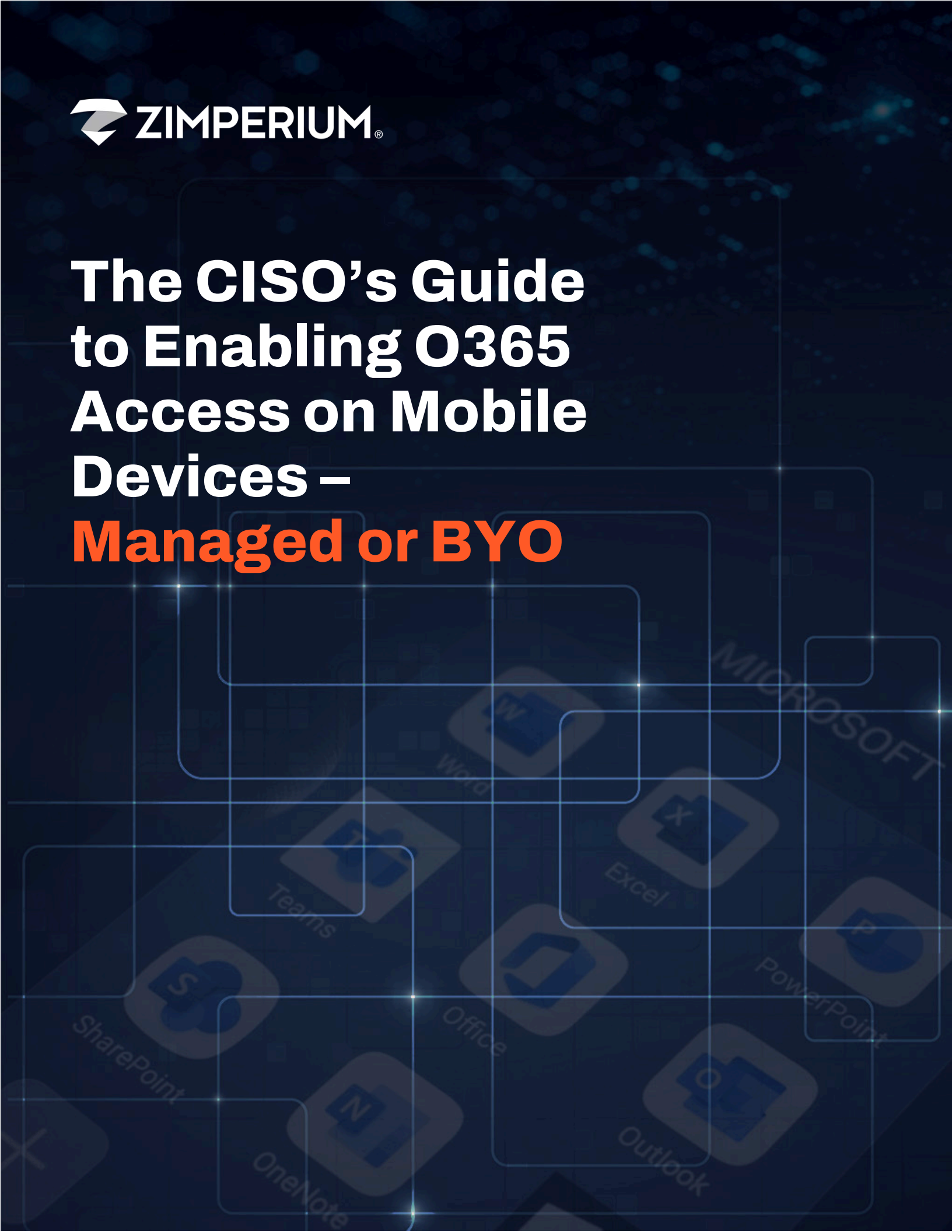
ZIMPERIUM®

The CISO's Guide to Enabling O365 Access on Mobile Devices – Managed or BYO



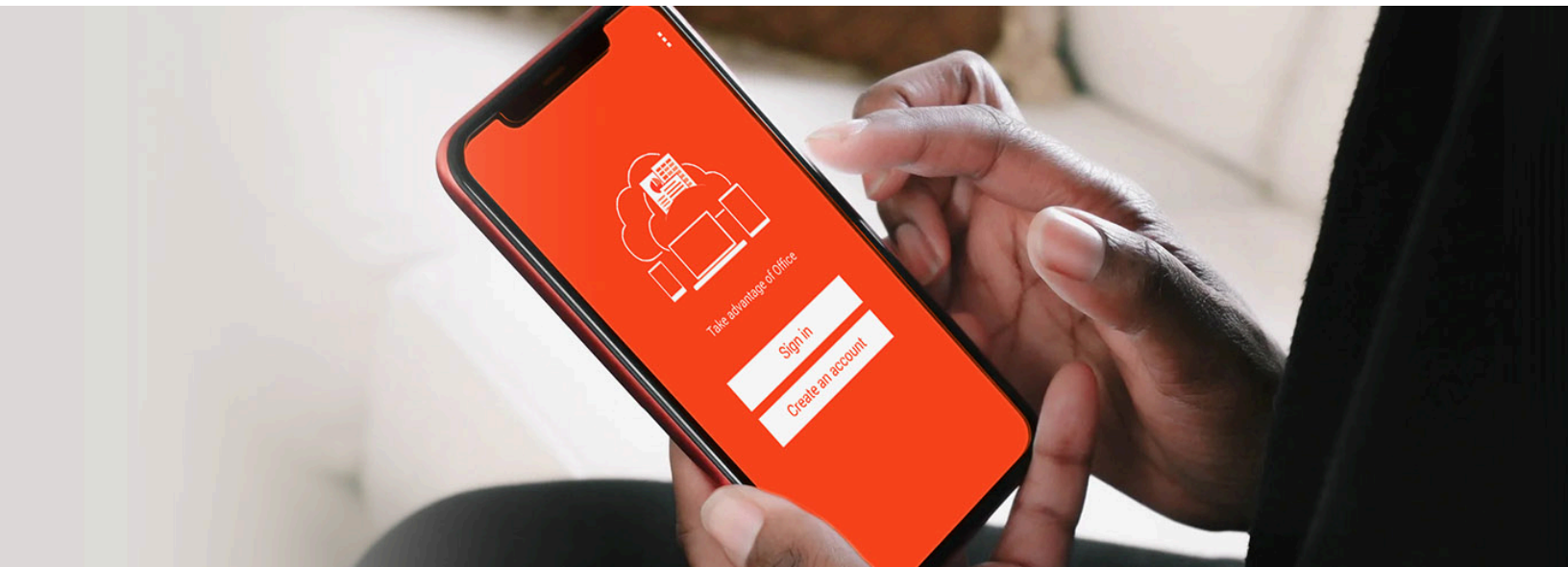
Introduction

Around 84% of organizations have Office 365 (O365) enabled on employees' mobile devices, yet more than 50% haven't deployed mobile threat defense solutions to prevent them from being compromised.[1] With that in mind, we asked Eric Green, working in business operations protection at TikTok, to share his perspectives on what organizations should be doing now to ensure that mobile access to O365 is both seamless and secure.

Z (Zimperium): Let's set the stage and establish some context for this topic, since effectively securing mobile access to O365 had been a challenge even before the pandemic hit. What was the environment and the sentiment for you and your team when the lockdown began in March 2020?

Eric: I was in my eighth month as Global Head of Mobile & Mac Security at HSBC. No one was prepared for the massive operational and security challenges we'd soon be facing. Almost overnight, we had a massive increase in the number of employees needing mobile access to O365. That was problematic since **O365 on mobile gives users the same level of access to proprietary and personal enterprise data as fully-secured desktops and laptops.** We had to move very quickly to ensure that access would be secure. Fortunately, we already had a robust MTD strategy in place.

