

Global Attack Surface Management Organization Trends and Challenges

According to research conducted by VansonBourne Research.

61%

Of global organizations confirmed they have been breached at least once over the last 12 months.

57,686

Physical and virtual assets are connected to organizational networks on an average business day.

And only **60%** of these assets are monitored.

<45%

Of the respondents, report using 10 or more different sources to collect data relating to threat intelligence.

Only 58% of this information is actionable.

75%

Of global respondents say employees are downloading shadow IT to connected assets in the work environment.

44%

Of respondents admit to still using manual spreadsheets.

49%

Of organizations claim to have complete visibility of the organization-owned and managed assets currently connected to their network.

Top 2

Consequences of a breach:

39%

Operational downtime

38%

Financial loss

40%

Of organizations report their vulnerability and patch management processes are known across the organization.

In the US,

78%

Of organizations have been breached as a result of a cyber attack in the last 12 months.

10+

sources are used to collect data relating to threat intelligence.

28%

of those organization's cybersecurity team feels overwhelmed by cyber threat information.

In the UK,

77%

Of respondents indicated a lack of visibility over employee owned assets connected to the business environment.

78%

reported a lack of control and management.

In France,

91%

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

ONLY 35% have a formalized process to examine vulnerability and patch management.

The read the complete report that includes findings for the UK, UK, France, Germany, Australia, New Zealand and Singapore go to <https://www.armis.com/attack-surface-management>