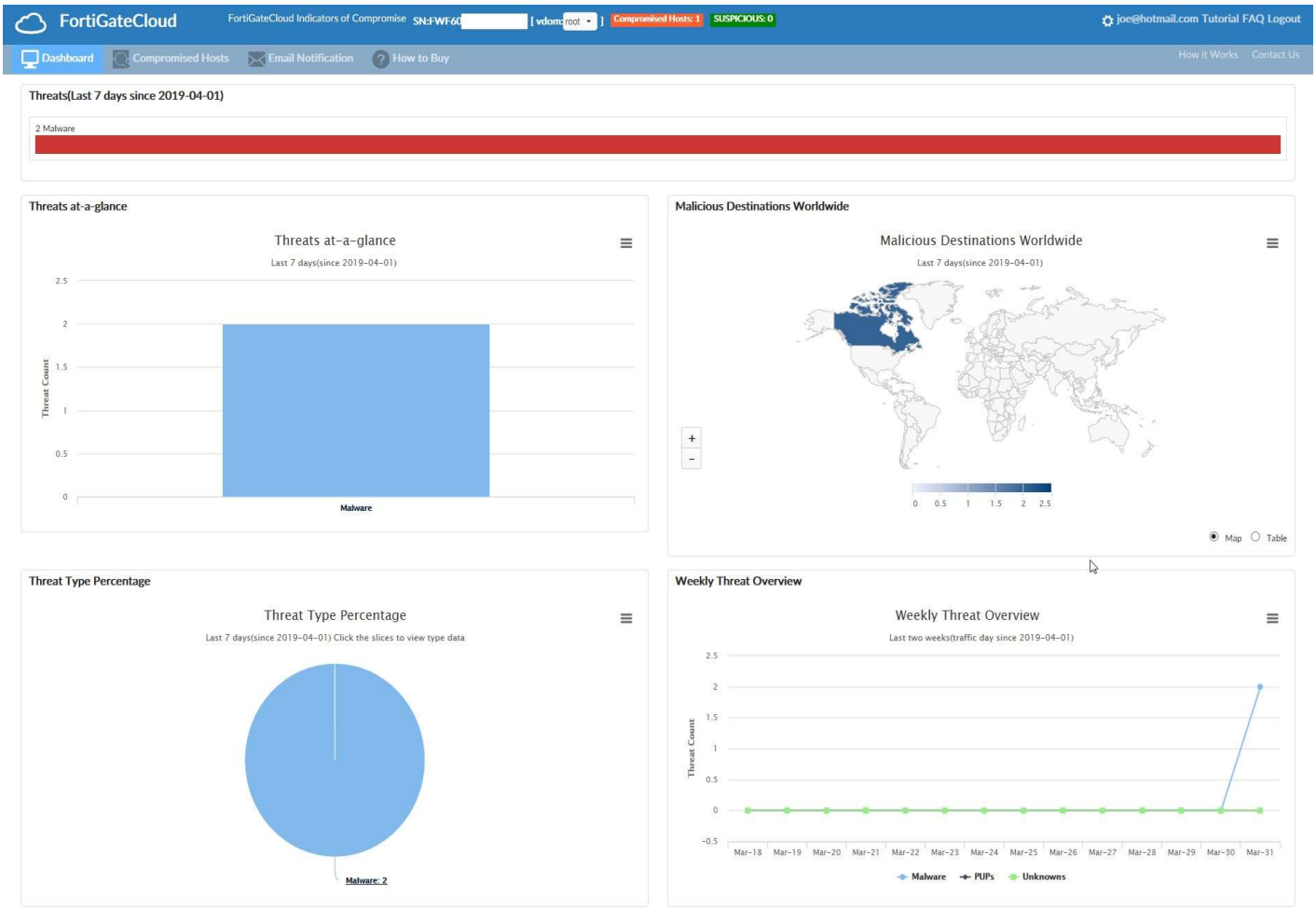
Welcome to the FortiGateCloud Indicators of Compromise



Here is an FAQ introduction of our service.

What is the FortiGateCloud Indicators of Compromise?

FortiGateCloud Indicators of Compromise (IOC) is a new service that alerts administrators about newly-found infections and threats to devices in their network. By analyzing UTM logging and activity, the service can provide a comprehensive overview of threats to the network.

What kind of threats can the Indicators of Compromise detect?

IOC can detect three types of threats, based on our evolving FortiGuard database:

- Malware - Malicious programs residing on infected endpoints.
- PUP - Potentially unwanted programs, such as Spyware, Adware, and toolbars.
- Unknown - Threats detected by signature but not associated with any known malware.

How do I get access to the Indicators of Compromise?
The IOC is currently being developed as a beta, and will be rolled out to existing FortiGateCloud customers over time. In order to be eligible for IOC, we require that you upload your UTM logs to FortiGateCloud.

Does the Indicators of Compromise require a subscription?
Yes. You can purchase a subscription for the complete IOC by opening the Plan page in the FortiGateCloud IOC site, selecting 'Buy Online', and completing the purchase process. A subscription grants you access to IP Whitelisting, which allows you to narrow your malware search by excluding safe IPs and domains, and Alert Emails, which notify you directly of detected network threats. It will also allow you to view the IPs of infected devices, allowing you to better control their access to your network.

I received a threat notification. I checked the AVLogs but could not find anything. Why is that so?
Malware is a constantly evolving threat. Antivirus serves to prevent the infection, but sometimes malware will go through and infects a Windows PC machine. Once infected, the machine behaves abnormally. It could contact malicious websites to receive commands to perform malicious actions such as uploading sensitive user passwords, or download and install other malware. These events could go unnoticed by the antivirus service. That is why you could not see any events in the AVLog.

Examples of attack vectors:

- External/Removable Media: Malware spreading from an infected USB flash drive
- Email: An attack executed through an email message attachment disguised as a PDF file, or word document.
- Improper Usage: An authorized user installed software in violation of an organization's usage policies. For example, installing file sharing software, and other free software with bundled malware/spyware leading to loss of sensitive data or performing illegal activities on a system.

FortiGateCloudIOC is a post-infection solution. We detect infected or highly suspicious devices in your network and notify you about them. As a result, you can clean up the infected device, and minimize your business risk, can instantly see which machines are infected.

Otherwise, you will need to search your AVLogs and other network logs such as WebFilter URL logs.

How do I register my subscription code, once I've purchased one?
You will receive your subscription code by email. Visit the Fortinet Support portal at http://support.fortinet.com, and log into your customer account. On the Asset page, register the subscription code as if it were a product serial number, and then enter the serial number of the FortiGateCloud-connected device that you want the service to monitor.

Are IOC licenses stackable by time?
You can buy IOC for the same device one after another and it increases the entitlement period.

Will Register/Renew on the Support Site filter FortiGate model ranges based on the SKU? Yes it will.

Do I need a FortiGateCloud license before I can buy FortiGateCloud Indicators of Compromise ?
Yes. FortiGateCloud Indicators of Compromise Service license has to work with FortiGateCloud license. FortiGatecloud account users need to buy IOC license to get Pro features.