Enabling Secure BYOD
How Fortinet Provides a Secure Environment for BYOD
Executive Summary

Bring Your Own Device (BYOD) is another battle in the war between security and usability. End users from the CEO down to line workers want the ability to use personal devices for work purposes, their belief being that personal devices are more powerful, flexible, and usable than those offered by corporate. Organizations also look to capitalize on this trend by shifting maintenance costs to the employee, eliminating the standard-setting role of IT. Workers have discovered the power of constant connectivity and have come to expect secure access to their corporate network regardless of location. The promises of increased productivity and worker satisfaction have brought BYOD to the forefront of most IT discussions today.

On the opposite side of this discussion is security. BYOD opens up numerous challenges around network, data, and device security along with blurring the lines of privacy and accessibility. Many organizations have tried a variety of approaches to allow for BYOD in their organizations, with limited success.

This paper will detail the security challenges posed by a BYOD environment. It will describe many current approaches to solving the problem – in terms of policy and products that a variety of vendors have introduced into the market. It will show how Fortinet provides security for users, applications, and data, enabling secure mobile device access in any networking environment, regardless of other technologies or solutions in place.
Contents
Executive Summary.......................................................................................................................... 2
Introduction .................................................................................................................................... 4
Addressing the Challenges Associated with BYOD ........................................................................ 5
  Bandwidth and Productivity Drains ............................................................................................ 5
  Data and Device Loss .................................................................................................................. 6
  Attacks against Mobile Devices ................................................................................................. 6
Policies and Products Used to Secure BYOD .............................................................................. 6
  Explicit Policies ......................................................................................................................... 6
  Technical Controls .................................................................................................................... 6
Fortinet’s Approach to the BYOD Challenge ............................................................................... 7
  The Power to Control the Network .......................................................................................... 7
    An Industry-Leading Firewall ................................................................................................. 7
    Intrusion Prevention ............................................................................................................... 7
    Antimalware/Antivirus ........................................................................................................... 8
  The Power to Control Applications ......................................................................................... 8
    Application Control ............................................................................................................... 8
    Data Loss Prevention ............................................................................................................ 9
  The Power to Control User Behavior ..................................................................................... 9
    Web Content Filtering .......................................................................................................... 9
    SSL and IPSEC VPN ............................................................................................................. 9
    Endpoint Protection ............................................................................................................. 9
Fortinet Supports a Wide Variety of BYOD Solutions ............................................................... 9
  Fortinet Supports MDM ........................................................................................................... 9
  Fortinet Secures VDI Environments ....................................................................................... 9
  Fortinet Provides Endpoint Security and Enforcement ....................................................... 10
How Fortinet Addresses Some Common BYOD Scenarios .................................................. 10
Conclusion .................................................................................................................................... 11
About Fortinet ............................................................................................................................ 12
About FortiOS .............................................................................................................................. 12
Introduction

The impressive sales of Apple’s iPad, the rapid adoption of the Android OS, and Microsoft’s introduction of Windows 8 – an operating system designed from the ground up for a mobile platform - illustrate the continuing trend towards mobility. Since 2008, when laptop sales first outpaced desktop sales, organizations of all sizes have had to contend with the challenges around securing a more mobile enterprise. This trend towards a more mobile workforce appears to be continuing, with no end in sight. Forecasts from Gartner, illustrated in Figure 1, shows the number of tablets sold per year increasing from 18% of total PC sales (laptops and desktops) in 2011 to 61% in 2015.

![Tablets as a % of PC Sales](image)

**Figure 1 - Tablets as a Percentage of PC Sales (Gartner)**

As sales of mobile devices increase, so does the use of personal devices for work purposes. A 2012 global survey of CIOs found that 28% of employees currently use personal devices for work related tasks with an inspected increase to 35% by mid-2013¹. A recent Forrester survey² also supports this trend (see figure 2) showing over 40% of companies either buying smartphones for employees to use or paying the monthly bill for the plan.

---

¹ Bring your own device – Agility through consistent delivery (2012) – PwC
² The State Of Workforce Technology Adoption, US Benchmark 2011
The use of personal devices for work purposes, which blurs the lines between work and personal activity, is the primary catalyst for the many concerns that organizations are facing around BYOD. Organizations struggle with implementing the right balance of technologies and policies to ensure that BYOD is both secure and effective. A 2012 PwC survey found that only 27% of respondents believed their company’s mobile security could pass an audit and only 43% reported that their organization had even implemented a policy for employee owned devices³.

This paper will detail the security challenges posed by a BYOD environment. It will describe many current approaches to solving the problem, in terms of policies and products that a variety of vendors have introduced into the market. Finally, this paper will show how Fortinet is an integral part of any BYOD solution, providing network-based security for users, devices, and data.

