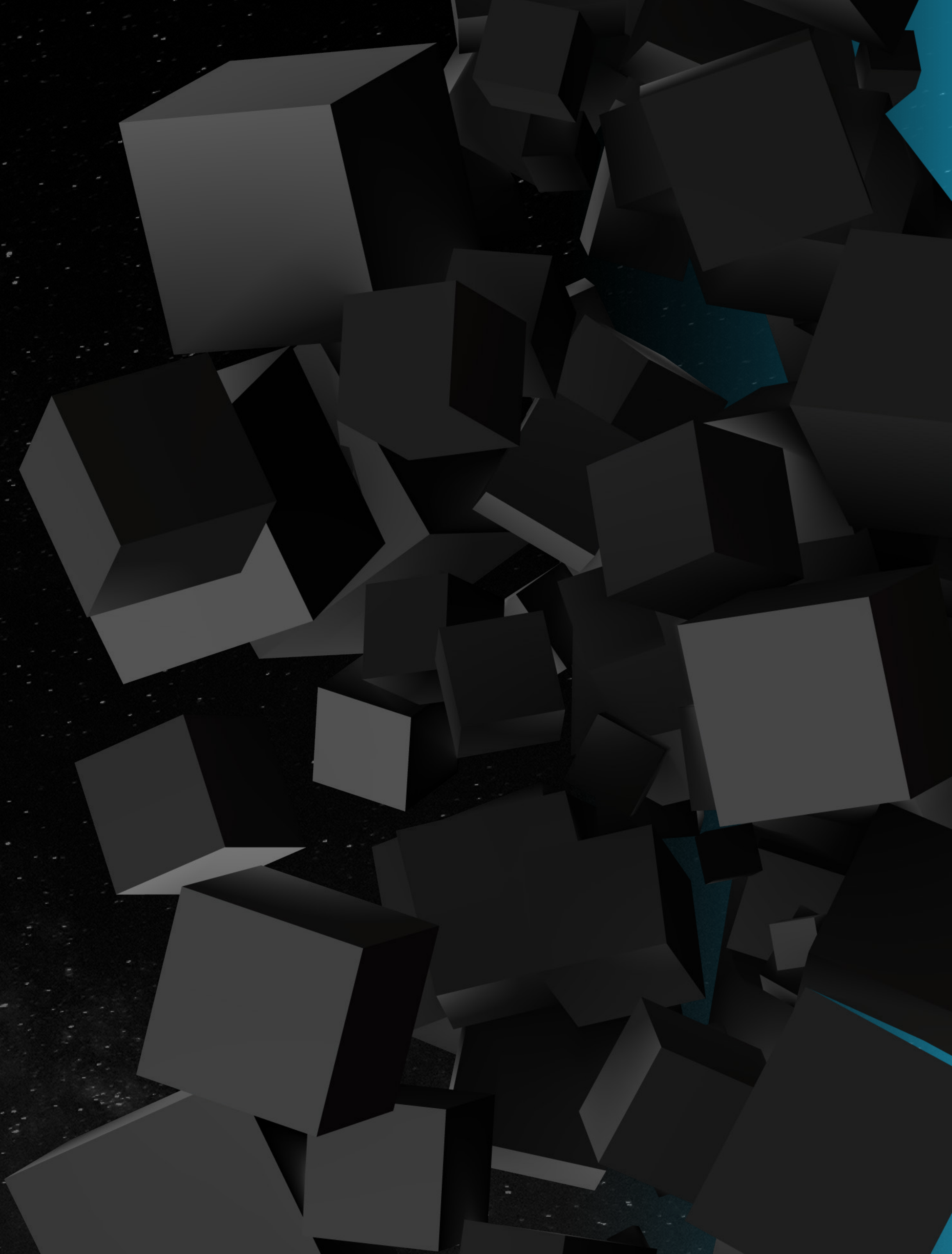
Discover how using the Intel vPro® platform together with ESET Endpoint Security software can help your organization stay safe from cybersecurity threats.

intel®

eset®

Digital Security
Progress. Protected.

