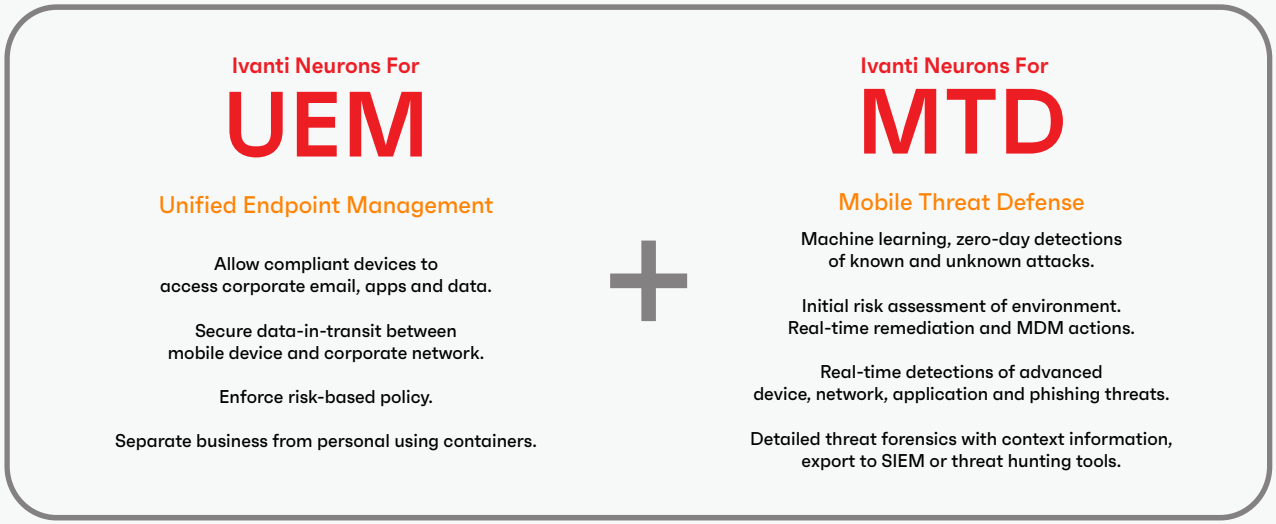
Mobile Security Made Simple with Ivanti

Enabling complete end-to-end mobile threat protection

Ivanti and Lookout have partnered together to offer an all-encompassing enterprise mobile security solution that safeguards employees and their Everywhere Work from evolving threats. With comprehensive protection at every level, including device, network, and application, the solution defends against phishing attempts and prevents attacks before they can do harm.



By bringing their expertise together, Ivanti and Lookout empower enterprises to manage and secure a wide range of mobile devices against virtually any type of attack. Lookout continuously analyzes and detects threats in real-time, providing Ivanti with valuable visibility to enforce policies and minimize the risk of data breaches. With Ivanti and Lookout, enterprises can mitigate the risks of mobile vulnerabilities and keep their networks, assets, and employees safe.

The integrated solution provides IT security administrators with a way to safely enable both Government Furnished Equipment (GFE) and Bring Your Own Device (BYOD) and strike the balance between empowering mobile employees to be more productive with the device of their choice, while at the same time securing mobile devices and the enterprise against advanced threats.

Key benefits

The partnership between Lookout and Ivanti introduces a powerful endpoint protection solution that makes mobile security easy and efficient. By integrating Lookout's technology with Ivanti Neurons for UEM, businesses can gain real-time visibility into mobile risk, and through machine learning engines fueled by Lookout's global sensor network, can stay one step ahead of the evolving mobile threat landscape. With integration into the Ivanti Neurons for UEM client, the enrollment and enforcement policies are simplified, driving to 100% user adoption.

Regulatory compliance

NIST 800.53

Special Publication 800-53, Revision 4, provides a more holistic approach to information security and risk management by providing organizations with the breadth and depth of security controls necessary to fundamentally strengthen their information systems and the environments in which those systems operate – contributing to systems that are more resilient in the face of cyberattacks and other threats. Lookout analyzes network connections and can accurately identify man-in-the-middle attacks, host certificate hijacking, hijacked SSL traffic, and TLS protocol downgrades.

NIST 800.124

NIST Special Publication 800-124 Rev. 2 section 4.2.3 states: "MTD systems are designed to detect the presence of malicious apps, network-based attacks, improper configurations and known vulnerabilities in mobile apps or the mobile OS itself." Lookout provides comprehensive protection against the entire spectrum of mobile risk, which includes threats, vulnerabilities, and configuration risks across the four primary threat vectors - phishing, app, device, and network threats. In addition, the Lookout platform uses artificial intelligence to analyze data from nearly 200 million devices and over 100 million apps to protect you from the full spectrum of mobile risk.

General Data Protection Regulation (GDPR)

GDPR offers a comprehensive framework for protecting EU citizens' data privacy and ensuring security by imposing strict procedural and technical requirements. Complying with GDPR necessitates adherence to data protection principles, such as data minimization, accuracy, storage limitation, and secure data processing. Lookout provides essential security features that offer in-depth visibility into various mobile threats, vulnerabilities, and risky behaviors jeopardizing data security. With policy-based protection, Lookout addresses mobile risks at scale, enabling organizations to establish policies for timely threat remediation, minimizing data-leak risks, and upholding user privacy.

