Gartner Peer Insights ‘Lessons Learned’: Implementing Secure Web Gateways

Published 9 June 2021 - ID G00753574 - 8 min read

By Analysts Peer Contributors

Initiatives: Infrastructure Security

This content, which provides opinions and points of view expressed by users, does not represent the views of Gartner; Gartner neither endorses it nor makes any warranties about its accuracy or completeness.

SWGs offer protection against online threats by enforcing internet policy compliance and utilizing features such as URL filtering, advanced threat defense and legacy malware protection. SRM leaders can learn from the implementation experience of their peers shared on Gartner Peer Insights.

Overview

Gartner Peer Insights is a free peer review and ratings platform designed for enterprise software and services decision makers. Reviews go through a strict validation and moderation process to ensure they are authentic.

We analyzed 205 Peer Insights reviews to identify lessons learned while implementing secure web gateways (SWGs). This report focuses on the responses to the questions: “If you could start over, what would your organization do differently?” and “What one piece of advice would you give other prospective customers?” To browse all reviews, see the full list of Secure Web Gateways reviews on Peer Insights.

Peer Lessons Learned

This edition of “Lessons Learned” summarizes clients’ firsthand experiences with implementing SWGs. The peer advice results both from successful implementation projects and learnings based on what went wrong. This peer perspective, along with the individual detailed reviews, is complementary to expert research and provides a holistic view to the implementation process. Reviewers who submitted their lessons learned represent a cross-section of small- to midsize and large organizations. (See Figure 1.)
Below are some key lessons learned and most cited recommendations by Peer Insights reviewers to help security and risk management (SRM) leaders in the implementation process of their SWG.

Lesson 1: Incorporate Stakeholder Concerns to Prepare the Organization’s Security Requirements

According to the peers, it is essential to protect the organization’s users, networks and data from internet-borne threats as the web becomes more decentralized. Therefore, they advise SRM leaders to factor in the organization’s holistic security and risk compliance requirements by ensuring stakeholder approval as well.

A peer envisages:

Figure out your business requirements by addressing these questions: Are you just protecting users when not on VPN or other corporate networks? Does user identity matter? If user identity matters, can you get active directory administrators time? Answering these and other related questions will help your vendor selection go very smoothly.

— Infrastructure and Operations Professional, Healthcare Sector

A peer also remarks:
If the organization could start over, it would do a requirement analysis through various surveys among the end users. Then, compare solutions based on the demands of the user community and cost-efficiency.

— Data and Analytics Professional, Healthcare Sector

Another peer adds:

The organization would prepare a requirements analysis document based upon the concerns from all the stakeholders on information security and evaluate the best solution possible. The deployment would then be swifter.

— Data and Analytics Professional, Healthcare Sector

Peer recommendations include:

- Gather the security and risk compliance requirements of the IT teams and necessary insight from all other departments.
- Evaluate key websites that impact the organization’s day-to-day operations to understand the present scenario. Prepare a list of all critical, essential and required websites that facilitate seamless functioning of the organization.
- Finalize the requirements and the list of websites by acquiring buy-in of all key stakeholders to minimize issues during the vendor selection and deployment phase.

Recommended reading:

Selecting the Right Strategy for Securing Web Access

Lesson 2: Perform POCs to Test the Capabilities of the Suitable SWG Vendors

The peers recommend SRM leaders to assess the core functionalities, feature sets, market responsiveness, customer experience, pricing and ease of operations of the available vendors to shortlist appropriate vendors. They suggest carrying out proofs of concept (POCs) of the shortlisted vendors to evaluate the alignment of services with the requirements of the organization.

A peer states:
Before purchasing a product, a detailed feature analysis should be done to uncover the best features that the solutions provide. It will surely help in comparing its capability and need with respect to the organization.

— Technical Professional, Energy and Utility Sector

A peer then provides guidance about conducting a rigorous POC:

Clearly define your solution’s expectations and test these during your POC. For example, if you know that you need to be able to view a certain type of web traffic report, be sure to test that upfront and provide those requirements to your vendor representative.

— Security and Risk Management Professional, Media Sector

Another peer contemplates:

If we could start over, we would have done ample performance testing for the solution throughout the organization and would have checked whether it provides appropriate level of security across various departments or not. If it meets all our requirements, we would then recommend its implementation throughout the organization.

— Data and Analytics Professional, Healthcare Sector

Peer recommendations include:

- Execute a thorough analysis of the available vendors’ services, functionalities, security, management, cost and integration capabilities to shortlist suitable vendors.

- Run a detailed POC to check compatibility of the appropriate solutions within the existing security infrastructure. Test in various departments to ensure the solution’s performance is aligned with the organization’s requirements.
Recommended reading:

Gartner Peer Insights ‘Voice of the Customer’: Secure Web Gateways

Lesson 3: Foster SWG Technical Skills by Training the Workforce Prior to the Implementation

A cross section of the peers advocates that it is paramount that the end users are instructed on the technical skills required in the effective management of the SWG, before its deployment. They opine that a prior understanding of the solution would enable the team to drive increased value and ensure maximum security.

