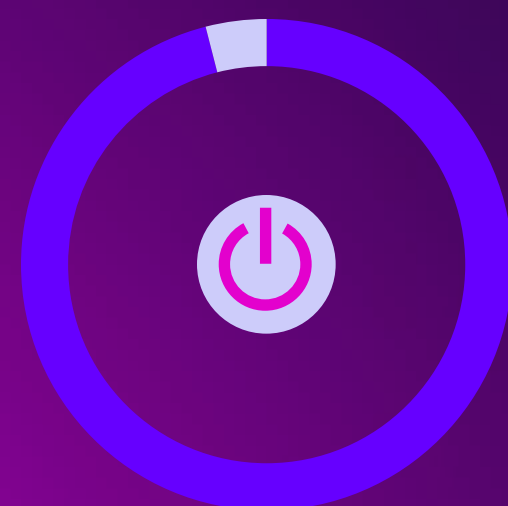


# DATA CONTEXT: THE RANSOMWARE GAME-CHANGER

In a live simulation, 100 security leaders responded to a ransomware crisis. Their decisions were tracked first without data context, and then again after being provided with detailed data insights, revealing a dramatic and measurable shift in their approach.

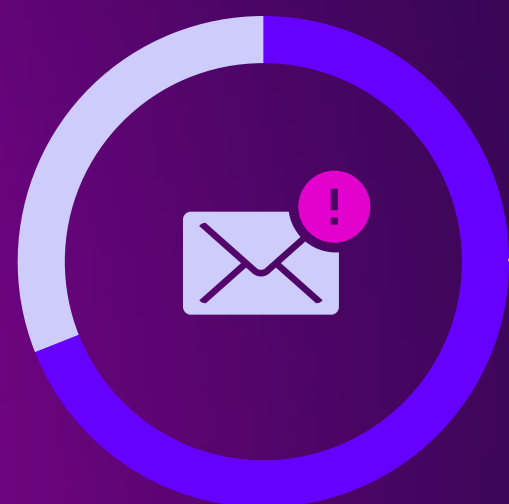
## DECISIONS WITHOUT DATA CONTEXT



**94%**

VOTE TO SHUT  
DOWN SYSTEMS.

This decision was based solely on  
observing a suspicious activity spike.



**69%**

1.3 MILLION CUSTOMERS.

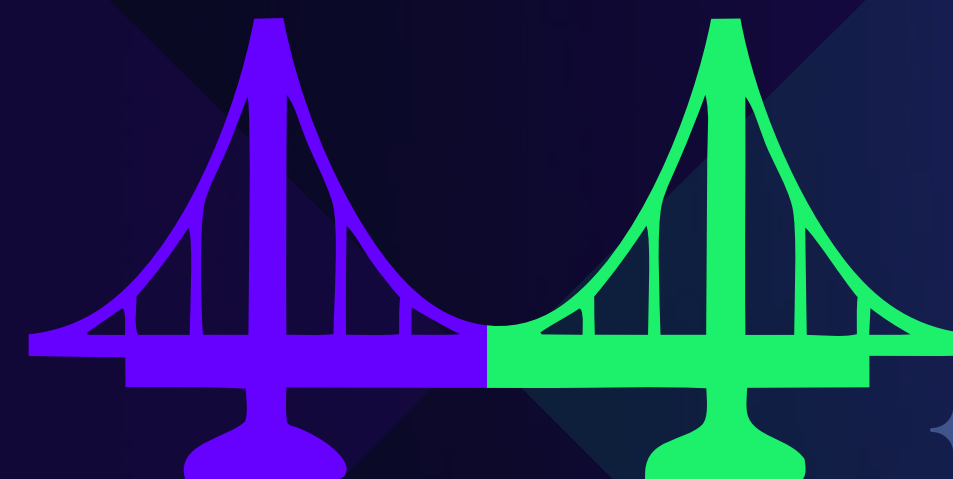
A massive over-notification planned due  
to uncertainty about the breach's scope



**MOST  
LEADERS**

LEAN TOWARDS  
PAYING THE RANSOM.

A common default reaction when  
critical information is missing.



See where you are and get the roadmap for  
where you want to be with a full-scope  
data risk evaluation.

## DECISION WITH DATA CONTEXT



**82%**

CORRECTLY IDENTIFY THE  
ACTIVITY AS HARMLESS.

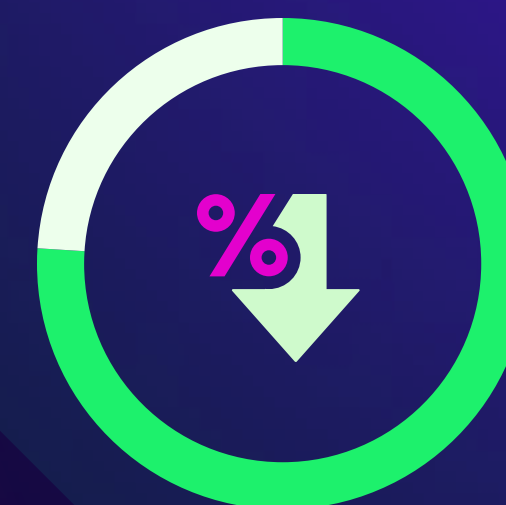
Context revealed the data was not at  
risk, preventing unnecessary downtime.



**91%**

REFUSE TO PAY THE RANSOM.

They were confident the attackers never  
actually accessed the sensitive data.



**76%**

REDUCTION

Customer Notifications reduced  
by 76% to **312,000** → **312,000**  
Customers