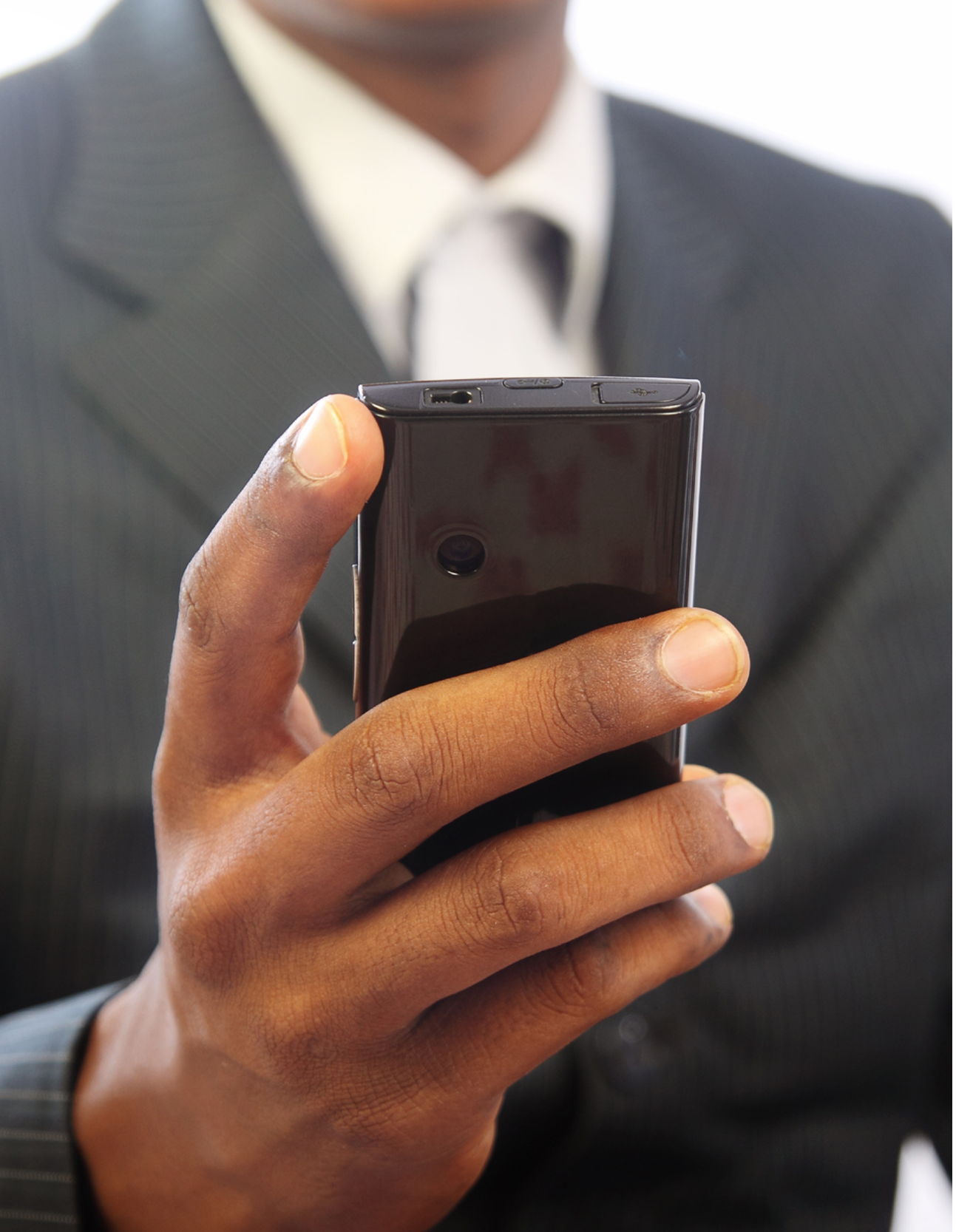
An Intellyx White Paper sponsored by Dispersive Technologies

Intellyx White Paper: Rethinking BYOD Security

Jason Bloomberg

May 28, 2015



1965: You want to run a report, so you submit a job. Two days later you get a large binder full of striped paper, festooned with inscrutable data.

