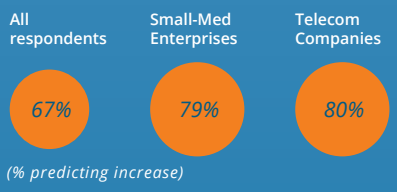
Changing Information Security Spending Landscape

The Voice of the Enterprise (VotE): Information Security, Budgets and Outlook survey represents the second in-depth look at security budgeting. A year-by-year comparison and predictive look into the future, shows security budgets increasing but also coming under various forms of stress that are currently shifting spending allocations and portend future changes. These shifts are taking the form of increased spending on software- over hardware-based security solutions, opex over capex and endpoint-based solutions over network-based ones.

Spending for Security

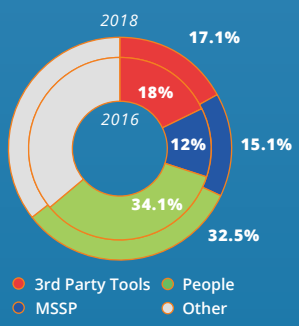
Security budgets everywhere are increasing — SMEs and the telecom industry are seeing the most widespread increases.



Compliance concerns boosting spending:

21% of respondents cited Compliance as a top security concern, up from 16% in Q4 2015; among them, more than half cited HIPAA and PCI as the largest.

Changing Spending Distribution



Respondents project a 3-point spending increase in managed security services spending at the expense of spending on people and third-party tools.

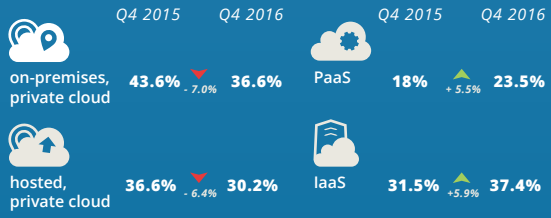
Vendor-based tools

Endpoint Security and Network Security will experience the most dramatic changes.

	2015	2016		2018
Endpoint Security	26.3%	29.4%	+ 2%	28.3%
Network Security	40%	37.5%	- 4.2%	35.8%

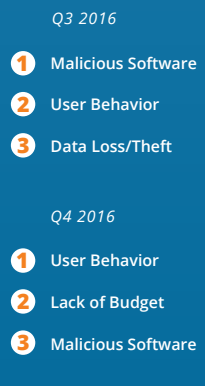
> "Most people are very focused on the here and the now and keeping the lights on…putting layers upon layers upon layers and bolting bits on the side and on the top and on the bottom and everywhere, rather than starting a fresh with a clean sheet of paper…so it's a complicated area where there's a big reluctance to make big changes. People within organizations are quite happy to commit resources to something that is incremental rather than a big bang."
>
> —IT/Engineering Managers and Staff, $1bn-$4.99bn, Government/Education

Security Barriers Lessen as Public, Hosted Cloud Gains Traction



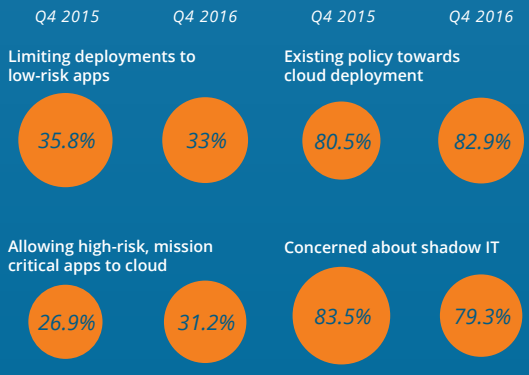
Top Security Pain Points

It's no surprise that respondents project an increase in overall spending in security: by the end of the year, Lack of Budget became the second top-cited pain point, after User Behavior.



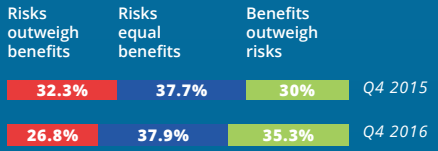
Security Diminishing as an Inhibitor

A key differentiation among cloud providers is how they respond to security concerns. As these responses grow more sophisticated, security is progressively being removed as an inhibitor to cloud deployment plans.



Benefits of Cloud Are Outweighing the Risks

Enterprises increasingly find that the benefits of cloud are outweighing the security risks.



