mobileiron

Mobile threat detection through machine learning

Discover the ideal technology for detecting unknown, zero-day mobile threats

Executive summary

The types of threats targeting enterprises are vastly different than they were just a couple of decades ago. Today, successful enterprise attacks are rarely executed by the "lone wolf" hacker and instead come from highly sophisticated and professional cybercriminal networks. These networks are driven by the profitability of ransomware and the sale of confidential consumer data, intellectual property, government intelligence, and other valuable data. While traditional PC-based antivirus solutions can offer some protection against these attacks, organizations need highly adaptive and much faster mobile threat defense (MTD) for enterprise devices.

To protect devices and data from these advanced attacks, the use of machine learning in MTD has quickly evolved as a highly effective security approach. Machine learning models can be trained to instantly identify and protect against potentially harmful activity, including unknown and zero-day threats that other solutions can't detect in time. Just as important, when machine learning-based MTD is deployed through a unified endpoint management (UEM) platform, it can augment the foundational security provided by UEM to support a layered enterprise mobile security strategy.

This paper examines some current MTD approaches to help organizations understand where those solutions may fall short — and how machine learning-based MTD can expand upon those capabilities by providing immediate, on-device protection against mobile attacks.

Introduction

Machine learning has quickly emerged as an important technology in MTD because it allows computers to develop more sophisticated behavior, such as pattern recognition, without being specifically programmed for it. Machine learning is a powerful yet unobtrusive technology that continually monitors application and user behavior over time so it can identify the difference between normal and abnormal behavior — and, most importantly, what might lead to malicious activity on a mobile device.[1]

The use of machine learning in enterprise security has gained momentum in recent years because of the speed, accuracy, and scale it provides compared to more common security approaches such as traditional desktop antivirus. As the mobile threat landscape evolves, security professionals need technologies that can quickly detect and remediate threats at the device level and escalate the most critical threats to the top of the pile. This is how machine learning-based MTD can help, because these capabilities go well beyond what cloud-based and antivirus solutions provide.

> "By observing how devices behave, you can determine what is normal and what is abnormal behavior, and what might lead to a malicious action. Machine learning is one of the ways to speed this process up."
>
> – Lucas Merian, "The best mobile threat defense is mobile threat detection." Computerworld, Nov. 2017

For example, many organizations are already using machine learning to solve mobile security challenges such as:

- **Machine-speed attacks:**
  Today's attacks, including unknown, zero-day threats, are executed at machine speed so IT must respond just as quickly. Machine learning can help admins quickly detect these threats and take appropriate action.
- **Device security:**
  There are billions of devices in the world, and many of them are highly vulnerable to mobile attacks. UEM is the ideal way to keep a large-scale mobile fleet safe from these exploits by deploying machine learning-based threat detection to millions of devices anywhere in the world.
- **Mobile threat intelligence:**
  Targeted attacks usually produce a very subtle change in the device and most of them are invisible to a human analyst. Sometimes detection is only possible by correlating thousands of device parameters through machine learning.
- **IT admin shortage:**
  There are simply too many security alerts, and too few humans, to detect and respond to threats in a reasonable amount of time. Machine learning can take a huge chunk of the threat processing load off their shoulders.

This paper covers the many benefits of machine learning in MTD to help organizations make informed decisions about their mobile security strategy moving forward.

1 https://www.computerworld.com/article/3238032/mobile-wireless/the-best-mobile-threat-defense-is-mobile-threat-detection.html

