

SECURITY & COMPLIANCE

DEFENSE IN DEPTH



Like a castle protected by walls, towers, sentries, moats, and archers, your data demands a multi-faceted approach. Good security comes in layers, and getting beneath the surface requires commitment, expertise, and investment in the right resources.

Availability, integrity, and confidentiality - the tip of the iceberg **AVAILABILITY,** when it comes to defense in depth. Essential to your clients and **INTEGRITY,** users, these key assurances often define your products and **CONFIDENTIALITY** services. But there's always more than meets the eye. PHYSICAL SECURITY Key cards, security staff, mantraps, and CCTV all help prevent **GOVERNANCE & AUDITS** physical access to your systems. Ensure IT and business strategy are working towards the same objective. Frameworks set you up ممير for success while audits validate **NETWORK SECURITY** Properly configured firewalls, 618 VLANs, data encryption, intrusion **POLICIES & PROCEDURES** detection/prevention, antivirus and From mobile device usage to more will keep bad actors out. vendor management and data retention, proper creation and upkeep of your policies and procedures is essential to your cvbersecurity. **CONFIGURATION HARDENING** Are your virtual machines and ॐ≡ network devices deployed with **ACCESS CONTROLS** default configurations? If so you're asking for an intrusion. Mobile device management, on/offboarding, authentication methods, and password vaults ensure you're limiting (and auditing) access into your systems.

SAFE. SIMPLE. SMART. Rev 04/2021