Cybersecurity
INSIDERS

ATTACK SURFACE MANAGEMENT MATURITY REPORT

oomnitza

OVERVIEW

Cybersecurity leaders continue to calibrate and extend their attack surface management capabilities as their organizations contend with a worsening threat landscape, as well as on-going hybrid workplace, hybrid cloud, and digital business growth.

The 2022 Attack Surface Management Maturity Report has been produced by Cybersecurity Insiders, the 500,000 member online community of information security professionals, to explore the current state, exposures, and priorities that organizations need to consider to fortify their security posture.

Key findings include:

- 60% of organizations have low confidence in their ability to manage attack surface risk.
- 53% of organizations find remote workers deviating from security policy.
- 80% of organizations are pursuing a hybrid or multi-cloud strategy, and many organizations are experiencing qualified staff, infrastructure and misconfiguration visibility, and control automation cloud protection challenges.
- Only 45% of organizations have advanced asset intelligence with visibility and insight for over 75% of their assets, with the majority of respondents expressing asset inventory blind spots.
- Only 30% of organizations are very confident in their patch management efficacy.
- Organizations are considering platforms (46%) to leverage their tool investments, as 39% of respondents are unsure about replacing their siloed management tools to secure the entire IT estate.

We want to thank Oomnitza for supporting this important industry research. We hope you find this report informative and helpful as you continue your efforts to protect your organizations against evolving threats.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

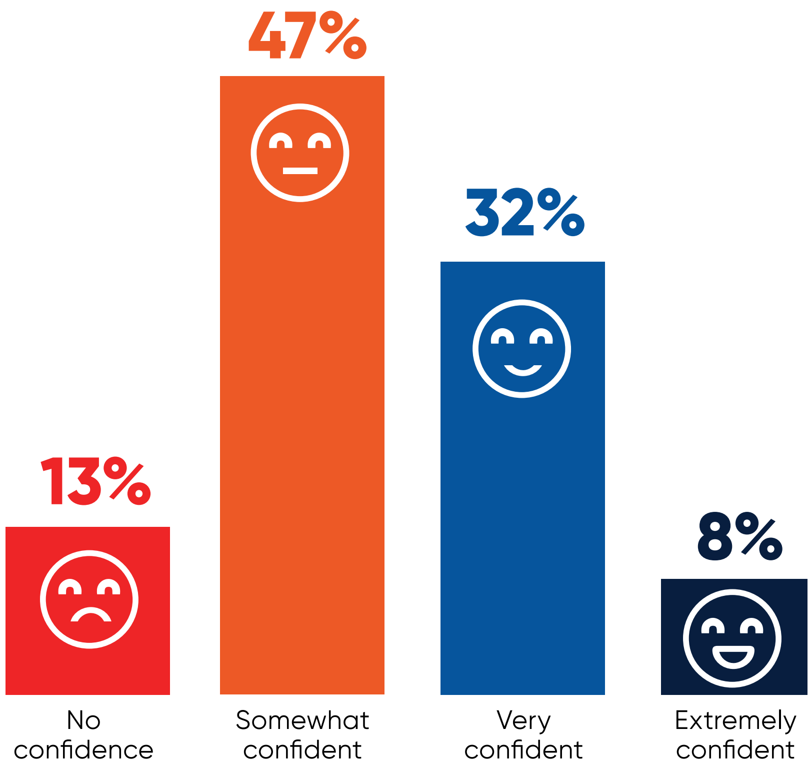
CONFIDENCE

Organizations are showing a significant lack of confidence in their capabilities to manage attack surface risks. Sixty percent say they have low confidence in their attack surface management risk capabilities.

How confident are you in your organization's capabilities to manage attack surface risk?

60%

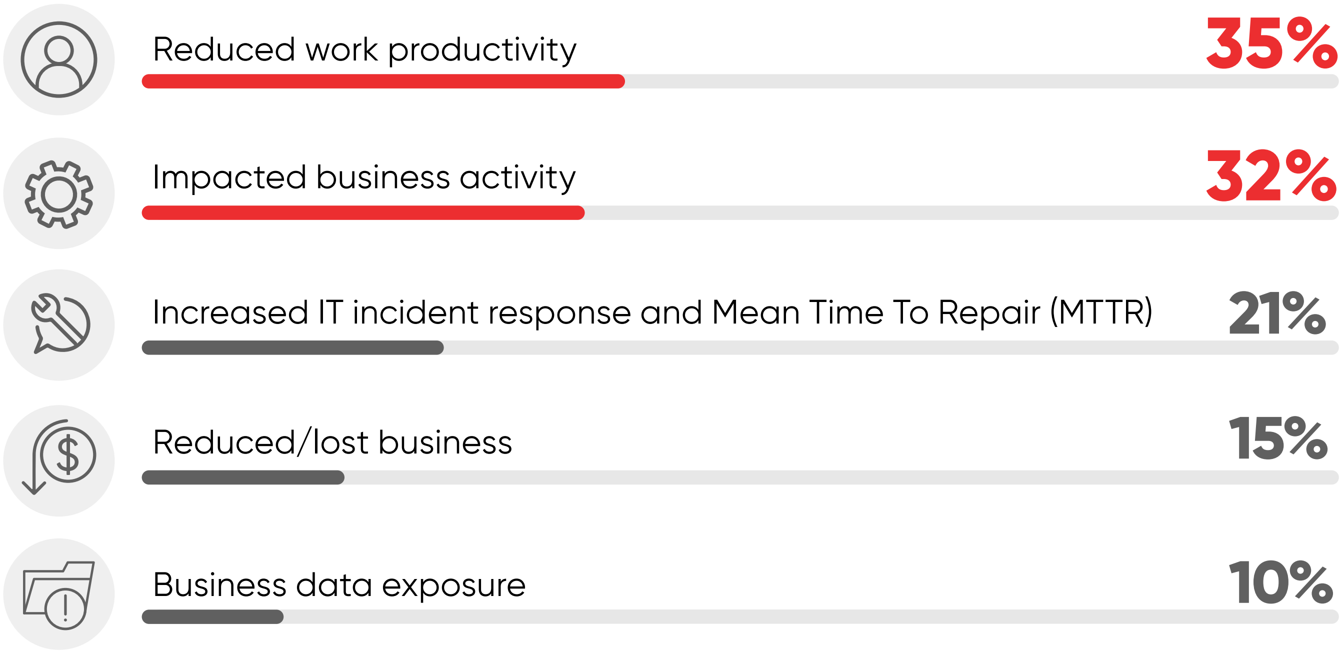
of organizations say they have low confidence in their attack surface management risk capabilities



