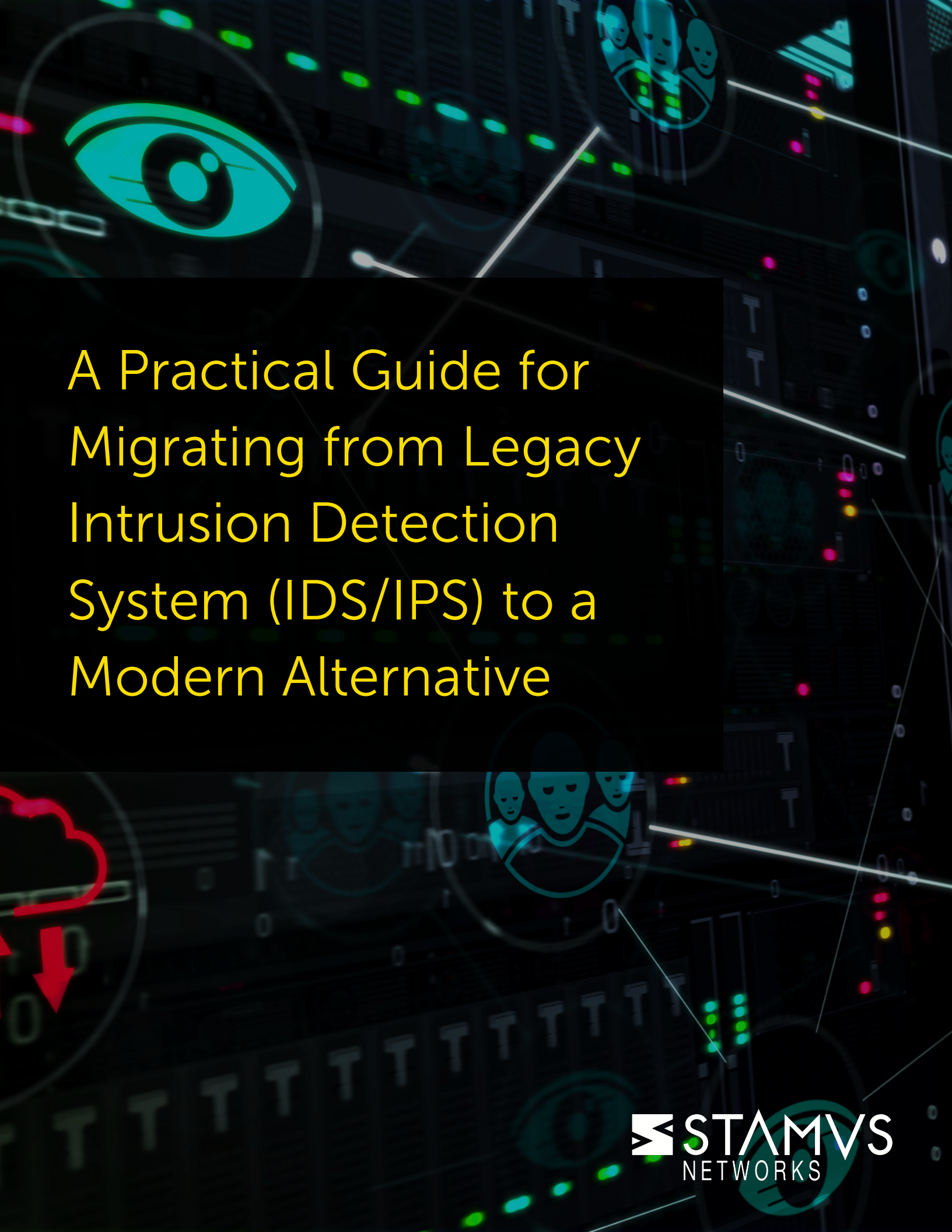

A Practical Guide for Migrating from Legacy Intrusion Detection System (IDS/IPS) to a Modern Alternative

STAMUS NETWORKS

TABLE OF CONTENTS

INTRODUCTION AND OVERVIEW

Stamus Networks has helped many organizations around the world migrate their legacy intrusion detection and prevention systems (IDS/IPS or IDPS) to a more effective modern alternative. And in the process, we have gathered a number of insights that we hope can help you along your own journey.

