TANIUM

Insights Study

The Crisis Of Visibility: Do IT Security Teams Really Understand What's Happening On Their Networks?

Exclusive data from

IDG CONNECT

Introduction

Even before the arrival of COVID-19, IT organizations were struggling to manage and secure increasingly complex network environments. COVID-19 has brought with it, large-scale working from home and in many cases, significant investment in cloud technologies by organizations adjusting to shifting patterns of consumer demand. Overnight, the world has become a lot more complex for many security and operations teams.

How well are IT organizations coping with these new realities? How good is their visibility into the network? What do they know about endpoints and how quickly can they recognize and shut down new threats?

Security has always been about resourcing defenses to the point at which risks are reduced to an acceptable level. But what was acceptable yesterday may not be acceptable today or tomorrow, against the backdrop of an increasingly complex IT environment.

The following analysis suggests that overconfidence is an issue for some IT organizations. Now more than ever, security organizations and corporate leaders need to reconsider not just their risk assessments but also the technologies they depend on to manage those risks down to an acceptable level.

“

Security has always been about resourcing defenses to the point at which risks are reduced to an acceptable level. But what was acceptable yesterday may not be acceptable today or tomorrow, against the backdrop of an increasingly complex IT environment.

What are the Biggest Challenges to Remaining Compliant With Data Protection Regulations?

Criteria: Please select up to three options, identify one as the most important

52%
Silos between IT operations and security teams

47%
Slow processes or tools that prevent an effective assessment of our environment

44%
Lack of tools to do a complete audit of the IT ecosystem

44%
Lack of visibility into all our endpoints

41%
Inability to enforce policies to ensure compliance

38%
Too many tools we are struggling to manage

23%
Not clearly understanding where our sensitive data resides

1%
No challenges exist to maintaining compliance

The Challenges of Data Protection Compliance

We asked respondents to identify up to three barriers that make it difficult to remain compliant with data protection regulations. The fact that 92% of respondents selected three barriers from the list (rather than one or two), suggests that there is no shortage of challenges in remaining compliant. Each option we offered respondents, apart from one, was selected by at least 40% of respondents. [1]

The challenge most frequently selected by respondents (52% of them) was the persistence of silos between security and operations teams. This was something on which executives within IT largely agreed: half or more of both constituencies selected this as a major challenge.

Notably, the problem is not so much difficulty in terms of humans collaborating with one another (elsewhere in the survey, we asked whether improving this aspect was a priority for the coming year. Only 9% agreed that it was). Instead, what seems to hamper collaboration are the hard-to-compare read-outs from siloed tools and data sources on either side of the divide. Both sides would undoubtedly benefit from access to a single, shared, source of truth.

Once we set aside the operations and security divide, we encounter harder-edged complaints. Around half identified as barriers slow processes or tools that prevent effective ecosystem assessment (47%), lack of the tools required to complete a full audit (44%) and lack of visibility into all of their endpoints (44%). In the end, all three of these complaints boil down to one word: visibility.

These are alarming findings, even more so because these views are held by roughly equal numbers of operations and security professionals, and because – with a few exceptions – they are held by respondents regardless of whether their organization operates a small number of security tools, or a very large number of them. Not for the first time in this survey, as we'll see, using a large number of security tools does not necessarily generate higher levels of confidence in an organization's ability to deal successfully with threats.

1. The exception, identified as a barrier to data compliance by 23%, was "not clearly understanding where our sensitive data resides".

Visibility Gaps Between IT And Security

One of the positives uncovered by this survey is the way in which IT operations and security teams broadly think in similar ways about security. For example, the responses of both groups track one another closely when asked about levels of confidence in their organization's ability to identify devices on the network.

But when we asked about more concrete scenarios, perspectives began to diverge.

For example, 47% of IT operations professionals say they are very confident in their organization's ability to accurately assess its IT risk posture. Only 38% of security professionals we surveyed agree.

Another area of divergence is the risk introduced by widespread working from home during the COVID-19 pandemic. Two-thirds of IT operations respondents (65%) regard this as challenging to assess, compared with 75% of IT security professionals.

