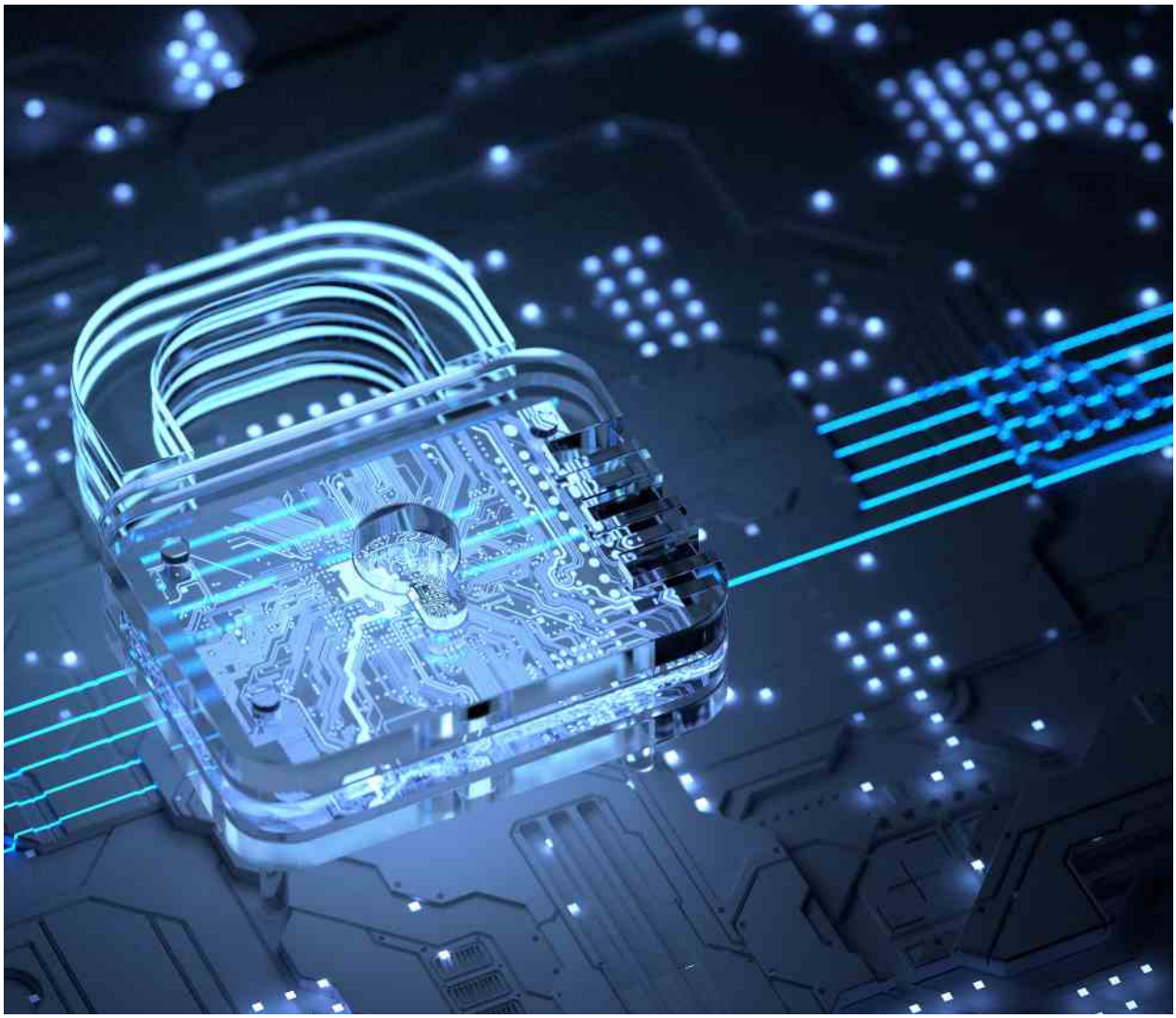
Global Security Report: Rapid Increase in Ransomware Threats Drives Need for Security Controls That Speed the Kill Chain

Venafi

Introduction

Ransomware has plagued organizations for years. But now it's increasing faster than ever, with the number of ransomware attacks increasing by 93% in the first half of 2021 over the same time period in 2020. This surge suggests that the COVID-19 pandemic may have brought about an acceleration in growth.[1] By the end of 2021, it's estimated that an organization will be hit by ransomware every 11 seconds.[2]

A Venafi-sponsored study conducted by Sapio Research evaluated data from 1,506 IT security officers across the U.S., U.K., Germany, France, Benelux and Australia to explore how InfoSec leadership is responding to the rapidly growing risk of ransomware attacks. What follows are some of the more significant findings from this study.



