FROST & SULLIVAN

The Evolution of Mobile Security

Breaking Down Barriers for a Holistic Security Ecosystem

A Frost & Sullivan Executive Brief

www.frost.com

Jason Reed, Senior Industry Analyst

Cybersecurity

50 Years of Growth, Innovation and Leadership

UBIQUITOUS MOBILITY

The contemporary workforce relies on mobile devices for day-to-day productivity. In a recent survey of senior business leaders, Oxford Economics found that 80% believe that mobile devices are essential for employees to do their jobs. The report concludes that "**modern work is mobile work.**" The evidence supports their conclusion: 75% state that mobile devices are a critical component for their workflow, and approximately two-thirds expect that employees will be available remotely on their mobile devices.[1]

The ubiquity of mobile computing is apparent among senior executives, who often conduct a significant share of emailing and other business activities on a mobile device. Given that emails containing sensitive information are routinely opened for the first time on a mobile device, implementing robust security controls on these devices should be a top priority for any organization. **Too often, however, mobile security is less of a priority than more traditional network and endpoint security deployments.**

It would be an overstatement to suggest that mobile devices have replaced desktop computing, but it is clear that the augmented capabilities that modern devices offer will only increase in importance in the coming years. There is, however, little uniformity among organizations in how mobile devices are integrated into business processes: it is estimated that a majority (72%) either permit or plan to permit some kind of bring-your-own-device (BYOD) model for their business operations.[2] The plethora of devices and operating systems in enterprise ecosystems can make the task of keeping mobile devices secure extremely complicated.

1. https://image-us.samsung.com/SamsungUS/samsungbusiness/short-form/maximizing-mobile-value/WHP-HHP-MAXIMIZE-MOBILE-VALUE-JUN18.pdf?CampaignCode=https-www-samsung-com-us-business-short-form-maximizing-mobile-value-thank-you-form-Maximizing-Mobile-Value-download-now
2. http://www.techproresearch.com/article/byod-iot-and-wearables-thriving-in-the-enterprise/

Enterprise mobility management (EMM) solutions offer a starting point for securing mobile endpoints in a company-issued mobile environment; however, as the mobile threat landscape evolves and more sophisticated hackers target mobile users, these management systems are not sufficient for current enterprise needs. An EMM platform's core functionality includes:

- Ensuring policy and configuration standards are met;
- Tracking device location and activity;
- Updating device operating system and applications; and
- Remotely resolving technical issues.

These functions, while important, are not a substitute for a mobile security solution. EMM is an effective management and policy enforcement tool, but organizations must do more than install an EMM solution to address mobile security concerns. By understanding the current mobile threat landscape, and tracing the evolution of mobile security solutions, organizations can move toward a holistic model of mobile threat defense.

THE MOBILE THREAT LANDSCAPE: THE EXPANDING ATTACK SURFACE

The widespread adoption of personal devices that run divergent types of hardware, operating systems, and applications poses enormous challenges for cybersecurity professionals. The prevalence of mobile devices in the workforce represents a substantial broadening of potential attack surfaces, which would otherwise be limited to internal networks and traditional endpoints, such as desktops or laptops.

Modern devices introduce several new attack vectors that must be taken into account by security professionals. The vulnerabilities in each attack vector require tailored countermeasures that nevertheless maintain overall coherence and functionality within an organization's security deployment. The main mobile threat vectors are:

- Network: When mobile devices connect to public Wi-Fi they are exposed to man-in-the-middle attacks. Whether assisted by an external device such as a Wi-Fi Pineapple, or executed without one, these attacks allow hackers to intercept traffic on poorly secured Wi-Fi networks. This traffic might include login credentials, financial information, or other sensitive business data.
- Applications: Whether by infecting an application with malware or by using another technique to install innocuous (but damaging) malicious software onto mobile devices, the application layer provides near-limitless opportunities for hackers. In addition, unsafe apps are available in

app stores. These apps are not designed to be malicious, yet pose a threat to sensitive corporate data by virtue of poor design, inherent vulnerabilities, or reliance on third-party services. In a BYOD environment, this attack vector is of even greater concern, as it is often impractical for security teams to prepare for every possible new application vulnerability on personal devices used for business.

- Operating Systems: A common concern for security professionals is the number of vulnerabilities routinely found in operating systems such as iOS or Android. Security updates for operating systems appear regularly; however, enforcing user compliance in installing these patches can be challenging for the security team.
- Device: Hardware itself is also vulnerable to attacks from hackers. Bluetooth and near-field communication, for example, are both vulnerable to attackers with the right tools. Other times, devices can be compromised at the hardware level to render encryption useless unless it is protected with additional hardware-secure elements. Finally, malicious public charging stations can also compromise devices.

