

Global Attack Surface Management Organization Trends and Challenges





Physical and virtual assets are

on an average business day.

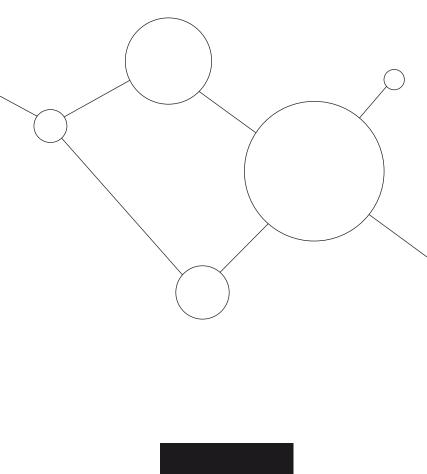
monitored.

connected to organizational networks

And only 60% of these assets are



Only 58% of this information is actionable.



75%

Of global respondents say

in the work environment.

employees are downloading

shadow IT to connected assets

44%

Of respondents admit to still using manual spreadsheets.

49%

Of organizations claim to

have complete visibility of

managed assets currently connected to their network.

the organization-owned and

39% 38%

Operational

downtime

Financial

loss

40%

Of organizations report

their vulnerability and patch

management processes are

known across the organization.

sources are used to collect data relating to threat intelligence.

of those organization's

cybersecurity team feels

overwhelmed by cyber

threat information.

reported a lack of control

and management.

In the US, _

In the UK,

In France,

Of respondents indicated a

owned assets connected to

the business environment.

lack of visibility over employee

78%

Of organizations have been

attack in the last 12 months.

breached as a result of a cyber

Top 2

Consequences of a breach:

28%

91% Of IT Pros believe their organization needs enhanced policies and procedures to address security vulnerabilities.

process to examine vulnerability and patch management.

go to https://www.armis.com/attack-surface-management

2023 Armis Research Report

ONLY 35% have a formalized

The read the complete report that includes findings for the UK, ARMIS UK, France, Germany, Australia, New Zealand and Singapore

© Copyright Armis 2023

2023 Armis Research Report **Global Attack Surface Management Organization Trends** VansonBourne and Challenges