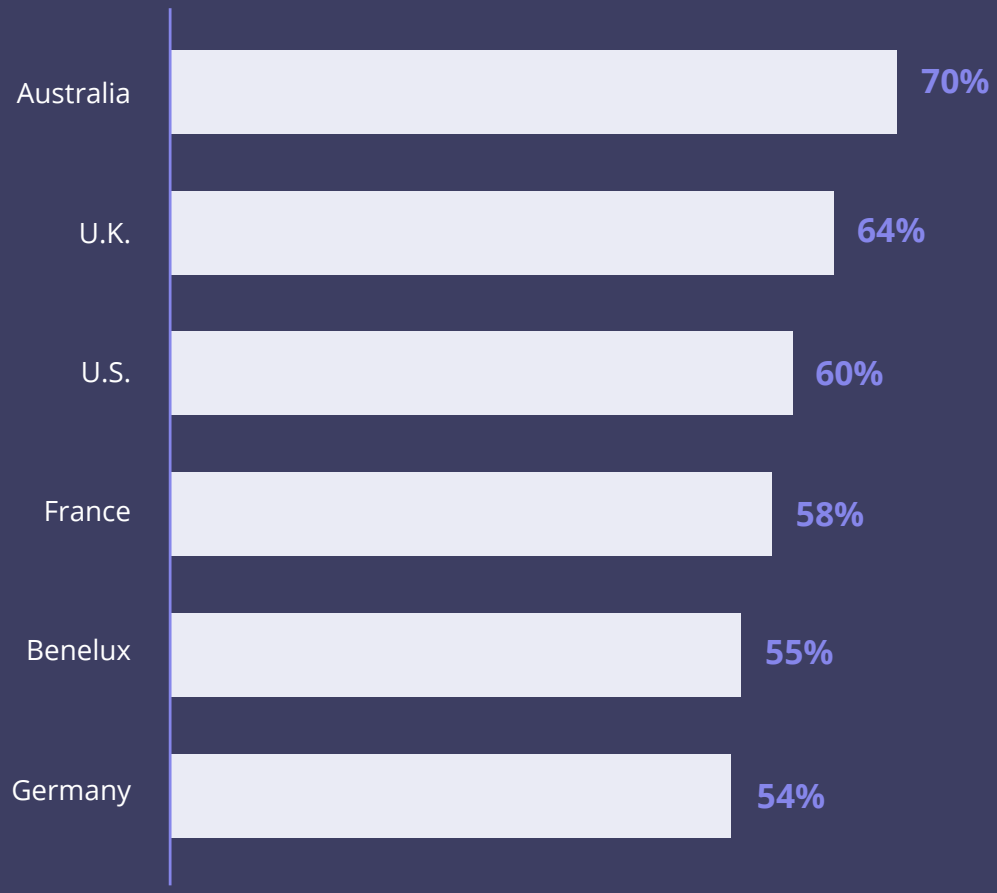
Section 1: Ransomware threats are equivalent to terrorism

In June 2021, the U.S. Department of Justice (DOJ) said the agency would now treat ransomware attacks at the level it previously reserved only for terrorism.[3] FBI Director Christopher Wray echoed the DOJ, comparing ransomware attacks to the 9/11 terrorist attacks.[4]

Overall, 60% of InfoSec leaders agree with the DOJ's decision to prioritize ransomware threats at the same level as terrorism.