This guide presents the collection of these insights. We hope it can help you answer the following questions and perhaps spawn a few more:

- When is the right time to upgrade your current intrusion detection system?
- What are realistic goals when migrating to a modern IDS/IPS alternative?
- Who should you involve in evaluating the decision-making process?
- Which criteria should you use to evaluate an upgrade to our current IDS/IPS?
- Should you issue an RFI, RFP or RFQ? And if so, at what point in the process?
- What are reasonable steps to take when doing your final due diligence?
- What are some of the best ways to engage with the vendor community?

TODAY'S NETWORK SECURITY

The idea of monitoring your network for attacks and anomalous behavior has been around since the early days of the Internet. In fact, this requirement has been codified in a number of regulatory compliance guidelines and cyber risk frameworks such as PCI DSS, and referenced indirectly as a critical control in many others such as NIST, ISO 27001 and ISO 27002, FISMA, SOC2, and SANS CIS.

The requirement for network security controls has most commonly been addressed by IDS/IPS which have been widely deployed - and widely disliked. And widely ignored. These legacy IDS/IPS are disliked for a number of very legitimate reasons.

At a minimum, the solution you migrate to from your legacy IDS should:

- Significantly improve the scope and accuracy of your threat detection
- Cost you significantly less to own and operate over its lifetime
- Easily integrate into your organization's current architecture

Here are a few examples of the common complaints leveled against legacy IDS:

- They produce a high volume of alerts which overwhelm security operations teams trying to ascertain their validity, or they are simply suppressed or ignored
- They employ inconclusive detection techniques (and the false positives this creates)
- They are unable to keep pace with the growing volume of network traffic
- They cannot detect many of today's sophisticated threats
- The alerts they log are missing contextual information needed to understand the event
- Their lack of deployment flexibility and east-west monitoring leaves users with numerous blind spots

Too often this leads to deployments that are ineffective at everything except satisfying the bare minimum "check box" compliance with one of these frameworks.

You can - and should - expect more from your network security system.

We suspect you are reading this paper because your current IDS/IPS solution has reached its end of life, come up for renewal, has reached the end of its support contract, or you simply want a more effective system for monitoring your network for intrusions and threats. Whatever the reason that is motivating you to change, we hope you find this guide useful.

At a minimum, the solution you migrate to from your legacy IDS should:

- Significantly improve the scope and accuracy of your threat detection
- Cost you significantly less to own and operate over its lifetime
- Easily integrate into your organization's current architecture

The good news is that all three of these are achievable with today's modern IDS/IPS alternatives. Of course, it is important to look closely at your alternatives in order to select the solution that is optimal for your organization.

WHAT TO EXPECT FROM A MODERN IDS/IPS ALTERNATIVE

Today's IDS/IPS alternatives are powerful platforms for threat detection, hunting and automated incident investigation. And some are even designed to drop right into your existing tech stack, easily taking the place of your existing IDS and growing with your organization as you mature your security infrastructure.

Characterized by multidimensional threat detection, guided threat hunting and automated incident investigation, the modern IDS/IPS alternative offers:

- Significantly improved visibility into what's happening with your network assets, in both your cloud and on-prem environments
- Behavioral anomaly detection by applying multiple analytical techniques including machine learning and statistical analytics to protocol transactions, network flow, and other events
- Powerful Suricata-based signature and reputation list detection which represents an order of magnitude improvement over classic IDS detection
- Easy integration with third-party sources of threat intelligence
- Conditional packet capture, adding to the already substantial evidence needed for incident and forensic investigation
- Built-in native incident investigation and threat hunting user interface and reports
- Automated event triage and guided threat hunting to reduce burden on the security operations team
- High-fidelity notifications that alert the security operations team only when they are facing serious and imminent threats
- Support for public cloud, private cloud, on-premise and hybrid deployments
- Easy to deploy and get started as a drop-in replacement for the legacy IDS in your existing security tech stack

And, even with all these improvements, the modern IDS alternative retains the positive characteristics of the legacy IDS, including openness, detection clarity, and a clear trail of forensic evidence to support incident investigations.

