2013
Server Security Survey Report

Executive Summary

In November and December of 2012, Bit9 conducted its second annual survey on server security, polling 966 IT and security professionals worldwide. In the past year, confidence in being able to identify and stop advanced attacks targeting servers has dropped while actual attacks on servers—and uncertainty about having been attacked—have risen.

Key findings:

1. In 2012, targeted malware continued to be the top server security concern for 52.4 percent of survey respondents—up 15 percent from 2011.

2. Confidence in the ability to identify and stop advanced threats has dropped. The number of respondents confirming they had been attacked jumped by 8 percent in 2012.

3. Interestingly, nearly half of respondents believe their virtual servers are more secure than their physical servers—despite findings from Gartner in 2012 that 60 percent of virtualized servers were less secure than the physical servers they replaced.[1]

4. 12 percent of the survey group ranked "too much administrative effort on security solution" as even more of a concern than actual attacks. 43 percent of respondents use more than 1 full-time employee (FTE) to manage server security.

The findings highlight the increased need for greater control in identifying and stopping advanced attacks on valuable server resources before they execute—while decreasing the security-related administrative workloads of IT and security professionals.

[1] Gartner: Virtualization security will take time, SCMagazine.com, March 2010

About Our Survey Participants

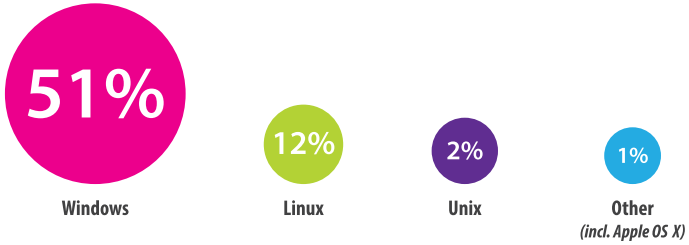
Most respondents (58 percent) administer up to 50 servers; 29 percent administer 100 to 500, with the remainder (13 percent) administering, on average, 2,000 servers.

Half of our respondents are running Windows as their primary platform (i.e., constituting more than 75 percent of total servers) while only 2 percent use Unix servers. Thirteen percent more respondents are running mostly Linux servers this year than last. Survey participants are advancing in the adoption of virtual environments. One-third of participants said that more than 50 percent of their servers are virtual; half of the respondents already have deployed virtual desktops, are in the process of rollout, or have plans to do so.

Only 28 percent have no plans to use cloud/hosting services for their servers and server-based applications; 36 percent are already using remote hosted services, managed either internally or by a third party and about an equal number are planning to use cloud/hosting services in the future.

How many total servers do you administer?

Percent of respondants with more than 75% of servers running on specified platforms

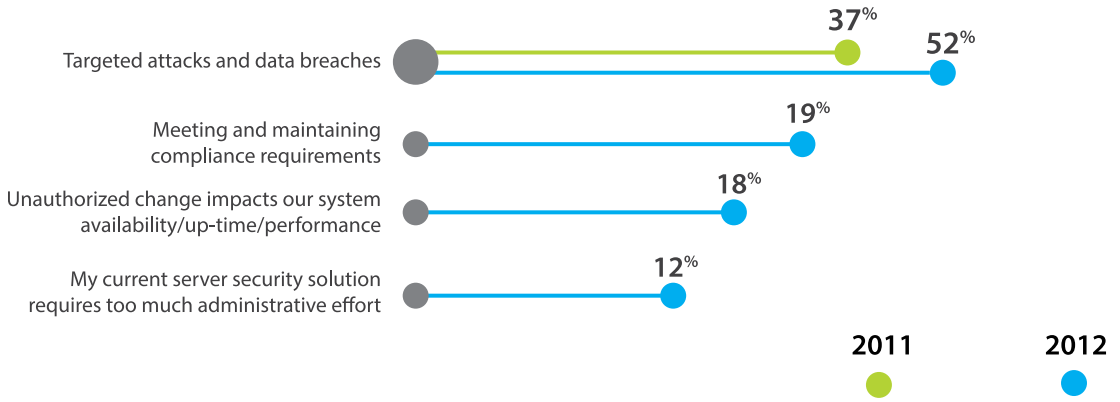


Key Survey Findings

Key Finding #1:

Targeted malware continues to be the top server security concern for 52 percent of survey respondents—up 15 percent from 2011.

What is your top concern regarding server security?