Addressing the Challenges Associated with BYOD

BYOD provides a variety of advantages to organizations, ranging from improved productivity to increased ROI for IT departments who make the migration. However, a BYOD environment also lacks many of the traditional security controls that organizations have relied on to secure their data, leaving gaps in their data and device protection strategy. The following are just a few of the most common BYOD pitfalls facing organizations today.

Bandwidth and Productivity Drains

Many employees have found that mobile devices often do not have the same strict policy enforcement capabilities as desktop devices. This policy gap enables many employees to use their mobile devices to access video streaming and other applications that are denied by standard corporate policy. With mobile devices offering a way to bypass the limits normally imposed on these applications and behaviors, users are putting a strain on the corporate network bandwidth and being less productive.

³ Bring your own device – Agility through consistent delivery (2012) – PwC
Data and Device Loss
With devices operating outside the confines of the traditional brick and mortar enterprise, the potential for data loss increases significantly. The threats to mobile users include the risk of malware infection, inadvertent or malicious sharing of critical business data or even the devices being lost or stolen. Additionally, rogue wireless networks exist in the public with the sole purpose of stealing unprotected data.

Attacks against Mobile Devices
Even mobile devices themselves are increasingly becoming the target of attack. Hackers have started to realize the potential goldmine of data that exists within mobile devices and unauthorized app stores provide an easy means of distribution for mobile applications—some of which are not legitimate.

None of these challenges are new, but in the past organizations have had the ability to lock down devices through policy or software in order to ensure that users were following corporate policy. In a BYOD world however, organizations are limited in their ability to force device and users to conform to corporate policies. As a result, several approaches to addressing BYOD have emerged.

Policies and Products Used to Secure BYOD
In order to address the balance between usability and security, organizations are taking a variety of steps. While some draconian approaches (such as denying all personal devices on the corporate network) might be warranted for extremely secure organizations, most organizations want to adopt a BYOD policy that offers some flexibility for users while enforcing corporate policies and adopting best practices. In order to address these requirements, organizations are taking the following approaches to addressing BYOD challenges.

Explicit Policies
Most organizations first address the BYOD challenges through explicit policies. This is where the organization should decide the extent of any BYOD program. Some organizations will still choose to limit access to certain data or applications. An organization may also choose to require employees to have specific software installed on their device in order to use a personal device on the network.

The organization determines what devices they will allow on the network and generates policies stating appropriate devices and acceptable behaviors. Many organizations also must decide which technical controls they plan to implement in order to enforce corporate policies.

Technical Controls
Creating the corporate policy is a necessary first step for creating a secure mobile environment but ultimately organizations need technical solutions in place to enforce policy. Technical controls can vary from network-based to device-based and no single solution is appropriate for all organizations. Some of the most common technical controls associated with enforcing BYOD policies are listed below.

Virtual Desktop Infrastructure (VDI)
Server-based VDI is the creation of a user’s desktop environment, from operating system through applications, in a virtual machine (VM), run on a hypervisor and hosted in a centralized server. The hosting server simultaneously supports multiple virtual desktops, with the number of virtual desktops supported limited by several factors, most notably the configurations of the desktops and the computing capacity of the server. The virtual machine instances that contain the virtual desktops are established and torn down based on business requirements—an on-demand attribute. Also, based on business requirements and rules, virtual machines can move from one physical server to another.

Allowing mobile devices to access VDI gives organizations the ability to leverage their existing investment in VDI and provides a secure window into the corporate network. VDI does not allow for cross-pollination of data between the user’s personal device and the corporate infrastructure. VDI helps alleviate policy enforcement concerns because the enforcement still occurs on the corporate network.
Mobile Device Management (MDM)
MDM has become synonymous with mobile security. However, MDM is not a complete solution to BYOD challenges as it does not provide a complete security solution—most MDM and endpoint clients are designed to address many challenges that are not security related such as:

- Software Distribution
- Policy Management
- Inventory Management and
- Service Management

MDM does provide an expanded level of policy enforcement that is not enabled by default. MDM allows policy enforcement on the mobile device itself and many solutions offer remote location/lock/wiping capabilities to protect against loss or theft. However, MDM solutions enforce different policies based on the mobile device they are supporting resulting in inconsistent security coverage.

Endpoint Security Clients
Endpoint security clients are an extension of traditional anti-malware clients. The majority of traditional endpoint security vendors have created mobile versions of their clients allowing for a combination of anti-malware, VPN, and remote wiping capabilities on the endpoint itself. Like their desktop counterparts, endpoint security clients increase management headaches by requiring the installation of an agent.

Network-Based Enforcement
As the name implies, network-based enforcement relies on the network to enforce policies and controls around what the client, data, and user can do or access. Network based enforcement requires a great deal of granularity and intelligence on the network to provide adequate access controls to prevent nefarious activity.

