Entitlement for AMP for Endpoints

Contents

Introduction

This document describes the process to get the Advanced Malware Protection (AMP) license entitled and access to the Dashboard.

Contributed by Uriel Islas, Cisco TAC Engineer.

Prerequisites

Requirements

Cisco recommends that you have the knowledge of:

- AMP for Endpoints license
- Email Account
- Computer

Components Used

This document is not restricted to specific software version, however this document in based on this software:

- AMP Public Cloud
- Outlook

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any step.

Configure

In order to entitle your AMP For Endpoints (AMP4E) product, you can refer to the eDelivery email or an entitlement email.

> **Note**: If you do not have access to the eDelivery email, you can contact: licensing@cisco.com or visit the online portal at http://cisco.com/tac/caseopen. After select

the appropriate technology and sub-technology, select **Licensing** listed under **Type of Problem**.

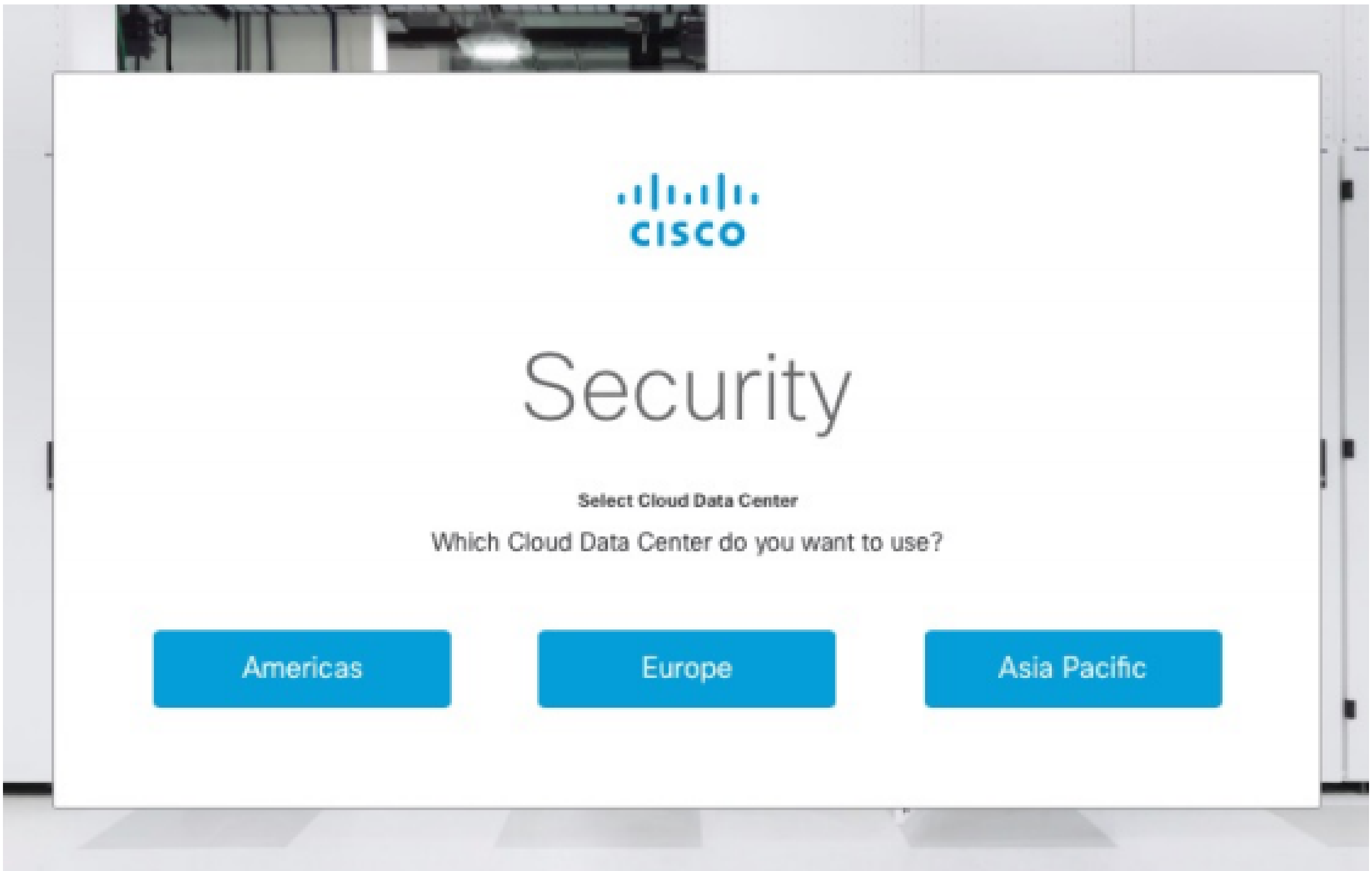
AMP For Endpoints Credentials

AMP4E credentials belongs to the Cisco Security Account (CSA) domain. As soon as the first Cisco Security accounts is set-up, you would be able to add further security admins within your organization. At the moment that you apply your license to raise a new cloud instance, you create a CSA or you can enter the license using your existing CSA credentials. Once done, an organization must be tied for your business.