OUTCOMES

Security incidents, due in part to attack surface exposures, have a significant negative impact on businesses. Reduced employee productivity (35%) tops the list, followed by impacted business activity (32%) and increased IT incident response and Mean Time To Repair (MTTR) (21%).

What were the outcomes of security issues in your organization in the past 12 months?

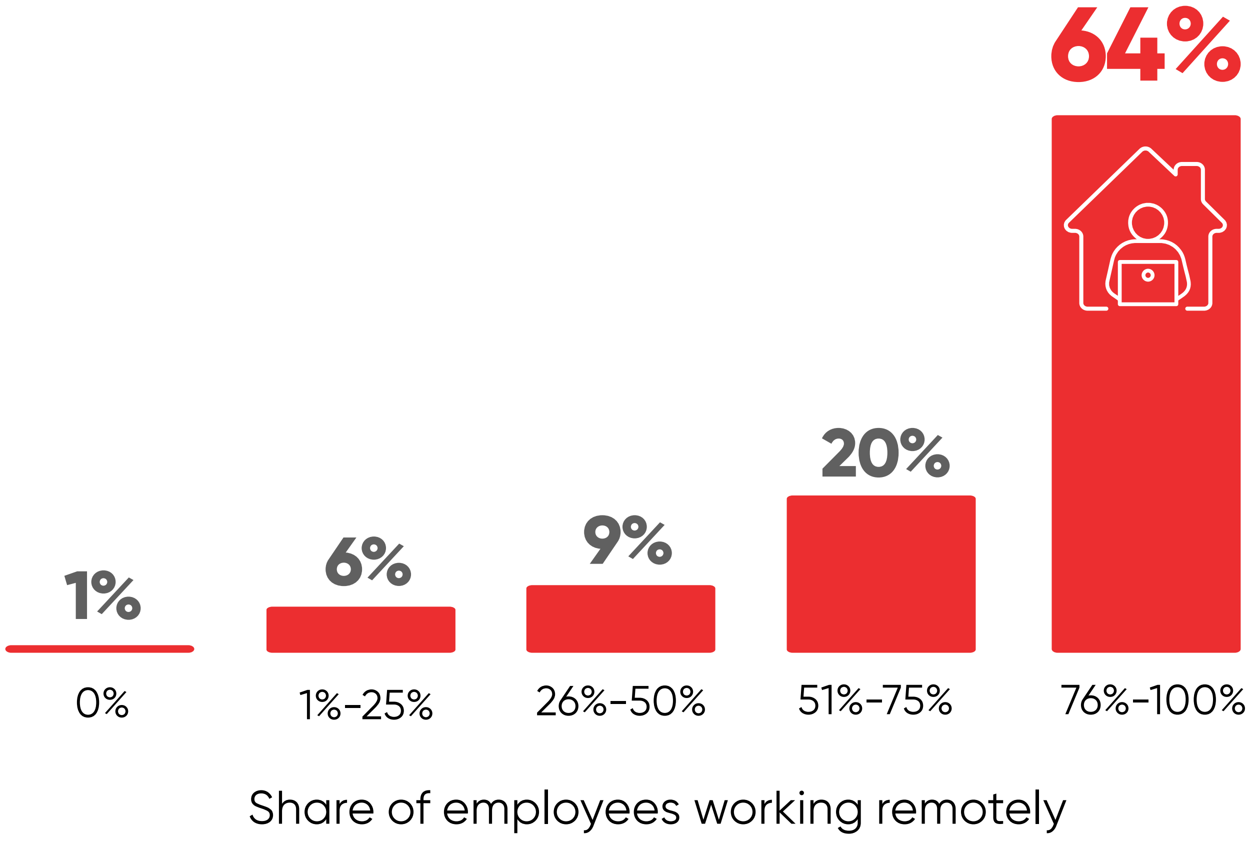


Compliance fines (7%) | Legal actions (7%) | IP compromise (7%)

REMOTE WORKFORCE

Following the COVID-19 pandemic, a majority of organizations made the shift to a remote workforce for a majority of employees, with 64% of companies having more than 75% of their employees working from a home office. Despite a trend back to on-site office work, a majority of employees will likely continue to work from home or have a hybrid workplace.

