Lost & Stolen Devices

Missing laptops, tablets, phones and other endpoint devices are a very real problem. But what should you do when a device goes missing? Your response to a missing device should begin with answers to these four questions.

Where is it?

When a device goes missing, you might think immediate quarantine is your first logical step. After all, you want to cut off anyone unlawfully trying to gain access to it and/or your network via the device. While that's true, shutting down access assumes you already have accurate visibility into where the now-missing device is located. Having the ability to precisely pinpoint your device's true location must be your first step in protecting it, and you.

What's on it?

Once you've discovered a device has gone missing, your next question should be 'what's on it' and therefore, 'how big of a risk' is the lost or stolen device to you. This is where good asset intelligence comes into play. Asset intelligence is more than a simple catalog of your devices; it also outlines the business function associated with each device. What is the device used for? Having a pre-defined understanding of asset intelligence is critically important for rapid, effective security incident response. Detailed asset intelligence will tell you if the missing device contains sensitive, personal, regulated data and knowing the answer to that will tell you what your next step needs to be.

What's on it?

In addition to knowing what's on the missing device, you also need to understand how the information is currently being protected. Compliance calls to mind encryption because it's a requirement of GDPR. If sensitive data resides on the missing device and it wasn't encrypted, your next step, as outlined by the EU data privacy regulation, is a breach notification. However, there's much more to data protection than a simple yes or no checkbox for encryption. Are other protection tools you implemented like anti-virus, security agents and apps still in working order? Good endpoint cyber hygiene is the most important control function you can take. 'Hygiene' is a manifestation of your security intent and all the defining attributes of the machine, combined and tracked for conformity throughout the device's lifecycle. Conduct a regular scan of your devices and see how each conforms to your pre-defined hygiene benchmark.

What can you do to secure it?

Every missing device calls for a custom response that is based on the circumstance. For this reason, you need to be able to automatically reach every device, quickly, in an informed manner so you can tailor every response for best results.

With so many untethered endpoints out there, devices are bound to be lost or even stolen – it's just a matter of when. Following these four steps will help you prepare for this reality, guide your response and ultimately, better protect your data. For more information on how you can protect yourself from lost and stolen devices, watch this short video below.

https://www.absolute.com/blog/lost-stolen-devices-4-steps/
https://youtu.be/QYgYTZPnU-Y