Solution Brief

3 Critical Questions to Answer Before a Legacy IDS/IPS Upgrade

Organizations may encounter several challenges when migrating from their legacy or aging intrusion detection and prevention system (IDS/IPS or IDPS) to a modern alternative

One of the most important considerations is timing - that is, when should you plan on making the move to replace your legacy IDS. The drivers and timing are different for each organization, but Stamus Networks customers have identified several questions that helped their security executives determine when they should budget to replace their legacy IDS.

In considering when to allocate budget for the project, try to answer these 3 essential questions:

- How much longer do you have with your current IDS/IPS?
- At what point will your legacy IDS/IPS no longer be enough?
- Are there staffing issues impacting legacy IDS/IPS operations?

How much longer do you have with your current IDS/IPS?

Evaluating, selecting and deploying an upgrade to your legacy IDS can take a highly motivated team up to 3 months. And in large enterprises, we have seen the process extend out to 12 months or longer. Therefore, it is important to understand the runway of your current solution.

This timeline can be dictated by your contract renewal cycle, or the end of a support contract, or through other internal organizational factors. To explore some of these reasons, download the solution brief, “12 Signs it's Time to Upgrade your Legacy IDS/IPS”, from the Stamus Networks website.

In order to answer this question, review the contract details for both your software licenses and any separate support arrangements you may have in place. And don’t forget to consider organizational policies that might impact your ability to continue using your current system.

As your network and organization evolves, so must your security controls. As a security leader, you must continually balance your security investments with your organization's risk tolerance. And you want to be confident that the controls you have deployed are sufficient to minimize your organizational exposure.

At what point will your legacy IDS/IPS no longer be enough?

If your IT infrastructure has undergone significant changes - such as a substantial shift to the cloud or massive increase in network traffic - it is critical that your network security monitoring has kept pace with these changes.

The typical high-end legacy IDS, for example, was designed to effectively inspect 1 Gbps of network traffic while running the full suite of detection rules. If your network traffic has increased to 10 Gbps or beyond, this will no longer be sufficient.

Similarly, if you have shifted a major portion of your computing and application infrastructure to a public or private cloud provider, your legacy IDS may not support that deployment model.

Each of these scenarios create blind spots in your network defenses. At some point, these blind spots can render your controls ineffective, eroding your confidence and increasing your exposure. The question, of course, is when?

Are there staffing issues impacting legacy IDS/IPS operations?

In today's employment climate, major personnel changes have become commonplace. These changes may adversely impact your team's ability to support the systems you have in place, including your legacy IDS.

In many organizations, the responsibility for operating and maintaining their network intrusion detection system falls on one or two individuals. The longer those systems have been in place, the more likely the original team of experts responsible for your IDS is no longer available.

Legacy IDS have developed the well-justified reputation of being "alert cannons" due to the overwhelming volume of information they generate. Without sufficient automation in place, these systems can place a massive burden on the security operations teams charged with managing them.

Often the staff responsible for the legacy IDS are your most productive and experienced and, therefore, become best candidates to be redeployed onto higher priority projects. Each redeployment can cause a gap in expertise managing and maintaining the legacy IDS.

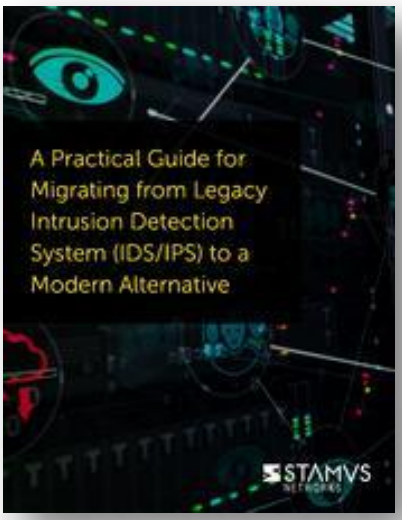
Personnel changes are inevitable, but to the extent that you are able to anticipate a transition, your organization can mitigate the impact of the changes. Ask yourself if there are personnel events or changes that might justify looking at migrating from your legacy systems.

LEARN MORE

At Stamus Networks, we have captured the insights gathered from our experience helping organizations migrate from their legacy IDS/IPS to a modern alternative in a practical guide designed to help you sort through the process.

Visit the Stamus Networks website to download “A Practical Guide for Migrating from your Legacy Intrusion Detection System (IDS/IPS) to a Modern Alternative”

Click here to request a download



ABOUT STAMUS NETWORKS

Stamus Networks believes that cyber defense is bigger than any single person, platform, company, or technology. That’s why we leverage the power of community to deliver the next generation of open and transparent network defense. Trusted by security teams at the world’s most targeted organizations, our flagship offering – Clear NDR™ – empowers cyber defenders to uncover and stop serious threats and unauthorized network activity before they harm their organizations. Clear NDR helps defenders see more clearly and act more confidently through detection they can trust with results they can explain.

STAMUS NETWORKS

5 Avenue Ingres
75016 Paris
France

450 E 96th St. Suite 500
Indianapolis, IN 46240
United States

contact@stamus-networks.com
www.stamus-networks.com

