TECH DOSSIER

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.

Given 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 exfiltrating 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

THIS IS YOUR WAKE-UP CALL

There's no doubt about it: IT organizations have their work cut out for them when it comes to security. In 2014 the "State of the CSO" report, an annual survey conducted by *CSO* magazine, provided some perspective on the scope of the problem. The most significant challenges CSOs face:

- Managing security of and addressing risks surrounding mobile devices and bring-your-own-device (BYOD)
- Cyberthreats from outside the organization, including APTs and distributed denial of service (DDOS)
- Security for technology as a service and cloud computing

Although there are commonalities among these three categories, there's also a lot of variation within each one. Mobile device security is rarely a matter of managing a single platform across the entire enterprise. Users want to use the device of their choice at any time, wherever they happen to be. The risk posed by cyberthreats varies from one system to another, and no two cloud-based services share the same risk profile. Risk management becomes exponentially more complex with the addition of each new technology.

Studies show that the security measures IT organizations are implementing **do not** reflect CSOs' concerns.

Unfortunately, studies show that the security measures IT organizations are implementing do not reflect CSOs' concerns. According to the "ISACA 2014 Advanced Persistent Threat Awareness" study, 96 percent of the respondents to its survey use antivirus and antimalware and/or traditional network perimeter technologies to thwart APTs. However, far fewer organizations address security for mobile devices and remote access technologies, both of which are increasingly being used within the enterprise, thus becoming high-risk factors.

And it's clear that IT security is getting short shrift among CIOs too. The *CIO* magazine "2015 Tech Poll" indicates that tech executives are putting investments in business intelligence, mobile apps, software as a service (SaaS) and the cloud—technologies that often open doors for more APTs—at the top of their priority list, with security applications falling to No. 6.

It is clear that IT organizations need comprehensive threat protection, but security controls must not reduce end user productivity. In addition—given the scope of the risk—management of controls must not be too complex or all-consuming for the security team.

MANAGING COMPLEXITY: KEEP IT SIMPLE

The traditional approach to security involves deploying a point solution for each part of the IT environment. This worked well enough when end user computing and server environments were relatively static. Today's computing and server environments, however, are anything but static. They are dynamic, with many facets. Deploying a point solution for each type of endpoint is costly and results in multiple management consoles. It becomes extremely difficult for IT organizations to gain insight or management control across this spectrum of systems.

It is virtually impossible to protect today's highly complex IT environments with traditional point solutions. Successful security management in the 21st century requires a new approach. IT organizations need a security solution that is comprehensive in two respects. First, it must protect the entire end user computing and data center environment, enabling a horizontal approach to securing technologies rather than a vertical approach with multiple disparate point solutions. Second, a comprehensive security solution must provide thorough threat protection—without degrading user performance. Put simply: Less is more.

There are several benefits to a horizontal approach. A comprehensive security solution gives IT the visibility it needs across all environments—be they virtual, mobile, and/or in the cloud. This is particularly important, in that many organizations are not currently logging events in these environments and