1985: IT sets up your first PC at your desk. It's difficult to use and even more difficult to fix. You're happy to leave it behind when you go home.

2005: You finally get your first laptop. Now you can bring your work home with you. Need support? Bring that boat anchor back to work.

2015: You use your laptop less and less. Instead, most of your day-to-day work takes place on your smartphone or your tablet. They belong to you, although your company may reimburse you for the bill. You might have an iPhone or one of any number of Android models—but that's not unusual, as your colleagues switch device models faster than millennials change their hair color.

Welcome to the world of BYOD—*Bring Your Own Device*. BYOD, and the consumerization of IT generally, continues to explode as devices become more powerful, diverse, connected, and affordable—improving worker productivity and morale.

Today, IT leaders realize that BYOD is a strategic value-add rather than simply a threat they now have to manage. BYOD is here to stay. Are you ready?

The Context for BYOD

Like it or not, BYOD is now a reality. Regardless of whether your company supplies devices or not, your employees will want to bring their own devices to work. They will try to connect them to the corporate network, and furthermore, they will want to do their work remotely with those devices.

Don't get caught by surprise. Both business executives as well as IT leadership must be proactive with their BYOD strategy. It's absolutely critical to implement a comprehensive BYOD program that provides users with a secure, approved method for accessing all necessary corporate resources from their personal devices.

The crux of such a program, of course, is ***security***. Protecting corporate data and other resources, as well as ensuring regulatory compliance, are paramount concerns. And yet, completely locking down employees' devices is not an option.

The result is a complex balancing act that focuses on empowerment of employees while protecting essential corporate assets. Err in one direction and risk a costly and embarrassing breach. Err in the other and risk lower morale and productivity—and possibly losing the organization's best people.

The BYOD Threat Profile

The first step to putting together a BYOD security strategy is to hammer out the organization's threat profile. The purpose of a threat profile is to understand the company's tolerance for risk. Some industries like financial services and insurance are more risk adverse, while others are willing to take more risks. Such factors impact the specifics of each profile.

To understand how BYOD fits into the threat profile, IT management must understand the impact that BYOD will have to the infrastructure as well as IT personnel. Both network architecture and management must rise to the challenge. Existing device management platforms must scale to accommodate the number of devices, and the network must support the increase of Wi-Fi traffic.

The corporate email communications infrastructure must also be ready to support remote devices. Identity management, SharePoint or other corporate portals, and any collaboration technology in place must support a wide range of access technologies.

The variety of device form factors and technologies also varies, and can be expected to increase over time. Android and Apple iOS, millions of mobile apps, and devices from watches to digital televisions may all interact with corporate assets.

Furthermore, simply excluding particular devices from the organization is a fool's errand, as employees will use them regardless—possibly without informing management. It is far better to have an inclusive BYOD strategy that allows employees to use any device than to have an overly restrictive policy that encourages people to break the rules.

What You Need to Protect

How, then, can any organization achieve its security goals with such an inclusive approach? The answer is to secure what needs to be secured—and don't worry about the rest.

Secure what needs to be secured—and don't worry about the rest.

The days of tightly controlled desktops and networks are long gone. It is essential to properly secure certain corporate data (often including emails and other business correspondence) and access to sensitive applications. Other information or device apps—

including personal information that belongs to the user as well as less sensitive corporate data—need not be as secure.

Therefore, isolating the user's personal information from corporate productivity apps and corporate data is an essential part of BYOD security. It's important to protect this sensitive content in the case of lost or stolen devices, attacks on devices, or the communication between them and corporate data sources.

There should also be an appropriate protocol in place should an employee leave the organization—wiping sensitive information and apps while leaving the rest of the device untouched, or better yet, preventing sensitive data from residing on the device in the first place.

Current Approaches to BYOD Security

The starting point for BYOD security, as with most other IT projects, is policy. Furthermore, BYOD policies have implications beyond the IT shop. They also impact legal, HR, and the broader security organization—as well as any department that leverages mobile devices. In other words, the entire company.