[1] Quick Poll Questions, December 2021 and January 2022 - home.pulse.qa -



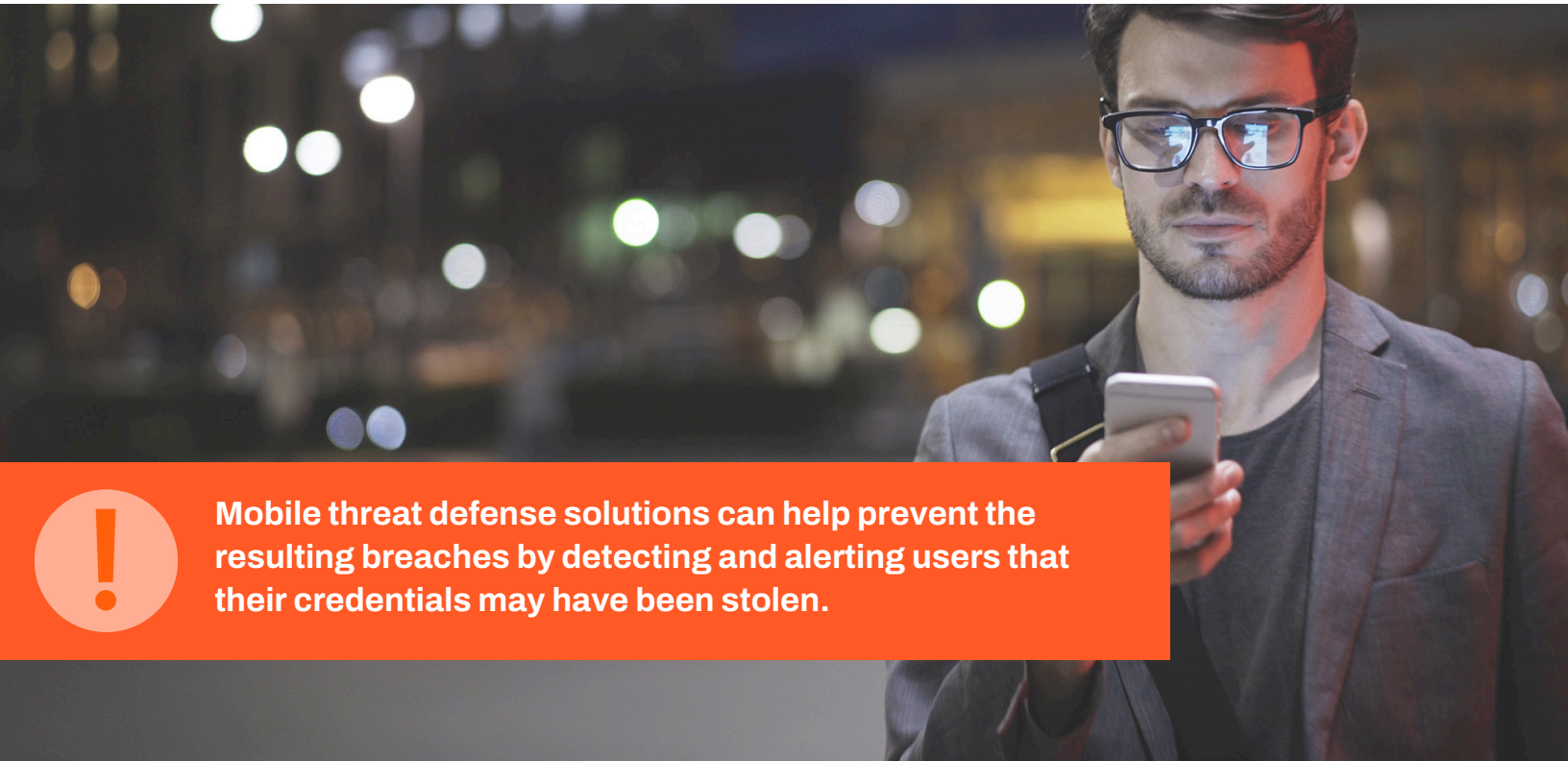
Z: How were your peers at other firms managing O365 mobile access security?