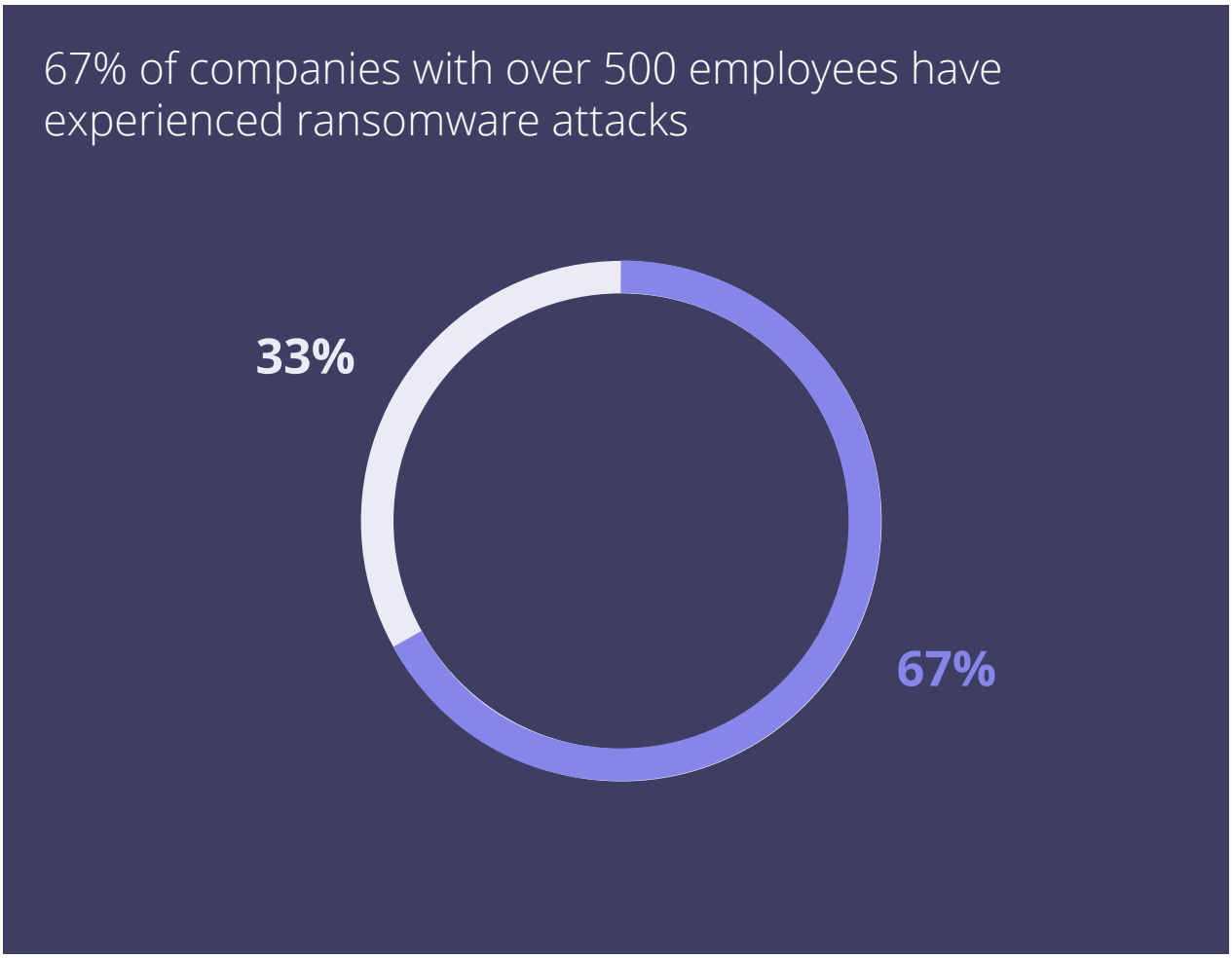
InfoSec leaders view ransomware threats at the same level as terrorism

Breakdown by country:



Section 2: Two-thirds of companies with over 500 employees experienced a ransomware attack over the last 12 months.

Given the increasing sophistication of ransomware attacks, it shouldn't be surprising that a high percentage of larger organizations have experienced ransomware attacks firsthand.



However, these attacks are not limited to larger organizations. Just over 60% of companies with between 100–500 employees also have experienced ransomware attacks over the past year.