CAVEATS

We want to be clear - our team has been very involved in many phases of the process, but our perspective has always been that of an outside vendor looking in. The insider knowledge we incorporate here has come from our discussions with those on the front lines working to scope the project, develop requirements, identify alternatives, select a solution, install and integrate the solution into their environment, and ultimately begin operating and reaping the benefits of the installation.

For this reason, we have chosen to refer to this as a "Practical Guide" loaded with tips and ideas for your consideration - and not position it as anything close to an "Essential" or "definitive" step-by-step guide.

That said, we hope this guide helps you consider a few things you may have overlooked and that you will derive a few nuggets of wisdom from reading it.

HOW TO USE THIS GUIDE

This guide is written as a series of stages in the process. For simplicity, we have written it as if the process of selecting and installing a replacement for your legacy IDS/IPS were linear, with each stage dependent upon the completion of the previous stage.

The reality is that most organizations do not follow each of these stages in order, many will omit or skip right over several of them, and still others will include additional steps in their process.

So, our recommendation is to scan the document, reviewing each heading and zooming into the sections that make sense for your organization.

We also provide companion resources that you may customize to help you with your own upgrade journey. These include:

- 3 Key Questions to Ask your Team (and answer) before Migrating from your Legacy IDS/IPS
- Evaluation Criteria for Migrating from Legacy IDS/IPS
- 10 Technical Considerations when Migrating from Legacy IDS/IPS
- 10 Business Considerations when Migrating from Legacy IDS/IPS
- Project Management Checklist for Legacy IDS Migration

DECIDING WHEN TO UPGRADE YOUR LEGACY IDS/IPS

If you haven't already decided to upgrade your legacy IDS/IPS, you will want to start here. At this point it is critical to evaluate the motivations to consider migrating from your legacy IDS.

Here are a few examples of factors that have motivated our customers to upgrade their legacy IDS/IPS:

- **License renewal** - the license for your legacy IDS/IPS is up for renewal or your support contract has expired
- **End of life** - your current generation IDS/IPS has reached the end of its life and is no longer functioning
- **Forced upgrade** - your current vendor is forcing you to rip-and-replace due to SNORT 3 migration
- **Tech stack update** - your organization is reviewing your IT security stack as a result of a merger, acquisition or business unit consolidation
- **Negative ROI** - The cost of maintaining your legacy IDS/IPS has exceeded its value to the organization
- **Alert fatigue** - your staff is no longer paying attention to the results/alerts from your current IDS, and you wish to reduce the risk exposure facing your organization
- **Consolidate functions** - you wish to reduce complexity and combine functions of IDS and NSM into a single platform
- **Shift to the cloud** - your infrastructure has evolved into complex hybrid cloud environments such that the legacy IDS/IPS no longer provides the needed network visibility, leaving you with blind spots
- **Performance limitations** - the demand for high-throughput networks is growing beyond the ability of your legacy IDS to process all the data, and you can't run all the IDS rules you are paying for
- **Breach reaction** - you've recently been breached and - following a review - you realize you need to improve your network security controls and monitoring
- **Accelerate response** - you came to the realization that with the right choice you can improve your mean time to respond (MTTR) with a more automated response
- **Realization that an upgrade is practical** - you have concluded that modern network security (IDS/IPS upgrade) technologies deliver better results for lower total cost of ownership and can be a drop in upgrade

Inevitably, budgetary and other factors will come into play in your decision. So, when considering the 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?

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.

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.

When will your legacy IDS/IPS cease being effective?

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.

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 10Gpbs 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 blindspots in your network defenses. At some point, these blindspots 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.

SETTING GOALS

As with any substantial new program, it is important to establish clear goals and objectives before beginning to evaluate potential solutions. Ideally these goals meet the five criteria outlined in the S.M.A.R.T. goal structure (as identified by George T. Doran in his seminal 1981 paper) - specific, measurable, achievable, relevant, and time-bound.