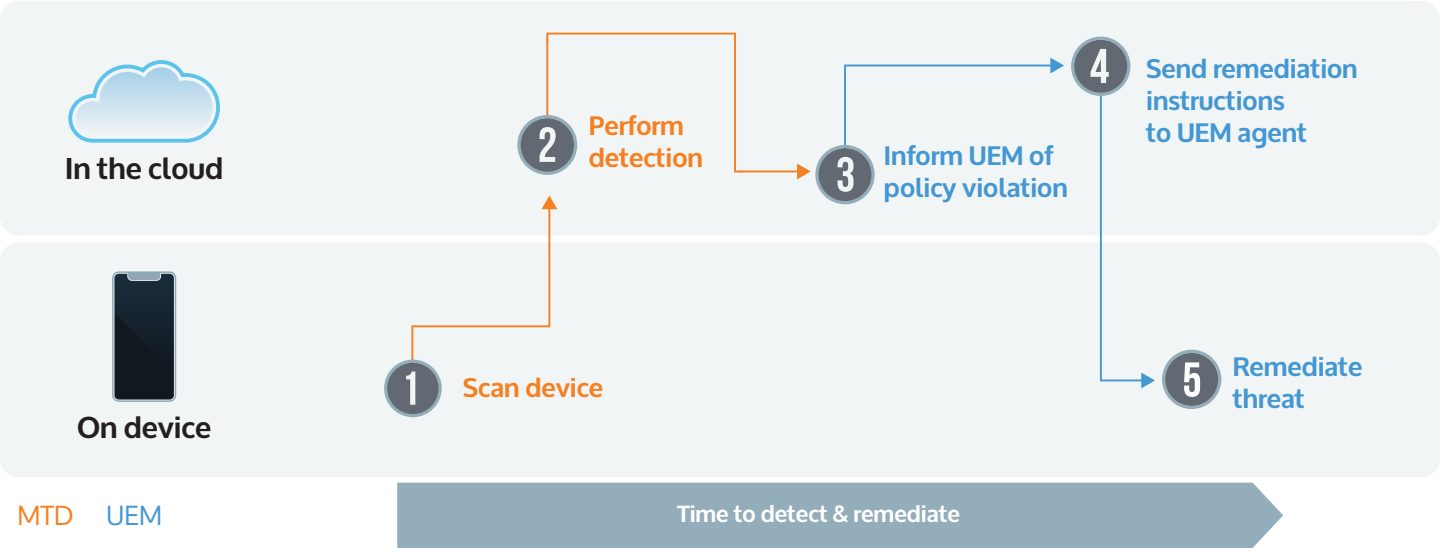
Today's threat landscape: Why some common solutions are less effective against modern threats

Cloud-based threat detection can delay threat remediation

Cloud-based threat detection solutions offer one approach to MTD, but they come with some drawbacks. First, these solutions can delay response time to device threats because they first must scan the device, then move that data off the device and send it to the cloud. The cloud agent must then inform the UEM solution about a potential security violation and send remediation instructions to a UEM agent on the device — a lengthy five-step process from device scan to threat remediation.

As part of this process, sensitive data such as a user's location is transferred to the cloud. This data transfer may be vulnerable to a man-in-the-middle (MITM) attack, which could prevent the remediation from ever being performed on the device. The exfiltration of sensitive data through this process can also violate many compliance regulations such as the General Data Protection Regulation (GDPR).

In addition, today's cloud-based solutions primarily detect known threats. Since they don't use machine learning algorithms, they are less adept at finding unknown, zero-day threats. Modern cyberattackers have become very skilled at changing some portion of the threat to avoid detection, so MTD solutions must be able to detect these anomalies as soon as they happen.



Traditional antivirus takes a reactive approach to mobile threats

When viruses originally targeted traditional desktops and servers, the attackers were often "lone wolves" motivated by the thrill of hacking. Since then, attacks have become far more sophisticated, driven by profit, and executed by highly organized cybercriminal networks.

To respond to threats, traditional security approaches have mostly focused on using signatures and sandboxing. These techniques first require a sample of the exploit to be identified and obtained. A security expert must then run the exploit in the sandbox to create a signature. This is nowhere close to the reaction time needed to stop highly adaptive mobile threats that move at machine speed. Mobile OS attack signatures are difficult to develop since security solutions don't have access to the same level of data, such as detailed file registries, that antivirus solutions have on traditional endpoints. Sandboxing restrictions on mobile devices limit access to user data. As a result, the updated signature file must be delivered to devices (if the solution delivers on-device detection) or to the cloud (for cloud-based lookups). This is too slow to be effective.

Signatures and sandboxing were adequate for slow-moving or older threats, but they are inadequate against malicious, unknown, and targeted attacks that are designed to remain stealth and persistent. While sandboxing and signature analysis can be useful for known attacks and some incident response efforts, traditional techniques are inadequate to combat unknown mobile attacks and exploit variants.

Machine learning: A requirement for mobile security

Hackers typically use three techniques to execute targeted mobile attacks:

