CODE42

Dissonance in Data Security

Why Traditional Security Tools Aren't Getting the Job Done

INSIGHTS FROM OVER 300 SECURITY LEADERS + CODE42 PERSPECTIVE

INTRODUCTION

THREATS RISING — DESPITE INCREASED SPENDING

The state of data security can be summed up by this troubling discord: breaches and security incidents continue rising, even as companies dedicate more resources to stopping them. Initial reports from the first half of 2019 show that overall data breaches increased by 54%[1] — and the Ponemon Institute found that insider threat incidents increased by 47% over the last two years.[2] These incidents are taking longer than ever to discover — an average of 279 days. Critically, these growing problems are not for lack of awareness or action. Companies are spending more than ever on cybersecurity, with cybersecurity spending increasing by almost 10% annually.[3]

Security leaders surveyed by Forrester reflect dissonance in data security

What accounts for this dissonance? To dig into that question, Forrester recently conducted a survey of IT and Security leaders of businesses with more than 1,000 employees across all industries. Forrester sought to understand:

- Security priorities companies are focused on now
- Tools they're using to tackle those goals
- Challenges they're encountering
- New solutions they're pursuing

The full Forrester survey study is available now, but here are three key takeaways — and two actionable insights that should be top-of-mind for Security and IT leaders as they look at 2020 and beyond.[4]

KEY TAKEAWAY #1

PRIORITIES ARE SHIFTING IN DATA SECURITY

One of the first Forrester survey questions asked respondents to compare why they bought a security tool against how they are currently using that tool. It's pretty clear that many companies are attempting to use DLP and CASB tools for an entirely different purpose than when they purchased the tools.

Top drivers of initial decision to buy DLP and CASB tools

1. Better control user access to data
2. Satisfy legal/compliance requirements
3. Reduce risk of insider threats

What companies are using DLP and CASB tools for today [4]

1. Better security threat visibility and monitoring
2. Improve detection and prevention of data-related attacks
3. Improve mitigation time when data loss occurs

Reading Between the Lines

Collaboration culture is moving the goalposts for data security

Scary statistics alone do not make a business case. To convince senior leadership and get top-down buy-in to implement a solution, most companies invested in DLP and CASB tools that were built to support traditionally clear data security objectives: Protect sensitive, regulated data by locking down access to that data, thereby reducing the risk of insider threats and stopping external actors. But the goalposts have moved. Digital business strategies have created a collaboration culture. Work increasingly happens via cloud- and web-based apps — driven by unprecedented and rapidly increasing levels of user, device and data portability.

Enabling that collaboration culture is critical to business success — and that means security and IT leaders can not simply categorize what's valuable and sensitive and block access or movement of that data. Companies want their users to work efficiently and productively, and that means security and IT need to enable collaboration and empower user mobility and ingenuity. Instead of stopping risks by categorically blocking abnormal activity, security and IT teams are increasingly prioritizing threat detection, investigation and response. In other words, they're embracing the "trust but verify" approach to find the right balance between user enablement and risk mitigation.

KEY TAKEAWAY #2

DLP AND CASB AREN'T SUITED TO NEW DATA SECURITY OBJECTIVES

After establishing that companies are using DLP and CASB tools to pursue the new objectives of their insider threat programs, Forrester asked how that approach was going. Less than 1 in 4 respondents said their DLP and/or CASB tools were significantly helping them — and nearly half (43%) said that DLP and CASB tools were actually hurting their efforts.

Biggest DLP/CASB Pain Points

1. Data identification/classification on collaboration apps, in the cloud and on endpoints
2. Creating/updating rules and policies
3. Noisy risk signal/alert fatigue
4. User workarounds & policy exceptions create gaps

How can security tools impede data security efforts?

Because these policy-based security tools are challenging to apply to the dynamic nature of detecting, investigating and responding to risk within modern collaboration culture.

