NEW SECURITY MODEL

Is the current security model for the enterprise workspace sufficient?

The security model for the enterprise workspace has not changed in many years. The conservative base assumption was that the enterprise provides its employees the needed services to do their jobs. Based on that premise, the IT's job was to guarantee the implementation and security of those services. A typical workspace security protocol is designed to protect the physical premises of the enterprise. It includes a multilayer security architecture at the data center's entrance and an endpoint security protocol which is based on three elements; the secured perimeter (container), the VPN connecting the container to the data center, and the enterprise device management (EDM) controlling the VPN.

These three components create a kind of a "fortress" around the endpoint. Over the years, an additional element was added to the model, the MTD (Mobile Threat Defense), designed to ensure that the device itself is safe.

Traditionally, the MTD is built of four layers:

1. **Device behavioral anomalies** – detected by tracking expected and acceptable use patterns.

2. **Vulnerability assessments** – found by inspecting devices for configuration weaknesses that can lead to malware execution.

3. **Network security** – provided by monitoring network traffic and disabling suspicious connections to and from mobile devices.

4. **Application scans** – done regularly through reputation scanning and code analysis to identify malicious apps.

The combination of a security protocol and an MTD seems to create a bullet-proof defense, but in fact it is problematic. This workplace security model assumes that its users haven't changed their behavioral patterns in the last 20 years, while, in fact, user behavior has changed dramatically. From the way users look at devices and applications, to the way they consume services at work. This 'new' user is what makes the current security model severely insufficient for the modern workspace.

This workplace security model assumes that its users haven't changed their behavioral patterns in the last 20 years, while, in fact, user behavior has changed dramatically.

The new users model vs. the prior users model

The new generation users have almost nothing in common with the old users. Mainly since the boundaries between "work" and "personal" life have blurred. The new users behave more like consumers than like the old users. As such, their work pattern is different, they look at all devices as their property, whether they were provided by the enterprise or truly theirs. They expect to have the freedom to use any tools and services, as well as to change or replace them easily and quickly if necessary

The new generation users have almost nothing in common with the old users. Mainly since the boundaries between "work" and "personal" life have blurred.

Comparison between the new user model and the prior user model:

	NEW USER MODEL	PRIOR USER MODEL
Working location	Works from everywhere	Works mainly at the office
Who chooses services/tools	The user	The enterprise
Number of tools used	Many, as much as needed	A limited set
Kind of services	Mainly SaaS	Enterprise provided
Key parameters	Agility, user experience, efficiency	Standardization, governance, security

A closer look at the usage pattern of the new user and its impact on security

In the past, three main parameters have helped the enterprise in keeping the user on a high governance path.

1. Before the BYOD age, devices, were mostly provided by the enterprise.
2. Network connectivity was less available, much more expensive, and usually sponsored by the enterprise.
3. Applications were heavy, tailored to the needs of the enterprise, expensive, and needed high integration processes to the enterprise's data center.

None of these factors are relevant today. Devices nowadays are owned by the user (or treated as such). Wireless networks are available everywhere, are much cheaper and can be provided by the users themselves. Applications today are mostly SaaS and cloud based and provided by many different vendors. In addition, most applications nowadays are free for limited or focused use and work on a subscription model. Thus, making it more cost effective and easier to integrate or change services if needed.

Another important characteristic of the new users is that they dislike VPNs and Containers. For a generation that puts user experience on a pedestal, users are not willing to tolerate slow connectivity or low-availability of VPN. Furthermore, for most of the services they would like to use, there is no containerized version.

Therefore, the security mechanism must change as well.

Is MTD still needed?

Realizing that the container, the EDM and the VPN are not as relevant as before, leads to re-evaluating the last traditional security element, the MTD. Enterprise security applications' base line is making sure that there is no malware running in the system. The automatic action is to purchase proper security that will monitor the health of the device and make sure that it is malware free. Surprisingly, there's no need to pay for these security features anymore; nowadays it comes for free, as part of the OS on the device. Instead of relying on a 3rd party application to secure the device, the OS vendor takes care of it. Apple was the first, followed by Google and Microsoft; The inherited sandboxing mechanism in iOS, mac OS and Android keeps applications contained. The built-in Microsoft Defender, or Apple ExpertX systems are top-of-the-line anti-malware.

Additionally, the signature database behind all leading anti-virus vendors belongs to Google.