How to Set-up a New Public Cloud

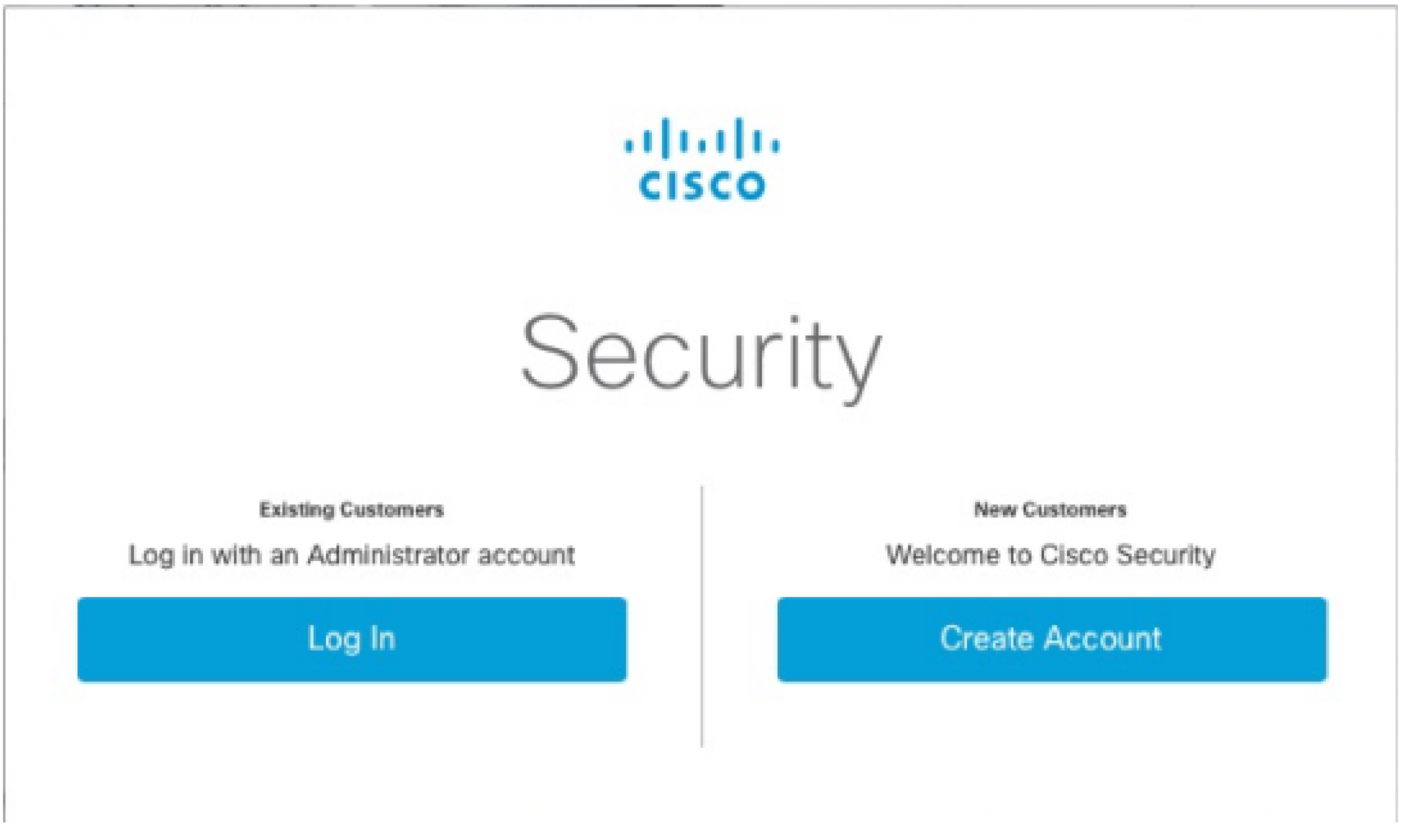
Step 1. Navigate under the URL provided in the eDelivery email or entitlement email.

Step 2. Select your prefer Cloud Data Center.



Note: Americas cloud can be used for all countries. There are no issues related with latency for countries that are far away.

Step 3. Link your Cisco Security Account to the AMP cloud.