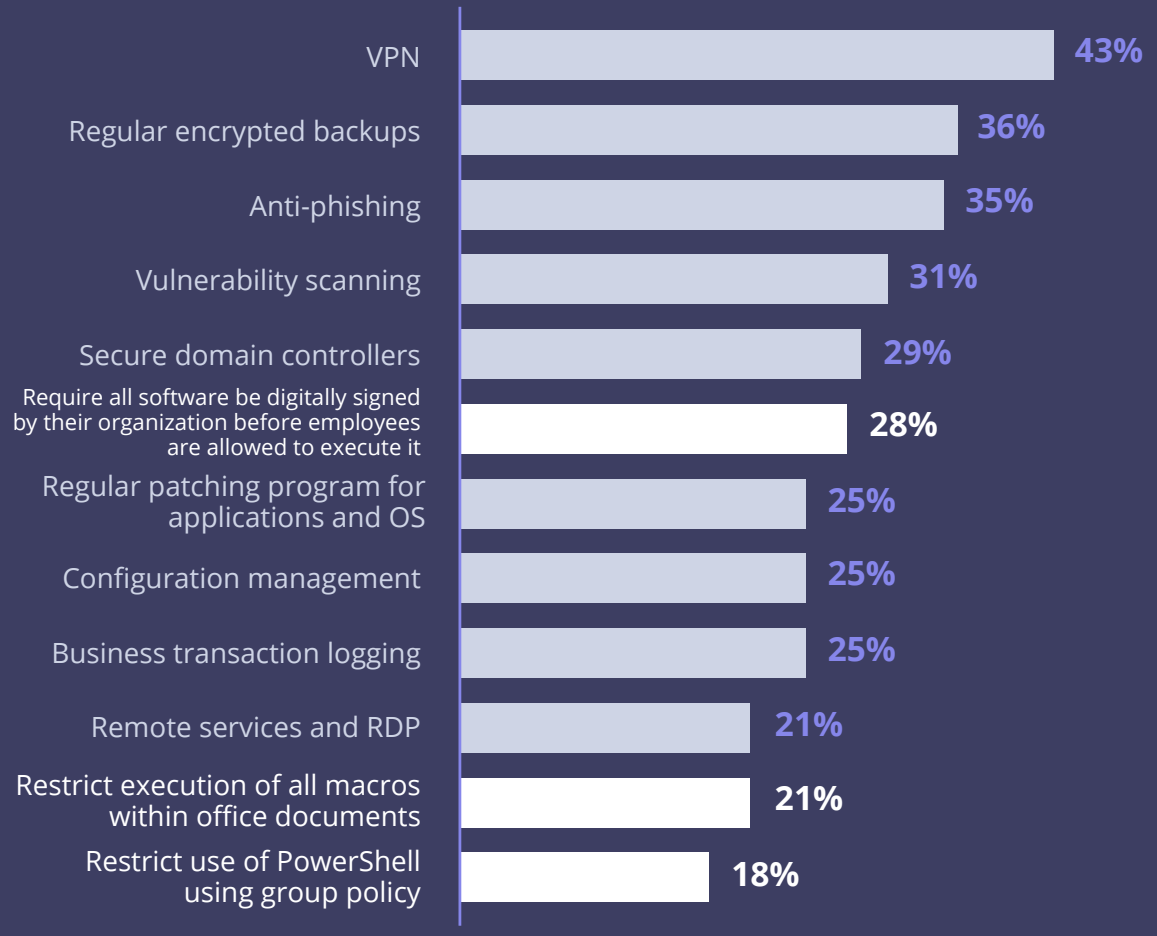
Section 3: 77% are confident that their current security tools will protect them from ransomware attacks.

Even though a high percentage of organizations have already been victims of ransomware attacks, more than three quarters (77%) of them are confident that their current security tools will safeguard them from future attacks. However, this confidence varies by job title, indicating slightly less confidence from security team leaders than from C-level executives in the efficacy of their current toolsets.

Section 4: Majority of current defense-in-depth security controls are not designed for modern IT infrastructures