As a result, establishing rules and policies for employees is the first step in any BYOD security program. These policies should cover asset management, encryption, passwords, protection of data on devices, and the configuration of email, virtual private networks (VPNs), and even Wi-Fi.

Selective Remote Wipe

The team should establish policies for what to do should a device become lost or fall into the wrong hands. *Selective Remote Wipe* is the standard approach today for dealing with lost or stolen devices, as it leaves the device in a usable state. With this approach, IT can send a signal to the device to order it to delete sensitive information while leaving personal information intact.

Furthermore, based upon policy, a device may automatically selectively remote wipe itself should it find itself out of communication from the IT department for a set period of time. However, this approach is not foolproof, as a determined hacker can copy the sensitive data from the device before the wipe order arrives, or they can simply remove the storage medium from the device altogether.

Encryption

Encryption is the standard approach for ensuring the confidentiality of data and is thus an important and broadly useful tool in the security professional's tool belt. Most encryption techniques follow ***P**ublic Key Infrastructure* (PKI) protocols that require the exchange of public keys between endpoints in a secure interaction.

Encryption, however, has its limitations. As available processing power increases, hackers are able to break increasingly sophisticated encryption protocols, leading to an ongoing battle between improved encryption technology and hackers seeking to compromise it. Encryption is also generally an "all or nothing" affair—if a message or file is encrypted, then little can be done with it unless it's decrypted, which may then open a security hole.

Furthermore, while private keys must be kept private, public keys must be public. However, if a hacker obtains a public key, they can use it to reduce the processing time necessary to gather information about the company that owns the private key and how they implement encryption, aiding the hacker further in their attacks.

Virtual Private Networks

VPNs are also a common and well-established security technique that can apply to BYOD scenarios. VPNs are secure channels between a server and a client that act like an open network (for example, an Internet connection), while in reality the entire channel is encrypted.

VPNs date back to the days of dialup modems, and are now prevalent for securing interactions between laptops and corporate servers. However, they can be difficult to use and are sensitive to adverse network issues. As a result, using them with mobile devices can be a frustrating experience—especially when a consistent, high-quality connection is necessary, for example, with live data streaming or video conferencing.

Additionally, VPNs—as well as encryption more broadly—impact performance, as they make messages larger and require the overhead of the encryption and decryption steps. The performance impact may be negligible on a wired network connection, but not so on many remote connections. However, users still expect high performance from mobile interactions—regardless of whether their devices are using Wi-Fi, 3G, or 4G.

As a result, there is typically a performance vs. security tradeoff—a tradeoff no organization wants to make.

Think Like a Hacker

Any worthwhile security strategy understands the types of attackers that may wish to cause damage, and what motivates them to do so. Some hackers are criminals with a straightforward profit motivation. Others simply want to cause mischief or damage for its own sake—or to show off to their friends. And then, of course, there are the governmental hackers with political or national security motivations.
Generally, however, hackers are after something—and they are interested in the simplest route to obtaining their goal. Therefore, they always look for vulnerabilities. Just as a burglar seek s the house with no security system and a pile of newspapers out front, hackers will poke around till they find the easiest way in.

Hackers will poke around till they find the easiest way in.

The value of the target is also an important motivator for hackers. If they can turn the data they seek into money in their pockets, then those data by their very nature become a target. It is important, therefore, for IT managers to focus their BYOD security efforts on their most valuable assets, as well as presenting a comprehensive security front whose weakest point is still stronger than targets the hacker might consider at other organizations.

The Man-in-the-Middle Problem

Because of the inherent complexity and unpredictability of modern distributed networks, a particularly appealing hacking approach is the *Man-in-the-Middle (MiM)* attack. With MiM attacks, the hacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

Sometimes the hacker is only interested in eavesdropping. In those situations, the hacker makes separate connections with both the sender and recipient of a message, and then acts as a relay between them—unbeknownst to either party.

As a result, both parties believe their conversation is private, but in reality the hacker controls the entire conversation. They can listen in, as well as change any message in either direction to suit their needs.

