Prevent cybercriminals from taking over your mobile device *yes*

Detect and stop attacks on mobile devices before they start.

Benefits

- Deploy any iOS or Android mobile device on your organisation's network with confidence
- Protect sensitive information on mobile devices from espionage
- Improve visibility and protection against the latest mobile threats with mobile security that integrates easily into your existing mobility and security infrastructures (MDM, MAM, NAC, SIEM, etc.)
- Augment the security measures of Microsoft Exchange and container/ wrapper solutions
- Enable rapid response to cross-platform advanced persistent threat (APT) attacks
- Enable contractors to access corporate data safely from unmanaged devices
- Preserve user experience and privacy, while adding the protection required by organisational or regulatory mandates.

Smartphones and tablets give us unprecedented access to the critical business information we need to work faster and more accurately. Providing your employees with access to that information on the mobile devices they choose has many benefits, but it also exposes your business to risk. Optus Mobile Threat Prevention (MTP) powered by Check Point, is an innovative approach to mobile security for iOS and Android devices that detects and stops mobile threats before they start. Whether your data's at rest on a device or in flight through the cloud, Optus MTP helps protect you from vulnerabilities and attacks that put data at risk.

Mobile security for the enterprise

Check Point provides a complete mobile security solution that protects devices from threats on the device (OS), in applications, in the network and in SMS messages, delivering the industry's highest threat catch rate for iOS and Android. Optus MTP uses malicious app detection to find known and unknown threats by applying threat emulation, advanced static code analysis, app reputation and machine learning. It safeguards devices from unprotected Wi-Fi® network access and Man-in-the-Middle attacks and stops access to corporate networks when a threat is detected. It uses real-time risk assessments at the device-level (OS) to reduce the attack surface by detecting attacks, vulnerabilities, changes in configurations, and advanced rooting and jailbreaking. Its dynamic threat response prevents compromised devices from accessing your organisation's network, and allows your organisation to set adaptive policy controls based on unique thresholds for mitigation and elimination of threats on the device.

Advanced app analysis

You can trust your employees to access your sensitive business assets, but can you trust their apps? Our solution captures apps as they are downloaded to devices, and runs each in a virtual, cloud-based environment to analyse its behaviour before being approved or flagged as malicious. Easy to understand, exportable analysis reports help your security teams ensure apps employees use are safe.

Network-based attacks

Public places are filled with unsecured Wi-Fi networks, making it difficult to know which networks are safe and which aren't. Cybercriminals can use these networks to hijack smartphones and tablets, assuming control of devices and valuable data like messages, files, and network credentials. Our solution detects malicious network behaviour and conditions, and automatically disables suspicious networks to keep devices and data safe.

Device vulnerability assessments

Cybercriminals make it their business to know the weakest link in your security before you do. That often includes weaknesses in operating systems and apps that other security solutions may not detect. Our solution continuously analyses devices to uncover vulnerabilities and behaviours cybercriminals use to attack devices and steal information. With better visibility into the threats mobile devices face, you can reduce the overall attack surface and risk.

1. Check Point Security Report 2016 http://pages.checkpoint.com/security-report.html

One in five employees will be the cause of a company network breach through either malware or malicious WiFi.

OPTUS | Check Point SOFTWARE TECHNOLOGIES LTD.

SMS phishing attacks

SMS phishing, also known as SMiShing, is a form of fraud in which the attacker tries to learn information such as login credentials or account information by masquerading as a reputable entity or person in SMS messages. A victim receives an SMS text message that appears to have been sent by a known contact or organisation. Links in the message may install malware on the user's device or direct the user to a malicious website set-up to trick them into divulging personal and financial information, such as passwords, account IDs, or credit card details. The solution detects malicious SMS messages and blocks them. Optus MTP anti-SMS phishing attacks is powered by ThreatCloud™, Check Point's collaborative network and cloud-driven knowledge base that delivers real-time, dynamic security intelligence.