Setting goals is valuable in helping you make decisions, track progress and - perhaps just as importantly - to help you refine your process and improve your ability to scope similar projects in the future.

While your organization will likely have unique circumstances, we have seen our customers create goals around the following areas

Cost - here you may work to set goals for up front costs, annual recurring software costs or total cost ownership over a 5 year period. In any case, you will likely want to establish both capital expense (CapEx) and operations expense (OpEx) budgets.

Detection coverage - are there specific blindspots you hope to eliminate? Are there types of attack vectors for which you want to make sure you have detection in place? Should you establish targets for the amount of third-party threat intelligence or signatures that the system must consume?

Timing - often this is focused on the end goal of when you hope to have the system fully operational, but you may wish to establish intermediate goals such as dates for when you want to enter and exit a proof of concept or lab trial, when you hope to make your final selection, when you plan to issue a purchase order. Here, it could be helpful to develop a project timeline, working backwards from your go-live date.

IDENTIFY STAKEHOLDERS AND ENGAGE THEM

As with any projects, there will be a number of people within your organization who will be impacted by the results. The impact on these stakeholders should be an important part of the process.

Based on the goals and scope of your project, these stakeholders may include personnel from:

- Senior leadership
- Network engineering and operations
- SOC engineering and analysts
- Incident response
- IT infrastructure
- Other areas .

Here you may consider creating a responsibility assignment matrix in order to clarify and define roles and responsibilities for tasks in what is most always a cross-functional project. A common model for this is the R.A.C.I matrix in which you identify which stakeholders are responsible, accountable, consulted, and informed for which portions of the project.

Start by identifying all the potential stakeholders for each phase of this project and then map each to their roles and responsibilities. This can bring clarity to the process and help avoid conflicts, finger pointing, and other issues along the way.

IDENTIFY CRITICAL REQUIREMENTS

After identifying your goals, it is important to identify the technical and business requirements that will be critical for your success. This will likely be one of the most important elements of your project plan.

Be sure to involve your stakeholders in the development of your requirements. You may choose to interview each stakeholder individually, capture their thoughts on a survey, or simply pull everyone into a meeting to interactively debate the merits of a given set of requirements.

Note: If you have decided to follow a formal request for information (RFI), request for proposal (RFP), or tender process, this set of requirements should be summarized into a set of questions you will send to the vendors on your short list.

While your requirements will be very specific to your unique organizational challenges, here are a few areas - both technical and business oriented - to consider developing requirements around.

Technical-oriented requirements

Deployment - you can only detect threats on networks where you have deployed some form of sensor. If your IT infrastructure is spread across multiple sites, branch offices and cloud environments, you will need to deploy sensors or probes in a set of locations that enable the IDS upgrade to inspect all traffic traveling between these sites (for intrusions, remote command and control, and extractions) and within each site (for lateral movement). So you'll need to identify a set of requirements around each of your deployment scenarios. Also, if getting the system up and running quickly (time-to-value) is important to you, you may wish to develop requirements around ease of deployment.

Detection - the success of any network security solution starts with its ability to autonomously detect threats and notify security personnel when something bad is happening. Here you may wish to consider a broad-spectrum of detection techniques. For example, traditional IDS signatures and dataset matching (e.g., domain and IP reputation lists) can provide definitive detection of known threats. Likewise, behavioral analytics techniques such as machine learning and artificial intelligence can help identify suspicious activity that is likely to be malicious. You may also wish to specify the time-to-efficacy and transparency of certain proprietary techniques - how does it work and how long does it take to be effective. All of these are important advancements in the state of the art. You will want to determine which are important for your environment.

Automation - often, one of the primary complaints about legacy IDS is that they require entirely too much human intervention to be effective. This is due to the overwhelming number of alerts they generate with very little context and lack of confidence indicator relative to false positives. For that reason, when you are upgrading a legacy IDS, you may want to define requirements around automation. Today's modern IDS alternatives are capable of automating the alert triage process with some really interesting tagging and classification mechanisms. In addition, the more advanced systems are able to deliver ultra high-confidence declarations of compromise that can be used to automate your response through incident management or another higher-level system such as a security orchestration automation and response system (SOAR).

