BlackBerry

Intelligent Security. Everywhere.

Building the Business Case for Least Privilege in a Modern Zero Trust Approach To Security

Zero Trust is really a modern take on least privilege access that is dynamically updated and tied to both network and identity-based behaviors and components. For any Zero Trust project, it's critical to build a least privilege business case that looks at the various ways a robust Zero-Trust-enablement technology can improve access control and organizational security across the board.

Here are some of the most common business drivers:

Diverse Endpoints and Users

The number and types of endpoints and users functioning within an organization is growing, in some cases, rapidly. Especially for large organizations with a massive and diverse set of technologies and user variations, choosing a technology that can accommodate all of these could vastly simplify the implementation and maintenance of access control.

Remote Access

As more organizations shift to remote workforce options, traditional virtual private network (VPN) clients are proving limited in helping to differentiate use cases and access models. With more capable endpoint protection and simplified endpoint client installation and support, organizations could easily consolidate remote access strategies.

Cloud and New Service Layers

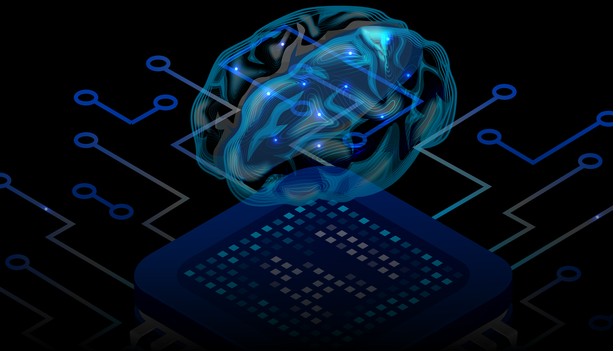
With the drive to hybrid and public cloud deployment models, the need to find technologies that support a wide range of hosting and infrastructure deployment grows rapidly. Consolidation and integration, as well as deployment support, could easily help to shift least privilege strategy to a unified technology solution that works in all environments.

Business Continuity and Contingency Planning Needs To Change Drastically

Many organizations are now realizing that business continuity and contingency planning needs to better embrace unexpected and unknown scenarios. Embracing more flexible approaches to endpoint technology and rapidly changing business use cases could drive access control models toward a ubiquitous Zero Trust strategy and technology implementation.

Artificial Intelligence/Machine Learning Improves Speed of Detection/Response

Artificial intelligence and machine learning techniques help security professionals recognize patterns in data. Threat intelligence data can be aggregated, analyzed, and processed for predictability models. These models are then fed back to Zero Trust access control policies and platforms to dynamically update detection and response capabilities.



For more information about how to build and execute a successful Zero Trust approach, including best practices, and a look at where Zero Trust security frameworks are headed, access a full white paper **here**.