How Lookout integrates with Ivanti:

Ease of deployment and upgrades

Lookout is already embedded into the Ivanti Neurons for UEM agent. This means the solution is already deployed to every device, and only requires activation to start protecting users. The configuration is done by adding Ivanti Neurons for UEM to the Lookout Console and enabling activation from the UEM to start protecting devices. No user interaction is required, and no new application deployment is needed.

Protect your corporate infrastructure

When Ivanti Neurons for Mobile Threat Defense detects that a device has been compromised, it can provide quick remediation to thwart the attack. Based on the attack and the setting, Ivanti can perform myriad protective actions including terminating the network connection, denying specific IP/domains and enacting specific quarantine actions. In addition, the Ivanti server can enact risk-based compliance policies to remediate depending on the severity of the threat. The policies can temporarily disable the mobile device's connections to corporate services (email or other apps, Wi-Fi and VPN) or even remove enterprise applications from the device. These actions stop the spread of the infection and prevent risk to corporate data.

Alerting and reporting

Ivanti provides comprehensive mobile threat forensics along with configurable end-user notifications and administrator alerts by attack type to suit the needs of any enterprise. Privacy data collection policies are provided to meet regional regulations as well.

Capability	Ivanti Neurons for UEM	Ivanti Neurons for MTD
Support for iOS and Android devices.	✓	✓
Provide initial vulnerability risk posture for OS/device, network, apps and phishing.	✓	✓
Detect if device has proper physical security enabled (pin code, device-level encryption).	✓ Basic	✓
Detect if device is jailbroken/rooted by user (using known hash values and file location).	✓	✓
Provide forensics into the tools and techniques of a device compromise or attack.		✓
Detect OS/Kernel and USB exploitations, profile/configuration changes, system tampering.		✓
Detect elevation of privileges attacks.		✓
Detect network attacks (man-in-the-middle, rogue Wi-Fi and cellular networks).		✓
Detect SSL stripping, fake SSL, attempts to intercept SSL traffic.		✓
Detect attackers conducting reconnaissance scans.		✓
Detect phishing, smishing, URL phishing, tiny URL, etc.		✓
Corporate app delivery and removal.	✓	
Secure corporate document sharing.	✓	
Secure line-of-business apps.	✓	

Capability	Ivanti Neurons for UEM	Ivanti Neurons for MTD
Detect malicious apps, known and unknown malware, dynamic threats using download and execute.		✓
Revoke access to non-compliant mobile devices.	✓	
Provide detailed mobile threat forensics.		✓
Enforce risk-based policy including lock or selective wipe for compromised devices.	✓	✓
Provide instant remediation once an attack is detected.		✓
Scan in-house developed apps for privacy and security concerns/risks.		✓
Receive privacy and security information from apps that have been installed on the device.		✓
Threat detection	**Ivanti Neurons for UEM**	**Ivanti Neurons for MTD**
Host-related critical and elevated threats		
Android device – possible tampering		✓
Abnormal process		✓
Developer options		✓
Device encryption	✓	✓
Device PIN	✓	✓

Threat detection	Ivanti Neurons for UEM	Ivanti Neurons for MTD
Host-related critical and elevated threats		
Device jailbroken / rooted MDM jailbreak/root detections are simplistic and easy to bypass. In addition, MDM does not provide any forensic visibility into the tools and techniques used in the attack.	✓	✓
Elevation of privileges		✓
File system changed		✓
Side loaded apps		✓
SE Linux disabled		✓
System tampering This is an advanced compromise of the device that may or may not use the additional step of jailbreaking or rooting the device.		✓
Suspicious iOS app		✓
Suspicious Android app		✓
Untrusted profile		✓
USB debug mode on		✓
Vulnerable Android version		✓
Vulnerable iOS version		✓

Phishing detection and prevention		
Always-on detection and blocking of phishing URLs.		✓
Time-of-click phishing detection stops phishing attacks in-motion.		✓
Network Related Critical & Elevated Threats		
MiTM		✓
MiTM - ARP		✓
MiTM – ICMP REDIRCT		✓
MiTM – SSL strip		✓
MiTM – fake SSL strip		✓
SSL/TLS downgrade		✓

About Ivanti

Ivanti makes the Everywhere Work possible. In the Everywhere Work, employees use myriad devices to access IT networks, applications and data to stay productive as they work from anywhere. The Ivanti automation platform connects the company's industry-leading unified endpoint management, zero trust security and enterprise service management solutions, providing a single pane of glass for enterprises to self-heal and self-secure devices, and self-service end users. More than 40,000 customers, including 78 of the Fortune 100, have chosen Ivanti to discover, manage, secure and service their IT assets from cloud to edge, and deliver excellent end user experiences for employees, wherever and however they work.
For more information, visit ivanti.com

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com