Security

Existing Customers

Log in with an Administrator account

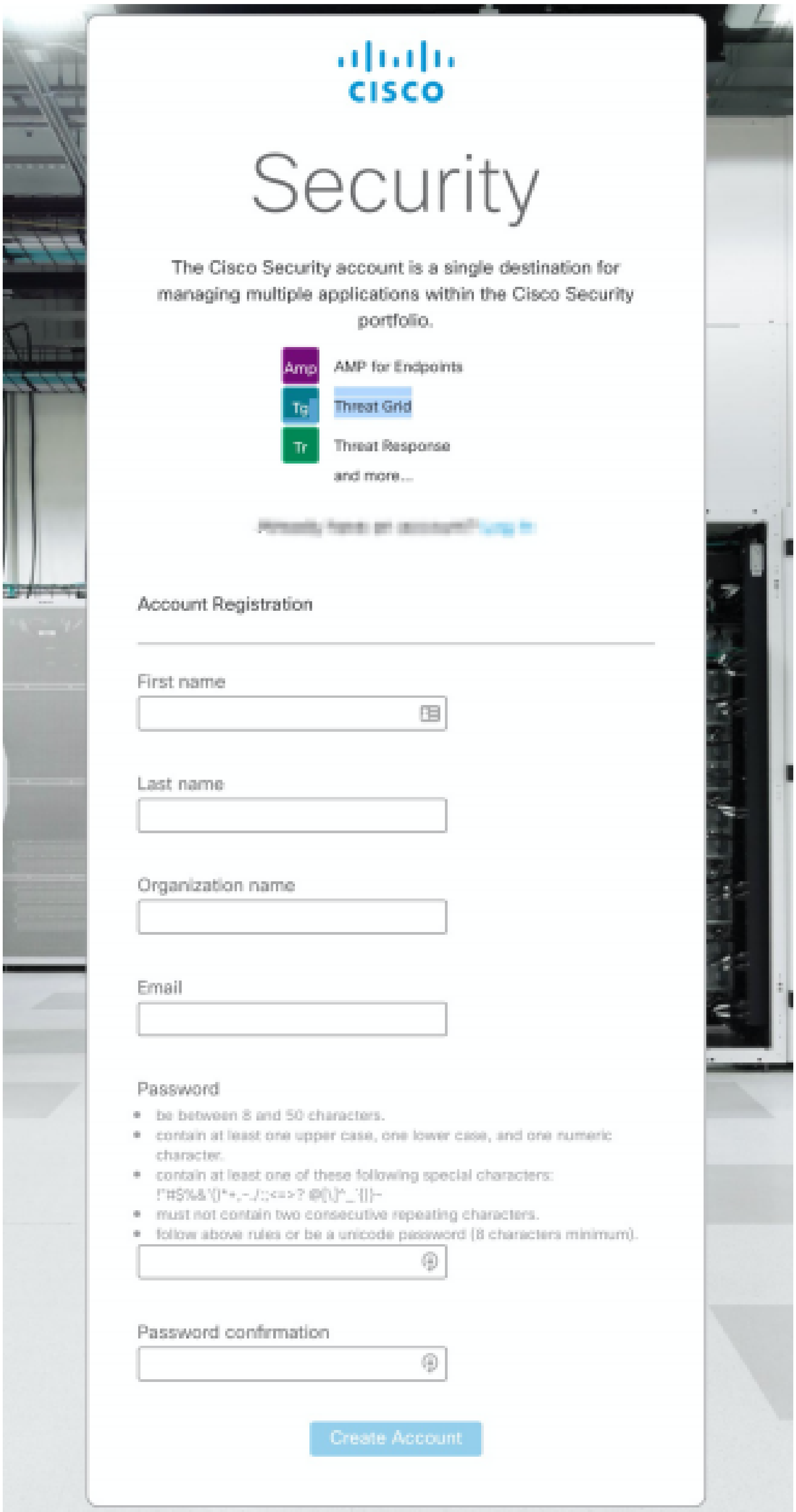
New Customers

Welcome to Cisco Security

a) If you already have the credentials for a CSA, but not for AMP4E, click on **Log in**. This option must link your CSA to the AMP cloud.

b) f you do not have an AMP cloud or Cisco Security Org set up, click on **Create Account** to apply the license for your company.

Step 4. If your company does not have a CSA, then enter the values for all the fields as requested to set up.



Security

The Cisco Security account is a single destination for managing multiple applications within the Cisco Security portfolio.

AMP for Endpoints

Threat Grid

Threat Response

and more...

Already have an account? Log in

Account Registration

First name

Last name

Organization name

Email

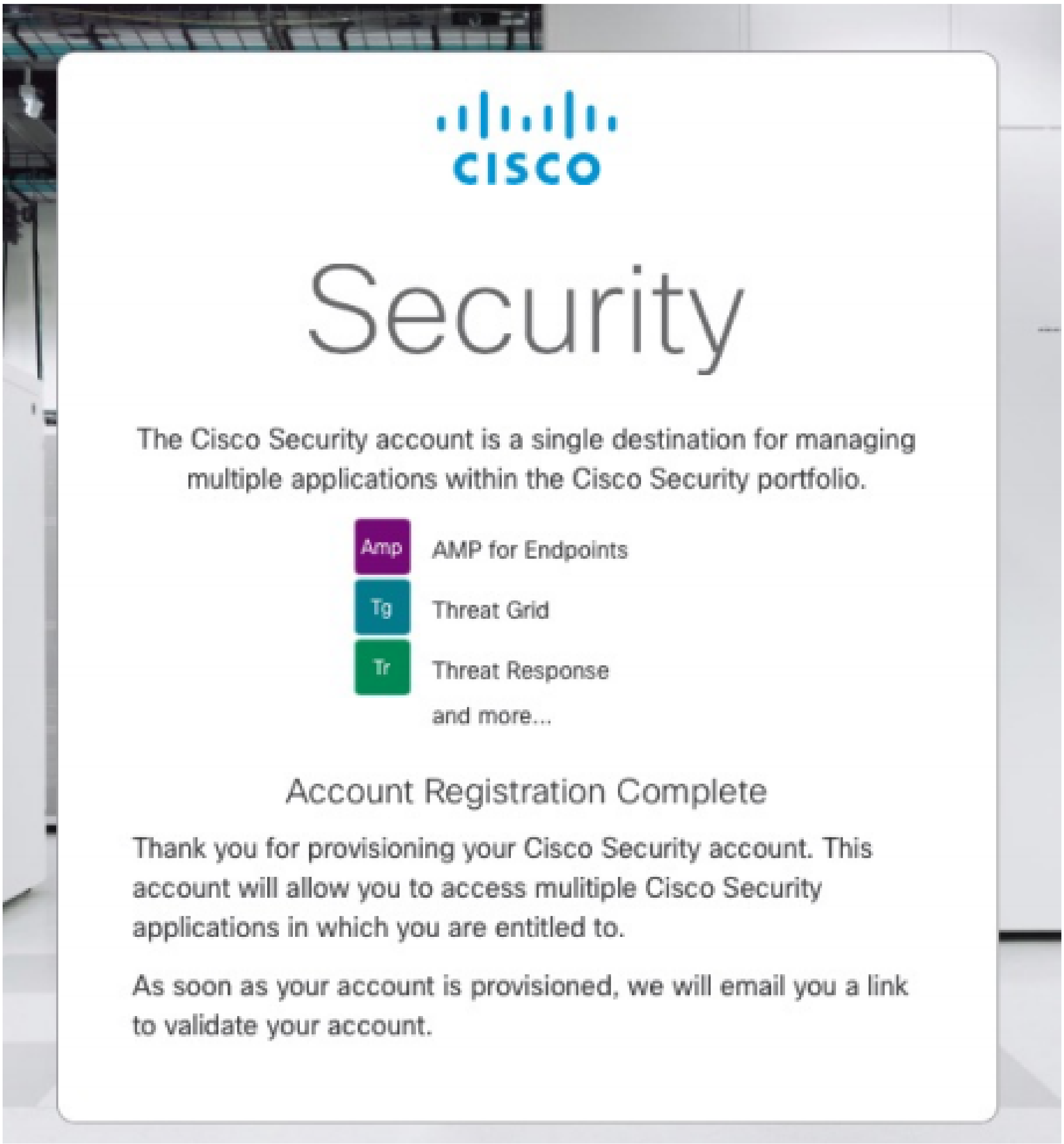
Password

- be between 8 and 50 characters.
- contain at least one upper case, one lower case, and one numeric character.
- contain at least one of these following special characters: !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~
- must not contain two consecutive repeating characters.
- follow above rules or be a unicode password (8 characters minimum).

