BYOD WHITEPAPER
THE HIDDEN THREAT

www.spirent.com
TABLE OF CONTENTS

1. EXECUTIVE SUMMARY .......................................................... 1
2. NEW CORPORATE REALITY ................................................... 2
3. NEW NETWORK REALITY ...................................................... 2
4. INCREASED RISKS FROM BYOD ........................................... 3
5. DON’T FIGHT CHANGE—EMBRACE IT ..................................... 4
6. SELECTING A TEST SOLUTION ............................................... 4
7. CONCLUSION ............................................................................ 6
8. LEARN MORE ........................................................................... 7
1. EXECUTIVE SUMMARY

Cybersecurity risk is now one of the highest priorities for company executives and boards of directors.

Chart 2

<table>
<thead>
<tr>
<th>INDIVIDUAL RISKS, PRIORITY AND PREPAREDNESS SCORES 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk</td>
</tr>
<tr>
<td>---------------------------------</td>
</tr>
<tr>
<td>1 HIGH TAXATION</td>
</tr>
<tr>
<td>2 LOSS OF CUSTOMERS/CANCELLED ORDERS</td>
</tr>
<tr>
<td>3 CYBER RISK</td>
</tr>
</tbody>
</table>

Score out of 10 ranked by priority score then by preparedness score

Source: Lloyd’s Risk Index 2013

The reason: Your network is critical to your company’s on-going success. But it is also a complex animal with many moving parts that all need to be understood, managed and controlled:

- Applications
- Platforms
- Markets
- Corporate changes
- Users and customers

In recent years a new complication has appeared, called bring-your-own-device (BYOD). This trend allows your employees to use their own personal devices (smart phones, tablets, laptops, etc.) for company business. While there are good reasons to allow it (reduces equipment costs, improves user productivity, and increases user involvement), it also means that threats can walk through the front door and past security in your employee’s briefcase without them, or anyone else, being aware until the damage is done.

What you may not even realize is that your employees are using their own devices whether your company policy permits it or not.

While employees worry most about the cost to replace a device if it’s stolen, the risks to the enterprise go far beyond theft:

- Loss of company or client data
- Risks of exposure if an employee leaves the company
- Increased attack vectors to penetrate your network

“Few (IT decision makers) are prioritizing BYOD security... Failing to prioritize BYOD security could leave their organizations vulnerable to attack.”

—Source: “Protecting the Organization Against the Unknown” 2/14
To satisfy your company’s need for a secure network, you must have sophisticated testing solutions that can quickly and easily pinpoint the risks from BYOD. Total visibility and continuous monitoring are essential, validated through realistic testing that demonstrates the ability of the solution to detect and stop all threats. The test solution you use should support configurable and repeatable test scenarios, emulate actual application payloads, draw on a continuously updated repository of known attacks, and have the power to test your solution at the scale of the Internet. The test solution must also test all the platforms that you must support, including mobile devices.

2. NEW CORPORATE REALITY

Nothing in today’s business stays the same from one day to the next. You are experiencing constant changes:

- New corporate configurations (mergers, acquisitions, divestitures)
- New applications (website metrics, ERP, revenue-generating services)
- New regulations
- New geographical locations

Your business is also more interconnected than ever before, as a deeply integrated partner in ever-expanding ecosystems with suppliers, vendors, customers and service providers.

In addition, your customers demand that you utilize mobile technology to market to and support them. Your sales, support and marketing teams are already hip-deep in determining the best mobile device strategies.

3. NEW NETWORK REALITY

Today’s data center is light years away from those of just a few years ago. While increasing in importance, it has also exploded in complexity:

- New platforms (virtual, open architectures)
- Heterogeneous mix of hardware, software and applications
- Global access and support
- New capacity requirements (seasonality, bandwidth demands)
- Outsourced data centers (private, public, hybrid clouds)
- Line of business controlled applications (Salesforce.com, Dropbox)

The cherry on the sundae is the BOYD movement. Almost makes you want to sell used cars, instead!
4. INCREASED RISKS FROM BYOD

The changes in your business model, together with your ever-evolving network demands, means your business is under increased pressure from attackers and threats. The newspapers are flooded with stories of the latest breaches, the latest vulnerabilities and the latest targeted assaults.