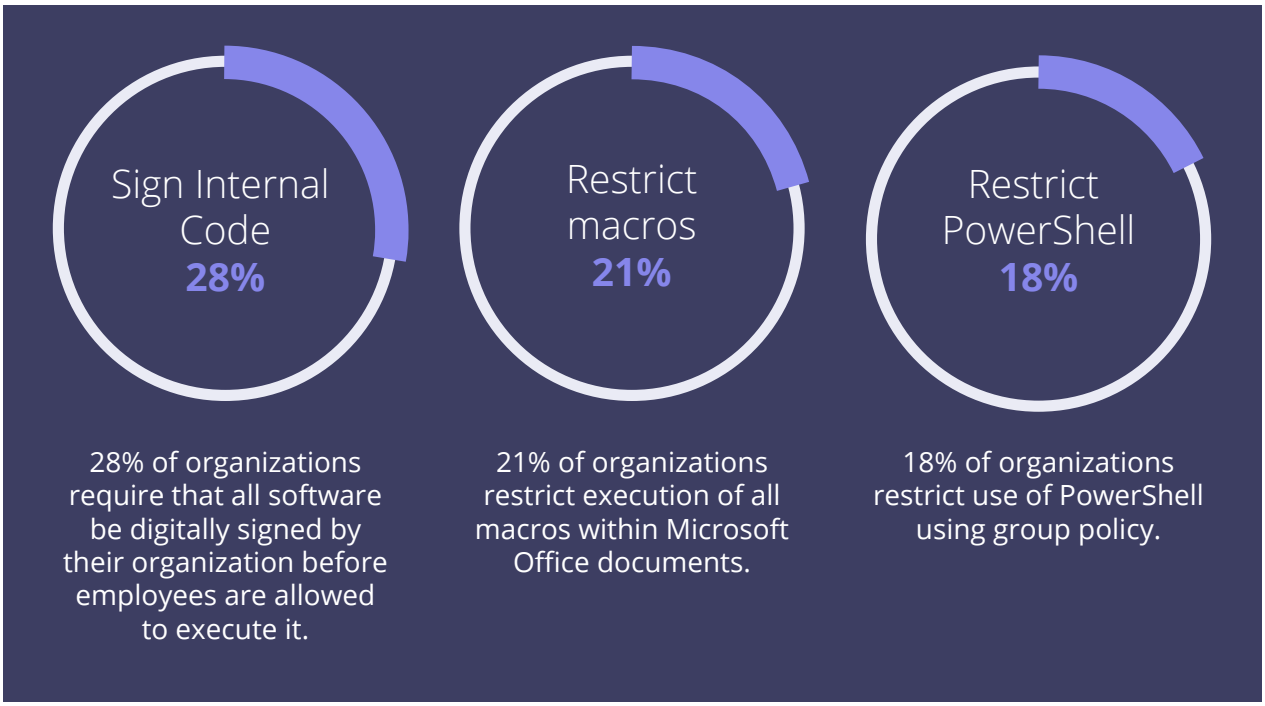
Organizations use a wide variety of security controls designed to protect against or limit the impact of a ransomware attack. However, most of these security controls are not optimized to handle perimeterless networks, let alone the infrastructure changes resulting from digital transformation. In particular, DevOps methodologies and software-defined networks require different security strategies to break the ransomware kill chain.

Current security controls used to protect against or limit the impact of a ransomware attack



Section 5: Are organizations adopting the most effective tools to break the ransomware kill chain?

Of the tools cited in the previous section, only three are designed to add specific new layers of control for cloud and DevOps environments that help break the ransomware kill chain. Yet these three tools have very low adoption rates.