Password confirmation

Note: If someone already has a CSA on your company, then navigate under castle website to authenticate your credentials. Select the URL based on the cloud that was configured on number 2. **Americas Cloud**: https://castle.amp.cisco.com **Europe Cloud**: https://castle.eu.amp.cisco.com **Asia Pacific Cloud**: https://castle.apjc.amp.cisco.com.

Step 5**.** Once the CSA is created, it displays an Account Registration Complete page.



Security

The Cisco Security account is a single destination for managing multiple applications within the Cisco Security portfolio.

AMP for Endpoints

Threat Grid

Threat Response

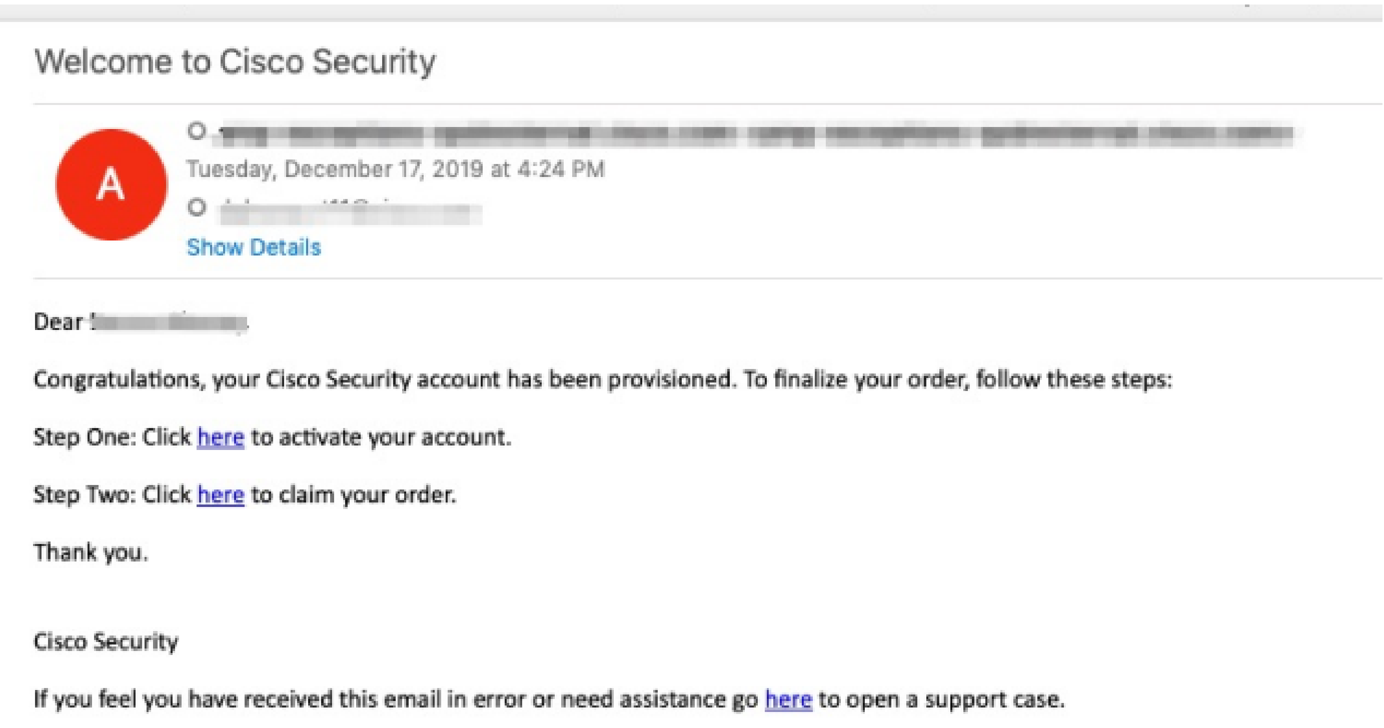
and more...

Account Registration Complete

Thank you for provisioning your Cisco Security account. This account will allow you to access mulitiple Cisco Security applications in which you are entitled to.

As soon as your account is provisioned, we will email you a link to validate your account.

Step 6. Verify a new Welcome to Cisco Security email from no-reply@amp.cisco.com.



Welcome to Cisco Security

A

○ [redacted]

Tuesday, December 17, 2019 at 4:24 PM

○ [redacted]

Show Details

Dear [redacted]

Congratulations, your Cisco Security account has been provisioned. To finalize your order, follow these steps:

Step One: Click here to activate your account.

