Tanium Study: Over 90% of Global Organizations Surveyed Have Major Gaps in IT, Despite Tens of Millions Spent on Compliance

Research of 750 IT decision makers shows that:

Organizations spend big to minimize compliance risk, but critical visibility gaps are widening

$70.3M

is the average amount spent by organizations in the last year to ensure data protection

$185M

87% of organizations have set aside or increased their cyber liability insurance by an average of $185 million each, to deal with the consequences of a data breach

37%

claim that a lack of visibility and control of endpoints is the biggest barrier to maintaining compliance

Increased spending isn't solving critical visibility challenges

94%

admit that they have discovered endpoints in their organization that they were previously unaware of

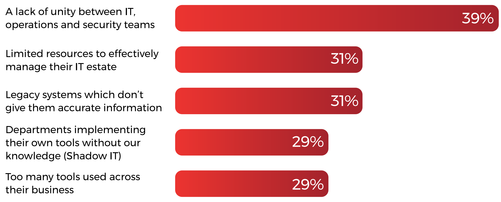
26%

say they feel completely in control of gaining instantaneous visibility of the devices on their network

71%

of CIOs discover new endpoints on a weekly basis

Top five challenges causing visibility gaps



IT complexity and tool sprawl perpetuate visibility gaps

43

is the average number of IT operations and security tools used by organizations

91%

point to fundamental weak points in their IT environment that cause visibility gaps

IT leaders have a false sense of confidence in their data

90%

claim to be confident of reporting all required breach information to the regulator within 72 hours

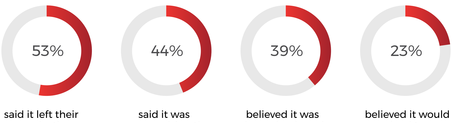
However

47%

report they have challenges in getting visibility into connected computing devices on their network

This level of confidence appears to be misplaced. A single missed endpoint could be a compliance violation waiting to happen

Poor visibility leaves networks susceptible to disastrous outcomes



Technology leaders must regain control of their IT environment to minimize risk.

We suggest taking these important steps:

1. **Instant endpoint visibility:**
   Create a single, unified view of the entire IT environment in real-time.

2. **Stronger collaboration:**
   It's crucial that IT operations and security teams unite around a common set of actionable data.

3. **The right investments:**
   To effectively manage technology risk, organizations must invest in processes, policies, and technology that enforce continuous visibility and control of endpoints, respond to audits and erasure requests, and detect and investigate unforeseen incidents.

About the research

A total of 750 IT decision-makers were surveyed by Vanson Bourne from September - October 2019 in the United States, United Kingdom, Australia, France, Germany, Japan, Netherlands and Canada. The respondents were from organizations with at least 1,000 employees and could be from any sector.