Cisco Domain Protection

Automates DMARC Authentication and Enforcement to Protect Your Brand and Your Customers

Provides defense for on premise email deployments as well as cloud email platforms like Office 365 and GSuite

Email is the most critical form of communication organizations use to engage with their customers and prospects. And, it remains the number one threat vector used by cybercriminals to target an organization’s customer base through phishing attacks.

Companies are increasingly relying on third-party, cloud-based email senders for their brand communications. This practice leaves customers and partners vulnerable to attack by those who use a domain without authorization. And, the damage affects a brand’s reputation, destroys customer trust and negatively impacts an organization’s bottom line.

Cisco® Domain Protection automatically identifies, monitors and manages emails sent on your behalf. This provides an easy way to identify and eliminate illegitimate email messages and block malicious ones to prevent phishing attacks impersonating your company’s domain. Domain Protection even detects the use of look-alike domains so the malicious URLs can be quickly taken down.

The most effective way to mitigate these vulnerabilities is to use the DMARC standard to authorize and authenticate your email senders, protect your customers from cyber attacks and safeguard your brand’s identity. DMARC is a technology that makes it easier for email senders and receivers to determine if a message is from a legitimate sender. Identifying all legitimate senders can be challenging because of the complexity of an organization’s email ecosystem. The process can also be time consuming and difficult to implement without the right tools, processes, and knowledge.
At a glance
Cisco Public

Benefits

- Prevent brand abuse through impersonation of your company domain
- Protect customers through visibility into your internal and third-party senders who use your domain to send email on your behalf
- Automate the Domain-based Message Authentication, Reporting, and Conformance (DMARC) authentication and enforcement process to identify illegitimate senders
- Block unauthorized senders and set up DMARC protection to reduce illegitimate emails from your domain and protect the value of your brand
- Correlate information into an easy-to-read report for fast visibility
- Increase outbound email marketing effectiveness and campaign revenue

Additional Protections

- Automated DMARC deployment reduces administration and management commitment
- Email cloud intelligence identifies and visualizes sender domains and IP addresses
- EasySPF quickly and automatically builds error-free SPF records
- EasyDKIM automates selector identification and overall management of DKIM

Cisco Domain Protection automates the DMARC email authentication process and gives you visibility into your own and third-party email senders using your domain. It automatically correlates information into an easy-to-read report that lists who is sending email on your behalf and whether they are DMARC compliant. For those senders who are not DMARC compliant, Cisco Domain Protection provides the tools to help you achieve compliance. Cisco Domain Protection also provides guidance on how to block unauthorized senders.

Your Organization

Email Receivers/ MTAs

Cisco Domain Protection

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

(1110R) 04/2019

Cisco Domain Protection provides an additional layer to augment Cisco Email Security’s industry-leading features and more effectively secure your email environment. It can be purchased with any bundle to further safeguard your company’s domain and increase your digital marketing effectiveness.