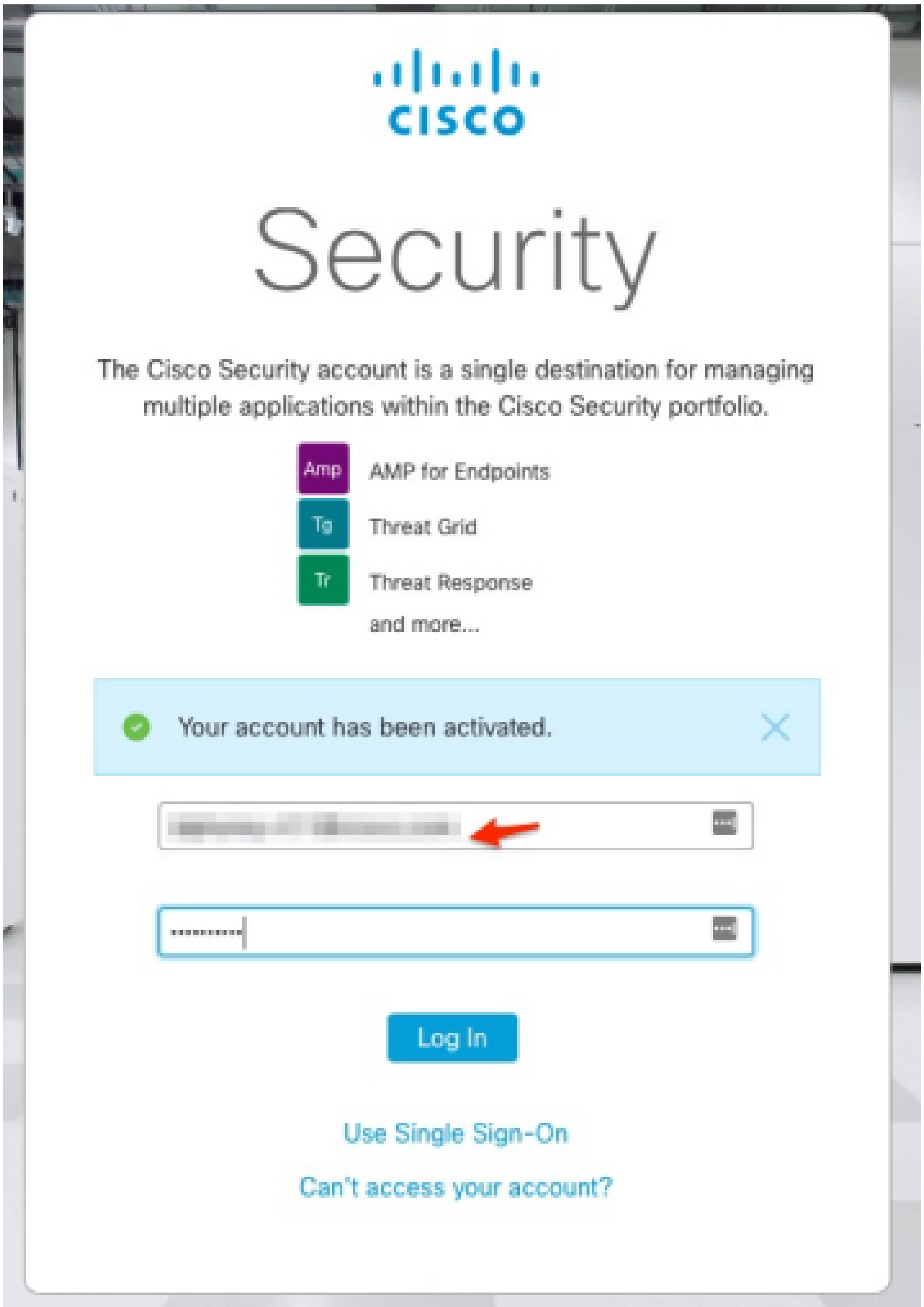
Step Two: Click here to claim your order.

Thank you.

Cisco Security

If you feel you have received this email in error or need assistance go here to open a support case.

Step 7. Activate your account from the welcome email on step 1



Security

The Cisco Security account is a single destination for managing multiple applications within the Cisco Security portfolio.

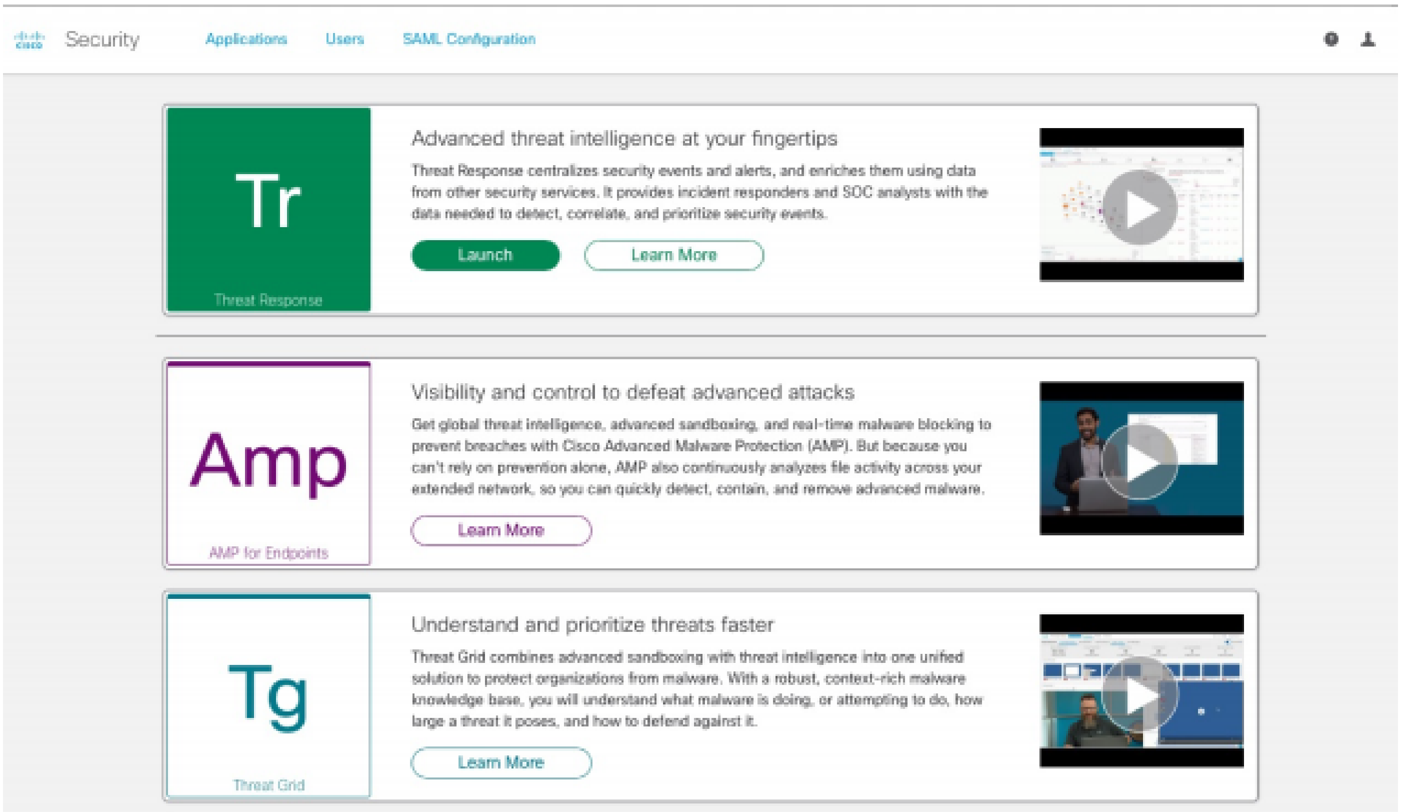
- Amp AMP for Endpoints
- Tg Threat Grid
- Tr Threat Response
- and more...

