VansonBourne observe it

Trust your people and verify with your technology

Trust is one of the cornerstones of everyday life. In today's highly collaborative working environment, we trust and depend on colleagues and partners to achieve personal and company success. To manage the risks associated with high levels of trust between employees and third parties, protectors of organizations (such as cybersecurity teams) need policies and tools to monitor and detect risky user activity and data movement.

Increasing trust within the workplace is key for business success

Nearly three quarters (73%) of surveyed senior IT decision makers report that trust is a core principle for their organization when it comes to keeping systems and data secure. The top intellectual property is produced by teams of smart people often spread across multiple locations. IT and cybersecurity have no choice but to expand the circle of trust beyond a small number of vetted technologies and privileged users. The survival of the business depends on this high level of trust.

Historically, the team of "No" and "Shadow IT"

In the past, IT and cybersecurity teams were perceived as blockers to the ease of conducting business because they relied on heavy-handed preventive controls. With this perception and the growth of cloud technologies, employees started buying and using software on their own without IT involvement. The technologies matched their needs but little, if any, consideration was given to risk. This led to a growing problem of "shadow IT" and significant gaps in the ability to protect users and data. Flying blind undermines cybersecurity's role as the protector of the organization.

Despite the majority of respondents stating that trust is a core principle in keeping systems and data secure, nearly half (46%) of senior IT decision makers believe their organization doesn't trust its workforce when it comes to information security. With the number of insider-related incidents on the rise, proactive cybersecurity teams are complementing prevention with detection and response technologies to verify that trust is not misused.

Balance trust and visibility

Senior IT decision makers feel their organization's clients and customers are more likely to care about cybersecurity (54%) as compared with their general employees (36%), contractors/freelancers (36%) and third-party vendors (35%). Poor security awareness in an organization often leaves it prone to data loss through credential theft from unprotected passwords or unprotected data on publicly accessible servers.

For a culture of sensible trust within the business, it is important that a balance is struck between gaining visibility into detecting risky actions early and blindly trusting employees will do the right thing. HR onboarding and offboarding policies alone aren't solving the problem.

When it comes to establishing visibility for early detection, the overwhelming majority (92%) agree that investment in new technologies, specifically for monitoring insider threats, will be crucial for them to keep their organization secure over the next 18 months. At the moment, only half (53%) of those surveyed are using technology that provides visibility into user and data activity to detect and respond to insider threats.

Conclusion

Organizations don't have an easy ride when it comes to the trust they place in their workforce. Not trusting them led to the uprising of shadow IT – yet without trust, businesses will flounder. To thrive in today's competitive landscape requires workforces to collaborate more and use critical corporate systems more than ever before. After all, from the manufacturing shop floor, through sales and marketing, to software developers, we are all reliant on technology to be more productive and make our lives easier.

It's easy to overlook the importance of verifying trust with technology that provides visibility and context into user actions. However, this can leave the organization open to the risk of losing data that is sensitive to the employees, customers and the business. Today's technology empowers cybersecurity teams to enable business and better protect employees, customers and the organization.

VansonBourne

observe it

Methodology

ObserveIT commissioned Vanson Bourne to conduct 600 interviews with senior IT decision makers on the topic of trust within the workplace. Respondents were from organizations in the private and public sector with 2,500+ employees, across the US (200), EMEA (200) and APAC (200).

About Vanson Bourne

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets.
For more information, visit https://www.vansonbourne.com

About ObserveIT

ObserveIT, the leader in Insider Threat Management, delivers comprehensive visibility into user and data activity providing security organizations with a powerful tool for protecting employees and valuable assets while saving time and resources. With more than 1,900 global customers across all major verticals, ObserveIT empowers security teams to proactively detect insider threats, streamline the investigation process and enable rapid response.
For more information visit: https://www.observeit.com