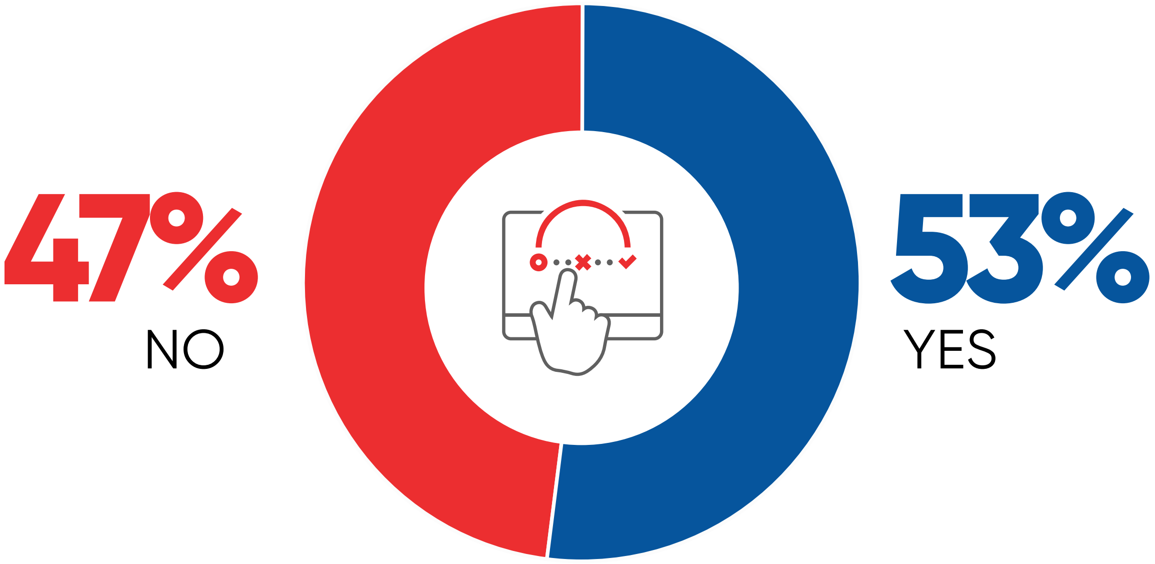
What percent of your workforce is working remote?



POLICY ADHERANCE

Even with strong security policies and controls in place, organizations are still at risk unless they can motivate employees to comply. This is even more challenging with a remote or hybrid workforce, as many employees are not in the office to work with their IT team to deploy and utilize the latest technologies and processes. A majority (53%) of organizations have experienced employees deviating from established security policies and controls.

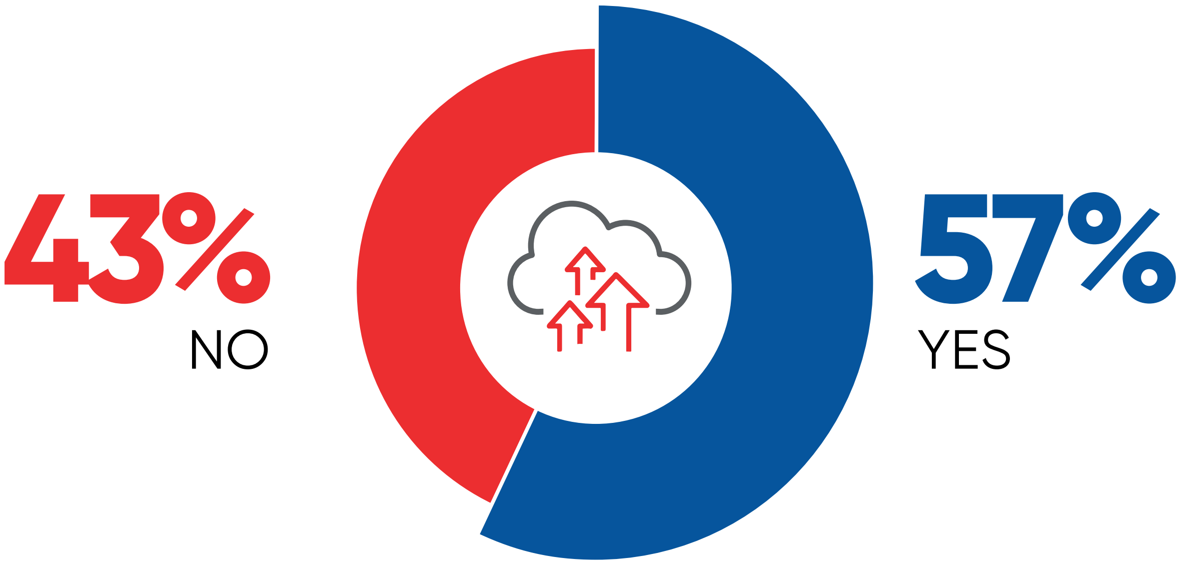
Has your organization experienced remote workers deviating from established security policies and controls?



CLOUD ACCELERATION

The majority of organizations in our survey (57%) are accelerating their move to cloud-based resources, applications and SaaS following the COVID pandemic.