Eric: Most organizations took the traditional approach, deploying UEM solutions (including MDM and MAM) like Microsoft Intune to control access to O365 and other resources from mobile phones, tablets, and laptops.

UEM solutions provide the visibility needed to monitor and enforce user authentication, data access, and acceptable use policies. When a risk level is exceeded, they can also apply automated remediations, such as disabling an O365 application, wiping the device, or taking it offline. **But UEM solutions can't detect sophisticated phishing, malware, device, and network-based attacks.** The risk to enterprises has increased exponentially with the rapid rise of employee-owned devices. The pandemic dramatically expanded a large and vulnerable attack surface that was already extremely difficult to monitor and secure.

Z: Some organizations have suggested that VPNs can help secure O365 on mobile. Why don't they provide sufficient protection?

Eric: VPNs are effective in point-to-point situations, where you need to encrypt traffic between mobile devices and on-premises resources. **But VPNs can't detect or respond to mobile threats.** They're less suited in scenarios where you're accessing cloud services with a browser, especially if you have to backhaul traffic before sending it to the cloud. That quickly escalates network costs and creates performance bottlenecks for users. VPN products are not foolproof either. And if an attacker steals an employee's VPN credentials, they acquire the same level of access to the corporate network. Mobile threat defense solutions can help prevent the resulting breaches by detecting and alerting users that their credentials may have been stolen.



Mobile threat defense solutions can help prevent the resulting breaches by detecting and alerting users that their credentials may have been stolen.

Z: What about Microsoft Defender for Endpoint? How well does it address mobile O365 security risks?

Eric: There are benefits and drawbacks. On the plus side is the built-in integration between Microsoft products. For example, you can establish a service-to-service connection between Defender and Intune to share data and device profiles. That allows you to define risk levels in Defender that trigger conditional access controls in Intune.

However, Defender is a comparatively new product, and the mobile threat defense features are primitive. For example, Defender doesn't provide enough detail about the state of a mobile device to accurately determine if it's trustworthy, jailbroken, or compromised. Mature mobile threat defense solutions offer more comprehensive capabilities for detecting and automatically remediating threats at the user, device, application, and network levels. They also provide the extensive forensic and telemetry data analysts need for root cause analysis and threat hunting.

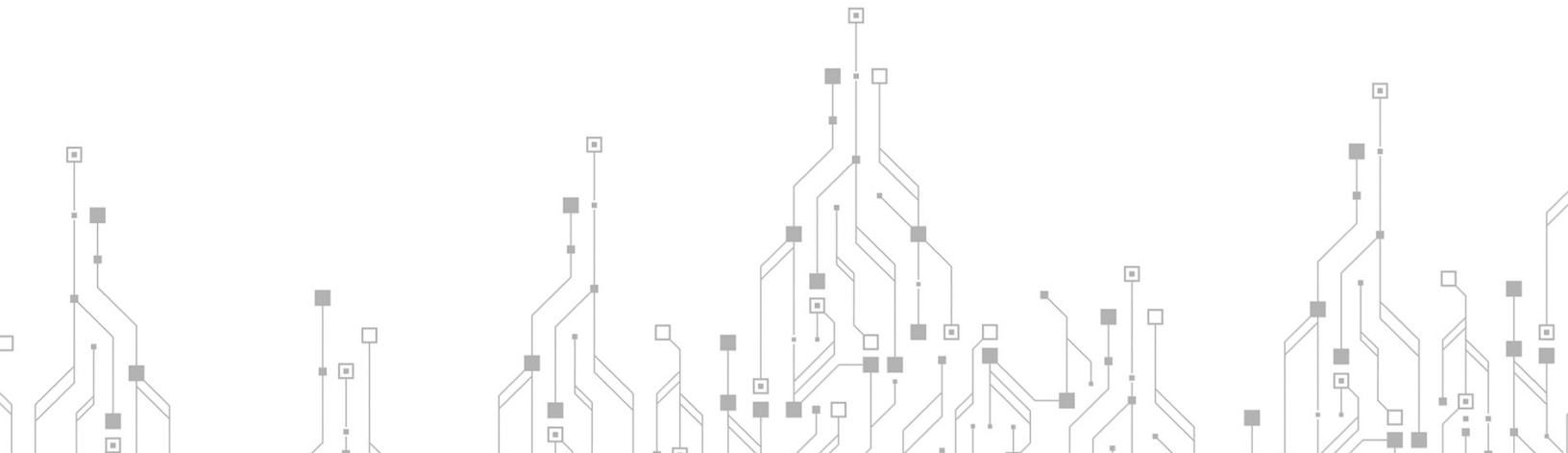
Flexibility and future-proofing are critical. mobile threat defense solutions should easily integrate with your SIEM, identity provider, and other security investments.