Contents:

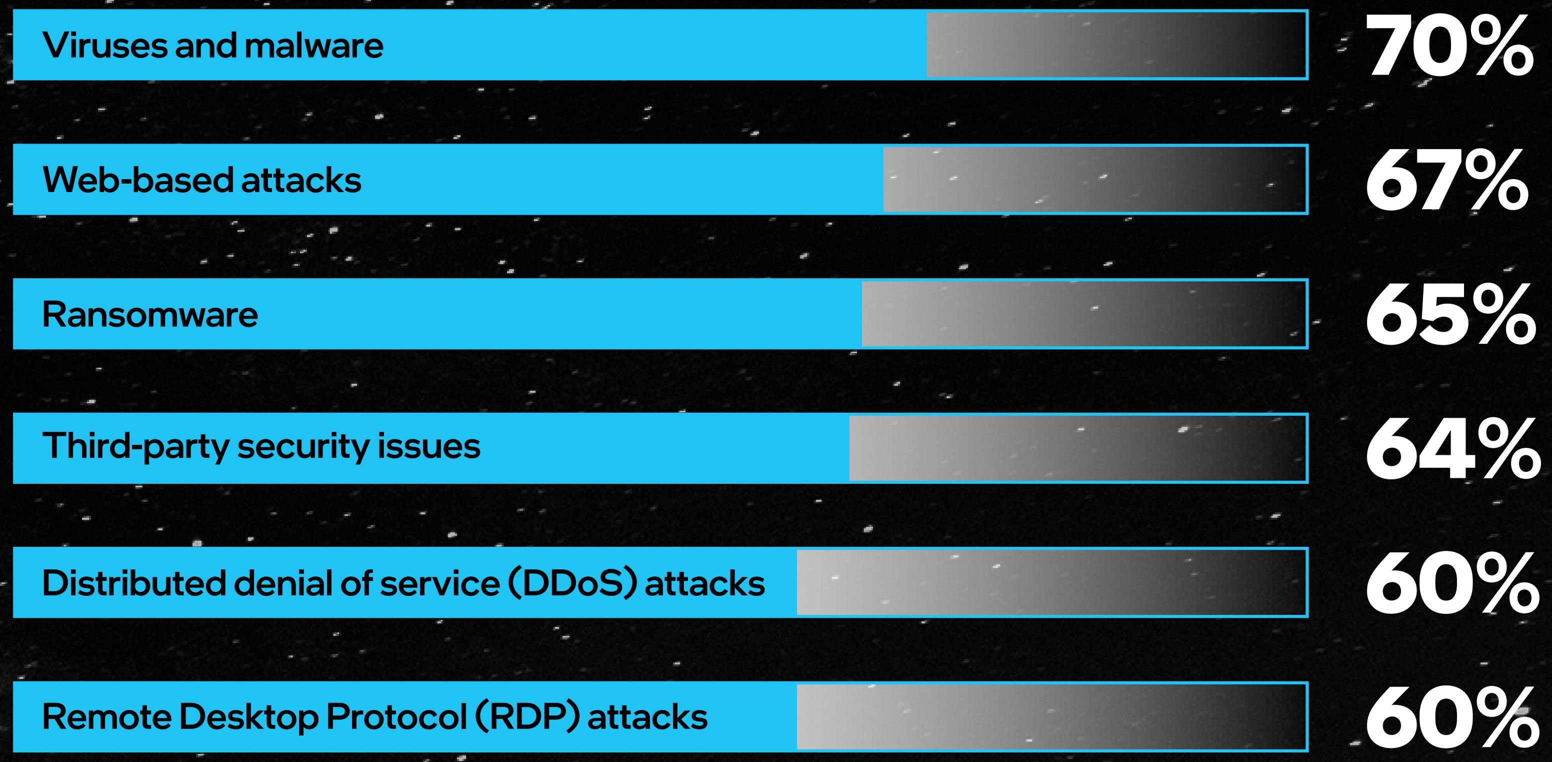


Bad actors look for ways to attack

While tech advancements have enabled SMBs to grow, they have also enabled more advanced security threats. When surveyed in 2022, 70 percent of small and medium-sized business (SMB) owners in North America and Europe reported their biggest cybersecurity concern for the next 12 months was viruses and malware. This was followed closely by web-based attacks, ransomware, and third-party security issues.[1]

Given their size and resources, it's no surprise that 74 percent of these businesses believe that they are more vulnerable to cyberattacks than larger enterprises.[1] One reason for such vulnerability could be that these organizations have fewer safeguards in place to prevent attacks—making them attractive targets for bad actors.