MiM attacks depend upon the ability of the hacker to impersonate each endpoint well enough to fool the person at the other end. Encryption techniques, including Transport Layer Security (TLS—the successor to SSL) is the traditional approach to preventing such attacks. Unfortunately, these traditional techniques are not sufficient for protecting sensitive enterprise data in a BYOD scenario.

For example, a large PC manufacturer recently put adware on their computers, with the intent of placing ads into certain customer web interactions. Unfortunately, this adware was easy to compromise, and led to the "Superfish" MiM attack.

The more recent FREAK attack was even more damaging, since it hit all major operating systems, including the popular Android mobile device OS. This SSL/TLS vulnerability resulted from an intentional weakness in the public key infrastructure intended to allow the NSA with all its processing power to spy on encrypted messages—only now a few dollars of cloud computing power will suffice.

Phishing is also a common way for MiM attacks to circumvent traditional encryption approaches. The hacker tricks a user into downloading a file or clicking on a malicious link in an email, giving the hacker sufficient access to internal systems to mount such attacks.

Perhaps the most sobering aspect of an MiM attack is that it may not be apparent that a hacker has penetrated the organization's network. Shrewd hackers will hide their tracks as long as they can, stealing what information they are able to for as long as they remain undiscovered. Clearly, it is absolutely essential to be proactive with BYOD security to prevent such attacks.

Dispersive Technologies: Securing BYOD without Compromise

With offices in Georgia and Virginia, Dispersive Technologies has taken a page out of military communications security and applied it to the Internet in spectacular fashion. Their novel cybersecurity approach increases the degree of difficulty that even the most determined hacker must face in order to mount an attack.

What they offer their customers today, however, isn't the most important part of their story. The real win here is Dispersive Technologies' long-term ability to stay several steps ahead of hackers, even as the malefactors inevitably improve their own techniques.

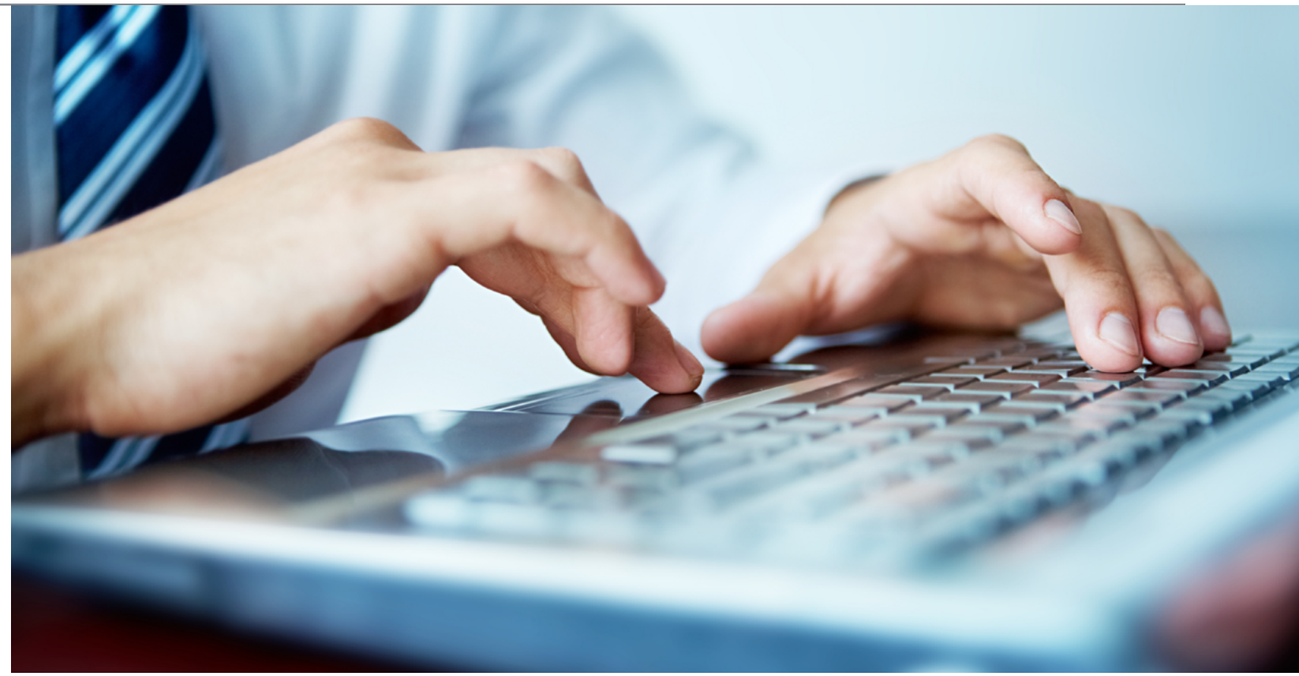
The real win is Dispersive Technologies' long-term ability to stay several steps ahead of hackers.

