DELL Technologies | McAfee Together is power.

Creating a zero trust strategy for end-to-end startup security

Protecting your startup is harder than ever, as cyber attacks become more frequent and sophisticated. In this checklist, learn how to move away from ad-hoc systems and adopt a more secure end-to-end strategy based around the zero trust framework.

01: Assess your startup's needs

Assess your organisation's software, devices and systems to understand your security needs. This is a good time to leverage outside help for an expert perspective.

02: Review regulatory requirements

Compliance can be a powerful asset for business growth. Review current and upcoming regulatory requirements to ensure your business continues to be compliant.

03: Put together a roadmap

Evaluate and prioritise workloads, considering both security needs and ease of implementation. Focusing on incremental improvements can help you fit changes around existing priorities.

04: Build controls around business needs

Document processes, roles and responsibilities, checking that they reflect your own needs. Remember your business drives the zero trust environment, not the other way round.

05: Apply capabilities across your ecosystem

Roll out core capabilities across your entire IT ecosystem to avoid critical security gaps. These should include multi-factor authentication and roles-based access.

06: Don't sacrifice user experience

Make sure that security enhancements like zero trust don't come at the expense of usability. Your security should support startup innovation and growth, not restrict it.