While mobile threat vectors are unique and require specific tools and techniques to address, organizations must be cautious not to allow mobile security to operate in a silo, independent from other security procedures and processes. Advanced threats often overlap and pose a risk to all endpoints, both traditional and modern. Moreover, mobile devices are often a point of entry for an attacker to gain access to more sensitive data held upstream in the corporate network, meaning that mobile security must operate in sync with other security products. Too often, mobile security is either an afterthought or the implementation is insufficient to properly protect sensitive business data.

THE EVOLUTION OF MOBILE SECURITY IMPLEMENTATIONS

There is an echeloned structure to mobile security implementations in enterprise environments. Most organizations fall somewhere on the spectrum between three stages, or tiers, of mobile security standards. These levels can be broken down into three levels of mobile security.

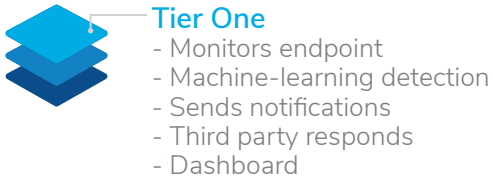
Exhibit 1: The Varying Levels of Mobile Security Implementation

Tier One: Detect and Alert

The Detect and Alert tier is the baseline mobile security implementation. A Tier One security configuration is focused on detecting irregular behavior or alerting IT administrators of a compromised device. These solutions monitor activity on a mobile endpoint in real time and send notifications of suspicious activity to administrators, who must then triage and respond to the alert. It is common for these administrators to be the third party. Often,

Tier One solutions include a dashboard where admins have visibility across all of the mobile devices that they are charged with protecting, and summary statistics regarding traffic flow and other activities are easily accessed.

Exhibit 2: Tier One Features



In today's advanced threat landscape, however, Tier One implementations leave much to be desired. The time required for an attacker to successfully exfiltrate sensitive data following a breach is often measured in single-digit minutes. The success of the Detect and Alert model depends on exceptionally fast response times from security professionals. There is a significant likelihood that the alert or the response will come too late to prevent substantial damage.

Tier One protection can also stumble when confronting a complex BYOD mobile environment. If organizations issue company-owned mobile devices, ensuring that each device is managed is more straightforward; however, in the modern workplace, many use their personal devices for business tasks. Other situations make it impractical to insist that every device that accesses sensitive data is managed via an EMM (for example, if the organization employs external contractors). Moreover, most organizations have adopted some form of hybrid model where some employees use company mobile devices and others use personal devices. Furthermore, these relatively basic Tier One configurations can fail to guard against the most sophisticated hacking techniques. Even more dangerous are social engineering methods, where activities are initiated by the user and seem legitimate. Relying on Tier One solutions for remediation in today's complex business environment is not sufficient.

Tier Two: Real-time Protections

The Real-time Protections tier is characterized by layering new capabilities onto the more simplistic, detection-based Tier One. Most vendors today are at various stages of rolling out Tier Two solutions.

Exhibit 3: Tier Two Features

Building on the features that are offered by Tier One solutions, Tier Two adds:

- **Targeted Protections:** Specific corporate resources can be identified and isolated for protection from suspected compromised devices. Examples include Office, salesforce.com, or even corporate Wi-Fi.
- **On-demand VPN:** VPNs are used for a number of reasons, but one specific advantage that an on-demand VPN delivers to mobile users is the ability to mitigate the risk of a man-in-the-middle attack when connecting to public Wi-Fi.
- **Automatically quarantine or remove unsafe applications or devices:** An advanced mobile security solution constantly scans applications and devices for safety risks and upon discovery can automatically quarantine an application or device and prevent it from accessing any data until its risk can be properly assessed.
- **Disallow connection to unsafe networks:** Even without a VPN enabled, Tier Two implementations can often detect network anomalies and prevent the user from connecting to a potentially compromised network.
- **Disallow unwanted downloads or unsafe URLs:** Effective in combatting phishing campaigns, modern mobile security deployments can prevent unintended downloads or block unsafe links contained in, for example, an email.

Many mobile security products on the market today have implemented some variation of the Tier Two feature set. These are generally grouped under the title Mobile Threat Defense (MTD).

While MTD is effective and is often sufficient to protect mobile endpoints, it is still to some extent limited by the degree to which these solutions are integrated into the overall security ecosystem. As they seek to attain new levels of functionality and protection, security vendors are rapidly racing to implement the next generation of mobile security solutions.

