MTL Security Checklist for 2018

5 Things you need to be working on

Mobile Thought Leaders (MTL) Research gathers insights from professionals focused on advancing or supporting mobile and digital transformation initiatives.

MTL members are always interested in security but the nature of those conversations has evolved over the years from device security to content security and now on to a much more sophisticated stack of technologies and management models designed to address the constantly changing nature of the threats.

The members are largely in agreement that organizations should be addressing the following five areas of security on an on-going basis. These five areas represent bundles of technologies and require cross-functional guidance and expertise. They also require:

1 Identity

Identity Management is the linchpin to many of the next phases of security. Understanding identity as a fully contextualized concern: a person or system, a machine, a time, a place, the nature of the request and so much more ought to be considered and you likely want to have multiple potential responses - not just yes or no, but many "yes if" pathways, like dynamic 2 factor, multiple paths for secondary validation. These things are needed to ensure that the gates are high and strong enough for savvy malicious actors but also melt away for legitimate communications. All of the other items on this list leverage Identity.

2 Single Sign-On

Your advances in Identity will be hard to appreciate until you are able to implement those rules across all the infrastructure and systems. 100% of MTL members report that there are SaaS applications being used in their organizations. Most members report that they know there are plenty of them being used that IT doesn't know about. Some SaaS applications will work fine through a proxy, but SSO is the carrot that greatly enhances user experience and is the carrot for increasing the chances that IT will know more about of the SaaS apps in use.

3 Unified Endpoint Management

Unified Endpoint Management (UEM) has come to full maturity as all the major management platforms have added traditional computing operating systems to their capabilities - and all the major operating systems have added sufficient open APIs to make management truly unified. You may already have a tool in place that has fully matured from EMM to UEM but now the real project is rationalizing your management approach to take advantage of these new capabilities. Part of this new discipline is getting very good at adapting and leveraging updates that happen far more often (and with much less notice) than with traditional (old fashioned, really) desktop management environments.

4 Digital Workspace

The debate about whether you should focus on native apps, web apps, or virtualization is over and the answer is "yes." MTL members have accepted that they will continue to have a variety of applications that need a portfolio approach to manage security that is dynamic and responsive to the context of the requesting user. Digital Workspaces allow for users to have one place and one way to get to their applications while the context of their request and their identity determines the method and amount of resources to deliver. This method allows all of the security controls and decisions to be managed on the backend so users can focus on work instead of getting to work. With all the right things in place, a worker could log into their workspace from a known device and get access to a native app with local storage or a borrowed device and be offered the virtual version of the same thing without any local storage - all hidden from the user.

5 Private Key Infrastructure and Certificate Management

If you don't already, you will have thousands or millions of things that need to communicate with systems. Most of those things will need to have their own means of validating their identity. While it is possible that blockchain technologies will get added to this requirement, the maturity and flexibility of current PKI and Certificate Management tools make them an absolute requirement for having a complete security portfolio.

There are two glaring omissions from this list. Neither of these areas can be left out of the security portfolio but have moved from the areas of focus because of the changing nature of computing.

1) **Document Management:** As much as digital rights management, scanning, watermarking and other leakage protections still have an indispensable place in the security arena, most organizations that are moving away from document-based work to places where the granularity of data and control is much smaller.

2) **Perimeter Protection:** For most mobile and digital transformation projects, the endpoints are the new perimeter. Even for on-premise concerns, the face and nature of network and perimeter has changed to a more fluid, virtual and responsive set of tools and controls. That said, most MTL members are more focused on projects that might leverage the internal network but not depend on it.

MTL Concierge Introductions

Click here if you would like to meet and gain insights from an MTL member on any of these topics.

Sponsor Spotlight

VMware WorkspaceOne provides most of the tools you need to achieve a future-proof security practice that is enterprise secure and consumer simple. The WorkspaceOne stack includes the leading UEM, an advanced digital workspace environment and Identity Manager (IDM). IDM can integrate across a wide range of sources of identity information, including the VMware UEM. The UEM includes industry-leading support for all the open APIs on iOS, Android, MacOS, Windows 10, ChromeOS and others. The WorkspaceOne digital workspace creates a unified and simple work environment for all users and all apps, including SaaS access, virtual apps, and native apps. Recently an MTL member organization tested having remote workers shift from laptops to tablets by providing all the apps they needed in WorkspaceOne. With the extensive data from app usage and access controls that WorkspaceOne provides they were able to determine that the mobile environment was more useful to the workers than their laptops, enabling them to eliminate a redundant and expensive piece of hardware from their kit.