Overall, IT security professionals are less confident than their colleagues from operations about their organization's ability to gain visibility into endpoints.

For example, three out of 10 security professionals (31%) told us they could only be confident that their organization enjoyed visibility into a maximum of 75% of endpoints. Only 22% of IT operations professionals agreed that their endpoint visibility rate was this low.

To some extent, differing job roles make these differences of perspective understandable. What's more concerning is the aggregate picture.

Overall, only 30% of respondents felt confident of their organization's ability to gain visibility into more than 85% of endpoints.

Two things are worth noting here. First, the fact that such a large number of organizations don't hit the 85% threshold for visibility. Second, we need to confront the question of how many more endpoints exist than those imagined by respondents. Given what respondents tell us about the size of the challenge inherent in identifying endpoints, it's hard to argue with the proposition that in the vast majority of organizations, a very substantial number of endpoints remain unknown and unmanaged.

Please Complete the Following Statement: I Feel Confident That We Have Visibility Into...

Criteria: Please select one of the following options

43.5%
76-85% of endpoints on our networks

26%
50-75% of endpoints on our networks

25%
86-90% of endpoints on our networks

4.5%
Over 95% of endpoints on our networks

1.5%
< 50% of endpoints on our networks

Organizations Using Many Tools Take More Time to Quarantine Suspicious Assets

Low tool usage organizations (up to 20 tools)

High tool usage organizations (more than 21 tools)

Adding More Security Tools Doesn't Necessarily Make You More Secure

If an organization uses more security tools, does this mean it is more secure? We asked respondents to answer this question directly. Their response? Overwhelmingly, they agreed (48% strongly agreed and 42% agreed).

On one level, it's hardly a surprise that running a large volume of tools should engender a sense of confidence. But we believe these high tool usage organizations need to temper their confidence levels.

We say this because the data also points very clearly to the challenges of using a large volume of fragmented point tools. In fact, if we look across all of the questions we asked in this survey and analyze the responses from only those organizations using large numbers of tools, it becomes very clear that these organizations perform worse, overall, than their low tool usage counterparts when it comes to basic security operations.

Using a large volume of standalone tools can create challenges with diagnosis. Reading across from the results generated by one tool to those produced by another can be fraught with difficulty. If security and operations teams are using different tools for similar tasks, it can take time to reach a consensus. The absence of a single version of the truth very often creates additional overhead in terms of the time and effort required for breach detection and remediation.

This may explain two findings in our survey among others. First, as we'll see in the next chapter, we asked respondents to tell us, on average, how long it took their organization to quarantine suspicious assets on their network. The data suggests a clear correlation: the more tools an organization uses, the longer it takes, on average, to quarantine suspicious assets. Organizations using fewer tools get the job done faster.

The second finding involves respondents' confidence in their ability to detect a breach among their distributed workforce as it happens. Here too, organizations that use a large number of tools have reason to feel less secure. For example, 34% of respondents in organizations using 21-30 tools are confident in their ability to detect breaches in real time. Among organizations using a smaller number of tools (i.e. 6-10), the number of respondents confident in their ability to immediately detect breaches rises to 42%.

A profusion of tools does not necessarily confer additional security benefits. What it may confer, however, is additional overhead in terms of the time and effort required for breach detection and remediation.

Operations: Detection, Remediation, Time-To-Quarantine

Beyond the traditional enterprise network perimeter, millions of employees worldwide began working from home during the pandemic. Many show little sign of wanting to return to the office full-time. As a result, it's clear that many IT teams will be expected to secure both long-term working from home and hybrid workforces. In addition, increasing numbers of organizations are running mainstream applications on SaaS, IaaS and PaaS, resulting in a significant rise in the volume of data in transit across external networks.

The enterprise network perimeter long ago ceased to be a definitive boundary. Endpoints are the new currency. And yet, as we've seen, a large proportion of enterprises fear that many endpoints remain invisible to them. As many as 75% describe gaining access to data from all endpoints (on-premises and in the cloud) as very challenging or challenging.
Against this backdrop, how do organizations perform when it comes to detection and remediation?