Dispersive Technologies plays three roles in the BYOD environment. First, Dispersive Technologies reduces the probability that a personal device will become contaminated with malicious software. Second, they help secure networks even while mobile devices are connected to them. Dispersive Technologies also offers a novel approach for securing data at rest—an essential capability that complements securing data in motion.

Spread-Spectrum Technology

Dispersive Technologies' software-defined solutions virtualize routing and data storage for IP-based networks. Their *Dispersive™ Virtualized Networks* offer a differentiated approach to cybersecurity that takes a page out of now-traditional military radio spread-spectrum security approaches.

With this technology, radios rotate frequencies randomly or split up communications traffic into multiple streams, so that only the receiving radio



can reassemble them properly. With Dispersive Technologies, however, the Internet (or any network) is now the underlying communications platform.

Dispersive™ Virtualized Networks (Dispersive™ VNs) not only split a single message into several different parts, but they can encrypt each component message separately and even route them over different protocols following independent paths. They can put this routing on servers, computers, and even mobile phones.

Dispersive Technologies' innovation doesn't stop with simply splitting up the messages. The data also "roll" dynamically to optimum paths—both randomizing the paths the messages take while simultaneously taking into account congestion or other network issues.

As a result, they're making an attacker work a lot harder. Hackers would have to figure out the paths, the hops, and what order to put the messages in—a daunting task. Better to simply move on to another target—at a different company.

Hackers would have to figure out the paths, the hops, and what order to put the messages in. Better to simply move on to another target—at a different company.

Spearing the MiM Attack

While encryption is traditionally the key defense to MiM attacks, the easy and inexpensive availability of today's parallel processing power makes all encryption relatively easy to crack. To fill this need, Dispersive Technologies' cutting-edge technology blocks MiM attacks.

A central element of the Dispersive offering is *SoftSwitch*, which is server-based network

management software that hosts the trusted peer database, stores communication protocols and route information, and authenticates all network components and their allowed services and service levels. SoftSwitch also tracks the changing identity of mobile devices to ensure that communications continue without interruption when devices are moving around.

Another key element of the Dispersive™ VN approach is their client, which allows an edge device to send and receive data via the Dispersive™ VN, configures devices automatically, and sets the parameters for device communications. Client software can typically reside on any IP-enabled device—not only mobile handheld devices, but even Internet-of-Things endpoints.

Better and Faster than VPNs

Encryption-based MiM prevention technologies like SSL/TLS as well as VPNs are point-to-point. However, today's complex digital world requires secure end-to-end communications, where traffic might cross many intermediate nodes—all of which become weak points ripe for MiM attacks. It's possible to mount MiM attacks simply by figuring out the SSL or VPN termination point.

Not only does Dispersive Technologies provide end-to-end security, their approach essentially removes the need for VPNs altogether. As a result, Dispersive Technologies offers better security and performance than VPNs with fewer headaches.

Securing Data at Rest

Dispersive Technologies also offers *Dispersive™ SDS*, which is a software-defined storage platform that divides data into smaller blocks and sends each block to a different device selected from a geographically dispersed, virtualized pool of available storage devices. It then shuffles the locations of these blocks dynamically and reassembles the data at the client upon request.

By dividing data blocks across multiple storage locations, Dispersive Technologies conquers traditional problems with securing data at rest. Dispersive™ SDS provides tighter security by thwarting hackers more effectively than encryption alone. Capturing usable information becomes a costly, time-consuming guessing game for a hacker, with little chance of success—even if the hacker has installed malware through a phishing attack.