77%
say DLP/CASB capabilities are **TOO DIFFICULT** to implement, maintain and administer

55%
say they **LACK THE TIME/ PERSONNEL** to manage DLP/CASB tools [4]

KEY TAKEAWAY #2

READING BETWEEN THE LINES

Policy-based tools creating headaches — and blind spots

While their priorities have shifted, security and IT leaders are still trying to make the most of their investments in DLP and CASB tools — even though they know these tools are much better suited to supporting legal compliance and locking down sensitive data than to detecting and responding to more-subtle insider threats. This square-peg-round-hole approach is frustrating security and IT teams as they try to create and update policies that keep up with their dynamic users and evolving businesses.

But here's a bigger problem: those frustrations are fueling rapidly expanding blind spots for security and IT teams. They already recognize that their existing policies are missing risk because of user workarounds and policy exceptions. But those policies fall further behind every day because security and IT teams 1) don't know where all their data lives, and 2) can't keep up with the business critical ways users are moving and sharing that data. In other words, the fatal flaw of a policy-based security tool is that it only sees what it's told to look for — and collaboration culture makes it harder than ever to put clear parameters around valuable data and risky behavior.

Moreover, isn't the purpose of an intelligent security tool to help you see risks and threats that you aren't looking for?

KEY TAKEAWAY #3

COMPANIES ARE LOOKING FOR NEW TOOLS TO FIT THEIR NEW PRIORITIES

The good news is that more and more security and IT teams are recognizing that their existing security tools can't effectively address their new priorities. The Forrester survey found that nearly 40% of companies are looking to add new security tools to improve their detection, investigation and response capabilities.

38%
of companies plan to add
NEW SECURITY TOOLS
to improve incident
DETECTION, INVESTIGATION AND RESPONSE [4]

Reading Between the Lines

Single-focus tools aren't the answer — the data, the user, and the vectors all matter

Forrester also asked security and IT leaders what types of tools they're using to fill in the gaps left by DLP and CASB tools. While many indicated they were using (or planning to use) tools that follow the data itself, such as endpoint detection and response (EDR) or file integrity monitoring, about half indicated that they were using user-focused tools such as user activity monitoring (UAM) or user behavioral analytics (UBA/UEBA). User-focused tools can be valuable for many security objectives — but they present their own set of problems when used for risk monitoring, detection and response. First and foremost, it proves exceptionally difficult to tune out the incredible noise of users' daily legitimate activity and create a high-fidelity risk signal. Then there are the complex privacy and culture concerns that come with surveillance of employees.

Ultimately, it is the data that you are trying to protect, but it's users who can put it at risk, often inadvertently — so your security tools should focus on all of those factors: users, data, and where data moves. The problem with DLP and CASB is that their policy-based approach is too limiting for the realities of risk in the collaboration culture. Security and IT teams need tools that look beyond a specified subset of valuable data to provide visibility to all data — on endpoints, in the cloud and on web-based apps. And those tools need to see all data movement — not just the risky actions that security and IT teams know to look for.

THE MISSING LINK: SIGNALS OF RISK

The simplest distillation of the Forrester survey results: DLP and CASB tools are not suited to monitoring, investigation and response because their outputs are too black-and-white for a modern world full of gray areas.

Traditional policy-based tools are designed to make an instant, firm decision, based on given criteria, about whether an action is risky or not. But the risks inherent in collaboration culture are much more opaque — and security decision-making is much more complex.

The key ingredient in enabling and accelerating effective detection and response to insider risk to data is analysis of the signals that data activity and movement can provide. Security and IT teams need data security tools that not only give them more comprehensive visibility to data risks at the user and organizational level, but also that know there's a difference between everyday collaboration and the events that represent real risk. These layers of detail provide the high-fidelity signal that helps security teams rapidly investigate and respond only to the threats that require investigation.

CODE42

The leader in insider risk detection and response

Corporate Headquarters | 100 Washington Avenue South | Minneapolis, MN 55401 | 612.333.4242 | code42.com

Code42.com/resources

[1] Norton
[2] Ponemon Institute: 2020 Cost of Insider Threats: Global
[3] Gartner
[4] Yesterday's Solutions Won't Solve Tomorrow's Data Security Issues: A Commissioned Study Conducted by Forrester Consulting on behalf of Code42, Date: June 2020