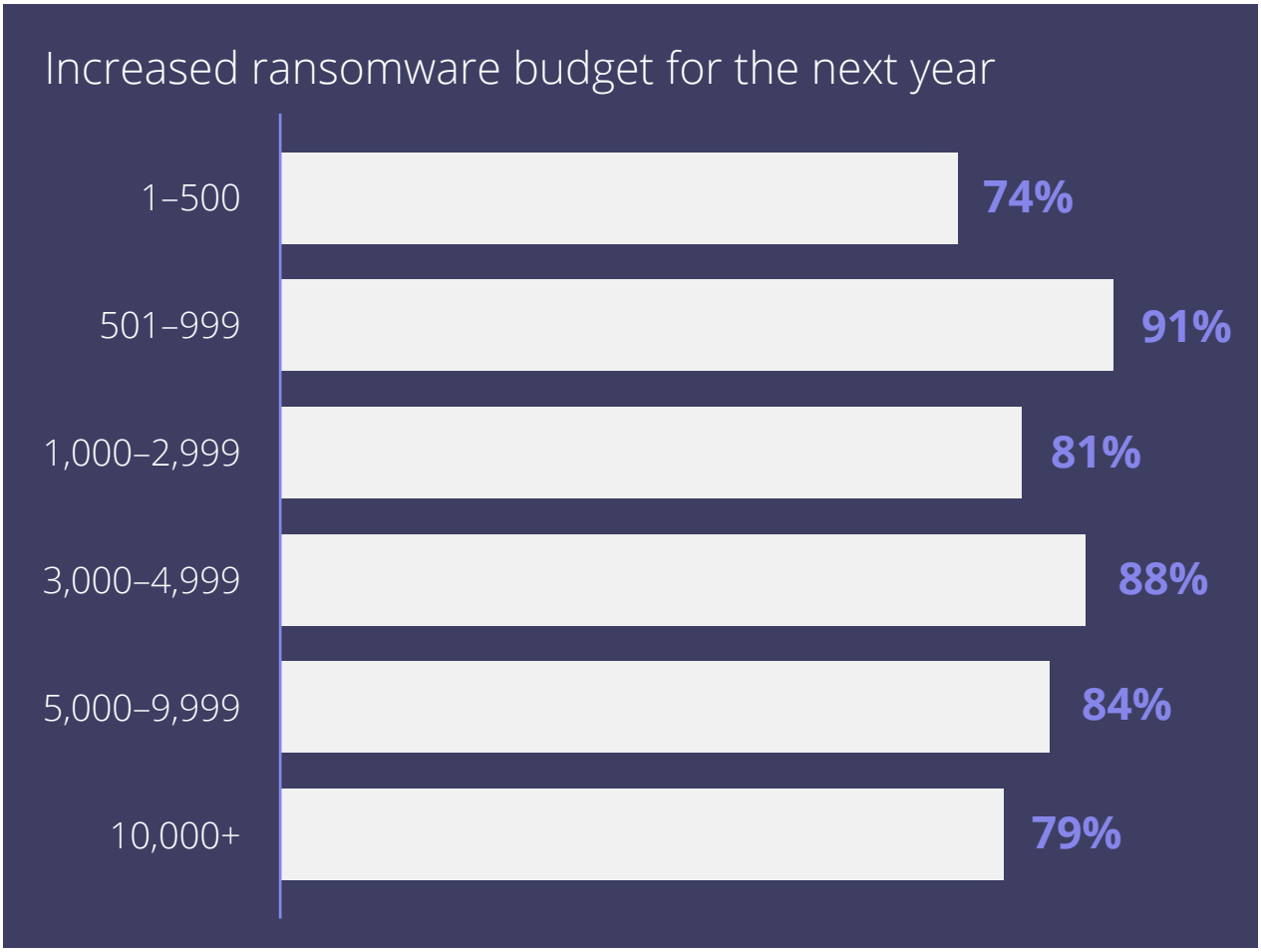


The first of these three controls, digital code signing, is currently being used by only 28% of respondent organizations overall, despite it being a deterrent to ransomware attacks. And while a higher percentage of large organizations (5,000 or more employees) employ digital code signing as a control, that percentage is well below 50%—despite the fact that such a high percentage of these organizations have already experienced ransomware attacks.

Restricting execution of unsigned Office macros can negatively impact productivity. However, 43% of all malware downloads are malicious Office documents in July 2021, up from 20% at the beginning of 2020.[5]

Section 6: How are organizations investing to prevent ransomware attacks?

In spite of their relative confidence in existing security controls, more than three quarters (77%) of organizations plan to spend more on ransomware protection in the next year. This is in response to the recent expansion in ransomware threats.



These numbers suggest that security teams realize their current strategies do not provide enough protection, along with the likelihood that ransomware threats will continue to increase in 2022. InfoSec teams may justify these investments because the cost of ransomware attack—regardless of whether it is successful—can quickly rise far beyond the cost of the ransom price itself.

Conclusion:
Investing in ransomware prevention

In 2020, the total amount of ransom paid by cyberattack victims added up to nearly $416 million in cryptocurrency.[6] This figure is projected to double in 2021 and double again in 2022. Moreover, Sophos predicts the total average cost to remediate ransomware attacks will be US $1.85 million in 2021, more than double the cost of US $761,106 reported in 2020.[7]

The rising costs of a ransomware attack and the increasing frequency of such attacks require more sophisticated security controls, explains Kevin Bocek, vice president ecosystem and threat intelligence at Venafi. "Organizational environments now extend far beyond traditional perimeters, and so we can no longer rely on yesterday's tools to win this high-stakes battle," says Bocek. "Controls like code signing, restricting the execution of malicious macros and limiting the use of unsigned scripts based on corporate security policies use a high level of automation to prevent ransomware in our machine-centric, digitally transformed world."