Performance - as your network has grown, the amount of traffic that your network security system must inspect has also increased. Not very long ago, an IDS might be required to monitor a combined 1 Gbps of traffic in a typical enterprise datacenter. Today, our customers are deploying multiple 40 Gbps probes and evaluating the need to deploy 100 Gbps probes. As you look to develop your specific requirements it is critical that you include a set of requirements around the system's performance. When specifying the performance requirements, be certain to articulate under what conditions those performance figures must be achieved. For example, should the system be required to process 100% of the traffic with all detection techniques enabled at full line rate?

Transparency, explainability and evidence - what we are hearing from experienced defenders is that the right solution for the rapidly changing threat landscape lies in a security infrastructure built upon open components - solutions that are open to third party threat intelligence and third party system integrations while openly delivering transparent results and the evidence to support the detection. They want to be able to understand what

triggered the alert and how it relates to their assets being attacked. They want to be able to access all related information associated with a threat declaration or incident in order to understand what happened. Believe it or not, there are a number of IDS replacement systems on the market that do not provide this detail. As such, you will likely want to include requirements around the system's visibility into the attack campaign and the impacted assets and to clearly communicate with the team responding to the incident.

Threat hunting - the proactive detection, isolation, and investigation of threats that often evade automated security systems has emerged as a key component of enterprise security strategies. As more and more sophisticated enterprises adopt proactive threat hunting programs, they are looking for their network and endpoint solutions to provide tools to make their jobs easier. Our customers have told us that this is an important feature in their IDS upgrade platform. They are seeking tools for both the experienced analyst as well as those who are not as skilled. If proactive threat hunting is important to your organization, you may wish to develop some requirements around critical capabilities that include search, filtering and pivoting on events and metadata using predefined and custom filter criteria. Also, if you plan to involve junior analysts in your threat hunting program, you may want to add requirements for built-in guidance and workflow aids that facilitate a consistent and repeatable process.

Openness and extensibility - our customers frequently remind us that our network detection systems are not the only tool in the security tech stack. And in order for organizations to take advantage of best-of-breed technologies, the IDS upgrade should provide open interfaces that enable straightforward integration with other systems such as SOAR, SIEM, XDR and incident response (IR) systems. Here, you may wish to include requirements around a unified data model or the availability of specific integrations. And because there are many reliable sources of threat intelligence, it is critical that your vendor does not lock you into only their proprietary threat intelligence and detection algorithms. If this is important to your organization, you will want to write requirements that speak to your ability to take advantage of third-party threat intelligence and customize detection in your environment.

Based on our work with customers, we have broken down the above into a list of 10 specific technical-oriented evaluation criteria to consider when upgrading your legacy IDS. See ***10 Technical Considerations when Migrating from Legacy IDS/IPS***. This guide can be found online and also includes a companion evaluation checklist spreadsheet (see next section) to help you score each of the solutions you are evaluating.

Business-oriented requirements

Process integration - your legacy IDS is currently part of a broader security process involving a number of systems, workflows, and personnel. Selecting and installing a new system can be very disruptive to these existing processes. In an ideal world the upgrade for your legacy IDS would drop seamlessly into your existing processes and workflow with very little disruption. With this in mind, you may wish to identify several key requirements that aim to make this integration as streamlined as possible.

Budget - very few enterprise purchasing decisions are made without considering cost. The factors that seem to impact our customers the most center around the general pricing models and the mix of upfront costs, recurring costs and payment terms. For example, some vendors offer fixed price perpetual licenses for different performance tiers, while others offer dynamic pricing based on the amount of traffic ingested into their systems. Still others offer a one-size-fits all license with no tiered pricing. If your organization prefers one pricing model over another, you may wish to document your requirements in this area. Of course, if you have an overall budget for the project, you will want to include a requirement specifying OpEx and CapEx budget figures.

