



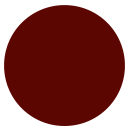















## Please rate how important the following statements are in your Zero Trust decision making process.

	Very Important	Moderately Important	Neutral	Mildly Important	Not At All Important
Understanding behavioral data to pinpoint deviations and malicious activity	 71%	 19%	 5%	 5%	0%
Limiting the attack surface with segmentation and least privileges	 90%	 5%	0%	0%	 5%
Automating security tied to context to improve the fidelity of alerts and incident response	 25%	 65%	 5%	 5%	0%
Continuously verifying access with the least friction for users, IT, and security teams	 66%	 24%	 10%	0%	0%
Attack path visibility across endpoints, identity stores, workloads, and container environments	 45%	 40%	 10%	 5%	0%

Source: TechValidate survey of 21 users of CrowdStrike



TechValidate  
by SurveyMonkey

✓ Validated

Published: Jul. 20, 2021 TVID: 861-524-021