Your account has been activated.

[redacted]

••••••••••

Step 8. Authentication into castle website depends on the previous cloud configured on your business.



Advanced threat intelligence at your fingertips

Threat Response centralizes security events and alerts, and enriches them using data from other security services. It provides incident responders and SOC analysts with the data needed to detect, correlate, and prioritize security events.

Visibility and control to defeat advanced attacks

Get global threat intelligence, advanced sandboxing, and real-time malware blocking to prevent breaches with Cisco Advanced Malware Protection (AMP). But because you can't rely on prevention alone, AMP also continuously analyzes file activity across your extended network, so you can quickly detect, contain, and remove advanced malware.

Understand and prioritize threats faster

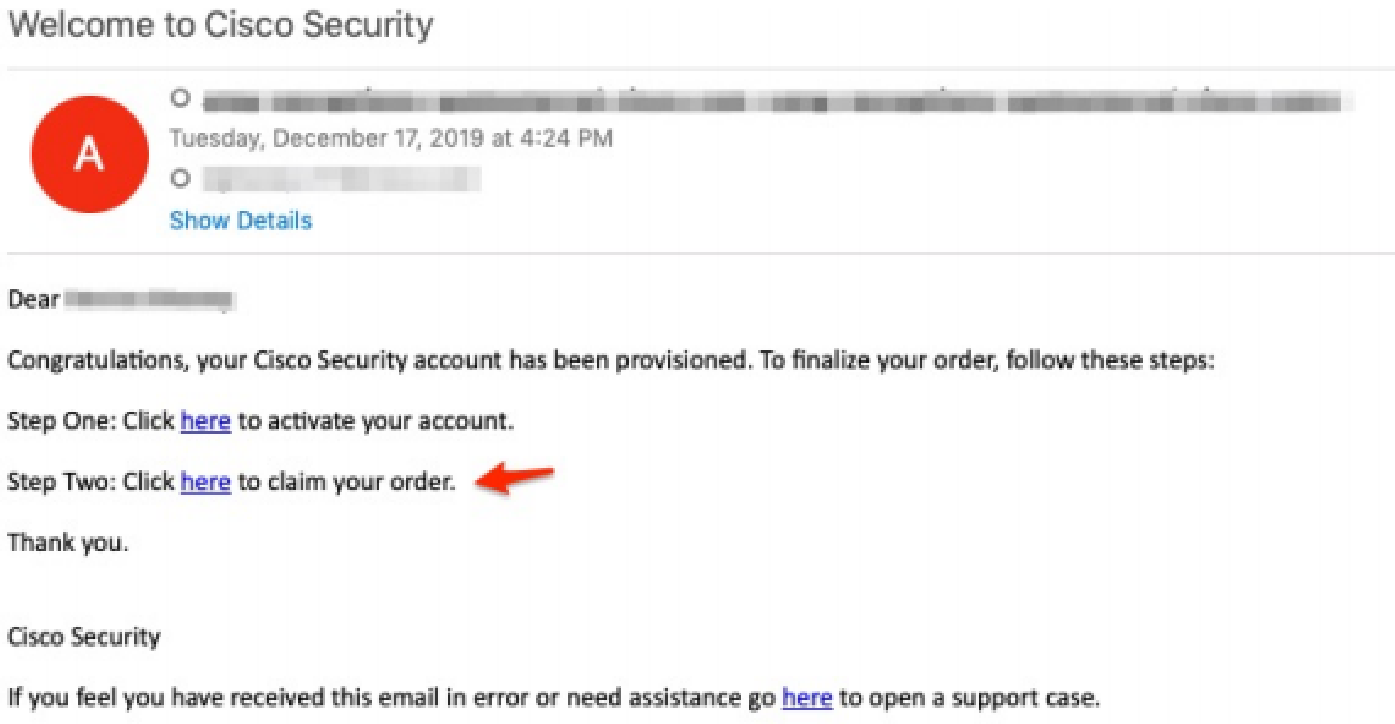
Threat Grid combines advanced sandboxing with threat intelligence into one unified solution to protect organizations from malware. With a robust, context-rich malware knowledge base, you will understand what malware is doing, or attempting to do, how large a threat it poses, and how to defend against it.

