The New IT Acronym: KISSME (Keep IT Security Simple, Manageable and Effective)

Computing environments have evolved to enable users to be more productive and IT to be more agile. And yet attackers have evolved their methods too, adopting polymorphic malware to evade detection by preventive controls. Meanwhile, IT organizations continue to practice a piecemeal, reactive process of plugging holes, and it's putting companies at grave risk.

›iven the nature of our dynamic computing environments and the sophistication of advanced persistent threats (APTs), a security breach is inevitable. The rise in the number of breaches over the past two years is evidence that no company is immune. As with the Target and Home Depot breaches, it's possible that malware is already sitting on your corporate network, surreptitiously exfltrating data as you read this. The question is: How soon will you catch it?

By adding point solution after point solution, IT organizations are essentially putting up a welcome sign for attackers. IT is too busy managing controls to manage risk, so APTs enter the network undetected and hide in systems into which IT has limited visibility. Unless IT organizations adopt a new approach to security, these threats will continue to steal data and move about the network undetected.

IT organizations must stop what they're currently doing and take a smarter approach to security—one that uses the best detection and prevention methods possible to avoid an attack while still minimizing—or even eliminating—security's impact on business performance.

IDG
INTERNATIONAL DATA GROUP

Bitdefender®

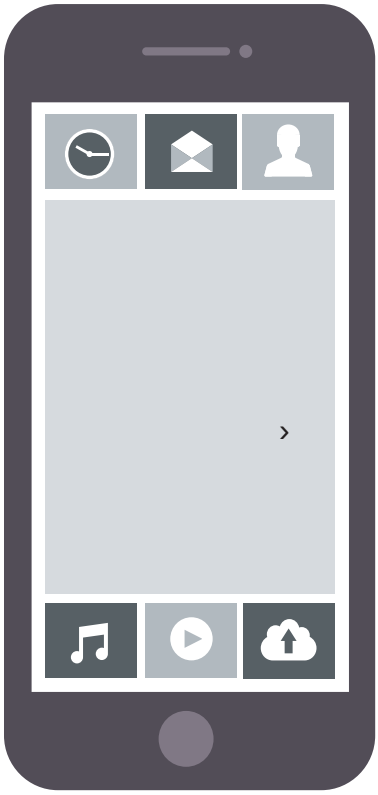
CSO

Q

Q

CIO

Q



i