This effects the MTD in a few ways. Starting with Google forcing all applications to run in sandboxing; which made it very hard for MTD software to get access to information or impact other applications and processes.

Another issue impacting the MTD's effectiveness is OS vendors limiting the number of MTD applications running in the background. Some vendors prevent this totally. That means, that unless the user activates it, and keeps it in the foreground, the MTD will have serious limitations on its productivity. Lastly, OS vendors (especially in the PC domain) enforce many restrictions on device manufactures. One example would be to not include anti-malware as a preloaded. Some OS vendors even eliminated anti-malware software from their App Stores. As it seems, those limitations are going to be further enforced in the future, making the OS based MTD the most effective protection on the device itself.

What about malicious applications?

MTD is not helpful leveraging exploits which are being published from time to time. Only the OS vendor can solve, exploit, and eliminate the risk of malicious applications. It is important to understand that OS vendors are patching things really fast. In fact, there are companies like Blackberry that claim that their device is the most secured (except Google's). That's because they claim to have the fastest update time, from the release of a new version of Android until it is deployed on their devices.

Consequently, as long as the OS and its browser are updated to the latest versions, the devise is reasonably protected. Even if it might not always be the best solution, it is still much more efficient in patching than any protection an MTD can provide.

The Coronet Solution

The modern enterprise should adapt a new way of thinking with three major changes in mind.

1. The security policies should consider the changes in the ways employees use their devices for work purposes. It needs to provide the same user experience as a consumer, with as minimal interference as possible.
2. They need to trust the OS vendors. They provide the best protection available for the device.
3. The protocol needs to be adjusted to enable users to use any service they wish, have their agility and productivity, and still maintain security compliance.

The security policies needs to provide the same user experience as a consumer, with as minimal interference as possible.

A cost-effective security solution that is targeted for the new user behavioral patterns

It is understood that for the core enterprise services, such as your core banking applications, and a limited set of internal applications, you need to maintain your container-VPN-EDM infrastructure. However, for most SaaS services that your employees use, with or without the IT knowledge, you need a much more cost effective, agile model. It should enable the introduction of services without a need for integration and allow usage of all services, on any device, anywhere.

...for most SaaS services that your employees use, with or without the IT knowledge, you need a much more cost effective, agile model.

The perfect security model elements: behavioral patterns

For the core internal services: Use the existing Container-VPN-EDM or any other virtualization solution as the main elements of the fortress.

For all other services (SaaS or Internal), that are not provided by IT, or non-managed at all, use a solution that is service, device, and network agnostic. It should not require integration and would be designed to protect the enterprise for all activities outside of the fortress (container-VPN-EDM).

Make sure that all in-use devices are updated and configured to their latest version and that all OS security elements are running. This will secure the OS your container/virtualization is running. It will also guarantee the integrity of the container and the applications used to approach the SaaS services by the user outside of the fortress.

Have visualness of the infrastructure that the user connects through. Be able to automatically perform these four types of activities on any infrastructure (public, private) of any type (Wi-Fi, Cellular):

1. Identify and guide the user to a safe infrastructure,
2. Ensure that the user will not be a victim of connection-phishing and social engineering attempts during the infrastructure connection,
3. Identify compromised infrastructure in the proximity of users, or compromised infrastructure that the user is already connected to, and
4. Identify and alert an attacker trying to manipulate the user on a legitimate infrastructure.

These four activities combined will guarantee that data communication with important services is not performed through risky channels.

Use a security engine that employs elastic security; an engine that is aware of who the user is, what is the exact situation (where he is, what is in his proximity), and then reports back to the enterprise. This will allow to perform a surgical precision intervention, which will eliminate the danger to the organization, and that the user will understand and appreciate.

Use a security engine that will allow to perform a surgical precision intervention, which will eliminate the danger to the organization, and that the user will understand and

Summary

Organizations must adapt their security approach for their workspace. Users' behavior has changed from the ground up; OS providers' role in device security has become different and larger; and the services that are used by the users have become more SaaS oriented and consumed outside of the organization's fortress. This requires an adjusted security model and a different set of security tools. It will allow the organizations to add security to any service in minutes, with no integration, zero degradation of user experience, at a fraction of the cost.

To learn more: www.Coro.net

... allow the organizations to add security to any service in minutes, with no integration, zero degradation of user experience, at a fraction of the cost.