ivanti neurons

DATASHEET

Ivanti Neurons for Mobile Threat Defense:

Cloud-based protection against phishing and malware threats

Key benefits

Ensure constant protection

Ivanti Neurons for MTD uses machine learning algorithms optimized to run continuously on-device, enabling it to detect and remediate local threats, and secure threat intelligence to identify zero-day web-based malware and phishing threats.

Improve threat visibility

Gain immediate and ongoing visibility into malicious threats across all mobile devices and detailed analyses of risky apps.

Achieve 100% user adoption

No user interaction is required, and no new application deployment is needed to activate Ivanti Neurons for MTD on enrolled mobile devices.

Protect against mobile threats

In today's Everywhere Workplace, mobile devices are essential enterprise resources. Employees use them to access virtually everything. And because most users have subpar, if any, mobile security measures in place, hackers are taking advantage.

Ivanti Neurons for Mobile Threat Defense (MTD) allows you to protect both corporate and employee-owned Android and iOS devices from advanced threats. It enables enterprises to monitor, manage and secure devices against attacks that occur at the device, network and application levels as well as prevent mobile phishing attacks.

Unlike other solutions, Ivanti Neurons for MTD pushes a local compliance action that detects and remediates both known and new mobile threats on-device and can identify and stop zero-day malware and phishing threats in-motion. Additionally, no user interaction is required to activate Ivanti Neurons for MTD on enrolled mobile devices. This helps organizations achieve 100% user adoption to ensure they stay protected from mobile threats.

Ivanti Neurons for MTD capabilities

Advanced threat detection and remediation

Machine learning-based protection against device, network and application-level and phishing attacks keeps mobile devices secure. Real-time analysis of device traffic ensures protection from zero-day threats.

Phishing content protection

Ivanti Neurons for MTD uses secure threat intelligence to identify phishing threats at the time of click and assess in real-time if a link is malicious. The solution's anti-phishing capability can detect and remediate phishing attacks across all mobile threat vectors, including email, text and SMS messages, instant messages, social media and more.

100% cloud administration

With Ivanti Neurons for MTD, all administration is performed through the cloud administration console. No local server or connectors to deploy and manage.

Proactive remediation approach

Policy-based compliance actions provide alerts of risky behaviors, block access to corporate resources and apps, quarantine device to lock down and protect company apps and data, remove provisioned credentials and as a last resort retire the device completely from inventory, removing all provisioned content and settings.

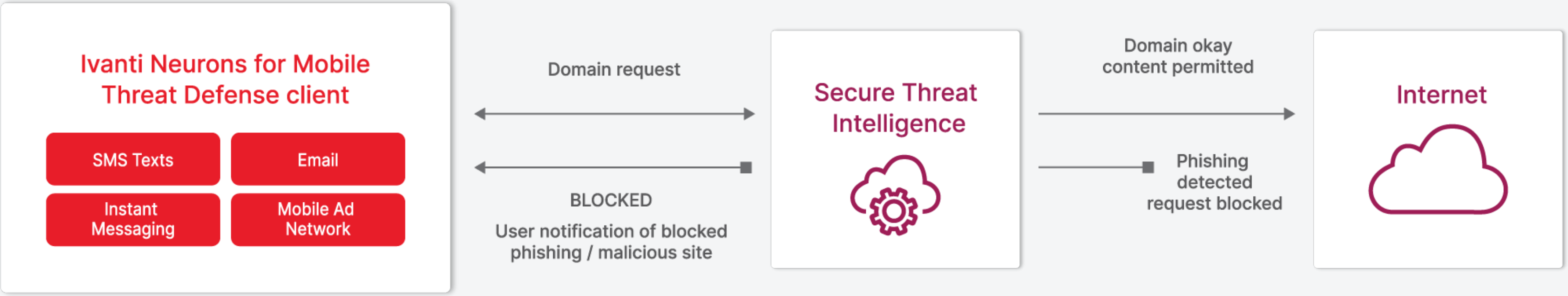
In-depth reporting

Dashboards and reports help you gain visibility and awareness into device, OS, network and application risks and arm you with actionable information so you can respond quickly and effectively to threat vectors.

UEM integration

No new application deployment is needed to activate Ivanti Neurons for MTD on enrolled mobile devices, helping to drive 100% user adoption. Further, compliance policies can be created and enforced to prevent users from disabling Ivanti Neurons for MTD or removing it from their device.

Phishing Content Protection


Ivanti Neurons for Mobile Threat Defense client
SMS Texts
Email
Instant Messaging
Mobile Ad Network
Domain request
BLOCKED
User notification of blocked phishing / malicious site
Secure Threat Intelligence
Domain okay content permitted
Phishing detected request blocked
Internet

Real-world examples

Ivanti Neurons for MTD protects against device-, network-, application-level and phishing attacks.

Device exploitation

Utilizing multiple infection vectors include clicked links, vulnerable apps, and messaging, attackers were able to infect mobile devices through zero-day exploits, in some cases with no interaction from the end-user. Once the device was infected, attackers had full visibility into the device communications and usage including contacts, call logs, messages, photos, web browsing history, settings and even allowed the attackers to run arbitrary code.

Network attacks

At a coffee shop near their office, a Wi-Fi man-in-the-middle (MITM) attack against a company redirected users to a spear phishing page where corporate data was stolen.

Malicious apps

Unsuspecting users installed an app from a third-party app store. The app abused permissions, executed a device exploit, leaked data and was used as a weapon to penetrate internal networks via lateral movement in search for more sensitive data.

Leaky apps

Apps installed from official app stores may take advantage of granted permissions to siphon user data off the device unbeknownst to the user, including accessing photos, contacts, messaging and web history.

Phishing attacks

Leveraging social engineering, a bad actor tricked an unsuspecting user into clicking on a link and providing their corporate login credentials. The attacker was then able to log in as the user and access corporate resources.

About Ivanti

Ivanti makes the Everywhere Workplace possible. In the Everywhere Workplace, 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 96 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 neurons

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