

Emphasizing Prevention with Microsegmentation

Cybersecurity has become more difficult as applications become increasingly distributed and the threat landscape continues to evolve. The negative impacts of successful attacks require a preventative approach via zero trust, with microsegmentation uniquely positioned to ensure that the impacts of an incident are limited. To foster broader adoption, solutions supporting microsegmentation must be easy to use and straightforward to deploy, generating accurate, automated policy recommendations.

Security Teams Struggle to Keep Pace with Modern Environments

Application environments are more complex than ever, even as the threat landscape continues to evolve. Further, security incidents can have a variety of negative impacts on security teams, IT teams, and the business overall. This makes ensuring the security and availability of applications a high priority for nearly all organizations.

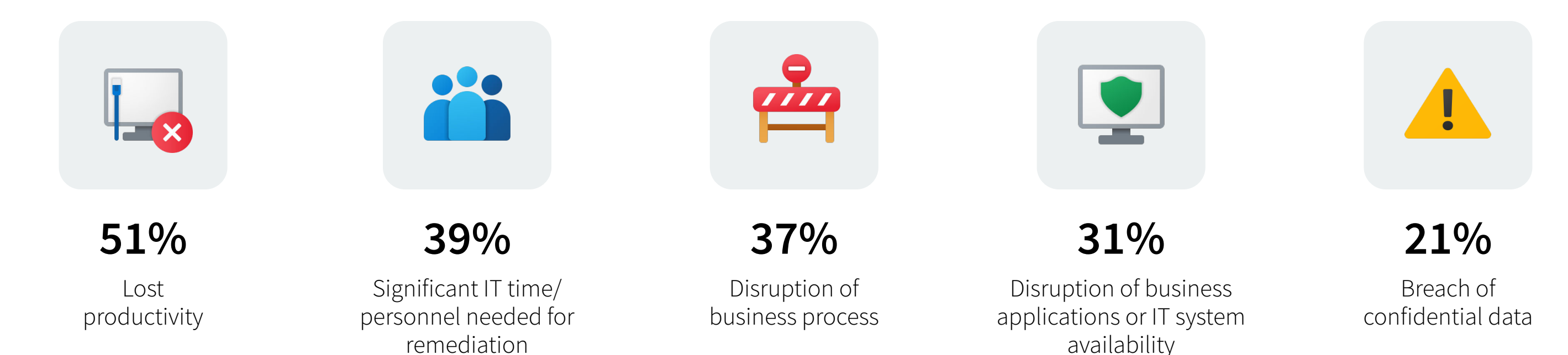
» The expansion of application environments makes cybersecurity more difficult

88% support at least 100 business applications.

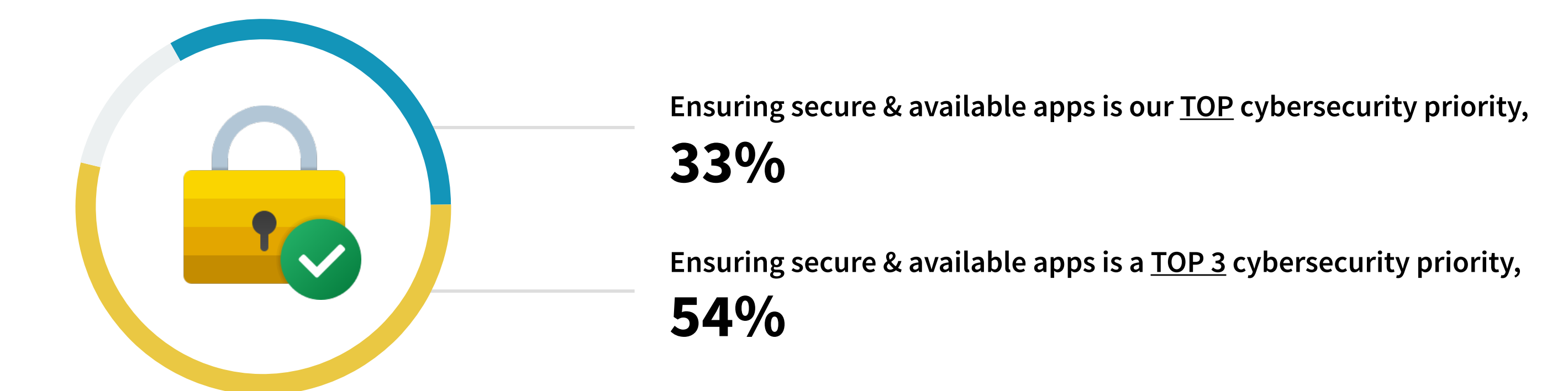


59% of respondents say cybersecurity has become **more difficult** than it was 2 years ago.