Vendor - enterprises prefer to do business with organizations that make it easy to work with them, demonstrate a strong degree of integrity, are financially stable, and are committed to both the market and solution. While these sound like table stakes type requirements, they are still worth documenting and articulating. Additionally, you may prefer to do business with an industry innovator - typically a smaller, younger firm with a strong pedigree. Or you may prefer a more established player with a longer track record. Or, you may have a values-based desire to support the open source community. If you believe strongly in any of these attributes, consider adding requirements that capture these ideas.

Onboarding - once you've made the decision and it's time to bring the new IDS upgrade into your environment, you want to ensure the process goes smoothly. The onboarding experience can vary widely depending upon your particular situation. You may wish to document requirements around installation, customization, training, and ongoing support. These factors can greatly impact your time-to-value for the solution and your ability to meet the goals you set out for the project.

Based on our work with customers, we have created a list of 10 specific business-oriented evaluation criteria to consider when upgrading your legacy IDS. See ***10 Business Considerations when Migrating from Legacy IDS/IPS***. This guide can be found online and also includes a companion evaluation checklist spreadsheet (see next section) to help you score each of the solutions you are evaluating.

The output of this exercise will be a list of requirements that you will then use to inform your selection criteria.

ESTABLISH EVALUATION CRITERIA AND PROCESS

While we discussed the importance of listing all your requirements in the previous section, it is crucial to establish which of these requirements are mandatory to the success of your project. So here, we need to map these requirements into evaluation or selection criteria to help manage the complexity of the comparison process.

The tool used by most of our customers for this exercise is a simple spreadsheet that looks something like the figure below

	A	B	C	D	E	F	G	H	I
1	Evaluation Criteria for IDS Upgrade								
2									
3	Technical Criteria								
4			Requirement Level (Yes/No)				Vendor Scores (1-5)		
5	Criteria	Description	Required	Desired	Admired	Weight (1-5)	Vendor 1	Vendor 2	Vendor 3
6	Operation on-prem and in the cloud	The solution may deployed to monitor network traffic on-premise and in cloud (public and/or private) environments.				2			
7	East-west as well as North-south traffic	The solution is optimized for both east-west as well as north-south traffic and perform analysis on both types of traffic patterns				2			

Some of our customers have chosen to rank their requirements by their importance using a three-level system which identifies any given requirement as either required (must have), desired (would like to have), admired (nice to have).

By way of example, we have provided a template with both business requirements and technical requirements that you may customize for your particular organization. See the companion spreadsheet, entitled Evaluation Criteria for Migrating from Legacy IDS/IPS.

Once you've defined your evaluation criteria, you will want to develop a workable method of evaluating the proposals. Oftentimes a simple weighting and scoring system can help here.

For example, if you assume that the "alignment" or "fit" of a potential solution can be quantified for each requirement, then you can use a five- or ten-point scale to assign a relative value for each potential solution. The idea here is to use this score to compare potential solutions against a single evaluation criteria or requirement.

Additionally, one of the evaluation criteria may be more important to you than another. In order to accommodate these differences, consider assigning a weight (from 1-5, for example) to each criteria, where 1 represents a less significant criteria than a 5. Now you can multiply the potential solution score in each criteria by the criteria's weight, allowing you to easily compare the solutions using a single number that represents the total of all the weighted criteria scores for each solution.

CREATE PROSPECTIVE VENDOR LIST

After you have established your selection criteria and begun mapping out the process you will use to evaluate the solution, you can begin looking for solution providers (vendors) who meet those criteria.

At this stage you likely already have a "starter" list based on your preliminary research of what is possible and even conversations with peers, advisors or industry analysts. Because the vendor landscape is constantly changing and new solutions are introduced frequently, you may want to encourage your team to take a fresh look at what is available. While looking for alternatives, remember to vary your search keywords because different providers refer to their solutions using different terminology.