In this regard, a peer reflects on the importance of prior training by sharing their organization’s experience:

We watched some live webinars which somehow took us through the onboarding process. I wish we would have signed up and watched those videos before trying to do it ourselves. There are lots of resources out there to help you understand it before attempting the deployment yourself.

— Infrastructure and Operations Professional, Manufacturing Sector

A peer lends further insight:

In our organization, the training sessions could have been more focused on practical and real-time experience, rather than just reading documents or going with theoretical approaches.

— Infrastructure and Operations Professional, Manufacturing Sector
Another peer states:

Take the training sooner — before deploying the solution. That way, the interface becomes pretty simple to understand and you learn about all the capabilities, all the way to the most advanced.

— Security and Risk Management Professional, Finance Sector

Peer recommendations include:

- Disseminate the available documentation to ensure the team fully understands the navigation of the solution’s deployment and the intricacies of its dynamic environment.
- Schedule training sessions on the capabilities of the solution to facilitate optimized configuration, according to their requirements, during the deployment stage.
- Encourage the team to go through the vendor’s user community and support forums for any doubts/concerns to cultivate a culture of self-sufficiency.
- Ensure administrators are properly trained and are willing to steer the training effort throughout the organization.

Recommended reading:

Magic Quadrant for Secure Web Gateways

Lesson 4: Integrate the SWG With DLP Functionality on All Endpoints; Leverage Vendor Assistance for Deployment

The peers direct SRM leaders to integrate the solution with a data loss prevention (DLP) program to ensure a comprehensive classification capability that enables the organization to filter out and block any sensitive traffic. It is imperative to deploy this on all endpoints due to the increasing prevalence of remote working and cloud-based SWGs in the marketplace. Further, they suggest ensuring a robust implementation by utilizing the vendor’s deployment services.

About integrating the SWG with a DLP program, a peer asserts:
Implement the gateway in combination with a DLP program. This will surely work more efficiently to assure maximum security, risk compliance and confidentiality of information.

— Security and Risk Management Professional, Finance Sector

Regarding deployment on all endpoints, a peer indicates the following:

Don’t wait to deploy the agents to all the endpoints. Deploy them sooner to address the remote working challenges sooner rather than later. This would be a big security improvement since home and remote networks are not under corporate control.

— Infrastructure and Operations Professional, Media Sector

A peer further advises:

Use the vendor’s implementation team. They are there to help you get the solution off the ground. You might find yourself getting confused in the interface at first until you get used to it. Thus, save yourself the confusion and onboard that implementation partner.

— CxO, Education Sector

Peer recommendations include:

- Address privacy and regulatory concerns by ensuring Transport Layer Security (TLS) decryption as this will enable other inspection functions of the SWG. Set clear terms about the data that should and should not be decrypted. Establish a “break-glass” procedure for admin access. Integrate the gateway with a mature DLP program to ensure robust filtering of restricted traffic.

- Deploy all endpoint agents that not only perform local filtering enforcement but also ensure remote management of the proxy settings on all devices that are a part of the cloud. Identify and flag any
web applications that do not use the default certificate store.

- Set an acceptable use policy at an enterprise scale to ensure appropriate use filtering so that the end users are unable to access websites that are in violation of the company policy.

- Allocate an internal team of engineers that are proficient in SWG technology to collaborate with the vendor’s deployment team. Ensure their team systematizes the solution’s default ruleset.

Recommended reading:

**Using Secure Web Gateway Technologies to Protect Users andEndpoints**

**Methodology**

Of the Peer Insights survey data considered for this market, only those responses meeting the following criteria were included in this synthesis:

- Reviews less than 12 months old.
- Responses that pertain to the project experience and are not tied to the capabilities of a vendor.
- Reviews were clustered into the top-four most-referenced categories (lessons learned) and then listed in order of relevant phases in the project life cycle.

The results of this synthesis are representative of the respondent base and not necessarily the market as a whole.

“The data used in this report is drawn from reviews on Peer Insights, a crowdsourced enterprise review platform that relies on dynamic data. Key to maintaining the integrity of the site is our ongoing moderation and validation of those reviews. Reviews are examined before publishing to the site and periodically, post-publishing. Due to the dynamic nature of the data, the external Peer Insights site will always have the most updated view of the data in this report.”

**Document Revision History**

Gartner Peer Insights 'Lessons Learned': Implementing Secure Web Gateways - 15 April 2020

Peer Lessons Learned: Implementing Secure Web Gateways - 23 April 2019

**Recommended by the Author**

How to Avoid Failures When Migrating to a Cloud-Based Secure Web Gateway

Quick Answer: How Do We Optimize the Cost of Secure Web Gateways?

Infrastructure Security Primer for 2021
How to Make Cloud More Secure Than Your Own Data Center

Innovation Insight for Extended Detection and Response

© 2021 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by Gartner's Usage Policy. Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "Guiding Principles on Independence and Objectivity."