TANIUM

Whitepaper

Visibility Gap Study

Out of sight, out of compliance?
How visibility gaps in digital assets across the IT estate are leaving organizations vulnerable

Executive Summary

The cybercrime economy is estimated to be worth $1.5 trillion annually, with the number of new security threats soaring at an alarming rate. According to just one report, 7.9 billion records were exposed in the first nine months of 2019. This compounds the burden on already stretched IT teams who are tasked with tackling the daily challenges precipitated by shadow IT, cloud computing, containers, zero-trust, and software-defined everything.

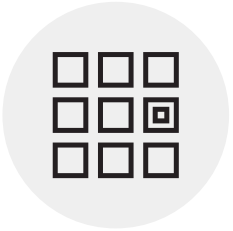
And what do most observers see as the common culprit for all of this chaos? Visibility gaps.

As modern IT networks become more complex and distributed, organizations face mounting pressure to manage thousands upon thousands of networked devices. And, with regulations like GDPR and CCPA, the complexity to protect sensitive information is exacerbated by an ever-changing risk profile.

To find out more about the challenges that organizations face, Tanium commissioned independent market-research specialist Vanson Bourne to survey 750 IT decision makers across the United States, United Kingdom, Australia, France, Germany, The Netherlands, Japan, and Canada. The report entitled the 'Visibility Gap' uncovered five key challenges for IT in 2020:

- **Spending big on compliance is the new normal.** An average of $70.3 million was spent complying with new regulations in the past 12 months, with almost nine out of 10 (87 percent) organizations actually increasing cyber-liability insurance, or setting aside budget, at an average of $185 million.
- **Critical visibility gaps are pervasive.** Virtually all IT decision makers (94 percent) admit to having discovered endpoints in their organization that they were previously unaware of, highlighting a startling lack of visibility that could lead to compliance violations, among other things.
- **Complexity and "tool sprawl" perpetuate the gaps.** Businesses use an average of 43 IT security and operations tools. Siloed teams (especially IT operations and security), shadow IT, and other basic weaknesses also persist.
- **There's a false sense of confidence when it comes to compliance readiness.** Ninety percent of respondents are certain their organization could report all required breach information to a supervisory authority within 72 hours. But with nearly half (47 percent) reporting they have challenges in getting visibility into connected computing devices on their network, this confidence appears to be misplaced — a single missed endpoint could be a compliance violation waiting to happen.
- **Poor visibility leaves networks susceptible to disaster.** Everything from vulnerability to cyber-attacks, damaged brand reputation, and heavy non-compliance fines can result from lack of visibility.

To keep pace with these challenges, technology leaders must regain control of their IT environment. They must focus on the fundamentals of managing and securing endpoints if there is to be any hope of effective compliance and risk management.



94%

discovered endpoints in their organization that they were previously unaware of

And the survey says:

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

Global organizations with at least 1,000 employees have spent on average $70.3 million each to comply with the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA) and other data-privacy regulations over the past 12 months alone.

A majority of organizations have also hired new talent (81 percent), invested in workforce training (85 percent), and introduced new software or services (82 percent) in an attempt to ensure continued compliance. In addition, 87 percent of organizations have set aside or increased their cyber-liability insurance, by an average of $185 million each, to deal with the potential consequences of a data breach.

Despite this increased investment, organizations still feel unprepared to deal with the evolving regulatory landscape. More than a third (37 percent) claim that a lack of visibility and control across endpoints is the biggest barrier to maintaining regulatory compliance.

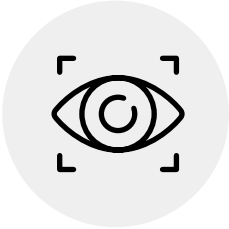
At an operational level, true visibility means gaining a comprehensive view of all computer and data assets within your IT estate. Visibility also means having insight into which machines are vulnerable at a specific moment in time so informed decisions can be made to prioritize remediation. Visibility further means being able to respond quickly to contain a breach and being confident in the quality of your regulatory reporting data.

$70.3M

is what the average organization has spent in the last year to ensure compliance with 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 potential consequences of a data breach



37%

Organizations still feel unprepared to deal with the evolving regulatory landscape, with over a third (37%) claiming that a lack of visibility and control of endpoints is the biggest barrier to maintaining compliance

Increased spending not solving visibility challenges

Nearly all (94 percent) of the IT decision makers surveyed have discovered endpoints in their organization of which they were previously unaware. And nearly three-quarters of CIOs (71 percent) say their teams discover new endpoints weekly.