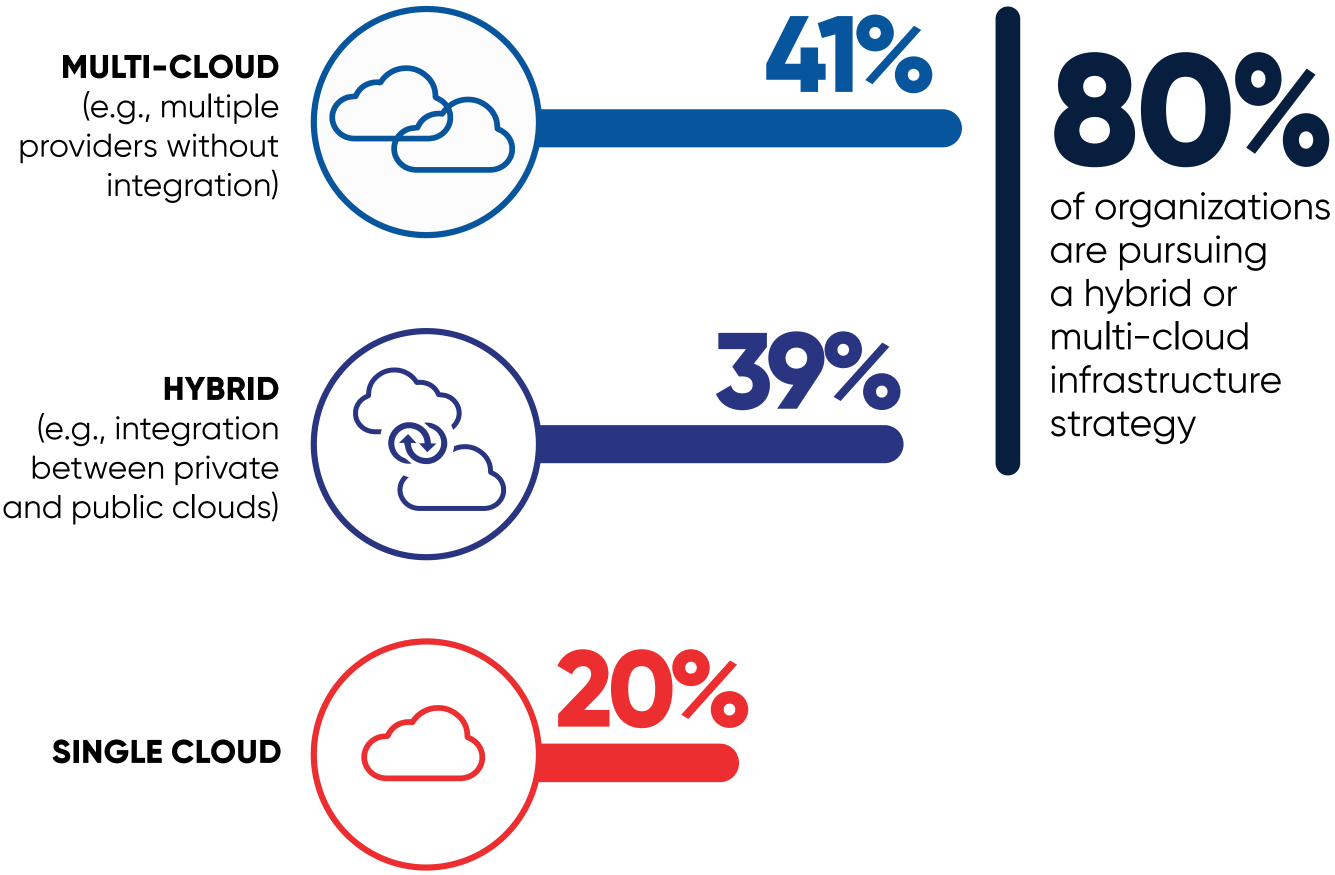
Has hybrid workplace growth (post COVID) increased your company's use of cloud resources, applications, and SaaS?



CLOUD CAPABILITIES

A majority of organizations (80%) are pursuing a hybrid or multi-cloud infrastructure strategy for improving capabilities, scalability, or business continuity. While overall beneficial, this strategy also increases the complexity of protecting multiple environments.

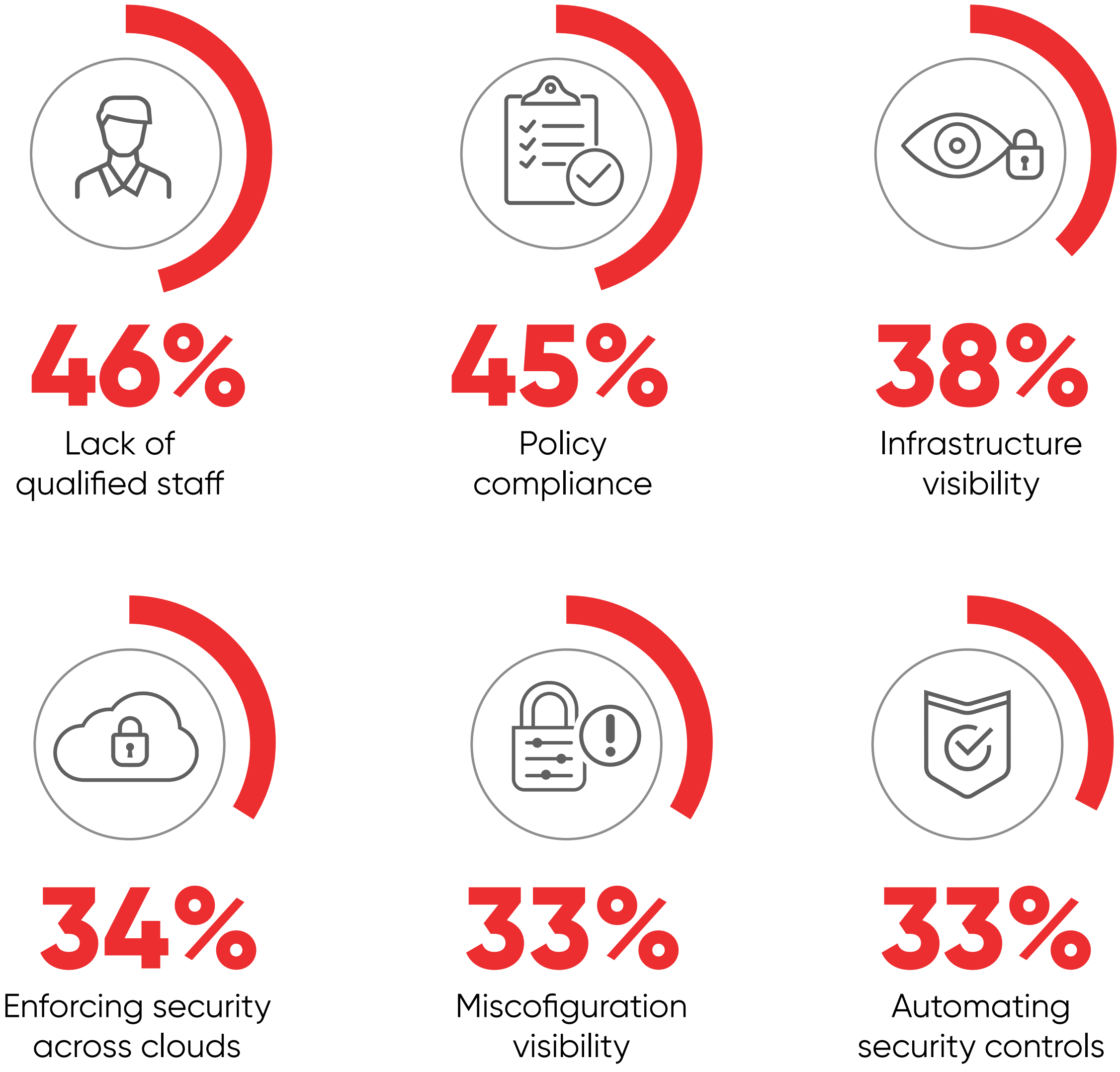
How is your organization implementing cloud capabilities?



