Gartner Peer Community. Lookout

# Why Data Protection Requires a Fundamental Shift in Strategy

Here's the reality that IT and security leaders are faced with today: data sprawled across a decentralized infrastructure that stretches from SaaS applications, private clouds, to on-premises data centers. Users are working from anywhere and connecting to corporate resources from any network and device they prefer, often not controlled by IT.

Amidst this increasingly complex landscape, IT and security teams manage a complex security stack that includes a mixed bag of perimeter- and cloud-based point solutions.

Lookout utilized Gartner Peer Community to understand how IT and security leaders are faring amidst an accelerated digital transformation and hybrid work adoption.

Data collection: July 19, 2022 - January 3, 2023

Respondents: 542 IT and security leaders

## Top security concerns shaped by lack of control

With hybrid work and cloud adoption, IT and security leaders are finding it increasingly difficult to control what's entering, leaving, and happening within their infrastructure.


## Data sprawl and IT complexity challenge security leaders

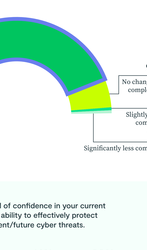
Sensitive data now resides across countless cloud apps and is more accessible than ever. But this means it's harder than ever to enforce security, especially as organizations deal with a fragmented security stack.


**Other responses include:**
Securing cloud and web access **38%;** Protecting sensitive data while enabling productivity **32%;** Keeping up with regulatory compliance/data privacy laws **31%;** Visibility into shadow IT (unsanctioned apps and devices) **24%;** Keeping up with vulnerabilities, zero-day threats and/or vendor security updates and patches **23%;** Having enough security personnel to handle our security needs **19%;** None of the above **0%;** Other **0%**

## Data breaches aren't going anywhere

With a much more complex environment to manage, breaches are becoming a common occurrence.

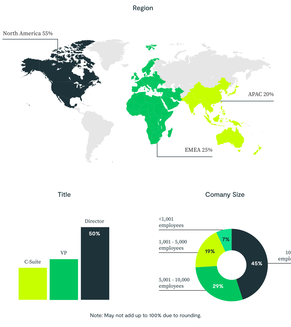
Has your organization suffered data breach (malicious or accidental) in the past 2-3 years?




n=542
Note: May not add up to 100% due to rounding.

## Accidental insider threats contribute to breaches

Breaches don't have to start with a malicious act. With data sharing so seamless in the cloud, it's just as likely for employees to accidentally share sensitive information to unauthorized users.




**Other responses include:**
Credential theft or account compromise **2%;** Stolen or lost device **2%;**
HR data compromised via cloud-based human capital management system **2%;** Other **1%**

## Landscape complexity lowers confidence of security leaders

With an accelerated digital transformation and hybrid work adoption, IT and security leaders are faced with an increasingly complex security landscape, and lowered confidence in their ability to protect their data.







## Respondent Breakdown




Note: May not add up to 100% due to rounding.