SMB leaders' top cybersecurity concerns for the next 12 months[1]



Throughout the trek, challenges abound

If you are facing constantly evolving ransomware threats, combined with budget limitations and shifting business policies, you are not alone. What cybersecurity challenges are keeping you and your SMB peers awake at night? According to the SMBs surveyed, top challenges include employees' lack of cyber awareness (43%), vulnerabilities in the partner ecosystem (34%), and continued hybrid or remote work (32%).[1] Additionally, 70 percent of SMBs admit that their investments in cybersecurity have not kept pace with the threats, especially with changes to operational models like the move to hybrid work.[2]

43%

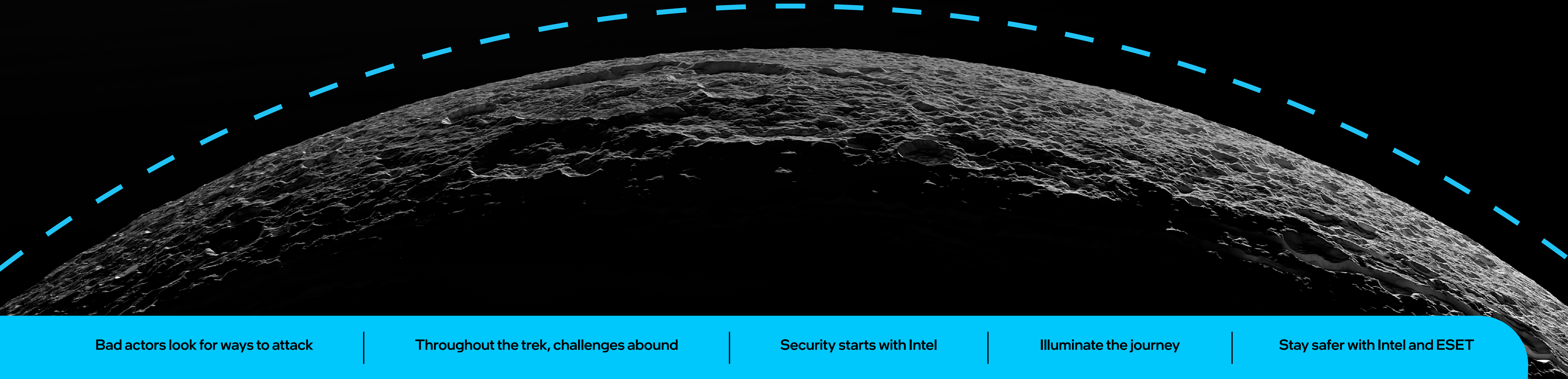
Lack of employee **cyber awareness**[1]

34%

Vulnerabilities in the **partner/supplier ecosystem**[1]

32%

Continued **hybrid or remote working**[1]