CLOUD CHALLENGES

Cybersecurity professionals are facing numerous challenges when it comes to protecting cloud infrastructure. While lack of qualified staff (46%) remains a key challenge, policy compliance (45%) and infrastructure visibility (38%), followed closely by enforcing security across clouds (34%), misconfiguration visibility (33%) and automating controls (33%) are among the top cloud protection challenges.

What challenges are you facing to protect cloud infrastructure?



46%
Lack of
qualified staff

45%
Policy
compliance

38%
Infrastructure
visibility

34%
Enforcing security
across clouds

33%
Miscofiguration
visibility

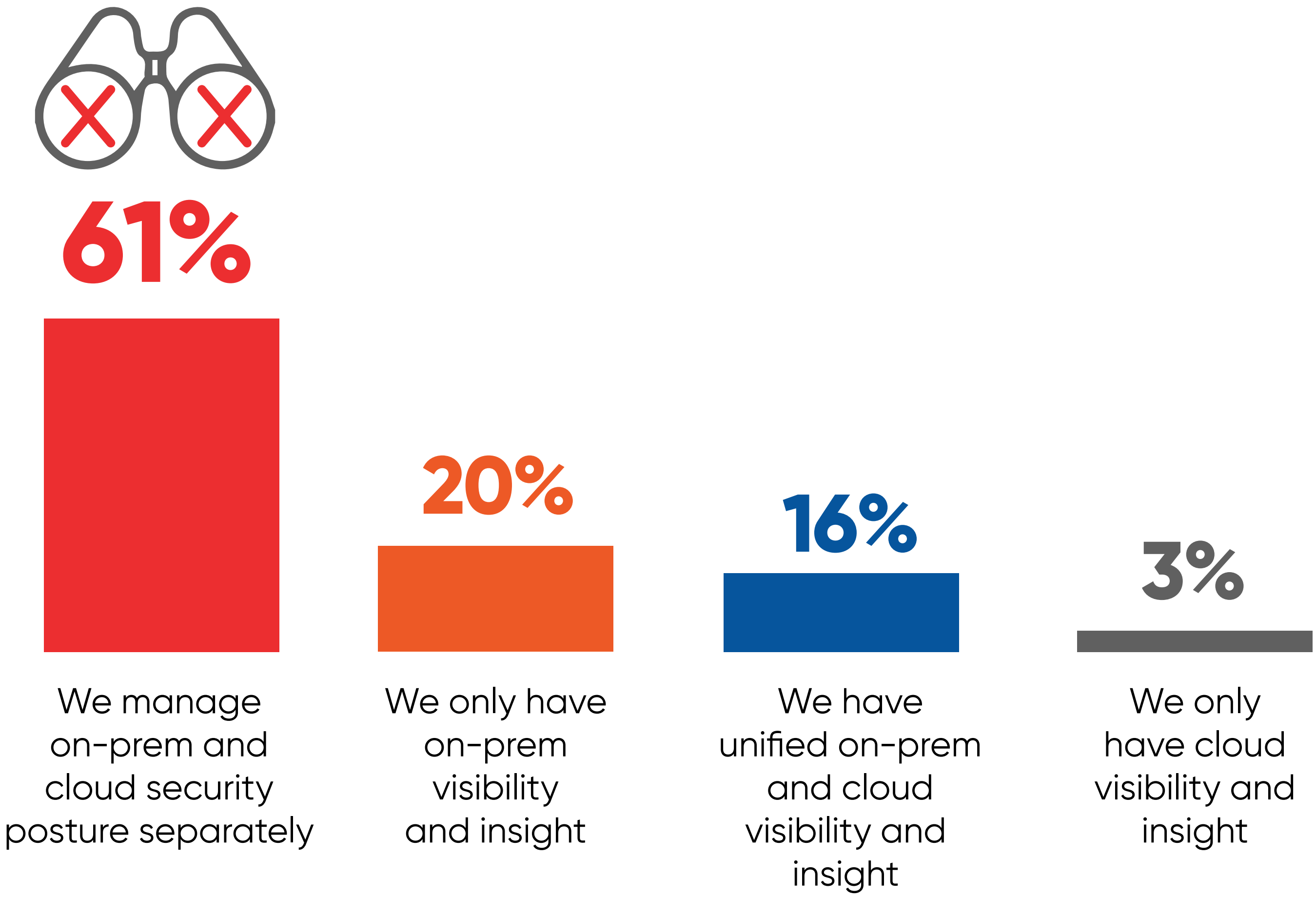
33%
Automating
security controls

Setting consistent security policies 33% | Complex cloud to cloud/cloud to on-prem security rule matching 32% | Securing access from personal and mobile devices 30% | Setting the correct user access privileges 29%

HYBRID IT VISIBILITY

When asked about the ability to centrally manage their hybrid IT infrastructure security posture, most organizations (61%) confirm they are lacking a unified view of their cloud and on-premises security posture.

How confident are you in your organization's ability to centrally manage its hybrid IT infrastructure security posture?



ASSET INVENTORY

When asked how mature their organization's ability is to obtain asset inventory intelligence, which is a cornerstone requirement for all security frameworks, only 45% of organizations have advanced asset intelligence with visibility and insight for over 75% of their assets, with the majority of respondents expressing asset inventory blind spots.