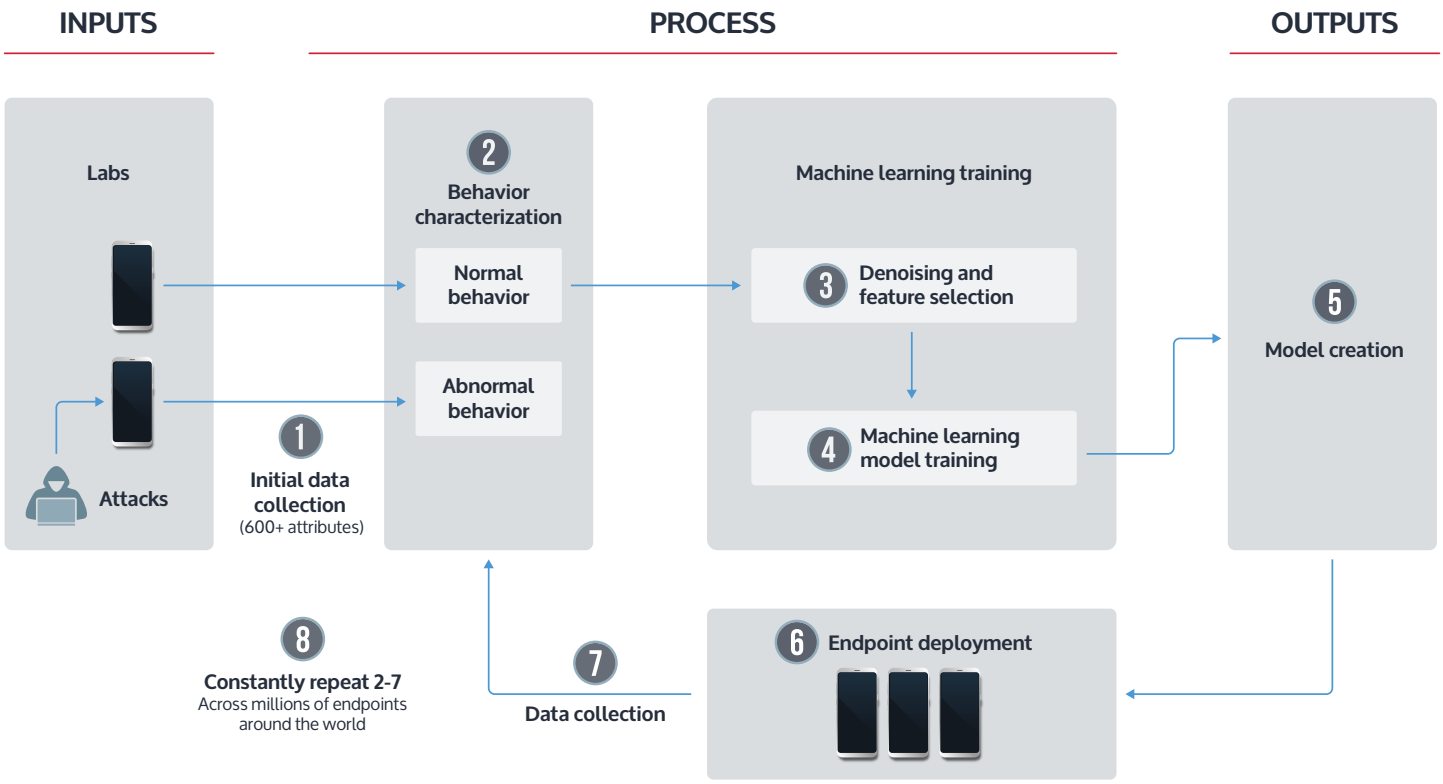
1. They use unknown or morphing attacks designed to avoid detection.
2. They focus on compromising the device, which is the primary way to remain persistent and control the device going forward.
3. They employ MITM attacks or phishing techniques to deliver the exploits required to compromise the device. This is far more efficient than dropping an app in the App Store or Google Play and hoping that someone from the targeted organization will download it.

The good news is, organizations can build upon the foundational security provided by UEM by adding on-device MTD that can:

- Augment traditional antivirus security with machine learning-based detection to stop unknown or morphing attacks.
- Simultaneously cover all attack vectors across the device (starting at the kernel), network, and app. This prevents a single point of failure from compromising a device.
- Detect threats on the device itself instead of requiring cloud-based lookups, which can delay a real-time response to threats.
- Combine cloud-based, machine learning training and on-device detection, which is the most effective approach to enterprise mobile security.
- Use the right environment for the right problem. This requires machine learning training on the billions of data points that need analysis, which should occur offline in the cloud. Detection, however, should occur on the device to prevent MITM circumvention and other risks associated with cloud-based approaches.

Cloud-based training for machine learning engines

To create highly accurate predictors of mobile threats, a machine learning engine must analyze (and reanalyze) billions of data points. In order to process a massive amount of data, the engine leverages dozens of high-performance computing clusters that live in the cloud to build machine learning models. The models are then distributed to the device to provide immediate detection of previously unknown threats — even without an Internet connection.