Americas Cloud- https://castle.amp.cisco.com

Europe Cloud - https://castle.eu.amp.cisco.com

Asia Pacific Cloud - https://castle.apjc.amp.cisco.com

Step 9. Apply your license on step 2.



Welcome to Cisco Security

○ [redacted]

Tuesday, December 17, 2019 at 4:24 PM

○ [redacted]

Dear [redacted]

Congratulations, your Cisco Security account has been provisioned. To finalize your order, follow these steps:

Step One: Click here to activate your account.

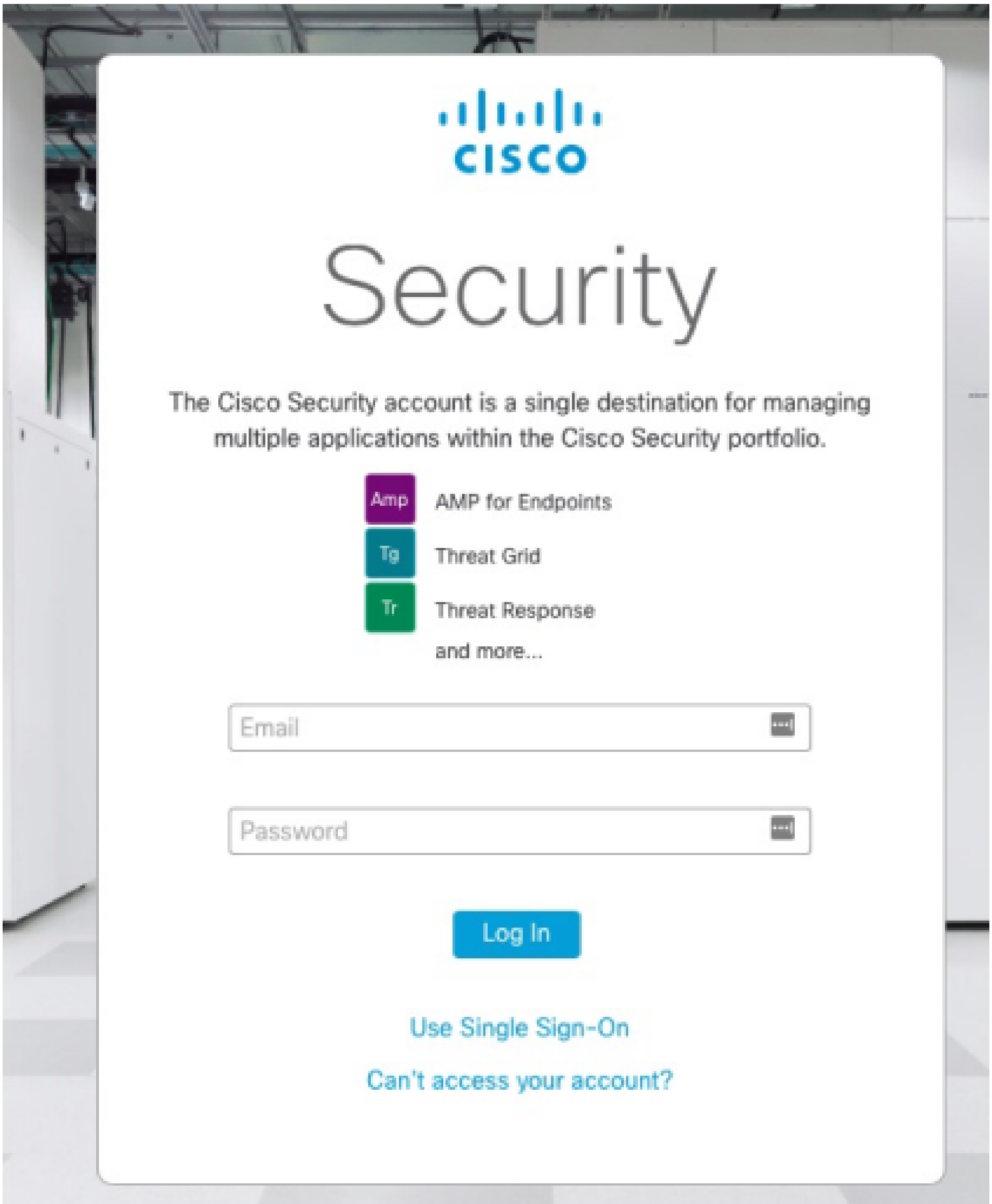
Step Two: Click here to claim your order.

Thank you.

Cisco Security

If you feel you have received this email in error or need assistance go here to open a support case.

Step 10. Log in with your Cisco Security Account.

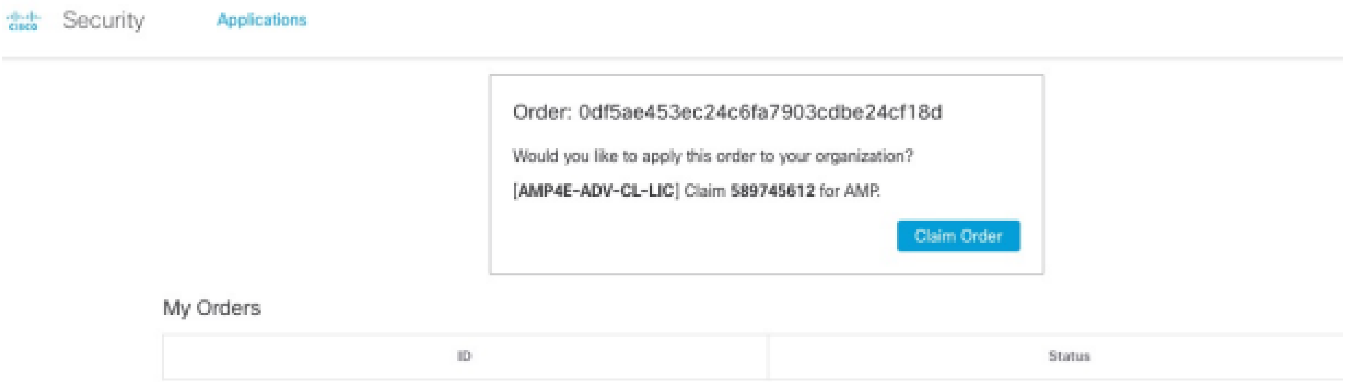


Security

The Cisco Security account is a single destination for managing multiple applications within the Cisco Security portfolio.

