PULSE | Bravura Security

While IT and Security Leaders Are Embracing Automated IAM, They Are Doing So Too Late.

Ransomware and cyber attacks have surged over the past year due to a variety of factors – including the work-from-home boom which resulted in new security risks and technical challenges due to the lack of centralized security protections and less secure at-home internet connections. As businesses prepare for the post-pandemic economy and lay plans to return to the office, it's becoming increasingly clear that hybrid work models are here to stay. As a result, IT and security leaders must re-think and re-prioritize their cybersecurity needs due to the rising risk of threats in their network.

While many IT leaders (58%) use technology to continuously monitor their environment for identity and access risks, the vast majority (95%) have yet to put technology structures in place to proactively identify security risks. To combat the rising threat of cyber attacks, organizations should be more proactive in adopting automated identity access management systems.

Bravura Security and Pulse surveyed 100 IT executives to understand the gaps that exist within their current technology stack and how automation is aiding their cybersecurity improvements.

Respondents: 100 IT executives

CYBERSECURITY IS A PRIORITY FOR IT EXECUTIVES, AND ORGANIZATIONS ARE MONITORING FOR IDENTITY AND ACCESS RISKS

Improvement of cybersecurity as a priority has been accelerated due to COVID-19 for 98% of IT executives.

To what extent has the COVID-19 pandemic accelerated the improvement of your cybersecurity posture as a priority at your organization?

IT executives say they are able to proactively detect identity and access risk from devices (70%), accounts (63%), and identities (57%) with their current technology stack.

Which of the following types of identity and access risk is your current technology stack able to proactively and automatically detect?

58% of organizations use technology to continuously monitor their environment for identity and access risks—though only 5% say their technology proactively identifies security risks.

Which of the following best describes the method through which your organization currently identifies identity and access risks and exposures?

CURRENT TOOLS FOR IAM PROCESSES STILL HAVE AUTOMATION GAPS

While many of these leaders say they use an automated tool as part of their identity and access management (IAM) processes, IT executives are still experiencing gaps with automation when it comes to identity and access vulnerability discovery. Only 1% of respondents have a completely automated IAM process. The majority (59%) say only up to 50 percent of their process is automated.

How automated is your identity and access vulnerability discovery and resolution process today?

100% of IT executives believe discovering and mitigating identity and access threats is a pain point for their IT department's resources.

On a scale of 1-5 (5 being high), how much does discovering and mitigating identity and access threats drag on your IT/security department's resources today?

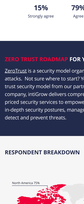
PRIORITIZING REMEDIATION IS STILL A MANUAL PROCESS

68% of IT executives use an automated solution once they've discovered a threat—though only 12% have a tool that proactively uncovers threats and provides solutions.

How does your team currently mitigate and remediate discovered identity and access threats?

When it comes to risk mitigation, IT executives (78%) are prioritizing vulnerabilities based on a standard security framework. Only 9% have a tool that automatically prioritizes the most critical risks.

Which of the following best describes your current method for prioritizing identity and access risk mitigation?



MOST LEADERS DON'T HAVE VISIBILITY INTO REPORTING AND METRICS

99% of IT executives don't have complete visibility into their organization's identity and access vulnerabilities and the success of their remediation efforts.

On a scale of 1-5 (5 being high), how much visibility do you have into reporting and metrics about the current state of your company's identity and access vulnerabilities—and the success of your remediation efforts?

As well, 99% of IT executives have experienced some level of difficulty integrating their identity and access risk discovery processes with their current security technology stack.

How challenging is it to integrate your identity and access risk discovery processes with your broader security technology stack?

To combat these challenges, 94% of IT executives agree that the access is a broad community of identity and access experts would improve how they understand and solve security threats.

To what extent do you agree with the following: "If we had access to a broad community of identity and access experts, we could better understand the security threats affecting us and better determine the appropriate resolution."

ZERO TRUST ROADMAP FOR YOUR ORGANIZATION

ZeroTrust is a security model organizations are adopting to prevent ransomware attacks. Not sure where to start? You're not alone. Get a roadmap for your zero trust security model from our partner, IntoGrow. A global enterprise security company, IntoGrow delivers comprehensive security solutions and competitively priced security services to empower you to achieve business-enabling defense-in-depth security postures, manage risk, improve compliance, and proactively detect and prevent threats.

RESPONDENT BREAKDOWN

REGION

TITLE

COMPANY SIZE

Data collected from Jan. 13 - Feb. 9, 2021

Insights powered by PULSE