A key advantage of network-based enforcement is the location of the targeted data ultimately resides on the network. Establishing controls on the network itself allows an organization to block malicious software or activities coming from mobile devices before any damage can occur to the network.

Fortinet’s Approach to the BYOD Challenge
Fortinet understands that there is no silver bullet to address the challenges posed by mobile devices. Solving the many problems required a technology-driven, multi-pronged approach. Fortinet has a wide portfolio of products that can address the new threat vectors provided by mobile devices and enforce policy compliance for users wherever they may be. Specifically, Fortinet provides secure mobility by protecting the network, the data, and the client.

The Power to Control the Network
The network is the core component of an organization. Any disruption to the network is a disruption of services for users and the business. Fortinet was built to effectively defend the network from a wide variety of threats and every Fortinet appliance provides the following:

An Industry-Leading Firewall
Fortinet firewall technology combines ASIC-accelerated stateful inspection with an arsenal of integrated application security engines to quickly identify and block complex threats.

Intrusion Prevention
Fortinet IPS offers a wide range of features that can be used to monitor and block malicious network activity including: predefined and custom signatures, protocol decoders, out-of-band mode (or one-arm IPS mode), packet logging, and IPS sensors.
Antimalware/Antivirus
Fortinet antivirus technology combines advanced signature and heuristic detection engines to provide multi-layered, real-time protection against both new and evolving virus, spyware, and other types of malware attacks in web, email, and file transfer traffic. FortiASIC™ Content Processors, integrated into FortiGate® and FortiWiFi™ products, accelerates both signature scanning and heuristics/anomaly detection for protection against viruses, while delivering performance that scales from entry-level appliances to multi-gigabit core network or data center platforms.

The Power to Control Applications
Next to the availability of services, the data is the next critical component for organizations. A loss of data can mean a violation of compliance mandates, the loss of critical intellectual property, and most importantly, the loss of customer trust. Fortinet provides granular protection of an organization’s most sensitive data through a variety of controls including:

Application Control
Web 2.0 applications, such as Facebook, Twitter and Skype are increasing the volume and complexity of network traffic, and expose organizations to a new generation of web-based threats and malware. Fortinet Application Control leverages one of the largest application signature databases available - the FortiGuard® Application Control Database. This allows for the control more than 2,200 different Web-based applications, software programs, network services and network traffic protocols. FortiGuard Services deliver regularly scheduled updates to FortiGate consolidated security appliances, ensuring that Fortinet Application Control always has the latest signatures available (see Figure 3).

Fortinet provides extremely granular control around applications. For any recognized application, Fortinet can control access to that application or behavior within the application (chatting within Facebook) and can provide this granular control by user, group, time of day, and numerous other criteria.
Data Loss Prevention

Data loss events continue to increase every year, resulting in fines, penalties and loss of revenue for companies worldwide. Many data loss events are caused by trusted employees who frequently send sensitive data into untrusted zones, either intentionally or by accident. Fortinet DLP uses sophisticated pattern matching techniques and user identity to detect and prevent unauthorized communication of sensitive information and files through the network perimeter. Fortinet DLP features include fingerprinting of document files and document file sources, multiple inspection modes (proxy and flow-based), enhanced pattern matching and data archiving.

The Power to Control User Behavior

Finally, the mobile client itself is at risk from attack when off the home network. Fortinet secures mobile clients – laptops, smartphones, and tablets – protecting end users while they are travelling or simply working from outside the office. Fortinet has solutions aimed at the endpoint itself that allow for protection of mobile devices and encrypted communications from any location.

Web Content Filtering

Integrated into all FortiGate® and FortiWiFi™ appliances and FortiClient™ endpoint security agents, Fortinet Web Filtering technology gives the option to explicitly allow web sites, or to pass web traffic uninspected both to and from known-good web sites in order to accelerate traffic flows. Users can receive real-time updates from FortiGuard® Web Filtering Services to determine the category and rating of a specific URL. You can also easily add Web sites or URLs to the local URL filtering list using both text and regular expressions.

SSL and IPSEC VPN

With the number of threats accelerating, secure communications between enterprise networks, businesses and partners, and corporations and mobile workers is now more important than ever. Data breaches, information leaks, and infected networks and systems are costing corporations and government agencies billions of dollars every year.

Endpoint Protection

The Fortinet FortiClient™ endpoint security solutions provide anytime, anywhere endpoint security for network endpoints. When used in connection with FortiGate® appliances, FortiClient provides a range of security features to protect the network and ensure policy compliance. Fortinet also has mobile One Time Password applications available for both Android and iOS to provide strong authentication.