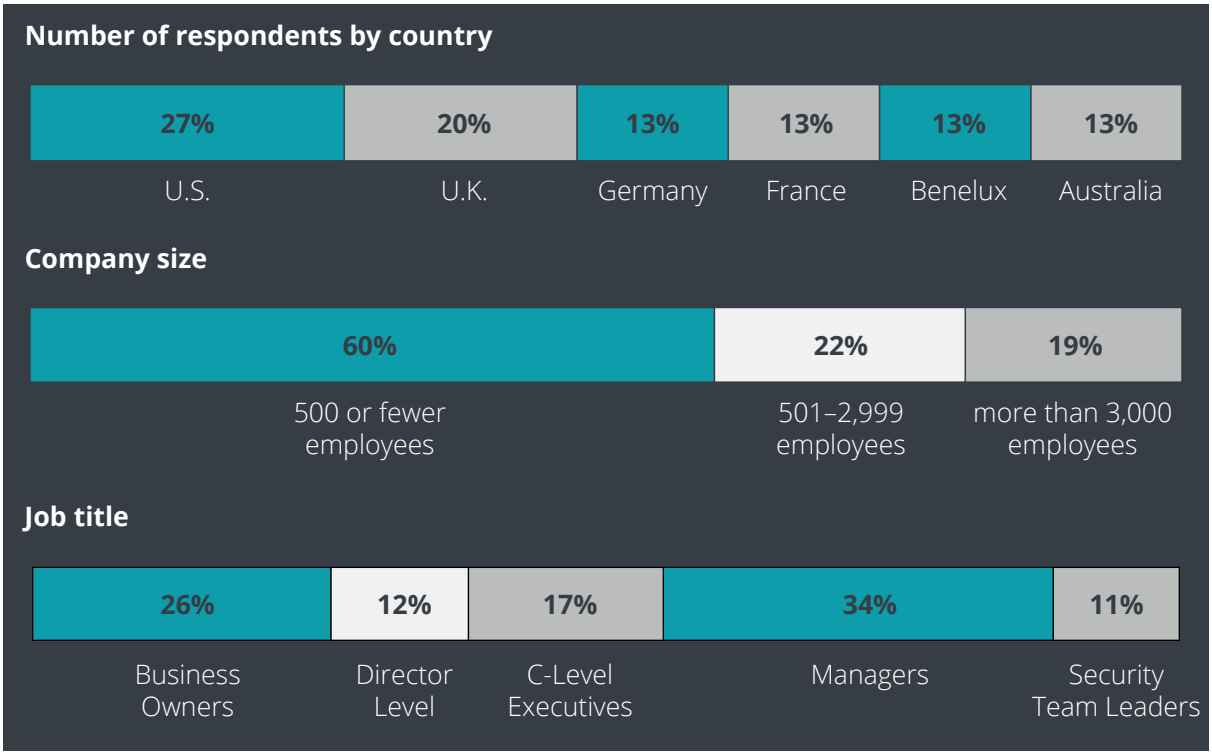
Find out how Venafi can help you break the ransomware kill chain at **venafi.com/platform/codesign-protect.**

References

1. Check Point Software Technologies LTD. Cyber Attack Trends: Mid Year Report 2021. July 2021.
2. Morgan, Steve. Cybercrime Magazine. Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021. October 21, 2019.
3. Bing, Christopher. Reuters. Exclusive: U.S. to give ransomware hacks similar priority as terrorism. June 3, 2021.
4. Viswanatha, Aruna and Volz, Dustin. The Wall Street Journal. FBI Director Compares Ransomware Challenge to 9/11. June 4. 2021.
5. Netskope. Hey, You, Get Out of My Cloud. July 2021
6. Chainalysis. Ransomware 2021 Critical Mid-Year Update. July 2021.
7. Sophos. The State of Ransomware 2021. April 2021. 12.

Appendix: Global Data Summary

This survey was conducted online in November 2021.



Venafi is the cybersecurity market leader in machine identity management, securing the cryptographic keys and digital certificates on which every business and government depends to deliver safe machine-to-machine communication. Organizations use Venafi key and certificate security to protect communications, commerce, critical systems and data, and mobile and user access. **To learn more, visit venafi.com**