"Defender doesn't provide enough detail about the state of a mobile device to accurately determine if it's trustworthy, jailbroken, or compromised."

Z: How does mobile threat defense address the Zero Trust initiatives many organizations have accelerated due to COVID?

Eric: The Zero Trust model requires users, devices, networks, and applications to prove they're trustworthy before granting access to resources like O365. The challenge is implementing Zero Trust without requiring admins to monitor every interaction or forcing workers to jump through hoops to perform routine tasks.

Mobile threat defense works well in a Zero Trust environment because it continuously monitors the mobile device for malware, phishing exploits, rogue access points, sideloaded applications, and other potential threats. If an employee isn't acting maliciously or inadvertently putting their mobile device at risk, their access to resources can remain unimpaired. If mobile threat defense detects a threat or potential compromise, the threat can be remediated immediately, reverting the device to a state where it's attested trustworthy.

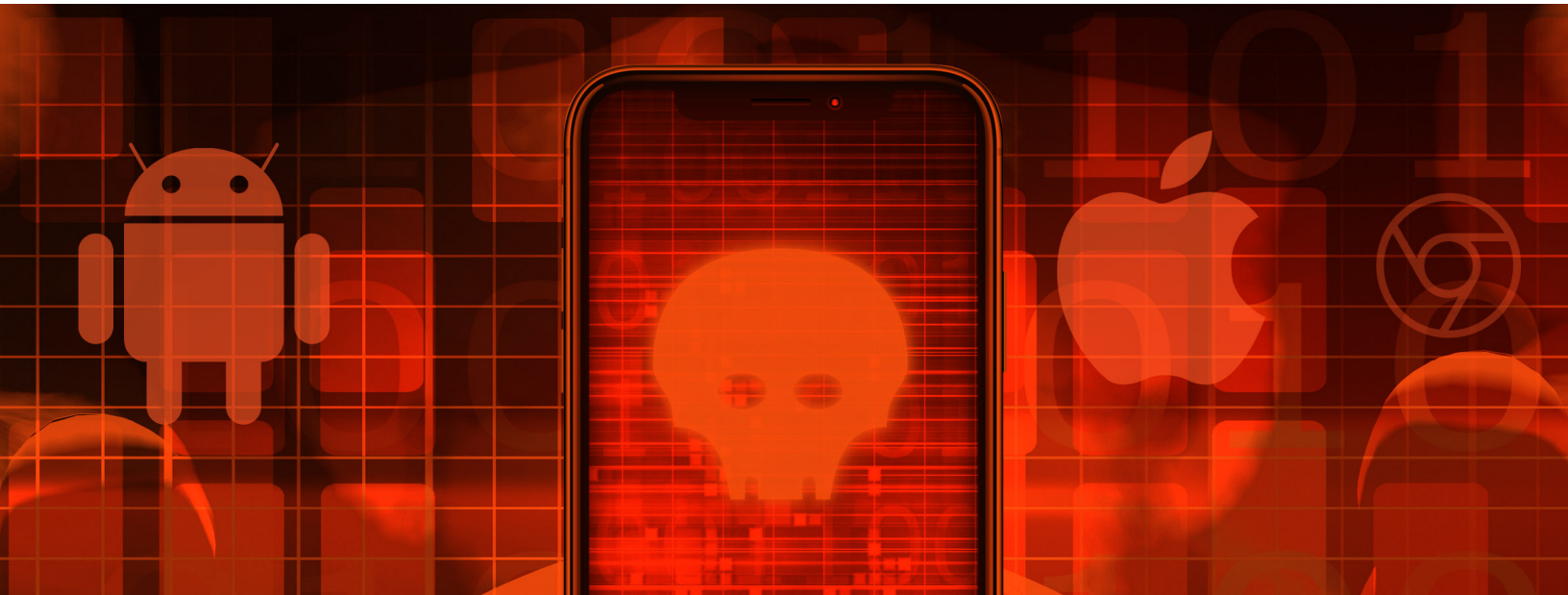


Z: How do the differences between iOS and Android influence your approach to securing O365 in a hybrid environment?

Eric: The tools and workflows will differ, but the goals will be the same. Android Managed Work Profiles separate work apps and data from personal apps and data. That makes it possible to define and enforce device compliance policies for workspace apps that are applied consistently whether the device is connecting to a cloud-based service like O365, or a database located behind the corporate firewall. This helps reduce risks from BYO devices without violating employee privacy. Apple is playing catchup with its Profile Manager. Eventually, the two products will achieve parity.

Otherwise, the differences between operating systems don't matter. An effective mobile threat defense solution should detect and remediate threats whether the device is running iOS, Android, or ChromeOS (on Chromebooks). The power of machine learning is detecting threats based on their granular features and process flows. The important thing is to deploy those models and their detection and response logic locally on each mobile device (on-device detection). A compromise can occur in milliseconds. You can't afford the latency that comes with cloud lookups and signature matching.

"An effective mobile threat defense solution should detect and remediate threats whether the device is running iOS, Android, or ChromeOS (on Chromebooks)."



Z: How about best practices around patch management? What was your approach there?