Furthermore, by presenting a "save" option at the client interface, the corporate IT department can force users to save their data to a virtualized pool of cloud-based storage, instead of on the local client's internal storage. As a result, there is no longer a need to remotely wipe drives if a personal device is lost or stolen, since no corporate data ever reside locally on the device.

The Importance of Centralized Management

It's important to remember that BYOD security is never solely about technology. Any comprehensive BYOD strategy balances technology solutions with the human component—both the responsibility of device users as well as centralized management within the IT shop.

In fact, centralized management, including provisioning devices, managing authorizations, and dealing with compromised devices are an important part of any BYOD plan. To this end, Dispersive Technologies offers broad capabilities to support centralized management.

The Dispersive™ VN Gateway Server is centralized management software which allows an edge server to handle communications for multiple devices at a physical location so they can send and receive data via a Dispersive™ VN.

As part of its BYOD policy, the corporate IT department can mandate that all personal devices used to access corporate networks must use Dispersive™ VNs. IT managers can then configure Dispersive VNs to intercept all application traffic and route via a Dispersive™ VN Interface Server.

The IT manager preloads this Interface Server with approved applications, and the server can also include white and black listing, deep packet inspection, and other approaches to protect against data exfiltration from the client device. This technique is especially useful in protecting against data compromise that might result from a phishing attack.

As part of a comprehensive BYOD approach, Dispersive Technologies' centralized management approach is the linchpin that allows for secure BYOD without compromising user flexibility. Furthermore, Dispersive Technologies' solution doesn't limit performance. In fact, it actually *improves* performance, as it adds multiple network routes automatically, thus increasing available bandwidth and routing around network bottlenecks.

In this way Dispersive™ VNs speed up the first and last mile—offering enterprises an unmatched combination of security, flexibility, and performance.

Dispersive Technologies offers enterprises an unmatched combination of security, flexibility, and performance.

Conclusion

Ongoing enterprise digital transformation—and the rise of mobile technologies in particular—have redefined how companies do business. And yet, we've only scratched the surface of what such new technologies will offer over time.

New IP-connected devices enter the market daily. End users—both consumers and within the enterprise—are rapidly incorporating these technologies into their day-to-day lives at home and at work. Such technologies transition from nice to have to absolutely essential at an increasing velocity.

And yet, with every technology advancement, new security challenges and threats emerge. The IT organization—and in fact, the entire enterprise—must consider these challenges and threats as part of a comprehensive threat management strategy. BYOD security is rapidly becoming an essential part of this new reality.

Dispersive Technologies is well-positioned to help its customers ride the wave of BYOD. Their approach makes MiM attacks quite difficult, and sometimes increased difficulty is all the prevention organizations need. But for other situations, simply raising the bar for hackers isn't sufficient.

Now that Dispersive Technologies also offers cutting-edge security for data at rest as well as in motion, these solutions are an even more important part of any comprehensive BYOD security plan. While no security can ever be perfect, achieving the right balance between risk and cost is a challenge every organization must address. Dispersive Technologies can be an important element of rising to that challenge.

About Dispersive Technologies
Dispersive Technologies creates software-defined solutions that virtualize routing and data storage for IP-based networks.

Its virtualized routing platform delivers data with speed, security and reliability—and does it across standards-based IP networks. Its software-defined storage solution securely stores at-rest data and moves it dynamically within the virtualized environment. When recalled or queried, data is delivered quickly, securely and reliably.

Together, these platforms improve software-defined networking and offer a holistic approach that protects both parts of the data equation. By streamlining and securing communications and data flow, Dispersive Technologies' solutions allow organizations to perform more efficiently and reduce costs. To learn more, visit us at www.dispersivetechnologies.com.

Dispersive Technologies
2555 Westside Parkway, Suite 500,
Alpharetta, GA 30004
1-844-403-5850
Sales: 1-844-403-5852
Support: 1-844-403-5851
info@dispersivegroup.com
www.dispersivegroup.com