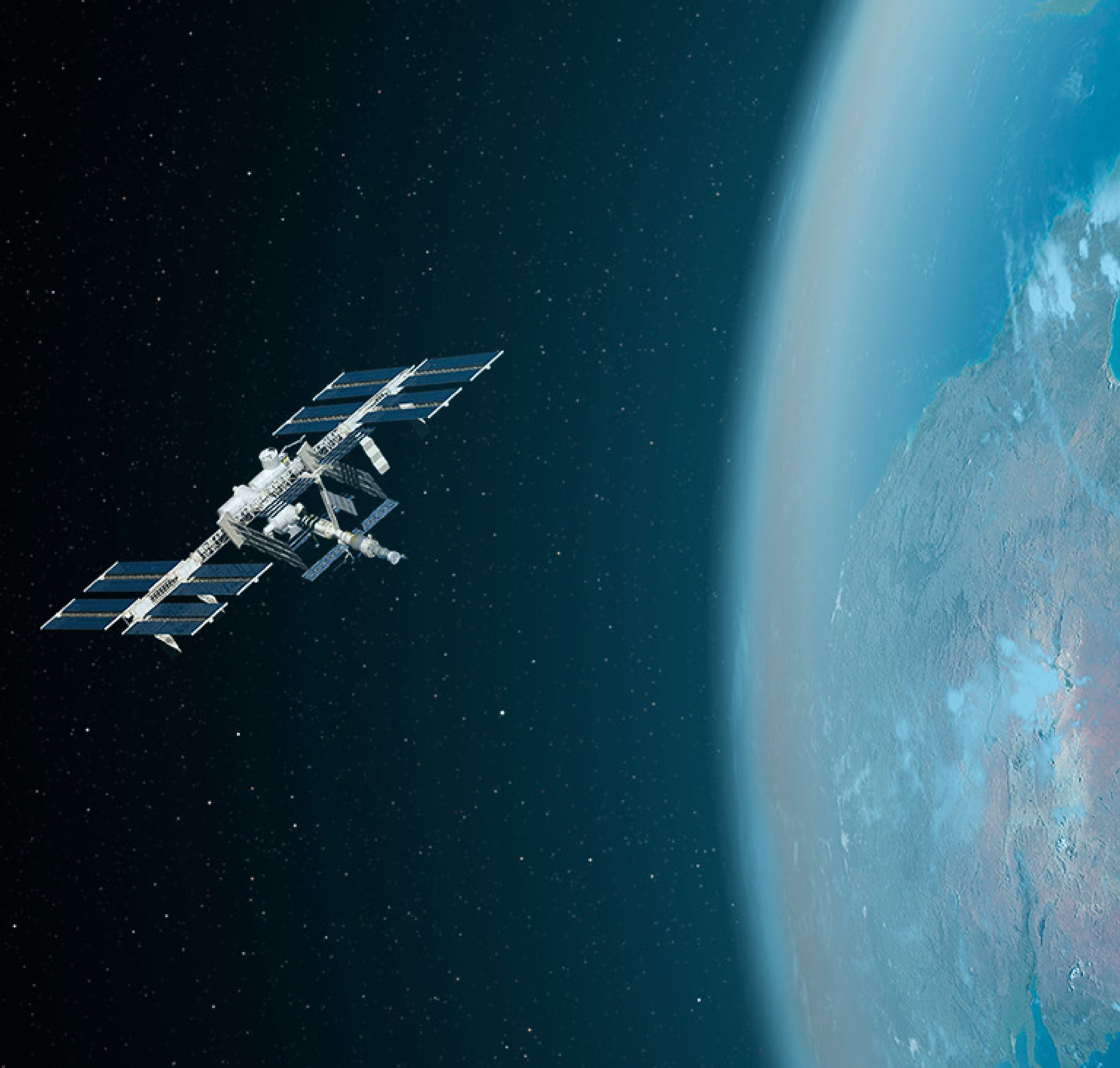
Security starts with Intel

SMB leaders appear ready to step up and protect their organizations. Of those surveyed, 65 percent currently use or plan to use advanced cybersecurity solutions, including EDR, XDR, or MDR, similar to those offered within ESET's comprehensive security portfolio.[1]

SMBs can improve their cybersecurity further by making use of the hardware-enhanced security features of the Intel vPro platform and ESET Endpoint Security.

The Intel vPro platform includes Intel® Threat Detection Technology (Intel® TDT), a suite of technologies that adds hardware-assisted detection of ransomware and other advanced threats.

ESET has integrated Intel TDT into its platform, thus gaining access to a plethora of unique hardware telemetry data. This data enhances the ability of ESET Endpoint Security to detect the presence of advanced threats like ransomware hiding in virtual machines (VMs).



Illuminate the journey

The Intel vPro platform and ESET Endpoint Security form a framework for maneuvering your way through cybersecurity challenges. ESET Endpoint Security and Intel TDT provide greater visibility into, and protection against, a wide variety of security threats and their effects on your business—from loss of data to financial impact and loss of customer confidence.[1]

Intel TDT detects ransomware through the Intel performance monitoring unit (PMU), which sits beneath applications, the operating system, and even virtualization layers, to gather CPU telemetry as it executes. With Intel TDT, ESET's endpoint protection platform can monitor for malicious behavior to help detect new variants and reduce blind spots.

Top business implications of attacks[1]