Eric: Users don't like being told to install patches, especially if the mobile device is personally owned. Many won't comply or wait until the last minute and they're about to lose access to corporate resources. Some mobile devices can't be patched because the hardware is outdated. You have to set priorities. Operating system updates are crucial since they often provide security fixes for critical vulnerabilities. Updating an app is usually less urgent unless it's an authorized workplace app, like Slack, that employees must use to be productive.

It gets more complicated when you have a mix of iOS and Android devices. Apple users tend to be pretty compliant. They're used to installing patches and updates on a regular basis. The Android ecosystem is much more fragmented. Hardware manufacturers and wireless carriers often control the timing and availability of OS patches and releases. Ultimately, you're playing a game of whack-a-mole. You have to prioritize patches based on your organization's risk profile and use case requirements. There are no perfect solutions. Patching is always going to be reactive. **That's why you need a solution that can detect and prevent attackers from detonating malware and exploiting vulnerabilities on every mobile device, regardless of the ownership model or level of compliance.**

Z: Given the current threat landscape, how would you summarize your recommendations for CISOs weighing whether and how they should be securing mobile access to O365?

Eric: Securing mobile access to O365 is essential, but it's honestly one piece of a much larger puzzle. Workers are going to continue accessing every corporate resource from mobile devices. Threat groups will continue finding new ways to trick them into making mistakes and exploit vulnerable mobile apps and operating systems. The key is to identify and prioritize the mobile threats that pose the most significant risks to your organization.

If you're using Intune, make sure your device management policies address those risks without being overly restrictive. Train users to practice good cyber hygiene. Make certain browsers are using appropriate encryption to access cloud services. Accelerate your transition to zero trust. That covers the basic blocking and tackling.

But you also have to deploy a mobile threat defense solution that's proven effective at detecting and mitigating mobile threats to users, devices, networks, and applications. Make sure the solution you choose works well with your existing management and security infrastructure and preserves the flexibility you'll need as your infrastructure evolves to meet new security challenges.