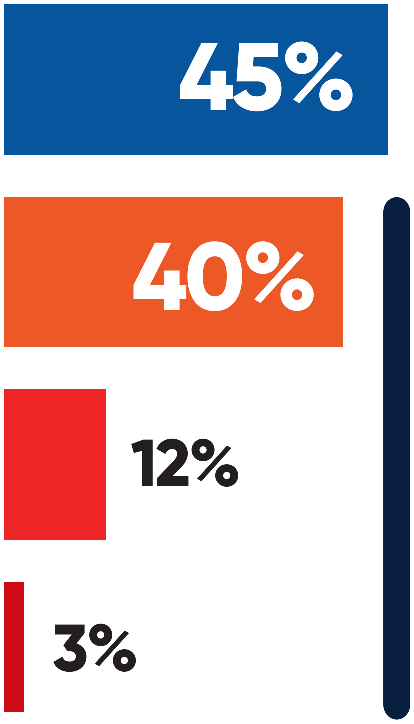
How mature is your organization's ability to gain intelligence on asset inventory across your IT estate?

Advanced asset intelligence
We have visibility and insight for over 75% of our assets, inclusive of business ownership, type and lifecycle state

General asset intelligence
We have some visibility for 50%-75% of our assets and inconsistent insight concerning business ownership, type and lifecycle state

Basic asset intelligence
We have limited visibility for less than 50% of our assets and nominal insight concerning business ownership, type and lifecycle state

Lax asset intelligence
We have varying control over asset visibility and operational insight

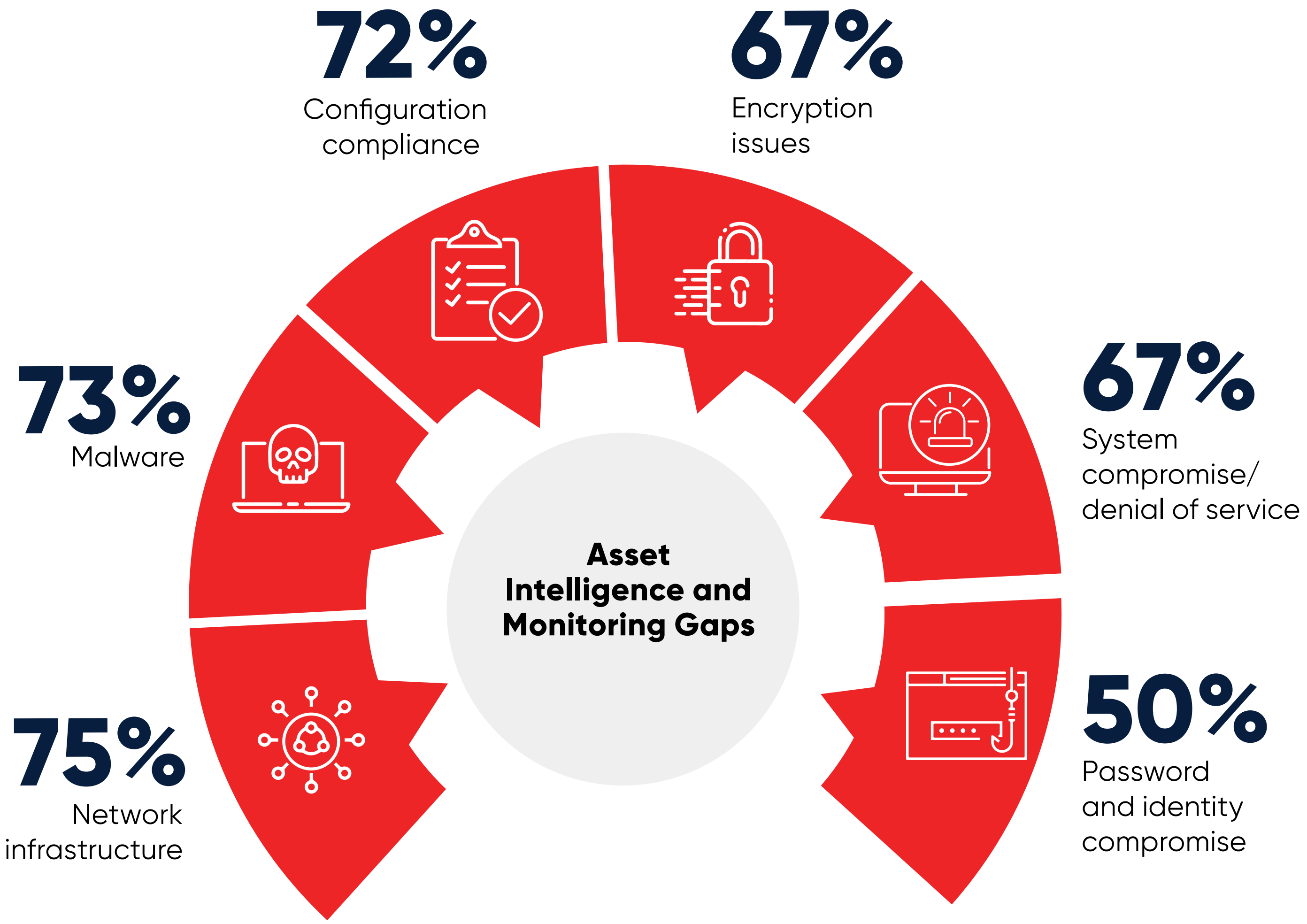


55% of organizations confirm they have less than 75% asset inventory intelligence coverage

ASSET INTELLIGENCE GAPS

We asked organizations where they experienced the biggest asset intelligence and monitoring gaps. Lack of network infrastructure visibility (75%) tops the list, followed by malware (73%) and configuration compliance (72%).

Where has your organization experienced asset intelligence and monitoring gaps?