29%
Loss of data

23%
Financial impact

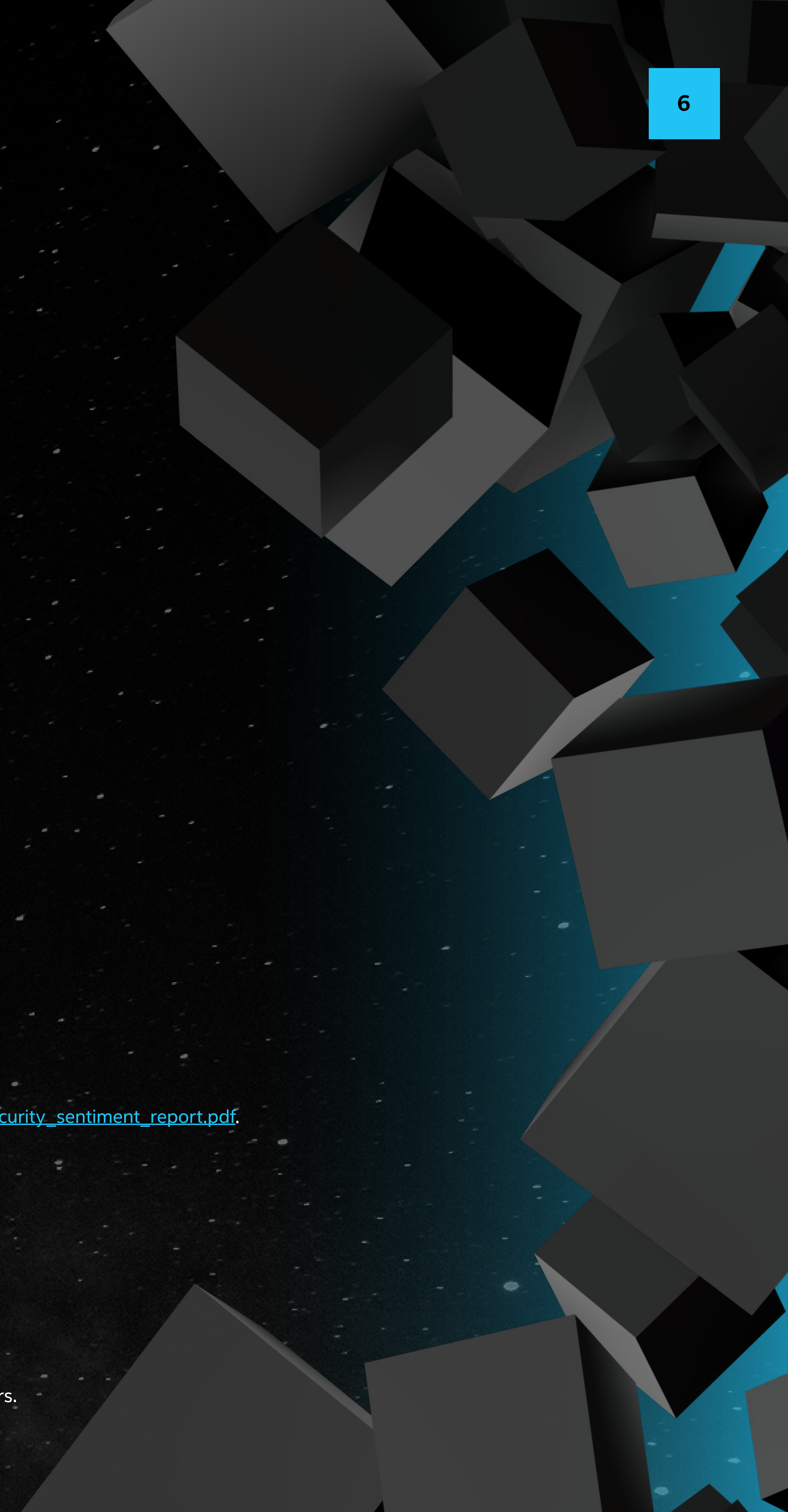
18%
Loss of customer confidence and trust

Stay safer with Intel and ESET

As an SMB leader, you might feel as if you are on a never-ending security odyssey. To help you overcome the challenges that you face, ESET and Intel provide a solution to bolster cybersecurity defenses and protect against new and unknown threats.

With the Intel vPro platform, you can gain business-class performance, hardware-enhanced security, and remote management capabilities. And ESET Endpoint Security offers both high performance and preemptive threat detection while helping to minimize false positives.

Confidently navigate your security journey, no matter how treacherous it appears, with the Intel vPro platform and ESET Endpoint Security. Learn more at eset.com/us/eset-and-intel-keep-smbs-safe/.



[1] ESET. "2022 SMB Digital Security Sentiment Report: Cyber Risks Driving SMBs to Enterprise Solutions." 2022. welivesecurity.com/wp-content/uploads/2022/11/eset_smb_digital_security_sentiment_report.pdf.

[2] ESET. "ESET Releases New SMB Research, Finds Cybersecurity Investments Not Keeping Pace with Threat Landscape." eset.com/us/about/newsroom/press-releases/eset-releases-new-smb-research-finds-cybersecurity-investments-not-keeping-pace/.

Intel technologies may require enabled hardware, software or service activation.

No product or component can be absolutely secure.

Your costs and results may vary.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

Printed in USA 0223/MG/PRW/PDF Please Recycle 354267-001US