How cloud-based training works

In the cloud

1 **Initial data collection.** First, the model collects and analyzes hundreds of attributes from dozens of devices under normal use.

2 **Behavior characterization.** Each of the analyzed behaviors is classified as "normal" or "abnormal" (potentially malicious).

3 **Denoising and feature selection.** Every DNA attack has a unique profile of "reactions" or changes that can be seen in system data. Data points that could lead to inaccurate results are identified and eliminated. For each attack type, the relevant attributes are selected and weighted.

4 **Machine learning model training.** The engine iterates and is trained for optimal detection accuracy.

5 **Model creation.** The machine learning engine creates endpoint threat detection models based on the unique, optimized, and denoised combination of data points for each DNA threat.

On the device

6 **Data collection.** The bulk of machine learning occurs in the cloud. Billions of forensic data points are collected from millions of devices around the world and then analyzed in the cloud. The data provided from the devices is then used to continually repeat the entire learning process and refine the models, which are then deployed to endpoints.

7 **Endpoint deployment.** Once the models are delivered to devices, all actual detection occurs on the device in real time. Unlike signatures, the optimized behavioral detection models do not need to be updated for any new threat. This is because each threat's unique combination of system data does not vary and is easily detected by models. Until attackers create a new way to conduct these attacks, machine learning models will continue to detect unknown, zero-day threats.

Benefits of on-device, machine learning-based threat detection

Compared to cloud-based threat detection and traditional antivirus solutions, machine learning MTD solutions provide a number of benefits in the ongoing campaign against modern mobile threats. The top benefits include:

- **Unknown threat detection.** Unlike traditional antivirus solutions, machine learning detects previously unknown or zero-day threats.
- **Machine-speed detection.** Since mobile attacks occur at machine speed, protection must be able to respond just as quickly. Cloud lookups cannot match the speed of on-device detection due to the delays associated with traversing networks back and forth.
- **Optimal privacy protection.** By doing all detection on the device, data that may be considered sensitive does not need to be exfiltrated to the cloud.
- **No network connection required.** On-device detection provides immediate protection against network attacks, such as MITM, that can render cloud-based detection useless. Only on-device detection can continue to provide protection even when disconnected from the network.

mobileiron

How to find the right machine learning solution

Today, many mobile security vendors claim to provide a machine learning-based approach to MTD. Here's how to assess the depth of their capabilities.

Step 1: Ask the right questions

- Does the machine learning capability work without requiring a patient zero or sacrificial lamb?
- How extensive is the machine learning math model and how many years of testing has it undergone?
- How often does the solution need updating, including new signatures, to detect the latest threats?
- Does the machine learning capability work in both connected and disconnected environments?
- Can the solution work in milliseconds, with little impact to CPU and battery usage?

Step 2: Read their literature

In addition to these questions, review the blogs and other disclosures of each vendor. Pay close attention to the gap between when attacks first hit devices and when they were discovered. This will help determine if the vendor's machine learning engine is delivering optimally. For example, if a vendor blogs about a malicious app that has been in app stores for months and has millions of downloads, it is safe to assume that manual discovery and validation occurred. On the other hand, a disclosure about an attack that only had a few thousand downloads before discovery would indicate their machine learning MTD solution is effective.

Step 3: Try it yourself

Request a demo or proof of concept from the vendor to see how their solution works in your environment. This will also give you some insight into the quality of the company's implementation and support services as well.

MobileIron Threat Defense

In contrast to cloud-based mobile threat detection, sandboxing, and signatures, MobileIron uses a machine learning-based approach designed specifically for enterprise mobile security. In partnership with Zimperium, the machine learning engine analyzes system data to identify malicious behavior, and then creates sophisticated math models to enable on-device detection. The engine is not looking for a fingerprint of a known bad threat; it detects device, network, and application (DNA) attacks while consistently learning and improving the engine's accuracy. As a result, it can quickly detect attacks, even those never seen before, by analyzing specific actions that indicate a threat is occurring or imminent. Just as important, our machine learning and on-device threat remediation capabilities are integrated into a single application that can be deployed to all your mobile devices without requiring users to take any action to activate or update the client.

For more information about MobileIron Threat Defense, visit www.mobileiron.com/threatdefense.

MobileIron is redefining enterprise security with the industry's first mobile-centric, zero trust platform built on a unified endpoint management foundation to secure access and protect data across the perimeter-less enterprise.

mobileiron

490 East Middlefield Road

Mountain View, CA 94043

globalsales@mobileiron.com

www.mobileiron.com

Tel: +1.877.819.3451

Fax :+1.650.919.8006

mobileiron