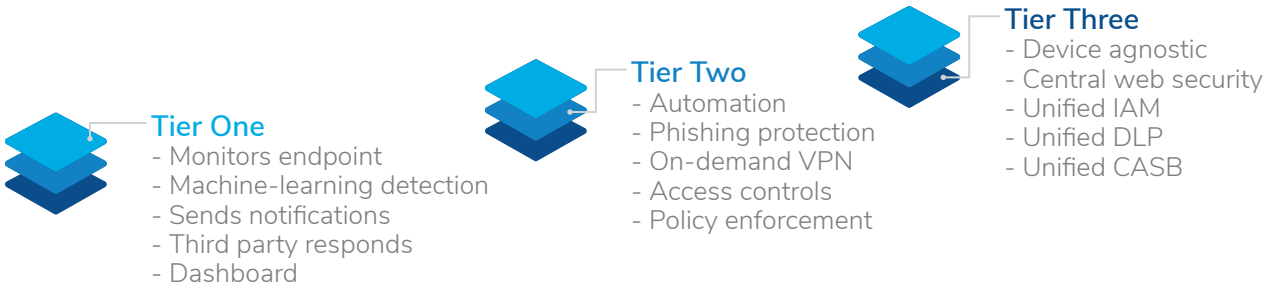
Tier Three: Integrated Defense

If Tier Two shows the current state of the mobile security market, Tier Three represents the direction that the market will be moving. Integrated Defense entails moving beyond security silos toward a fully integrated solution. This approach dissolves the boundaries between different types of endpoints and allows security professionals to visualize their entire network traffic and data flows in a fashion that is functionally device agnostic.

In this model, mobile security tools seamlessly communicate with other agents in an organization's security deployment, allowing for new capabilities that stretch beyond the still somewhat limited contemporary MTD model. Specifically, the Tier Three mobile security solutions allow organizations to centrally manage:

- Web security across all endpoints: A single policy that automatically adapts based on the device used to access the internet.
- Unified identity access management (IAM): Streamlining IAM processes so that all devices can be managed using a single solution.
- Unified data loss prevention (DLP): Streamlining DLP policies so that an overarching framework is built and controlled using a single solution.
- Unified Cloud Access Security Broker (CASB): CASBs are frequently deployed as security "gatekeepers" between traditional endpoints and the cloud; however, these are rarely seen in the mobile security ecosystem. Tier three defense systems will integrate CASBs into mobile security, unifying the defense of mobile endpoints with traditional endpoints.

Exhibit 4: Tier Three Features



Tier Three solutions not only secure individual devices but provide an integrated platform to enforce policies and processes. The enterprise market seems ready to embrace a consolidated, holistic approach to security that dissolves security silos and improves outcomes.

THE WAY FORWARD IN MOBILE SECURITY

Mobile security is frequently a lower priority compared to traditional endpoint protection, and too many organizations conceive of this field as discrete from other types of cybersecurity. While substantial organizational resources are directed to secure traditional endpoints, too often mobile endpoints are not weighted equally. This is to the detriment of overall organizational security posture, as mobile endpoints can make up 50% of the endpoints that access corporate data in a given organization.

Breaking down the barriers that separate mobile security from traditional security deployments is critical for the realization of a seamless security ecosystem. The barriers between products and tools lead to gaps in enterprise security armor and leave holes for hackers to exploit.

Fortunately, market trends point to the emergence of holistic security configurations that do not discriminate between devices or operating systems. Individual solutions such as the mobile security solutions described here must work in concert with other agents in an organization's security deployment to eliminate gaps in the security posture. Enterprises should monitor the market in the coming months for vendors that offer visionary, integrated solutions to maximize their data security and minimize the risk of a data breach.

FROST & SULLIVAN

Silicon Valley
3211 Scott Blvd
Santa Clara, CA 95054
Tel +1 650.475.4500
Fax +1 650.475.1571

San Antonio
7550 West Interstate 10, Suite 400,
San Antonio, Texas 78229-5616
Tel +1 210.348.1000
Fax +1 210.348.1003

London
Floor 3 - Building 5,
Chiswick Business Park
566 Chiswick High Road,
London W4 5YF
Tel +44 (0)20 8996 8500
Fax +44 (0)20 8994 1389

877.GoFrost • myfrost@frost.com
http://www.frost.com

NEXT STEPS

- Schedule a meeting with our global team to experience our thought leadership and to integrate your ideas, opportunities and challenges into the discussion.
- Interested in learning more about the topics covered in this white paper? Call us at 877.GoFrost and reference the paper you're interested in. We'll have an analyst get in touch with you.
- Visit our Digital Transformation web page.
- Attend one of our Growth Innovation & Leadership (GIL) events to unearth hidden growth opportunities.

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?