For a majority of organizations, the answer is clear: not particularly well. Less than half of respondents say they are very confident about their organization's ability to detect a breach as it happens (40%), remediate against a breach in real-time (38%) or take control of any endpoint on their network (45%).

We asked our respondents how long it takes, on average, to quarantine a group of suspicious assets. To identify the top performers, we asked whether respondents' organizations can typically impose quarantine within an hour of detection. Only 4% say their organization can achieve this within one hour on average.

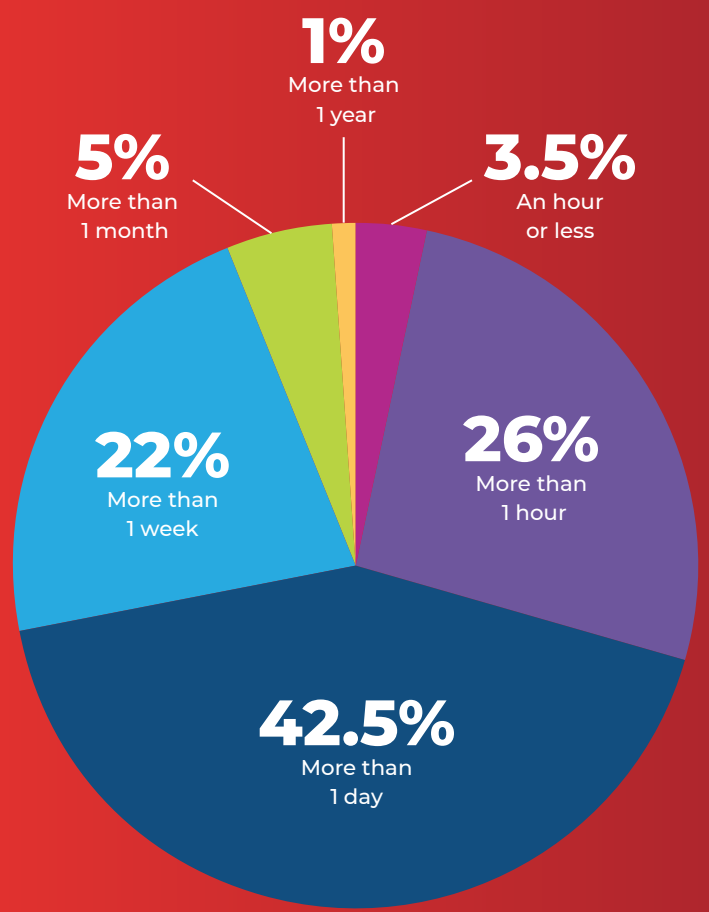
The number of organizations able to impose quarantine within an average of one day was surprisingly low: just 30% in total.

This leaves the largest single group of respondents (43%): on average, these organizations are only able to quarantine suspicious assets at some point between one day and one week after detection. In addition, a further 28% take more than one week to do the job.

Here, too, we detected divergence between IT operations and their security colleagues. Operations professionals tend to have lower expectations about the speed with which their organization is able to deal with suspicious assets. By contrast, IT security professionals are noticeably more confident about the speed with which they can nullify threats.

On Average, How Long Does it Take Your Organization to Quarantine a Group of Suspicious Assets?

Criteria: Please select one response



Percentage of respondents

How Would You Rate Your Level of Confidence in the Following?

Security capabilities	Very confident	Confident	Somewhat confident	Not confident	Unsure
Ability to accurately assess our overall IT risk posture	42%	39%	17%	2%	0.3%
Ability to effectively communicate our IT risk posture to leadership and or board	42%	39%	18%	1%	0.3%

Criteria: Please select one response per row

Analyzing Risk Posture and Reporting the Results Upward

We have already seen that many enterprises suffer from significant challenges with visibility across their network. Many grapple with data protection because of slow tools, processes and operational silos dividing security and operations. Time-to-quarantine can be remarkably long. The evidence is cumulative and convincing: enterprises simply don't know enough about what's happening on their networks and sometimes struggle to respond quickly.

