Zero Trust Series: Identity Management

March 23, 2021

Former Lead Research Analyst – Cybersecurity

Kacey Clark investigated offensive security methods and trends, defensive strategies, and security solution technologies.

Submitted by Kacey Clark on 23, Mar 2021
Zero Trust Series: Identity Management

IT leaders need to integrate the principles of zero trust into their security programs. Zero trust will help them successfully manage risks, accelerate value, and improve relationships with their business stakeholders. Failing to leverage zero trust introduces too much risk. But a piecemeal approach to zero trust is bound to fail. In this Horizon Report from Stratascale (an SHI company), we identify that when organizations build and execute strategies in line with a zero trust identity management methodology, they achieve the following benefits:

- Refine granular access control by permitting user access to only what is necessary to perform job duties, and limit lateral movement.
- Improve security posture across cloud and on-premises services and applications based on policies, such as permittance established by device hygiene or approved devices.
- Enhance visibility and metrics that can answer who, what, when, where, why, and how (5W1H) through service, application, and data usage; logging and monitoring; and auditing and compliance requirements.

- Enable segmentation to reduce the attack surface of critical systems and thwart exfiltration of sensitive data.
- Fortify sensitive data by controlling who can access certain data and under what conditions.
- Protect and secure the remote workforce by enhancing secure remote access and tightening policies around personal devices.
- Enhance security operations capabilities by proactively managing risks, reducing workload, and enabling improved system visibility.

To get further insights and recommendations around Zero Trust, read the full report.