» Top five results of security incidents



» Application availability and security is a top priority



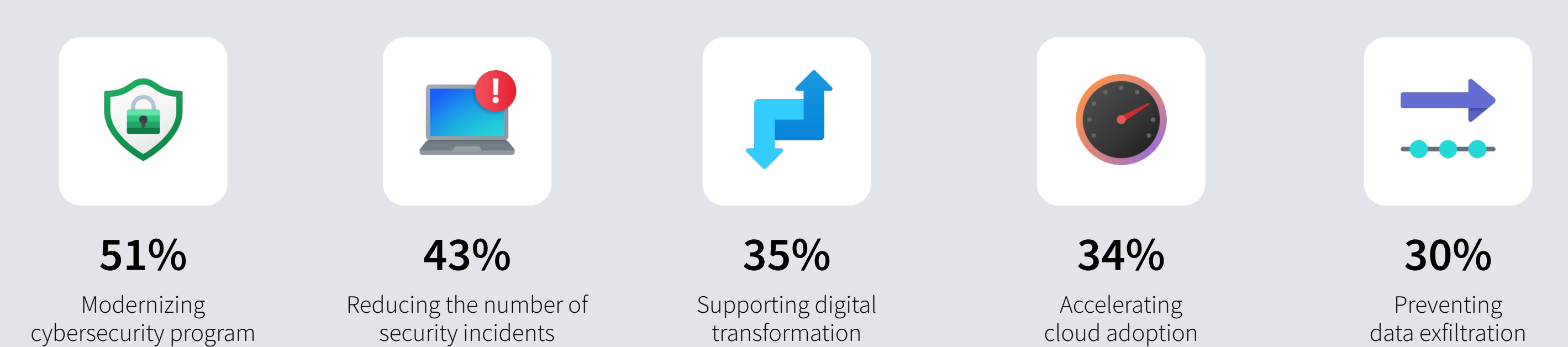
Prevention through Zero Trust and Microsegmentation

Zero trust strategies are being prioritized to address these challenges, modernize security, enable the business, and reduce incidents. While zero trust requires the granular policies microsegmentation supports, the practice has not been widely deployed to date, despite its ability to support business and security use cases.

» Zero trust adoption

89% have implemented or begun to implement zero trust across the organization and/or for specific use cases.

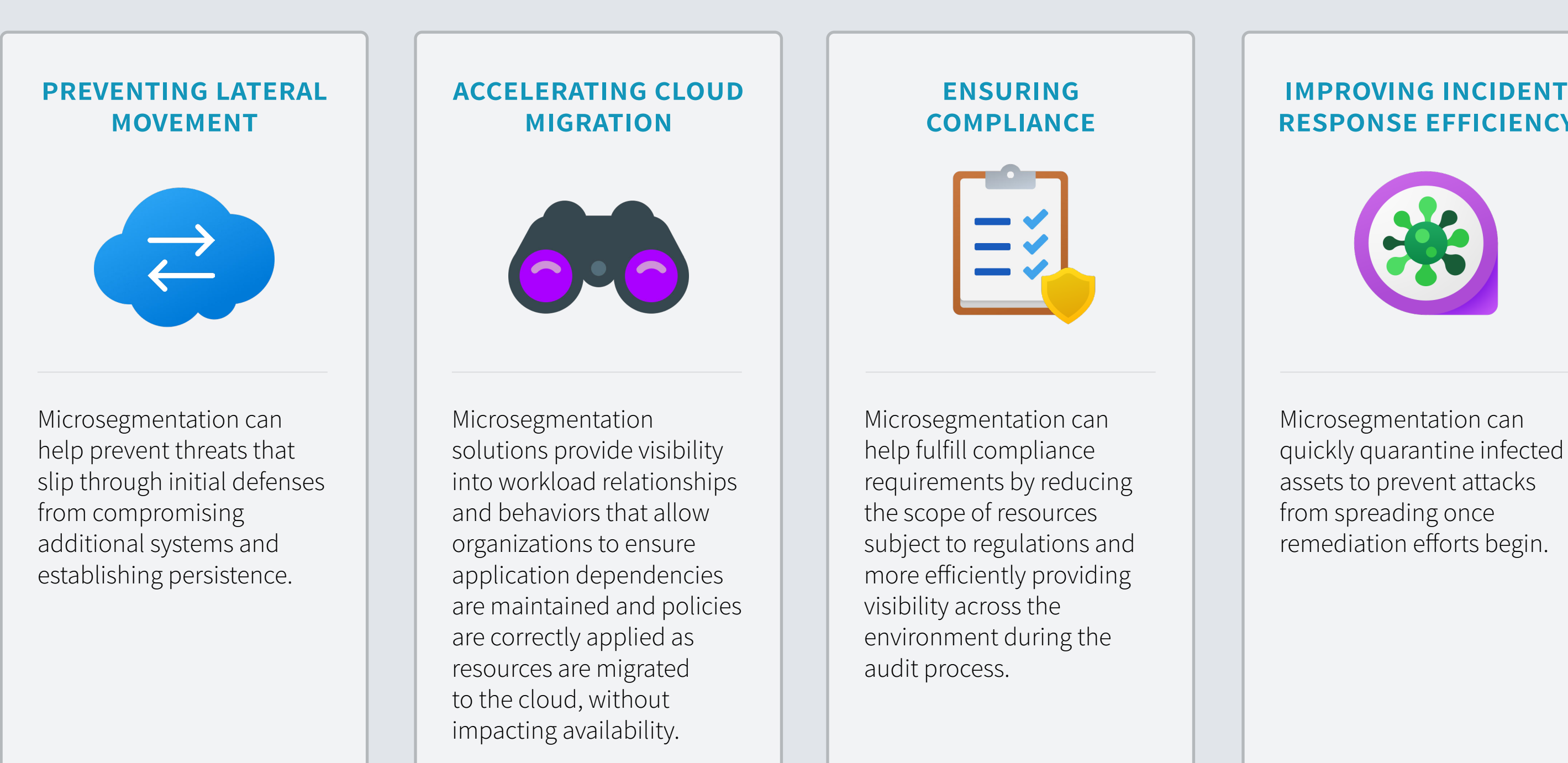
» Key business drivers for zero trust adoption