451 Research | VotE™ VOICE OF THE ENTERPRISE

Source:
451 Research's Voice of the Enterprise: Information Security Budgets and Outlook 2016

Voice of the Enterprise: Information Security

Covering 27 distinct Information Security Sectors across 145 vendors

VENDORS AND SERVICE PROVIDERS

Amazon Web Services (AWS)
Above Security
AccessData
AirWatch by VMWare
Akamai
Alert Logic
AlienVault
AT&T
ATOS
Authentic8
Avast
AVG Technologies
Barracuda Networks
Bitdefender
BitGlass
Blackberry Limited
Blue Coat (Symantec)
Bromium
BT
CA Technologies
Carbon Black
CenturyLink
Check Point
Checkmarx
CipherCloud
Cisco
Citrix
CloudCheckr
CloudLock
CloudMask
CloudPassage
Coho
Crowdstrike
Cylance
Darktrace
Datacard
Dell
Digital Guardian
Dome9 Security
Duo Security
EM
Ericsson
ESET
Evident.io
F5 Networks
Facebook
FireEye
FireLayers
Forcepoint (Websense)
Fortinet
FortyCloud
Fujitsu
Gemalto (SafeNet)
Global Knowledge
Google
Gridstore
Guidance Software
HPE
HID Global
Hitachi Data Systems
HP
Huawei
IBM
Identity Finder
Imperva
Imprivata
Intel
Invincea
JumpCloud
Juniper Networks
Kaspersky Lab
Lenovo
LogLogic
LogRhythm
Lumension
Malwarebytes
Managed Methods
Maxta
McAfee
Menlo Security
Micro Focus
Microsoft
MobileIron
NetApp
Netskope
Nokia
NTT
Nutanix
Ohanae
Okta
Optiv Security (FishNet)
Oracle
Palerra
Palo Alto Networks
PerfectCloud
PhishMe
Ping Identity
Pivot3
Proofpoint
Protegrity
Qualys
Rapid7
RSA (Dell EMC)
SafeNet
SANS
Scale Computing
Securonix
SentinelOne
SimpliVity
SkyHigh Networks
SolarWinds
SonicWall
Sophos
Sphere
Splunk
Springpath
Supermicro
Symantec
Synopsys
Tanium
Tenable
Teradata
Thomson Reuters
Threat Stack
Trend Micro
Tripwire
Trustwave
Unisys
Varonis
Vaultive
Veracode
Verizon
VIPRE
VMware
Vormetric
WatchGuard
Webroot
Websense
Whitehat Security
Wipro
Wombat Security
Yubico
ZixCorp
Zscaler

SECURITY SECTORS

Cloud Access Security Brokers
Cloud Encryption/Tokenization
Cloud Infrastructure Security
Computer Forensics/Incident Response
DAST/SAST/IAST/RASP
Data-optimized Infrastructure
Encryption
Endpoint Data Leakage Prevention (DLP)
Endpoint Security
Endpoint Security Management
Information Security Awareness Training
Innovative Security Vendor
Intrusion Detection/Prevention Systems (IDS/IPS)
Managed Security Services
Mobile Device/Enterprise Mobility Management (MDM/EMM)
Most Important Vendor
Multifactor Authentication
Network Firewalls
Primary Non-Converged Server Vendor
Security
Security Information & Event Management (SIEM)
Single Sign On/ Identity-aaS/Identity Federation
Standard Converged Infrastructure
Vulnerability Management
Vulnerability Management (Scanning)
Web Application as a Firewall
Web Application Firewall (WAF)
Web Content Filtering

VENDOR WINDOWS

Plus detailed evaluations from surveys of existing customers currently using each vendors' product plot enterprise adoption, promise and fulfillment to compare vendors' effectiveness in marketing and execution. Information Security Vendor Windows include: **Application Security, Endpoint Security, SIEM, DAST/SAST, Mobile Device/Enterprise Mobility Management.**

Multiple Ways To Access And Use The Data

Annual Subscription *Enterprise-wide Access* *Custom Data Cuts*
External Licensing *Single-Market/Multi-Market*

For more information or access to our data, contact our team at sales@451research.com

451 Research | VotE™ VOICE OF THE ENTERPRISE