Fortinet Supports a Wide Variety of BYOD Solutions

Fortinet is a network-based solution, but can also support the other methods of BYOD enforcement described above. Fortinet provides flexibility for organizations to choose technology partners that solve specific problems in their environment and then apply security policies to ensure that enforcement occurs when necessary. Some examples of this end-to-end support are provided below:

Fortinet Supports MDM

As described previously, MDM solutions provide additional controls to help control costs and enforce policy on mobile devices. Fortinet supports MDM by ensuring that any device authenticating on the network has a corporate approved MDM product installed on their endpoint. Fortinet can also ensure that the devices remain clean and that sensitive data is not transferred to mobile devices.

Fortinet Secures VDI Environments

VDI is another popular BYOD solution that Fortinet secures. VDI provides a seemingly secure window into the corporate network, but security challenges remain. The virtualized device at corporate is susceptible to malware and other attacks. Fortinet can secure the virtualized environment ensuring that data is not compromised by devices entering the network.
Fortinet Provides Endpoint Security and Enforcement
In addition to FortiClient, Fortinet can provide additional endpoint security to augment any endpoint client that the organization might choose. Fortinet can scan endpoints for malicious content and for corporate approved applications before they are allowed on the network.

How Fortinet Addresses Some Common BYOD Scenarios
Solving the challenges posed by BYOD is not limited to a single technology. This is the key reason that Fortinet is well positioned to tackle BYOD for organizations. Table 1 below illustrates several common customer scenarios that occur when implementing BYOD. Fortinet can address each of these scenarios out of the box, with no extra licenses or equipment to purchase.

<table>
<thead>
<tr>
<th>The Challenge</th>
<th>How Fortinet Solves the Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>A customer needs guest access to Skype on their iPad while visiting your headquarters</td>
<td>Wi-Fi Guest Access</td>
</tr>
<tr>
<td></td>
<td>Bandwidth Management</td>
</tr>
<tr>
<td>An employee to safely browse the web on his iPad at a conference</td>
<td>Content Filtering</td>
</tr>
<tr>
<td>An employee is at Starbucks and needs to communicate and be protected as if she was at HQ</td>
<td>VPN Technologies</td>
</tr>
<tr>
<td></td>
<td>Two-factor Authentication</td>
</tr>
<tr>
<td>An employee needs spam-free email when using the corporate network</td>
<td>Email Filtering</td>
</tr>
<tr>
<td>An employee has started streaming movies while at work through his tablet – this is against corporate policy</td>
<td>Application Control</td>
</tr>
<tr>
<td>An employee unintentionally shares a sensitive company presentation via his personal Gmail account on his Android Phone.</td>
<td>Data Loss Prevention</td>
</tr>
</tbody>
</table>

Fortinet secures this wide variety of scenarios and environments by providing a core foundation – FortiGate – with the ability to secure connections regardless of whether they are devices connected to a local LAN via a wireless controller (see Figure 4), or connecting through a WAN (see Figure 5) – via another organization’s network or even over a cellular connection. All FortiGate devices can provide control for wireless access points and many FortiGate models have wireless controllers built in.
Conclusion

Mobility can increase productivity for employees, enabling them to do more business outside the office. The challenge for organizations is to continue to provide the same level of security regardless of the device or location of the employee. Fortinet provides a rock-solid feature set that allows organizations of any size – from small business to mobile operator – to build a robust infrastructure and provide secure mobility to all their employees.

Fortinet addresses BYOD challenges by providing a robust solution that provides consistent application of security policies regardless of connection type. Fortinet’s inclusive licensing allows organizations to implement whatever combination of security policies and technologies they feel are most appropriate for their needs. The unique combination of Fortinet's
integrated wireless controls, extensive security technologies, and cost effective licensing make Fortinet an easy choice for organizations looking to implement a flexible and secure BYOD program.

**About Fortinet**

Fortinet delivers unified threat management and specialized security solutions that block today’s sophisticated threats. Our consolidated architecture enables our customers to deploy fully integrated security technologies in a single device, delivering increased performance, improved protection, and reduced costs. Purpose-built hardware and software provide the high performance and complete content protection our customers need to stay abreast of a constantly evolving threat landscape. Our customers rely on Fortinet to protect their constantly evolving networks in every industry and region in the world. They deploy a robust defense-in-depth strategy that improves their security posture, simplifies their security infrastructure, and reduces their overall cost of ownership.

**About FortiOS**

FortiOS is a security-hardened, purpose-built operating system that is the software foundation of FortiGate multi-threat security platforms. FortiOS software enables high performance multi-threat security by leveraging the hardware acceleration provided by FortiASIC™ content and network processors. This combination of custom hardware and software gives you the best security and performance possible from a single device. FortiOS helps you stop the latest, most sophisticated, and dynamic threats facing your network today with expert threat intelligence delivered via FortiGuard® Security Subscription Services.

FortiOS 4.0 software redefines network security by extending the scope of integrated security and networking capabilities within the FortiGate multi-threat security platform. Regardless of the size of your organization, you can benefit from the most comprehensive suite of security and networking services within a single device on the market today.