

OUT WITH THE OLD, IN WITH THE NEW!

BUSINESSES: 69% have security solutions that are outdated & inadequate

THE AGING SECURITY INFRASTRUCTURE:

65%

can't manage risks of unapproved apps

64%

can't manage risks of unapproved data

61%

lack technologies to protect information

55% outdated procedures & policies in place

60%

ineffective at protecting sensitive apps & data

AREAS OF FOCUS CAUSING NEGATIVE IMPACT:

Only **32%** claim that employee-owned devices do not allow access to corporate networks & data

63%

personal mobile devices

70%

businesses' cloud services & infrastructure

55%

employees use of favorite cloud apps

73%

businesses use of digital identities

WHAT THEY'RE MOST WORRIED ABOUT:

TOP SECRET

80%

nation-state attackers

76%

cyber warfare or terrorism

79%

breaches of high-value information

76%

malicious or criminal insiders

GOALS FOR A NEW FRAMEWORK

48%

keep pace with new or emerging attacks

43%

visibility into all business-critical apps or systems

53%

unified view of users across the enterprise

MODERNIZING SECURITY WITH INVESTMENT

98%

of businesses will spend over \$1 million in 2017

Survey Methodology The report conducted by the Ponemon Institute and sponsored by Citrix, "The Need for a New IT Security Architecture: Global Study" looked at global trends in IT security risks and reasons why security practices and policies need to evolve in order to handle threats from disruptive technologies, cybercrime and compliance mandates. The research features insights from more than 4,200 IT and IT security practitioners in Australia/New Zealand, Brazil, Canada, China, Germany, France, India, Japan, Korea, Mexico, Netherlands, United Arab Emirates, United Kingdom and the United States.