

# Mobile security and the consumerization of IT

Scott Gordon, of ForeScout Technologies, offers some tips on managing the multitude of private wireless devices now arriving on the corporate network

Today, organizations want to take advantage of anytime, anywhere access, to enable their users to work with the personal mobile devices of their choice in order to gain increased productivity and connectivity. As such, IT is being challenged by the inevitable proliferation of non-corporate devices accessing corporate resources – the ‘consumerization of IT’.

To enable greater accessibility and manage risk, mobile security is as much about people and process as it is about technology. Here are some tips to ensure connectivity, productivity and security:

**1.** Scope out the types of users and their necessary access to corporate applications, resources and data. Establish at least basic policy, monitoring procedures and controls that align to such policy. Policies and procedures should be published, and the controls monitored and enforced.

**2.** Create an acceptable use policy that informs end users of what mobile and personal computing devices are allowed access to corporate resources, what uniform monitoring of their use of resources may take place, as well as what restrictions and precautions should be followed by the end user to minimize potential threats such as malware, phishing or stolen passwords.

**3.** Clearly maintaining a current and secure operating environment for remote systems, notebooks, iPads, smartphones and other mobile devices is paramount. This would include keeping any device up to date (because updates remove potential threats), as well as using current anti-virus soft-

ware and possible personal firewalls. Employing secure remote access safeguards such as VPN (virtual private network) clients and the use of multi-factor authentication (name, password, other personal identifiable objects/information) should also be in place relative to the user type and access to sensitive resources and applications. Employing web filtering software can also help to restrict access to insecure and inappropriate websites.

**4.** Setting up perimeter defences, such as the use of firewalls and establishing a DMZ (demilitarized zone) is best practice. IT organizations can examine network security products, such as Intrusion Prevention Systems (IPS) and web application firewalls, which can help to identify and stop known threats and malicious behaviour indicative of attacks and breaches. This can further allow mobile and remote works access while minimizing external threats.

**5.** Where possible, implement separate wireless networks for employees and non-employees. While corporate wireless users can access the network, non-employees (guests) can just be provided with access to the Internet. Not only will separate wireless networks provide significantly more security, they will also preserve bandwidth for employee use. Staff should employ appropriate wireless access point (WAP) configuration standards that include strong WEP/WPA encryption. Examine technologies that identify and block rogue WAPs to prevent access credentials and other sensitive information from being unintentionally provided to malicious persons.

**6.** Two of the biggest problems that IT organizations face with mobile users are to understand all users and devices accessing their network, and to establish the means to enforce that access effectively – whether it be remote users potentially circumventing defences, or those bringing in smartphones and other mobile devices on to their network. Network Access Control (NAC) solutions provide endpoint and mobile visibility. In addition they can block, limit or automatically remedy access violations to ensure that all access to network resources and data is according to access policy. By

## Users: embracing the inevitable

Organizations must embrace the fact that employees, guests and contractors are using mobile devices, both corporate-provided and personal. By examining mobile device use, assessing use cases, risks and requirements, and implementing appropriate and reasonable safeguards, mobile end users can be allowed to connect, comply and compute with confidence.

automatically assessing who the user is (employee, contractor, guest, or other), what the user has (system, device, iPad, etc.) and the configuration integrity of the device, organizations can realize their investments in endpoint security and assure endpoint compliance.

With NAC solutions, corporates can readily know what devices – including mobile devices and respective users – are accessing their environment. This provides complete visibility to understand the scope of access types and potential policy gaps.

Furthermore, IT organizations can, in real-time, ensure current and active anti-virus, active data leakage prevention client, correct personal firewall setting, appropriate encryption client, etc. At the same time, they can dynamically restrict access to network resources and sensitive data without any change to their current network architecture. For example, unknown users with iPads and other mobile devices attempting to access the network can be re-directed to a registration page and subsequently be offered restricted access.

**7.** Lastly, monitoring solutions such as network monitoring, Security Information Event Management and log management applications, can centralize security controls, improve incident response and automate reporting – augmenting an organization's overall security posture and support for compliance mandates. These tools can enable an IT organization to get a handle on mobile use and track their access to resources.



**Scott Gordon** is vice-president of worldwide marketing for ForeScout Technologies, a provider of automated solutions for

network access control, mobile security, threat prevention and endpoint compliance