If this is the case, how confident are respondents in their ability to assess their organization's overall IT risk posture when asked to do so by corporate leaders?

The answer: they are surprisingly confident. In fact, 80% of respondents overall say they are confident or very confident about the accuracy of their risk assessments. The percentage of IT operations professionals expressing these views is slightly higher than the average (83%), and the percentage of IT security professionals agreeing is slightly lower (78%).

Among one group, however, confidence is noticeably lower. Our question about risk posture assessment asked respondents to say whether they were "very confident", "confident", "somewhat confident" or "not confident" about the accuracy of their organization's IT risk posture assessments. Specifically, senior leaders (i.e. CIOs, CTOs and CSOs) are less likely to be very confident about their organization's risk assessments, and far more likely to be just confident. It is surely no coincidence that this group – containing CSOs and close colleagues – should sound such a note of caution.

Overall however, a contrast remains. On the one hand, respondents express what can only be described as relatively high levels of confidence in their organization's ability to get the job done (whether this be in the case of detecting threats, remediating them or generating IT risk assessments). Psychologically, it's not hard to imagine corporate norms, pride in colleagues' achievements and esprit de corps playing a role here.

On the other hand, when we ask respondents about the challenges they need to confront in order to get the job done, a different picture emerges, involving fragmented toolsets, limits to visibility and operational silos.

In the world of enterprise IT security, this contrast between big challenges and high levels of confidence is nothing new. Under the twin impact of COVID-19 and accelerated cloud transition, the question is how long this psychological balancing act can remain undisturbed.

84%

say they strongly agree or agree on the need to move endpoint security to the cloud

Securing a Distributed Workforce for the Long-Term

The experience of COVID-19 already casts a long shadow over future security strategies. When we asked our audience to identify the single most important priority for their organization in the next 12 months, three requirements dominated: accelerating detection, response and remediation (identified by 27%), identifying and managing shadow IT (20%) and improving network visibility (18.5%).

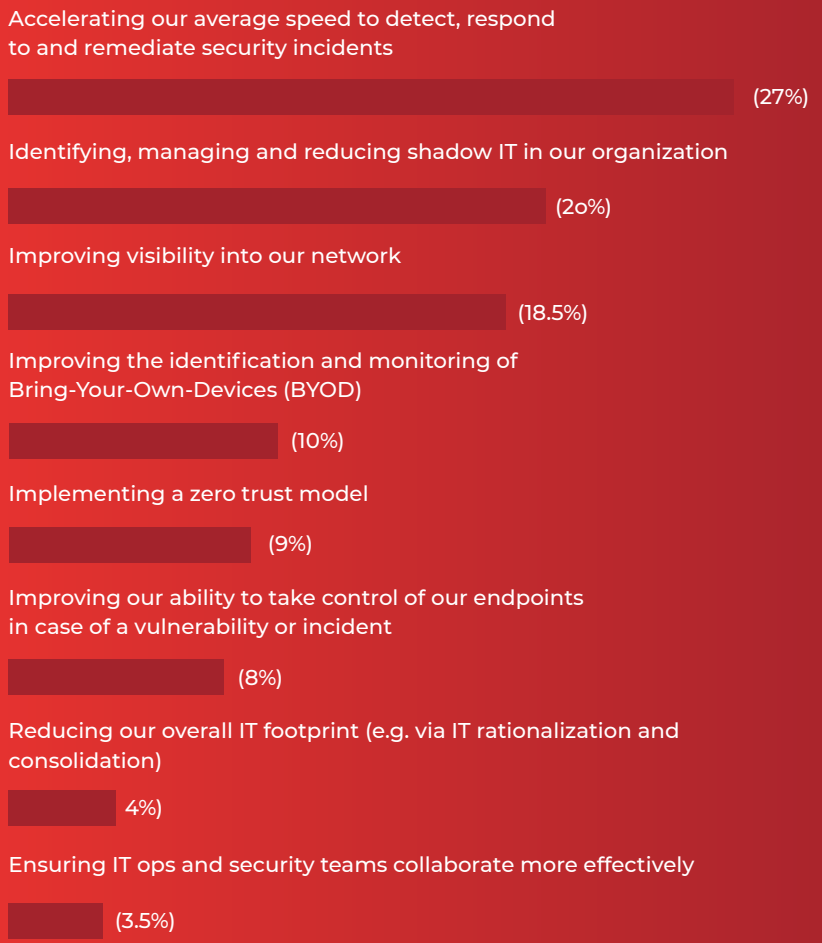
Very large majorities agree or strongly agree on the need for the adoption of new approaches. For example, 84% say they strongly agree or agree on the need to move endpoint security to the cloud. IT security decision-makers have a tendency to endorse this approach more strongly than IT operations decision-makers, but overall, this argument is settled. Only a tiny minority of respondents disagree with the case for managing endpoints in the cloud.

