

# Strained Relationships Between Security And IT Ops Teams Leave Businesses At Risk

Security And IT Ops Teams With Strained Relationships Struggle  
To Maintain IT Hygiene And Resolve Critical IT Issues

Get started →

## A Lack Of Collaboration Plagues IT Teams

IT leaders today face pressure from all sides. They must maintain compliance with an evolving set of regulations, track and secure data across devices, and manage a dynamic inventory of physical and virtual assets, all while fulfilling an executive mandate to make technology an enabler for growth. To cope with this pressure, many have invested in a number of point solutions. However, these solutions often operate in silos, straining organizational alignment and inhibiting the visibility and control needed to protect the environment.

As a result, IT leaders often settle for visibility and control that is “good enough,” leaving them vulnerable to attack. Many teams base cybersecurity decisions on data that is largely incomplete, indicative of a false confidence in tools and processes. Using a unified endpoint management and security solution that centralizes device data enables companies to accelerate operations, enhance security, and drive collaboration between security and IT ops teams.<sup>1</sup>

## Key Findings



Two in three enterprises (67%) say driving collaboration/alignment between security and IT ops teams is a major challenge. The strain put on this relationship widens visibility gaps and impedes issue resolution.



Only 51% of enterprises are confident of their visibility into risks, yet 89% have confidence in reporting that is based on this data.






Decision makers believe a unified endpoint management and security solution will increase security and IT ops alignment (48%), create faster response times to issues (53%), and improve data integration (49%).

## Have IT Investments Actually Paid Off?

It comes as no surprise that 81% of enterprises are very confident their senior leadership/board has more focus on security, IT ops, and compliance than they did two years ago. This has resulted in increased budgets and resources for remediating and identifying vulnerabilities. Enterprises that reported a budget increase saw a slightly larger increase in their security budget (18.3%) than their operations budget (10.9%). Teams that purchased additional security and operations products procured an average of five new tools (security: 5.0; operations: 5.1). Many have invested in numerous point solutions to drive continuous compliance, increased security, and advanced digital transformation. But the question remains — do these investments solve critical IT issues, or do they further widen the gaps between teams? Are these investments providing services to the entire organization, or only to a select few teams? And most importantly, are these tools fostering or inhibiting collaboration?

## Top changes IT teams have made to adapt to increased enterprise data and cyberattacks, in the past two years

- 1  Increased IT security budget
  - 2  Increased resources and effort around remediating vulnerabilities and risk in our environment
  - 3  Increased resources and effort around identifying vulnerabilities and risk in our environment
- TIE 
- 3  Invested in solutions and processes to further enrich the endpoint data we maintain

## False Confidence: Visibility Gaps Persist Despite Increased Investments

Most teams are confident in their ability to run critical IT processes. However, further investigation shows teams are admittedly suffering from visibility gaps, which undermine these efforts. Despite 80% of IT decision makers being confident they can instantly take action on the results of their vulnerability scans, with even more (89%) stating they can report a breach within 72 hours, only half believe they have full visibility into the vulnerabilities and risks (51%) and hardware and software assets (49%) in their environment. How effective can a process be if the underlying data on which the process runs is incomplete? There is misplaced confidence in processes and operations. With only 51% confidence in asset and vulnerability visibility, organizations are essentially leaving their security to a coin flip!

### “Rate your level of confidence regarding IT environment and IT/operations staff.”

(Fully/mostly confident options shown)

#### HIGH CONFIDENCE IN PROCESSES

89%

“Our organization can report a breach within 72 hours.”

80%

“We can instantly take action based on the results of our vulnerability scans.”

76%

“The results of our vulnerability scans are being seen by the appropriate team and quickly acted upon.”

#### LOW CONFIDENCE IN VISIBILITY

61%

“The data we collect from our vulnerability scans is up to date.”

51%

“We have full visibility into the vulnerabilities and risks in our environment.”

49%

“We have full visibility into all the hardware and software assets connected to our IT environment.”

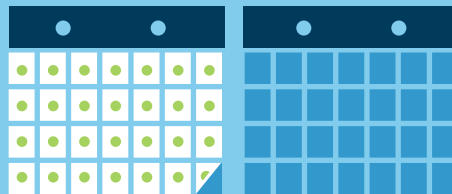
## Strained Relationships Between Security And IT Ops Have Material Impact On IT Hygiene

Visibility gaps and tool variety make driving alignment between teams difficult. Two-thirds of enterprises (67%) say driving collaboration and alignment between security and IT ops teams is highly challenging. This lack of collaboration between teams has a material impact. Four in 10 (42%) businesses with strained relationships consider maintaining basic IT hygiene more of a challenge than those with good partnerships (32%). Security and IT ops teams with strained relationships take 37 business days to patch IT vulnerabilities. That's 33%, nearly two weeks, longer than it takes teams with healthy relationships (27.8 business days) — a tangible consequence of these strained relationships. With this much at stake, why are organizations failing to address the rift between security and IT ops?