- AMP for Endpoints
- Threat Grid
- Threat Response
- and more...

Step 11**.** Once you get in, click on **Claim Order.**



Order: 0df5ae453ec24c6fa7903cdbe24cf18d

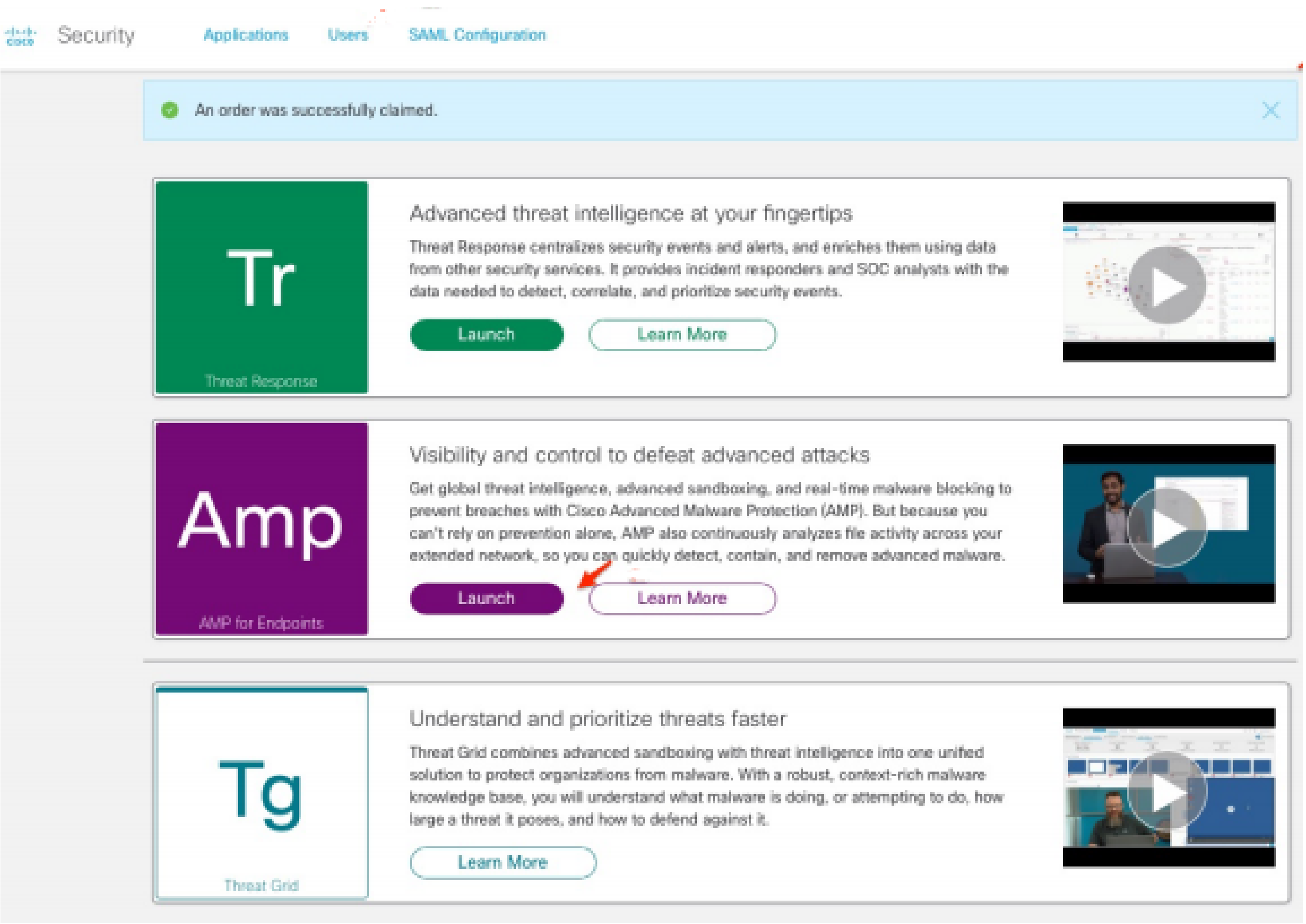
Would you like to apply this order to your organization?

[**AMP4E-ADV-CL-LIC**] Claim **589745612** for AMP.

My Orders

ID	Status

Step 12**.** Now your order is successfully claim and you would be able to launch the AMP4E console.



An order was successfully claimed.

Advanced threat intelligence at your fingertips

Threat Response centralizes security events and alerts, and enriches them using data from other security services. It provides incident responders and SOC analysts with the data needed to detect, correlate, and prioritize security events.

Visibility and control to defeat advanced attacks

Get global threat intelligence, advanced sandboxing, and real-time malware blocking to prevent breaches with Cisco Advanced Malware Protection (AMP). But because you can't rely on prevention alone, AMP also continuously analyzes file activity across your extended network, so you can quickly detect, contain, and remove advanced malware.

Understand and prioritize threats faster

Threat Grid combines advanced sandboxing with threat intelligence into one unified solution to protect organizations from malware. With a robust, context-rich malware knowledge base, you will understand what malware is doing, or attempting to do, how large a threat it poses, and how to defend against it.