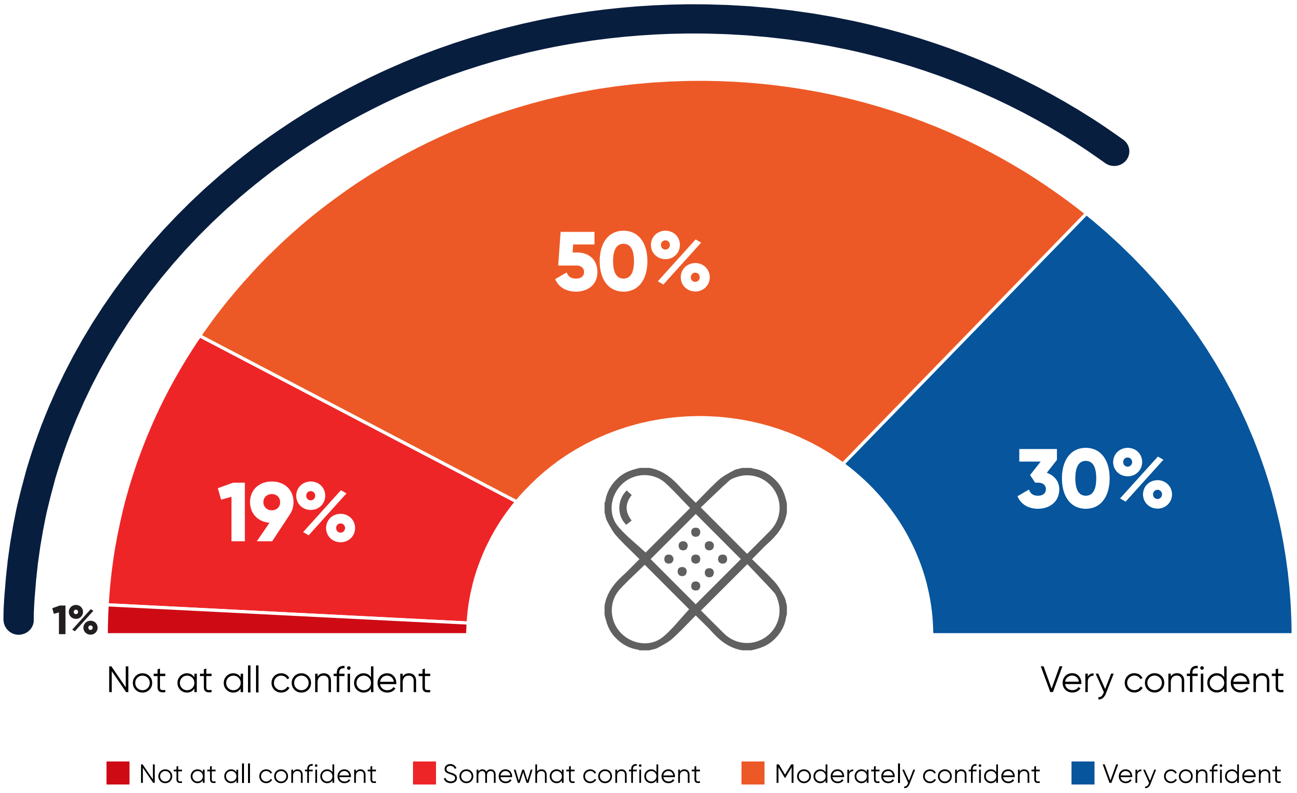


PATCH EFFICACY

A majority of cybersecurity professionals (70%) are, at best, moderately confident in the efficacy of security patches. Only about a third claim to be very confident in patch efficacy (30%).

How confident are you in your organization's patching efficacy?

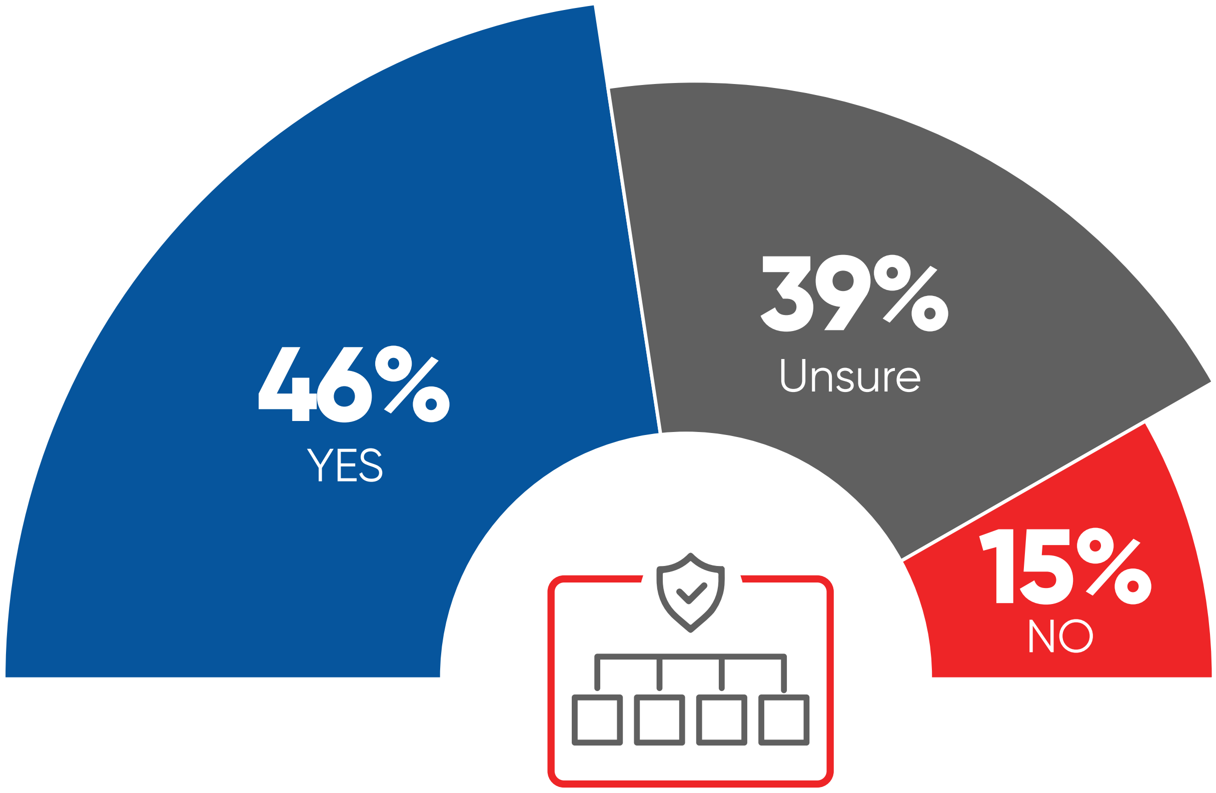
70% of organizations are, at best, moderately confident in the efficacy of security patches



PLATFORM APPROACH

Security leaders and practitioners are undecided (39%) whether or not to replace their siloed management tools. The response appears to favor (46%) moving to a centralized platform, which accommodates both consolidating and keeping existing IT tools to progress attack surface management capabilities.