Threats to the enterprise posed by an employee-owned mobile device can be as complex as a sophisticated malware attack designed to snoop on an employee's browsing activity or as simple as a lost phone in a taxicab.

Spam Rears its Ugly Head, Again

In the mobile world, it seems like it is 1990 again. Established techniques, such as pornography, spam and phishing— that worked well in the desktop world—are now successfully migrating to the mobile world. Since many of these tactics are device-agnostic, expanding the attack to target mobile devices is relatively simple: Phishing, scams, and spam target users on all devices, trying to get hold of users’ credentials, other confidential information (such as credit cards) or any sensitive corporation data that just happens to be on the device. While a good email security product can protect users from these types of attacks on corporate-owned computers, there are no such safeguards for mobile devices.

---

Top 10 Risks of BYOD

1. Employees who jailbreak their devices, allowing them to run potentially malicious apps
2. Employees using workarounds to access company network regardless of policy
3. Employees whose devices are permitted to connect to any open, unsecured Wi-Fi
4. Employees fail to patch applications, allowing older, unsecured version to run
5. Employees fail to password protect their device
6. Employees who don’t restrict applications from collecting as much data as possible
7. Employees who don’t read the fine print when installing applications and grant excessive permissions
8. Employees sign up for storage services that don’t meet corporate guidelines
9. Employees who refused to allow companies to remotely wipe their personal devices
10. Steady increase in mobile malware

5. DON’T FIGHT CHANGE—EMBRACE IT

Given human nature, it does no good to fight the BYOD trend. As a species, we gravitate to the next shiny object and are always anxious to adopt new technologies. We want to be connected (always on) with our friends, our communities, our world and our company.

To protect your company, you must create policies and procedures to facilitate the advantages of BYOD while managing the risks. “Embracing BYOD will make your company more agile, adaptable, reduce costs and make your team more productive,” says Craig Sroda, chief strategy officer of Pinnacle Group. “The upside is huge. So, don’t fight it or you may lose the opportunity to engage and motivate your team.” (Source: Don’t Fight Bring-Your-Own-Device (BYOD) to Work. http://craigsroda.com/dont-fight-bring-device-byod-work)

6. SELECTING A TEST SOLUTION

The selection of a network security solution is one of the most critical decisions your organization will make, and that decision is validated through testing. It’s no good to catch 95% of the threats when it only takes one to bring your network down or compromise your IP or customer data. Consequently, the choice of the right security testing solution is equally important.

When selecting a security testing solution, here’s what to look for.

Mobile environment application traffic generation capabilities:
You need complete visibility into the ability of your solution to inspect all the types of traffic it will encounter when in production. An exhaustive library of authentic protocol data units (PDUs) is essential for assuring that the solution is ready for the full range application traffic found on today’s mobile driven networks.

Latest attacks and malware prevalent in BYOD environment mixed with old attacks, which are getting recycled:
While cybercriminals are constantly inventing new ways to make your life miserable, some of the old tried-and-true threats remain in widespread use. Malicious spam is still prevalent, often in combination with some event with national or worldwide exposure, such as a disaster or sporting event. Brute-force login attempts increased three-fold in 2013. DDoS attacks have increased in both volume and severity, and are now being used as a distraction to draw attention from a different type of attack on the same target. Consequently, it is essential your security testing tool offers a complete encyclopedia of known attacks to test against your security solution.