89% say that implementing a zero-trust approach to security should be a priority for their organization. In this case, there's little or no disagreement between IT operations managers and their counterparts who are more closely aligned with IT security.

In both cases a similar proportion of respondents say that these steps are already a priority for their organization. To argue for these improvements is to push at an open door.

In turn, this helps to explain why 52% of respondents say that their IT security budget for 2021 has increased significantly compared to 2020. Beneath that global average, the regional numbers look broadly similar, with the exception of respondents in Asia, where 64% told us that significant budget increases are planned for 2021.

Which of the Following Actions do You Consider Most Important to Securing a Distributed Workforce During the Next 12 Months?



Percentage of respondents

Criteria: Please select up to three options, identify one as most important

Conclusion

IT security brings with it significant challenges. The results of this survey suggest another fact of life: relatively high levels of confidence in the ability of IT organizations to cope with those challenges.

In many ways, this is the sector's defining dynamic, one that is driven by the creativity of attackers, and the need for security professionals to respond with accurately-calibrated risk assessments. Budgets are not infinite. Risk management involves the calculation of fine margins.

However, we may be approaching a turning point. It's clear that many security professionals are struggling to secure the minimum viable levels of visibility across increasingly heterogeneous networks. Employees are increasingly working in a hybrid fashion – partly from home, partly in the workplace –a persistent trend that will outlast the pandemic. The widespread adoption of cloud technologies to cope with changes in consumer behavior during the pandemic has altered the attack surface, too.

Some of these changes result from the acceleration of long-term plans, while others can fairly be described as improvised responses to the pandemic. In this rapidly-changing environment, the need for a next generation approach to security that guarantees visibility and secures all endpoints is paramount. Our respondents can see the risks clearly: 51% told us that identifying, managing and reducing shadow IT was one of the most important things their organization could do in order to secure a widely-distributed workforce over the next 12 months.

When IT security teams are facing significant new risks, the fragmented and limited tools that respondents found very challenging to use pre-pandemic, may become just too challenging in its wake. The search for better solutions – including those that offer a single source of truth – is proceeding apace.

Tanium offers a unified endpoint management and security platform that is built for the world's most demanding IT environments. Many of the world's largest and most sophisticated organizations, including nearly half of the Fortune 100, top retailers and financial institutions, and six branches of the US Armed Forces rely on Tanium to make confident decisions, operate efficiently and effectively, and remain resilient against disruption. Tanium has been named to the Forbes Cloud 100 list of "Top 100 Private Companies in Cloud Computing" for five consecutive years and ranks 10th on FORTUNE's list of the "100 Best Medium Workplaces."

About this survey IDG Connect undertook this survey of 308 IT decision-makers worldwide in May 2021 on behalf of Tanium. All respondents work within IT organizations in enterprises employing between 1,000 and 25,000 staff. 61% of respondents told us that their roles were most aligned with IT security, and 39% were aligned with IT operations. One-fifth of respondents were CIOs, CTOs or CSOs. Other respondents included executive vice-presidents, senior vice-presidents, vice-presidents and IT directors.


TANIUM
tanium.com
@tanium
sales@tanium.com