That 15 percent more respondents identified targeted attacks and data breaches as their top server security concern was no big surprise in a year that saw a proliferation and greater diversity of cyberattacks. 2012, for example, saw the emergence of a "family" of advanced attacks (Flame, Gauss and mini-Flame), as well the Flashback Trojan that attacked 600,000 Macs.

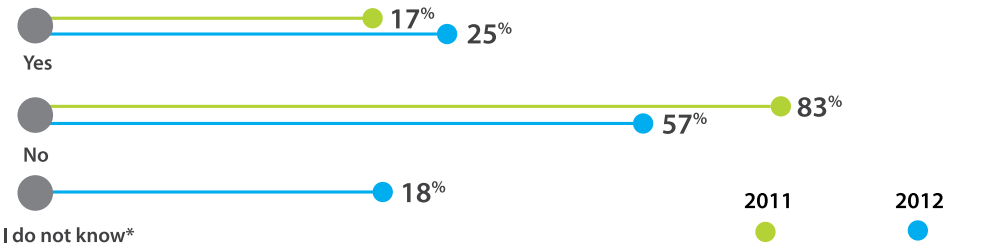
Key Finding #2:

Confidence in the ability to identify and stop advanced threats has dropped. The number of respondents confirming they had been attacked by advanced malware increased by 8% since 2011.

Server data has become much more vulnerable to attack: **94 percent** of all data compromised involved servers (up 18 percent from 2011).[2]

Indeed, the number of respondents saying they had been hit by advanced malware (25 percent) jumped by 8 percent over last year. In 2011, 83 percent of respondents said they had not been attacked—this year, 57 percent said they had not been attacked—and 18 percent said they didn't know.

Have you been hit by advanced malmare?

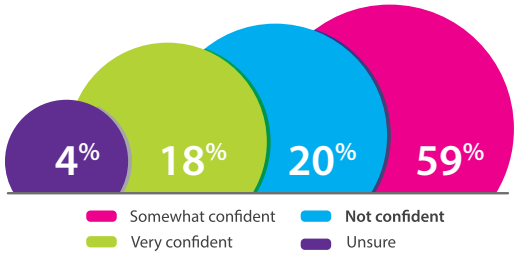


** Selection added for 2012 survey*

Overall, security professionals indicated they were aware of this situation, but their confidence in their ability to identify and stop advanced threats targeting servers declined in 2012.

How confident are you in your ability to identify and stop advanced threats?

In 2011, **10 percent** of those surveyed said that they were **not confident** in their ability to stop advanced malware. In 2012, that number is up to **almost 20 percent.**



[2] Verizon 2012 Data Breach investigations Report.

Learn More:

Download our Threat Advisor ***Securing Virtual Machines and Desktops*** to learn:

- *Why virtualization does not provide protection from today's advanced cyberthreats.*
- *How new security challenges are created with certain aspects of virtualization.*
- *Why shutting down and rebooting "clean" virtual machines or desktops is not a valid protection strategy.*
- *How certain user behavior on a virtual desktop infrastructure may be risky and provide a false sense of security.*

Key Finding #3:

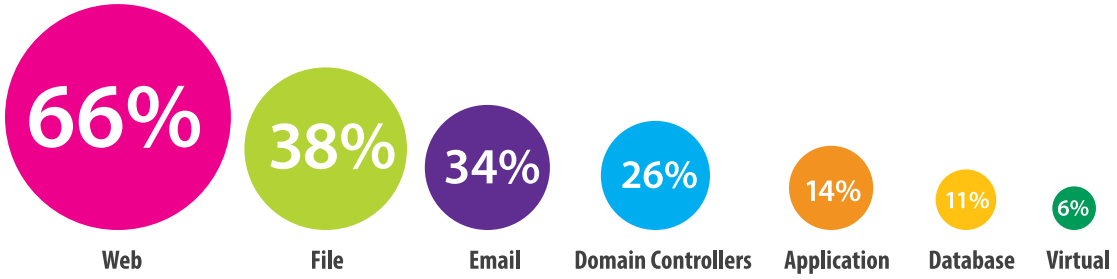
Almost half of respondents believe their virtual servers are more secure than their physical servers.

