

Zerô-Trust Security

Much more than just a buzzword!



The traditional perimeter-centric approach to security is no longer sufficient.



Given the growing attack surface, zero-trust security is the new solution for bolstering an organization's cyber resilience.

Prioritize the implementation of a zero-trust model to



Avert **5** cyber disasters per year.



Reduce average breach costs by at least **\$1.76** million.

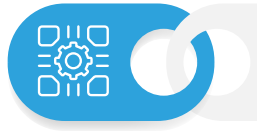


Save an average of **\$20.1** million in application downtime costs

Zero-trust security is not a 'quick fix' to a problem. It entails



Understanding the workflow of all the applications and services



Mapping the technological infrastructure



Configuring the systems to ensure maximum security

If implemented successfully, zero-trust model can help



Improve the security posture



Empower employees and enhance their efficiency



Boost overall user productivity

6

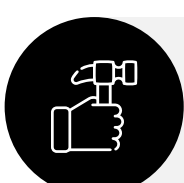
Best practices to successfully deploy a zero-trust security model



Identify and map the 'crown jewels'



Reconfigure and update the tech stack



Assemble a zero-trust toolkit



Design from the inside-out



Implement change management



Enable continuous monitoring

Check out SISA's latest whitepaper on

Six Best Practices for Effective Zero Trust Security Implementation

for detailed information on zero trust security, its key principles, and best practices.