Full mobile threat visibility and intelligence

Optus MTP's cloud-based dashboard makes managing supported devices and controlling mobile threats fast and easy. It provides your security and mobility teams with real-time threat intelligence and visibility into the quantity and types of mobile threats that could impact your business or users.

Integrate intelligence with existing systems

Optus MTP's stream of real-time threat intelligence pushes to Check Point SmartEvent automatically for monitoring of security events and for correlation with attacks on internal networks. There, this information is shared and correlated in ThreatCloud™ providing a broad set of threat intelligence that can be used within network environments to prevent cyberattacks from occurring. Threat intelligence can also be fed into existing enterprise systems like your security information and event management (SIEM) platform. This includes detailed logs and other indicators of compromise that can be filtered to trigger response actions that help your security team take action quickly to control and eliminate risk.

Deploying mobile security has never been easier

Security and mobility teams have enough to worry about. That's why Optus MTP is designed to help them secure mobile devices quickly and confidently through integration and cooperation with Mobile Device Management (MDM) or Enterprise Mobility Management (EMM) solutions. This helps make the solution highly scalable, and delivers strong operational and deployment efficiencies for managing mobile security within a broader security infrastructure.

Deploy advanced mobile security with ease

Whether you support 300 or 300,000 devices, integrating our solution with your EMM is fast and easy. Deployment and management can be done through your EMM automatically, accelerating adoption and reducing overall operational costs. The solution scales with your EMM, seamlessly protecting enrolled mobile devices. As a result, you can rest assured you have the layers of security you need to both manage and protect mobile devices, even in a highly dynamic environment.

Mitigate and eliminate threats right on the device

When a threat is identified, our solution automatically mitigates any risk until the threat is eliminated. If a threat can be eliminated on a device immediately, users are notified and prompted to take action, like deleting malicious apps or disconnecting from hostile networks. Integration with your EMM allows the solution to restrict secure container access, or make real -time, risk-based policy adjustments on compromised devices that EMMs on their own can't make. Our solution also activates an on-demand VPN to tunnel data traffic away from cybercriminals and to avoid data exfiltration while still keeping users connected.

Respect user privacy and device performance

End-user privacy is critical, so we never analyse files, browser histories, or application data. Our solution uses state and context metadata from operating systems, apps, and networks to determine if a device is compromised. It anonymises the data it uses for analysis to keep it and security intelligence information separated. Our analysis is performed in the cloud to avoid impacting device performance, and since protection runs in the background, so users are stay protected without having to learn anything new.

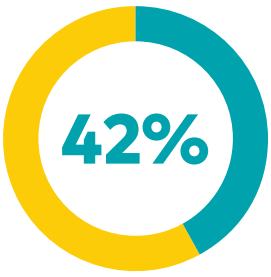
Stay on guard with ease

Your information assets are susceptible to attack at any time. Optus Mobile Threat Prevention protects your devices from advanced mobile threats, enabling you to deploy and defend devices with confidence

Trust is a vital component of every organisation's security regime. You can depend on Optus Business to provide peace of mind to your team, your stakeholders and your customers. Optus can also manage this solution on your behalf so that you can spend more time focusing on your most important asset – the success of your organisation.

Optus Business provides a broad range of telecommunications and ICT solutions, with security at the core. Our solutions help protect your organisation in an increasingly mobile and digitised world.

Optus can also provide you with an enhanced security solution across your enterprise from mobile devices and laptops through to your branch and data centre firewalls. Contact your Optus Account Manager for more information about Security Services.



of surveyed businesses suffered mobile security incidents costing more than $250,000.[2]

Researchers determined that if there are 2,000 devices or more in an organisation, there is a 50 percent chance that there are at least six infected or targeted mobile devices on their network. By platform, that breaks down to 60 percent Android and 40 percent iOS.[3]

2. Check Point Security Report 2016 http://pages.checkpoint.com/security-report.html

3. Check Point Security Report 2015 https://www.checkpoint.com/resources/2015securityreport/index.html

GMO_N 0365 0717MZ