A mere one-quarter (26 percent) say they feel completely in control of gaining instantaneous visibility of the devices on their network.

Complexity and "tool sprawl" perpetuate the gaps

The majority (91 percent) of respondents acknowledge fundamental weak points within their IT estate that are obstructing visibility.

These visibility gaps are being exacerbated by:

The report also found that organizations have implemented an average of 43 separate security and operations tools to manage their IT environments. Such sprawl further limits the effectiveness of already siloed teams and creates unnecessary complexity.

IT leaders have a false sense of confidence in their data

GDPR, CCPA, and other privacy regulations require notification and disclosure in the event of unauthorized access of personally identifiable information (PII). In the case of GDPR, it must be done within 72 hours.

However, IT leaders appear overconfident in their capabilities here. According to our research, most organizations believe they're well prepared for the implementation of GDPR (92 percent) and CCPA (67 percent) regulations. In addition, 90 percent of IT decision makers said they were certain they could report all required breach information to regulators within 72 hours. Nevertheless, with nearly half (47 percent) reporting they have challenges in getting visibility into computing devices connected to their network, this confidence appears to be misplaced.

Poor visibility leaves networks susceptible to disastrous outcomes

Visibility gaps can cause serious financial and reputational damage to organizations, respondents asserted. Slightly more than half (53 percent) say that endpoint blind spots can leave them exposed to cyber-attacks. And a third (33 percent) claim that they prevent teams from quantifying risk. Twenty-three percent raise the alarm over non-compliance fines.

Large numbers also suggest that visibility gaps can compromise the user experience (44 percent) and damage the brand (39 percent), all of which could even lead to customer churn by creating information gaps (31 percent).

A new endpoint vision for a new decade

GDPR and CCPA represent just the beginning of a complex new era of rigorous data-protection and privacy regulations. Organizations unable to manage and secure data flowing across their endpoints will face serious risks to the bottom line and corporate reputation.

While it's encouraging to see global businesses investing to stay on the right side of data privacy regulations, our research suggests that their good work could be undermined by inattention to basic IT principles. Many organizations seem to have fallen into the trap of thinking that spending a considerable amount of money on GDPR and CCPA is enough to ensure compliance. Yet without true visibility into, and control of, all their IT assets, they're leaving backdoors open to malicious actors. They will also be unable to prevent other forms of disruption, such as outages.

All of which makes it abundantly clear that technology leaders must regain control of their IT environment to minimize risk. They should do this not by purchasing more tools, but by focusing on fundamentals. This focus must start at the endpoint: the primary attack vector and failure point. Visibility into endpoints will help IT teams gain control of their environment and lay the foundations for effective risk management and regulatory compliance

IT leaders cite concerns that limited visibility of endpoints could:

How can CIOs and CISOs better prepare?

To help organizations ensure that they are on the right track, we suggest taking these important steps to build a unified endpoint-management and security strategy:

1

Instant endpoint visibility: Creating a single, unified view of the entire IT environment in real-time directly supports compliance and helps reduce risk. Having a complete view of all computer and data assets—including which machines are unpatched and vulnerable and where they are located—enables prioritization and immediate attention to exposed endpoints. It also accelerates incident response to contain a breach and ensures notification to regulators in 72 hours or less.

2

Stronger collaboration: It's crucial that IT operations and security teams unite around a common set of actionable data. The goal must be to empower individuals to ask questions about the state of every endpoint across the enterprise, retrieve data on their current and historical states, and execute change as necessary—all within seconds.

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 immediately. Proactively preparing for sensitive data-management and data-privacy regulations will ensure resilience should an incident ever occur.

By following this path, organizations can create a best-practice security and IT-operations culture that will help to support digital transformation, agility, and business growth long into the future. In sum, it must be understood that, as digital growth continues to expand visibility gaps and regulators sharpen their scrutiny, there's no time to waste.

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

Tanium gives the world's largest enterprises and government organizations the unique power to secure, control and manage millions of endpoints across the enterprise within seconds. With the unprecedented speed, scale and simplicity of Tanium, security and IT operations teams now have complete and accurate information on the state of endpoints at all times to more effectively protect against modern day threats and realize new levels of cost efficiency in IT operations.

tanium.com

@Tanium

info@tanium.com