Survey Reveals Organizations Are Unprepared for Changing Security Demands

Mar 04, 2013 7:00 AM

BYOD, virtualization, and the increasing complexity of threats create the greatest impact on today's enterprise organizations

SEATTLE--(BUSINESS WIRE)-- F5 Networks, Inc. (NASDAQ: FFIV) today announced the findings of its 2013 RSA Security Trends Survey, which revealed that organizations are struggling to keep pace with the changing face of security. Respondents were RSA attendees with IT responsibilities over planning, management, oversight, or implementation of security. The results show that security trends such as virtualization (73%), BYOD (66%) and the complexity of attack types (72%) have the greatest impact on securing today's organizations. Nearly half of respondents admit that traditional safeguards are *less than adequate* in protecting against threats related to these trends, with roughly one-third of respondents reporting that their security readiness is inadequate.

Key Findings

Security is changing, from the type of threats to those driving the threats.

When asked what security trends have the greatest impact on an organization's ability to achieve the level of security it desires, respondents answered:

- Virtualization (73%)
- The increasing complexity of threats (ex: Distributed Denial of Service attacks) (72%)
- BYOD (use of employee-owned devices such as smartphones for business use) (66%)
- The change in the bad guys (from hackers to espionage and political motivation) (62%)
- The shift from data center focused infrastructure to cloud-based infrastructure (61%)
- The shift from traditional client-server applications to web-based applications (60%)

BYOD is seen as critical in an organization's ability to achieve the level of security it desires, yet a sizeable number of organizations are not taking the appropriate steps to address it.

- Most (75%) see BYOD as being prevalent in their organization.
- Furthermore, two-thirds (66%) see BYOD as having a somewhat to extremely high impact on security.
- Despite this, one-third (35%) say they are not prepared to provide adequate security to protect against threats associated with BYOD.

Organizations are unprepared to properly address the shift to web-based applications and cloud-based infrastructure.

- Nearly two-thirds (64%) of respondents see the shift to web-based applications as a trend affecting security, yet 37% of respondents' organizations are not providing adequate security to protect against potential threats.
- Sixty-six percent of respondents see the shift to cloud-based infrastructure as a trend affecting security, yet 49% of respondents' organizations are not providing adequate security to protect against potential threats.

Threats are moving beyond the capability of traditional security safeguards.

There is a wide range of IT trends making security more complex. Below are the percentages of respondents who felt traditional safeguards were *less than adequate* in protecting against threats related to a variety of current IT trends:

- The shift from traditional client-server applications to web-based applications (44%)
- The shift from data center focused infrastructure to cloud-based infrastructure (49%)
- BYOD (use of employee-owned devices such as smartphones for business use) (45%)
- Increased external threats (spam and malware) (39%)
- The increasing complexity of threats (ex: Distributed Denial of Service attacks) (48%)
- The change in the bad guys (from hackers to espionage and political motivation) (47%)
- Increasing insider threats (49%)

"The security landscape continues to change rapidly and many organizations are struggling to properly address evolving threats," said Mark Vondemkamp, VP of Product Management for Security at F5. "Companies will do well to proactively address trends like BYOD and cloud security, but they should also look to raise their game in terms of threat detection and mitigation. With employee behavior, business priorities, and infrastructure demands further expanding traditional threat vectors, the proper tools and procedures are essential in maintaining a healthy level of security."

Recommendations and Best Practices

To prepare for threats posed by emerging security trends, F5 recommends organizations have:

- Centralized, flexible access policy controls that provide comprehensive protection and keep users productive.
- A DNSSEC solution that delivers security, improved performance, and global availability.
- A secure web application firewall and comprehensive, policy-based approach to web application security in addressing emerging threats at the application level.

F5 Networks 2013 RSA Security Trends Survey

The F5 Networks 2013 RSA Security Trends Survey is a result of research conducted on the exhibit floor at last week's RSA conference in San Francisco. Conference attendees were asked two initial qualifying questions to promote the validity of the survey results. More than 150 qualified respondents were then asked a total of five questions surrounding security trends.

Additional Resources

- RSA Security Trends Survey Results
- RSA Security Survey Results – Video
- BYOD 2.0: Moving Beyond MDM – White Paper
- BYOD Policies: More than an IT Issue – DevCentral Blog Series
- Mobile App Manager Deployment Service
- F5 Application Delivery Firewall Solution Page
- F5 Access Solutions Page

About F5 Networks

F5 Networks (NASDAQ: FFIV) makes the connected world run better. F5 helps organizations meet the demands and embrace the opportunities that come with the relentless growth of voice, data, and video traffic, mobile workers, and applications—in the data center, the network, and the cloud. The

world's largest businesses, service providers, government entities, and consumer brands rely on F5's intelligent services framework to deliver and protect their applications and services while ensuring people stay connected. Learn more at www.f5.com.

You can also follow @f5networks on Twitter or visit us on Facebook for more information about F5, its partners, and technology. For a complete listing of F5 community sites, please visit www.f5.com/news-press-events/web-media/community.html.

F5 and DevCentral are trademarks or service marks of F5 Networks, Inc., in the U.S. and other countries. All other product and company names herein may be trademarks of their respective owners.

This press release may contain forward-looking statements relating to future events or future financial performance that involve risks and uncertainties. Such statements can be identified by terminology such as "may," "will," "should," "expects," "plans," "anticipates," "believes," "estimates," "predicts," "potential," or "continue," or the negative of such terms or comparable terms. These statements are only predictions and actual results could differ materially from those anticipated in these statements based upon a number of factors including those identified in the company's filings with the SEC.

☐

F5 Networks, Inc.
Alane Moran, 206-272-6850
a.moran@f5.com
or
Connect Marketing
Ben Jolley, 801-373-7888
benj@connectpr.com

Source: F5 Networks, Inc.