CODE42

Case Study

HEAR FROM A CUSTOMER:

UserTesting and The New Age of Insider Threat

"With the insight Code42 Incydr™ provides, we are able to quickly and easily determine what is normal behavior and what is an indicator of insider risk." — Dustin Fritz, Senior Security Architect at UserTesting

UserTesting

About UserTesting

UserTesting provides on-demand usability testing and research solutions through its human insight platform.

Industry: Technology
Headquarters: San Francisco, CA
Global Reach: 5 offices between 2 states & 3 countries

Challenges

- To protect corporate data without the traditional perimeter
- To improve security without sacrificing agility and collaboration
- To implement a strong data loss prevention program without losing employees' trust

Strategies

- Detect and respond to real data risk as it happens
- Enable employees to collaborate and work from anywhere without compromising security
- Build relationships with internal business partners to understand user behavior and data movement vectors

Results

- Proactive, security-minded internal stakeholders
- Data secured in just two months without disrupting employee productivity and collaboration
- Company-wide and user-based understanding of high-risk activity to effectively mitigate insider threats

UserTesting and the Evolving Security Landscape

As a high-growth tech company, UserTesting employees are constantly creating, moving and collaborating on critical intellectual property and customer data. To fuel and protect UserTesting's innovation, their security team partners with the business to ensure data security amidst their culture of agility, collaboration and employee enablement.

This collaborative culture is increasingly important for high achieving organizations like UserTesting to maintain their speed-to-market and competitive advantage. As the popularity of cloud applications and remote work increases, the ability to rely on a perimeter to secure sensitive data will continue to dwindle.

“Things are changing. People are not beholden to security the way they may have been 20 years ago. Not everybody is behind a firewall anymore,” says Dustin Fritz, Senior Security Architect at UserTesting.

"You’re going to have to deal with devices that you don’t manage, you’re going to have to deal with data you don’t expect and you’re going to have to deal with providing access to folks anywhere on the internet wherever they are. That’s the new world we live in.”

When Dustin joined UserTesting, he was tasked with selecting and implementing a solution to protect data from theft, misuse and exfiltration. From his past experience building data protection strategies, he understood the complexities of implementing traditional DLP—not to mention the sheer amount of time involved.

“With traditional DLP technologies, the average rollout period, in my experience, is two years, and we wouldn’t get the context we need,” says Dustin. “Many DLP technologies also have a lot of issues at that low-kernel level and actually crash other applications and there’s a lot of debugging and craziness that can go into that implementation process.” Based on his past experience, UserTesting’s culture and the modern security landscape, Dustin quickly realized that this was an opportunity to approach UserTesting’s data protection strategy differently.

Finding a Solution

Dustin’s visionary approach to data security for UserTesting meant finding a solution that would allow them to protect their data in a reality where the perimeter no longer exists, without impeding the high-performance culture ingrained in their company values.

UserTesting Values	Insider Threat Strategy
Get Better	Embrace change and learn new data protection methods that can keep the business thriving while keeping data safe
Drive Results	Provide transformational benefits through data loss prevention to secure data without slowing down innovation
Customers First	Protect customer and UserTesting data while enabling productivity and collaboration
Be Kind	Assume positive intent and help others to avoid high-risk behavior
Keep It Simple	Make it so fast and easy to protect customers and UserTesting data, that everyone does it all the time

When selecting a solution to protect data from insider risk, Dustin says, “I had to find a partner and technology that shares our values. We need to be able to trust our employees, but we also need to be able to have visibility into risky data behavior so we can inform, engage and educate, and, where necessary, be able to detect and respond to actual risks before they become an incident.”

This criteria led Dustin to Code42 Incydr™. “The big differentiator with Incydr is that it doesn’t block—it actually has nothing to do with blocking. It has to do with gaining insight into risky behavior and using that information to inform and educate users or address that risk before it turns into a data breach,” says Dustin.

"Other vendors in the space might have a mode of operation that doesn't block, but they only focus on specific types of data. What I'm more interested in is the underlying behavior. First, I want to understand the characteristics of data movement and then I can determine what the data is and how sensitive it might be," Dustin explains. "I've used other technology and there is no technology like Code42 that I've experienced."

UserTesting + Code42

The first step in UserTesting's data protection strategy was to deploy Code42 Incydr on all endpoints. "We rolled out Incydr in two months. I don't know anybody who's able to do that with a company of 500 people. Even if we had more employees, it probably still would have been two months because time was spent on education, communication and impact on the business processes, rather than deployment complexity. That was a huge win for me and for UserTesting because we found something that was quick to implement and a good fit for the way we work."

After a seamless implementation, UserTesting's security team could clearly see data movement across the organization, making it simple to assess their data risk. Dustin explains, "for me, it's about actionable intelligence. Looking at the risk exposure dashboard every day is helpful to get a sense of our baseline. With the insight Incydr provides, we are able to quickly and easily determine what is normal behavior and what is an indicator of insider risk."

In situations where insider risk is more likely, such as cases involving departing employees or employees with access to high-value data, Dustin and his team can quickly investigate the details of potential risk factors using Incydr's Risk Detection Lenses. "The lenses have a higher level of granularity because they have predefined alerts when you use the Departing Employee Lens or High Risk Lens. That gives us that extra level of context to assure that we're taking a proactive step in monitoring for high-risk data movements during critical points of the onboarding and offboarding process."

The Benefits

The insights that Dustin gains from Incydr help him to provide actionable details to internal partners including IT, engineering, legal, and HR. Together they can determine and take the right-sized response to each incident based on the full picture of data movement—whether malicious or unintentional.

According to Dustin, these partnerships strengthen data security for UserTesting because "there are cases where we have to reach out to our business partners or to different functions within the company to understand the context of risky data movement we've detected. That collaboration helps us know when we may have to educate the business unit on what types of behavior we want to promote or when a different response is in order."

Rooted in assuming positive intent, this approach to tackling data security challenges ensures that UserTesting enables a collaborative, performance-driven culture while securing the data that powers their competitive advantages at the same time.

Additionally, by taking culture into account, Dustin ensured UserTesting's security team maintains a positive relationship with employees, which in turn leads to a more effective security strategy. Dustin explains, "The one thing that kills a security team's work to protect the business is poor relationships with internal partners and colleagues because we blocked something. Even if it was a legitimately risky action, and even if blocking it was the right thing to do on paper, most people are just trying to get the job done and move the business forward. You want to build trust and avoid situations that don't contribute to that goal - it's better that employees are mindful, proactive, and actually reach out to security when they see something risky instead of just seeing security as a roadblock and bypassing security altogether."

Now, with Incydr and their partnership with other departments at UserTesting, Dustin and the rest of the security team have the visibility they need to understand how, where, when and what data moves in and out of their organization. "Without Code42 we would have no way to learn those things and pinpoint what areas we need to educate our employees on so they can help us decrease those risks to sensitive data." This actionable insight ensures UserTesting actively reduces their insider risk exposure both now and into the future of the new age of insider threat.

See Incydr for yourself at www.code42.com/product

Dustin Fritz, Senior Security Architect at UserTesting

As senior security architect, Dustin is responsible for data and infrastructure security practices across corporate IT and SaaS platforms. In his 20+ years of experience with various IPOs and SaaS companies, including CISO positions for government agencies, he has managed SOCs, developed risk programs, and built security teams from the ground up. Dustin holds a CISO executive certification from Carnegie Mellon University and BS in information systems security and MS in cybersecurity and information assurance.