Almost half of survey respondents felt that their virtual servers were more secure than physical ones—in contrast with findings from a 2012 Gartner study that indicated 60 percent of virtualized servers were less secure than the physical servers they replaced.[3]

In fact, compared to other types of servers, virtual servers were ranked by survey participants as representing the lowest risk. Web servers, on the other hand, were ranked as "highest risk"[4] by two-thirds of respondents. This ranking is interesting, given the most valuable enterprise information is found on file servers (e.g., intellectual property), databases (e.g., customer information) and—above all—domain controllers. The latter are where the "keys to the kingdom" reside (e.g., passwords, administrative rights), making them a high-value target for advanced threats.

In considering the types of security concerns associated with virtual servers, 62 percent of respondents focused on operational issues (VM management, access control, auditing), with 26 percent citing technical vulnerabilities (attacks via hypervisor or service consoles).

Type of servers rated for" High Risk"



[3] Kaplan, Dan, "Gartner: Virtualization security will take time," SCMagazine.com, March 16, 2012.

[4] "Highest risk" means servers ranked first or second on a scale of seven, where "1 = highest risk").

Learn More:

For a hands-on exploration of the economics of managing security, download:
Getting (and Staying) Ahead of Advanced Threats: A Workbook for Assessing Your Advanced Threat Protection Posture

- *Analyze the effectiveness of your current security environment, assess your cost structures and uncover opportunities for savings and increased productivity across different functional areas and lines of business security.*

Key Finding #4:

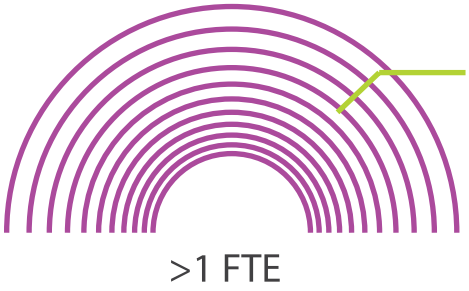
12 percent of the survey group ranked "too much administrative effort on security solution" as an even greater concern than actual attacks.

Nearly 12 percent of participants said that the amount of administrative effort required by their current server security solutions was their top concern—even more than an actual attack. **43 percent of respondents said that server security is managed by more than 1 FTE.** This is not surprising since more than 90 percent of respondents said that they are using antivirus software. There are significant performance issues associated with traditional AV scans: deploying signature updates requires testing that delays deployment, impacts effectiveness and compliance and makes additional work for the server team.

In addition to AV, a separate file integrity monitoring solution (FIM) is still needed for audits, compliance, ensuring system integrity and tracking unauthorized changes that impact system performance and stability. 39 percent of respondents are using FIMs.

In contrast, with **Bit9, the cost of managing server security can be reduced to less than 1 FTE**, according to research conducted among the Bit9 customer base.

How many FTE's are currently managing your server security solution?



43% said they have **more than 1 FTE** managing their security solution.

On average, Bit9 customers use 1 FTE or less.

Learn More:

Download the Frost & Sullivan White Paper "***Advanced Threat Landscape: What Organizations Need to Know***," which addresses:

- *Current cyberthreats impacting organizations today*
- *Misconceptions about what is considered security's weakest link*
- *Is endpoint security sufficient (antivirus solutions)?*
- *Challenges in protecting critical infrastructure*
- *Trust-based security systems*

Conclusion

There's good news and not-so-good news in our 2012 server security findings. The good news: greater awareness on the part of IT and security professionals about what they do and don't know about experiencing an advanced attack.

The not-so-good news is that the number of cyberattacks is rising and that confidence in the ability to identify and detect them before they can do damage is lower than ever. And clearly there is more learning to do about protecting specific types of servers containing valuable assets—especially in a virtual environment.

Maximizing server security while reducing administrative effort is best achieved with a proactive, trust-based security solution that detects malicious software and protects against advanced attacks that evade antivirus and other traditional security solutions.

About Bit9

The leader in Trust-based Security, Bit9 continuously monitors and records all activity on servers and endpoints to detect and stop cyberthreats that evade traditional security defenses. A cloud-based software reputation service combined with policy-driven application control and whitelisting provide the most reliable form of security in a model that can be rapidly implemented with less maintenance than traditional tools. Bit9 has stopped the most advanced attacks, including Flame, Gauss and the malware responsible for the RSA breach. Almost 1,000 organizations—from Fortune 100 companies to small businesses—use Bit9 to increase security, reduce operational costs, and improve compliance.

266 Second Avenue
Waltham, MA 02451 USA
P 617.393.7400 F 617.393.7499
www.bit9.com

Bit9
The Leader in Trust-based Security