» The importance of microsegmentation is well understood, but adoption is somewhat limited today

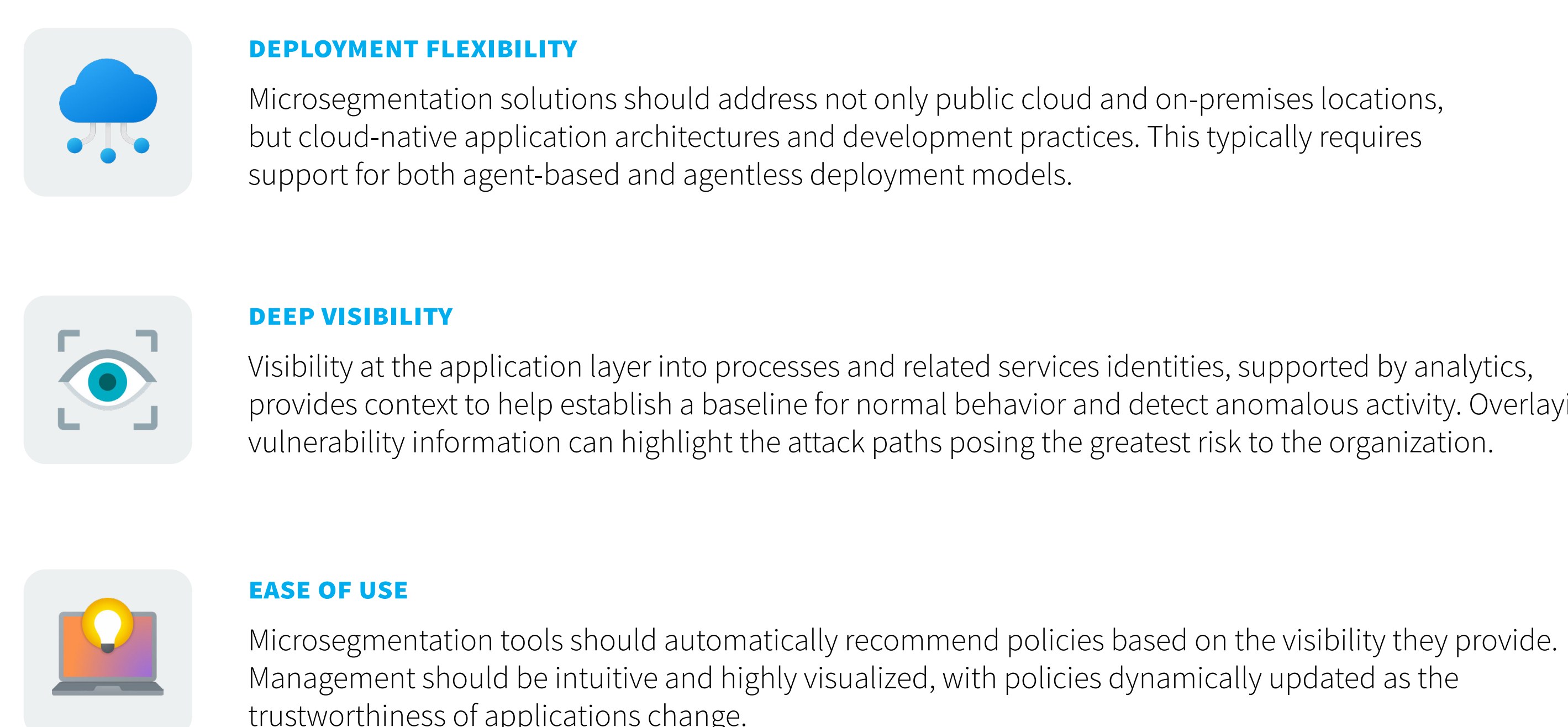


» Microsegmentation can address both business and security use cases



Deployment Flexibility, Deep Visibility, and Ease of Use Are Critical for Microsegmentation to Be Successful

While needs will vary from one organization to the next, there are some capabilities to prioritize in microsegmentation solutions that will benefit most organizations.



The Bigger Truth

Application environments have changed dramatically since the first microsegmentation tools were deployed ten years ago. Environments are more distributed and dynamic, and attackers are more motivated than ever before to target these valuable resources. For all these reasons, organizations should recognize microsegmentation as a critical component of their zero trust strategy and prioritize tools that deliver deployment flexibility, deep visibility, and ease of use.