Installing email protection solutions

Installation | TRITON AP-EMAIL | Version 8.3

TRITON AP-EMAIL is a Forcepoint on-premises, appliance-based system that prevents malicious email threats from entering an organization's network, and protects sensitive data from unauthorized email transmission.

The Forcepoint TRITON AP-EMAIL solution is available on a V-Series appliance or an X-Series appliance security blade. You may also deploy TRITON AP-EMAIL on a virtual appliance, which can be downloaded from the Forcepoint My Account downloads page.

See the following topics for related TRITON AP-EMAIL deployment and configuration information.

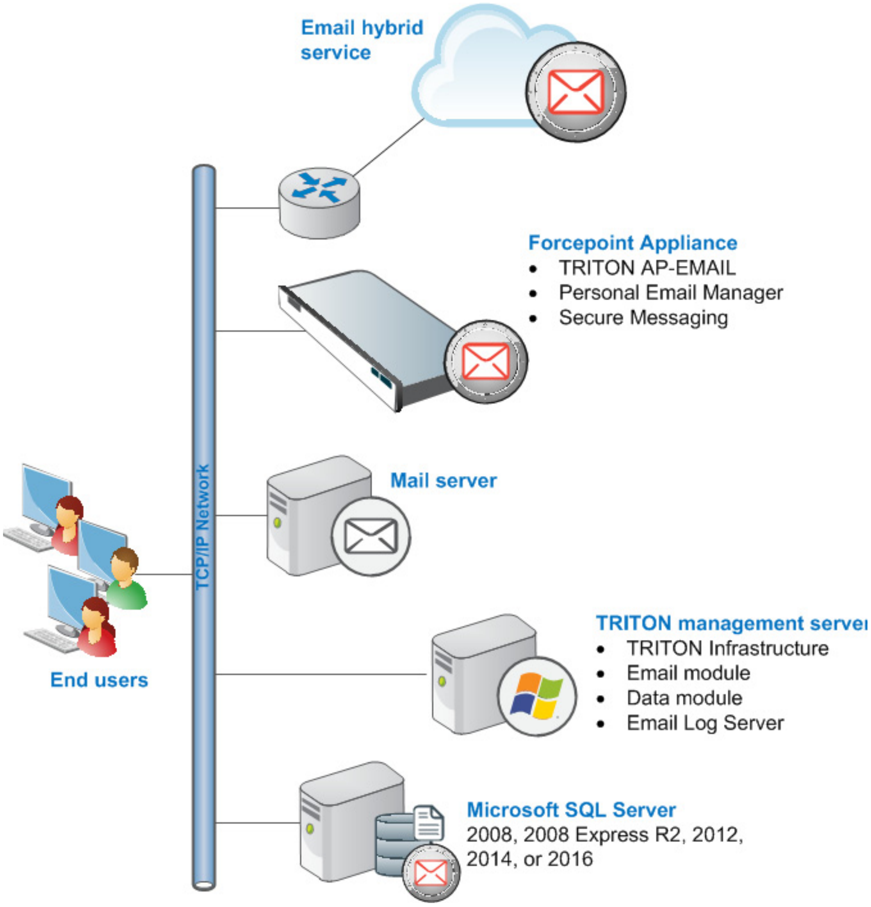
- System requirements
- Single-appliance deployments
- Multiple-appliance deployments
- TRITON AP-EMAIL initial configuration

Contents

TRITON AP-EMAIL brief overview

The following illustration is a high-level diagram of a basic appliance-based deployment of TRITON AP-EMAIL, which includes the Email Hybrid Module. The TRITON Manager must also include the Data module (TRITON AP-DATA) for access to email DLP functions.

Note that this illustration is intended to show the general distribution of components and does not include network details (such as segmenting, firewalls, routing, switching, and so forth).



Installation steps for email protection solutions

Complete the following procedures in the order in which they are listed.

1. Make sure that Microsoft SQL Server is installed and running in your network (see Obtaining Microsoft SQL Server and Installing with SQL Server).

   If you intend to use SQL Server 2008 R2 Express (installed using the TRITON Unified installer), skip this step. You will install the database engine with TRITON management server components.

   Keep in mind that the performance limitations of SQL Server Express make it more appropriate for evaluation environments or small organizations than for larger deployments.

2. Install and configure your Forcepoint appliances. See TRITON Appliances Getting Started Guide for detailed set-up and configuration instructions.

> **Note**
>
> If you have already completed the appliance set-up steps, continue with the next step.

3. Install Email Log Server.

   See Installing email protection components.

4. Install TRITON Infrastructure, the Data module (for email DLP functions), and the Email module.

   See Creating a TRITON Management Server.

Important

To ensure that you install all required components of your email protection solution, including data loss prevention, we recommend that you select TRITON AP-EMAIL on the Installation Type page of the TRITON Unified Installer, rather than performing a Custom installation of the product.

When you select TRITON AP-EMAIL on this page, TRITON AP-DATA is automatically selected as well. Data loss prevention functions are installed along with email protection functions.

A Custom installation does not automatically install TRITON AP-DATA with TRITON AP-EMAIL.

Important

On the Select Components screen in the TRITON upgrade installer, ensure that the TRITON AP-EMAIL option is selected. This option is required if you are running your email protection system on a V- or X-Series appliance or an on-premises virtual appliance.

The TRITON AP-DATA Email Gateway option applies to a cloud-hosted virtual appliance running with TRITON AP-DATA. See the topic titled “Email Gateway for Microsoft Office 365” in the TRITON AP-DATA Installation Guide for details about this product feature.