### Average business days in IT vulnerability patching lifecycle

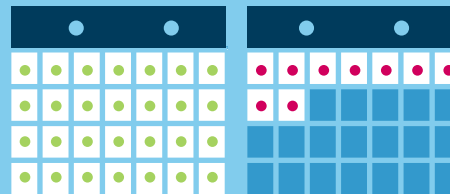
(Includes patching vulnerabilities, scanning and rescanning environment, and reporting on patches)

#### SECURITY AND IT OPS TEAMS WITH HEALTHY RELATIONSHIPS



27.8 average business days

#### SECURITY AND IT OPS TEAMS WITH STRAINED RELATIONSHIPS



37.0 average business days

## Misplaced Confidence Leads To Debilitating Consequences

Misplaced confidence, strained relationships, and complex IT environments have a material impact on a business's cybersecurity posture. Four of the top five challenges that IT leaders face relate to visibility and data quality. Businesses must have good visibility to act on threats, but 71% report challenges in gaining complete end-to-end visibility of endpoints and their health. Poor visibility can have business-level consequences relating to IT hygiene (74%), agility to secure the business (68%), vulnerability to cyberthreats (67%), and collaboration between teams (65%). Given the effect these visibility gaps and strained relationships have on a business's security posture, it is time businesses seek a new approach to endpoint management and security.

### Challenging tasks for security and IT ops

(Very and extremely challenging results shown)

Stitching together data across IT systems to generate actionable insights **(76%)**

Identifying new/unmanaged assets that we were not aware of **(74%)**

Getting real-time data on our environment **(71%)**

Extracting ROI from our existing tools and resources **(71%)**

Gaining complete end-to-end visibility of endpoints on our network & their health **(71%)**



### Consequences of challenges

(Extreme and significant negative impact results shown)

IT hygiene **(74%)**

Ability to operate with the speed and agility our business requires **(68%)**

Vulnerability to attacks and cyberthreats **(67%)**

Ability to scale to the level that our business requires **(66%)**

Alignment and collaboration among teams within our organization **(65%)**

## Endpoint Visibility Strengthened By Unified Endpoint Management Platforms

A unified endpoint management and security platform — a common tool set for both security and IT ops — helps alleviate the challenges introduced by tool sprawl and poor collaboration. A unified endpoint solution allows enterprises to operate at scale (59%), decrease vulnerabilities (54%), and improve communication between security and IT ops teams (52%). In fact, companies with weaker security and IT ops relationships are nearly twice as likely to cite the reduction in number of point solutions as a benefit of a unified endpoint solution, compared to those with healthier relationships (53% vs 29%). These benefits lead to faster response times (53%) and more efficient security investigations (51%), while improving visibility through improved data integration (49%) and accurate real-time data (45%). These benefits improve collaboration to address critical issues and help solve for the lack of visibility across teams.

### Benefits of a unified endpoint management and security solution

#### BUSINESS BENEFITS

Ability to operate at scale (59%)

Decreased vulnerability to attacks (54%)

Improved IT hygiene (52%)

#### TECHNICAL BENEFITS

Faster response times to issues (53%)

Efficient IT security investigations (51%)

Improved data integration (49%)

Secure operations (49%)

## Unified Endpoint Platforms Increase Collaboration Between Security And IT Ops

IT decision makers agree with the benefits of a unified approach to endpoint management and security. They agree this approach could relieve tensions between teams, helping them improve visibility, strengthen workflows, and avoid having to “run around each other.” Ultimately, such an approach would reduce risk and improve a firm’s security posture.

### Relationship benefits of a unified endpoint solution

Improved communication between security and IT ops teams **(52%)**

Increased alignment and collaboration between security and IT ops teams **(48%)**

### On having a common tool set for security and IT ops:

“I think with these collaborative capabilities, one can **defend against security breaches and proactively identify and mitigate security risks.**”

“The **relationship between security and operations would change drastically.** We will be able to secure critical information without any double thoughts.”



“It would help **tremendously** because right now they’re having to basically **run around each other.**”

“This clearly is the **best way to improve communication** between both security and operations teams.”

“Easily **detect, understand, and act on** endpoint threats.”



## Conclusion

Today, security and IT ops teams have a false confidence built on an incomplete view of their environment. These visibility gaps are further widened by teams' strained relationships. A unified endpoint platform will align teams and provide a complete view of the environment, thus strengthening workflows and having a significant impact on business outcomes. Our study revealed that:

- Strained relationships between security and IT ops leave businesses at risk. A unified endpoint platform reduces risk by aligning teams and driving collaboration.
- Despite poor visibility into their environment, decision makers are still confident in their ability to take action. Unified endpoint platforms heighten visibility and increase the impact of actions and key processes.
- A unified endpoint platform provides visibility into risks and vulnerabilities so teams are able to act and react appropriately to threats.

### **Project Director:**

Emily Drinkwater,  
Market Impact Consultant

### **Contributing Research:**

Forrester's Security &  
Risk research group

## Methodology

This Opportunity Snapshot was commissioned by Tanium. To create this profile Forrester Consulting supplemented this research with custom survey questions asked of 415 global IT decision makers responsible for or with insights into endpoint security. The custom survey was completed in September 2019.

### ENDNOTES

<sup>1</sup> Source: Our use of endpoint refers to physical and virtual network-connected devices such as laptops, servers, containers, virtual machines, and cloud instances.

### ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit [forrester.com/consulting](https://forrester.com/consulting).

© 2019, Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. For additional information, go to [forrester.com](https://forrester.com). [E-45087]

## Demographics

### RESPONDENT LEVEL

C-level: **11%**

VP: **18%**

Director: **59%**

Manager: **12%**

### GEOGRAPHY

US: **49%**

UK: **32%**

Australia: **19%**

### TOP FOUR INDUSTRIES

Retail: **9%**

Manufacturing: **9%**

Telecom: **8%**

Technology: **8%**

### COMPANY SIZE (BY EMPLOYEES)

5,000-14,999: **62%**

15,000-24,999: **24%**

25,000-49,000: **10%**

50,000 or more: **4%**



FORRESTER®