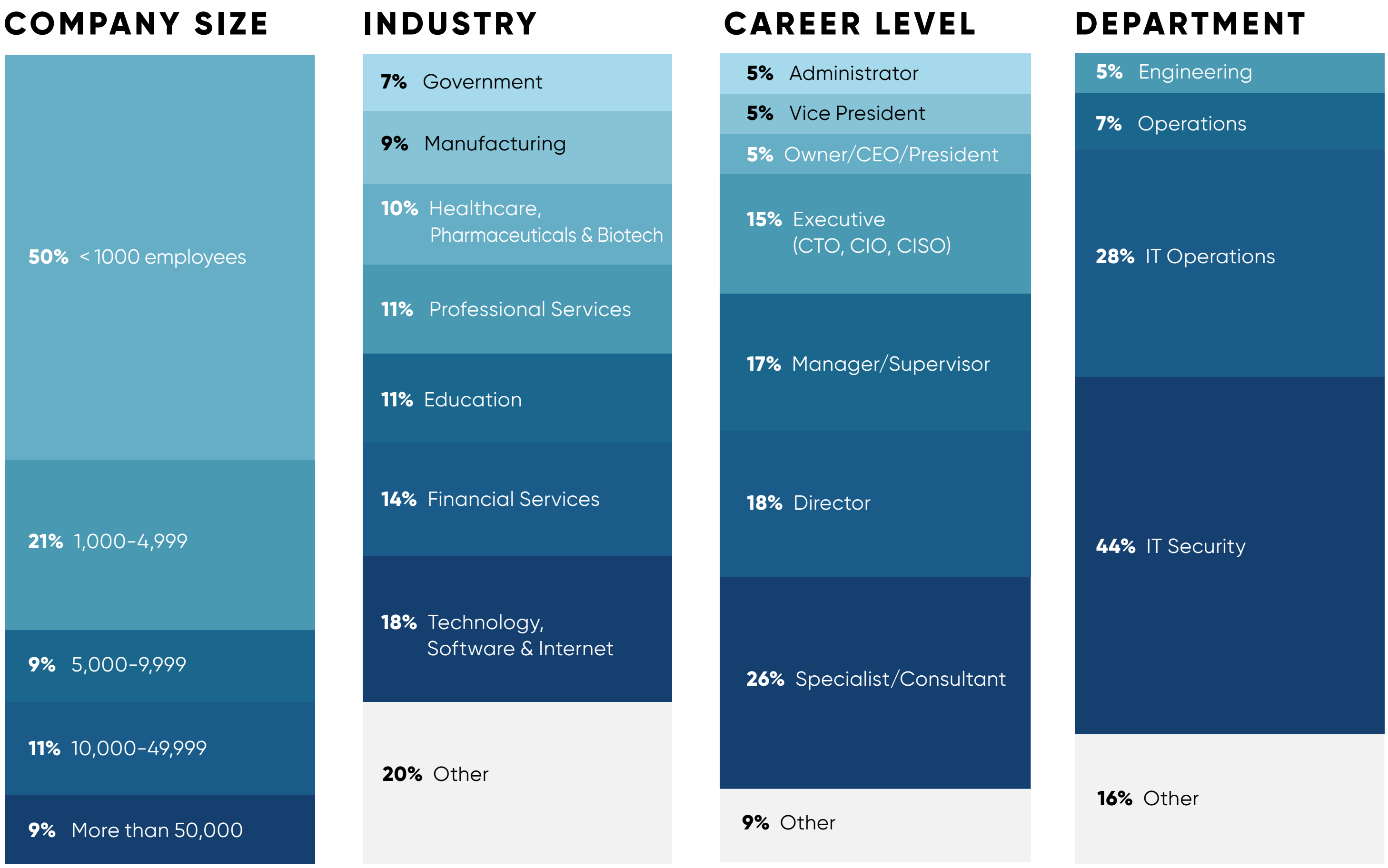
Is your organization planning to replace siloed management tools for a centralized platform to secure the entire IT estate?



METHODOLOGY & DEMOGRAPHICS

The 2022 Attack Surface Management Report is based on the results of a comprehensive online survey of 351 cybersecurity professionals to explore the current state, exposures, and priorities that organizations need to consider to fortify their security posture.

The respondents range from technical executives to managers and IT security practitioners, representing a balanced cross section of organizations of varying sizes across multiple industries.



oomnitza

Oomnitza offers a versatile and automated Enterprise Technology Management platform that delivers multi-source visibility and control across endpoints, software, network infrastructure, and cloud.

Our SaaS solution, with rapid integrations, best practices, and no-code workflows, allows enterprises to leverage their existing systems to gain unified asset inventory analytics, standardize lifecycle processes, and ensure security and compliance.

This platform approach complements security posture management programs by identifying cyber attack surface gaps, enhancing asset intelligence to reduce incident triage and response times, and enabling teams to streamline audit and policy compliance verification tasks.

We help some of the most well-known and innovative companies to optimize business resources, mitigate cyber risk, expedite audits, and fortify digital experience.

www.oomnitza.com

Cybersecurity
INSIDERS

Cybersecurity Insiders is a 500,000+ member online community for information security professionals, bringing together the best minds dedicated to advancing cybersecurity and protecting organizations across all industries, company sizes, and security roles.

www.cybersecurity-insiders.com