The real challenge presented by BYOD for businesses is in the area of security-IT administrators may be unprepared to deal with various security issues that may occur from the use of personal devices in the workplace. (Source: “Understanding Mobile Security in the BYOD Era.” 4/4/14. http://www.dqindia.com/dataquest/feature/212360/understanding-mobile-security-byod-era/page/1)
The power to test at the scale of user traffic and of the Internet: Given the behavior of the always on, always connected generation, the amount of strain on your network from a user experience perspective is higher than ever. Some user activities, while non-critical to business success, slow down the network for legitimate users, who become frustrated. To exploit this situation the cybercrime community has amassed a daunting array of network and computing power to overwhelm your security infrastructure. Your security testing solution must be able to match the scale of the attacks your security solution will encounter, and to go beyond today’s levels to ensure your network is ready for what will hit it in the future.

Configurable and repeatable test scenarios: Repeatability is the foundation of meaningful testing. When you detect a problem, you must be able to test the new build or configuration under the same conditions that produced the problem to know it really fixed the problem. Your testing solution must be configurable to create any environment or condition required, and then be able to recreate it on demand.

Interoperability with all the platforms you need to support, including mobile devices: If your BYOD strategy allows tablets, then your test platform must be able to test the ability of your security solution to detect and stop threats coming from tablets. Otherwise, the increased risk posed by BYOD has not been mitigated or addressed.

Easy-to-configure interface and quick time-to-test through pre-configured test scenarios: Your test platform should test your security solution, not your team. They have enough demands on their time without working with a test platform that requires significant training to understand and configure. Your IT team may not have decades of security testing under their belt, and they shouldn’t have to. Look for a test platform that accelerates time-to-test by building in best practices discovered through years of experience by career testing professionals in the form of pre-configured test scenarios.
7. CONCLUSION

Security professionals have long recognized the weakest link in their best laid plans is the user sitting in front of a screen—regardless of whether it’s a 32-inch Full-HD LED-Lit monitor or a 4-inch retina display. Gone are the days of IT-controlled devices.

BYOD is here to stay. The global market is expected to reach USD 238.39 billion by 2020 and industry analyst Forrester Research predicts that by 2016, 350 million employees will use smartphones and 200 million will bring their own mobile devices to the workplace.

(Sources: http://www.prweb.com/releases/BYOD-Market/GrandViewResearch/prweb11744138.htm

The result will be a great boost to productivity, but your job is to balance the benefits of BYOD with the mission of keeping your enterprise safe.

Luckily, there are sophisticated tools that help you make sure that your security measures are intact, no matter what your users think of next. Tools that quickly and easily allow you to:

• Manage bandwidth demands
• Withstand both new and recycled types of attacks
• Mitigate the risks from unknown applications
• Safeguard critical data during connections to unsecured networks
• Protect your company from itself

At the end of the day, your company’s continued success depends on the security of its data. It’s up to you to uncover and destroy the hidden threats to your network.
8. LEARN MORE

Find out more about how to protect your network from BYOD threats and learn more about Spirent’s Security Authority by visiting us at www.spirent.com. Check out our Network Security Testing and Application Security Testing solutions.

Spirent Security Testing provides our customers with the confidence and knowledge to trust that their network is secure, risks are mitigated, and that customer and company data is protected. We develop the highest quality products that allow our customers to easily, quickly and thoroughly prove they are prepared to face tomorrow’s challenges and grow their business with confidence.

Spirent Communications is a global leader in test and measurement and offers an extensive portfolio of solutions to test network and application security, data centers, cloud computing environments, high-speed Ethernet networks and services, 3G/4G wireless networks and devices, and global navigation satellite systems.

Spirent solutions for security testing include:

- **Security:** Verify the detection and prevention of malware, spam, DDoS and known attacks, and the effectiveness of fuzz testing and application white/black lists
- **Traffic Detection and Classification:** Verify that the latest applications and protocols are detected
- **Application Control:** Validate the ability to control detected applications through features like white listing, connection/rate limiting, application QoS, URL filtering and data loss prevention/data exfiltration
- **Congestion Management:** Confirm bandwidth and connection-rate control capabilities
- **Policy Enforcement:** Ensure applications do not evade application signatures
- **Scalability and Performance:** Validate the ability of the network security components (e.g., IPS/IDS, ALG, proxy and NAT) to handle millions of users running real applications