Here are a few common searches to consider:

- *Alternatives to intrusion detection system*
- *Types of intrusion detection systems*
- *Replacing my legacy ids/ips*
- *Upgrade my intrusion detection system*
- *Replacement for intrusion detection*
- *Modern IDS*
- *Next-generation IDS intrusion detection*
- *Get more out of your IDS*

In addition to general purpose Internet searches, you may want to look at one of the many online enterprise software review sites, such as Gartner Peer Insights, G2 or Capterra. The result of this effort should be a reasonably short list of solutions and vendors with whom you want to engage in a more detailed evaluation. Our customers have typically considered between 4 and 9 solutions for a preliminary evaluation.

CONTACT VENDORS AND REQUEST INFORMATION

Once you have identified your list of prospective solutions, it's time to contact each supplier and engage them in a detailed discussion around your requirements and their product's capabilities.

In this process, it is important to remember that successful businesses are built on successful relationships. Many organizations forget to approach the supplier partner relationship with the same attention as with their customers. In our experience, transparency is key to building trust which, in turn, is key to building a healthy relationship.

When you do reach out to your prospective supplier partner, it is important to be upfront about your goals, the selection process you intend to follow, and the timeline.

The approach you take in the initial contact with your prospective supplier partner will depend on your timeline and on how much you already know about the available solutions. The three common starting points are:

- Request for information (RFI)
- Request for proposal (RFP)
- Request for quotation (RFQ)

Should you start with an RFI?

If you are unsure about what the market might offer and you have the time to do so, you may wish to consider starting with a request for information (RFI) - a document that asks suppliers for general information about the solutions they can provide and makes vendor comparison easier.

A typical RFI might include the following sections:

- Statement of need - your goals and objectives
- Background - context about your organization, architecture, tech stack, etc
- Qualifications - vendor attributes and credentials you're looking for
- Information requested - what you hope to learn about the solutions
- Selection of the solution - your evaluation criteria
- Time for response - the deadline

In the section above entitled “Information requested”, you may start by generalizing your requirements and re-writing them as open-ended questions.

Keep in mind as you create your RFI to write it in a way that will make it easy to compare solutions, provide a clear format for vendor responses, ask for general information while avoiding being too specific, and finally, be brief and respectful of the supplier’s time.

An RFI is especially helpful if you’re new to the solution space. Your bidders’ responses will not only demonstrate their expertise, but also inform and educate you with very little time invested by either party. Their answers can also help you establish more definitive questions for an eventual RFP.

Bonus: because an RFI collects general vendor information, some organizations use RFI templates to create vendor profiles for recurring procurement projects.

Should you issue a formal RFP?

If you have a very good handle on your requirements and are ready to evaluate solutions based on a set of known criteria and/or are required to bid out the project, consider moving right to a formal request for proposal (RFP). RFPs are similar to RFIs, except they contain more specific questions, and they imply an intent to purchase.

In the RFP, you will ask specific, detailed questions about the product and the supplier’s business.

The RFP is not about getting as much information as possible in the hope of being able to differentiate further downstream. Rather, the RFP is about discovering and exploiting a subset of information that will accentuate differentiation in the early phases of the process.

You may consider including one section that allows the vendor to showcase its expertise unconstrained by a specific response format. Commonly, vendors will use this section to cover vertical expertise, comparable client examples or implementation best practices. This should give the evaluation team an insight into where the vendor considers its strengths lie. It will also define how well it has understood your organization, the RFP and the intended security operations strategy.

There are numerous online resources available to help you develop your RFP, but a typical RFP will include the following sections:

- **Executive summary** - your project, the goals and objectives
- **RFP overview** - project background, scope and deliverables, timeline, minimum requirements, evaluation and scoring criteria
- **General company questions** - this section is intended to simply collect all relevant information about the company
- **Product and service questions** - this will represent the bulk of your questions, pertaining mostly to feature and functionality, competitive differentiation, and product roadmap
- **Past performance questions** - the goal of these questions is to assess past experiences, staff expertise, and ask for customer references
- **Culture and compatibility questions (if applicable)** - designed to assess the vendor risk and any sustainability or diversity requirements
- **Cost proposal questions** - make sure to cover pricing model and payment terms
- **Attachments and addendums** - here you may include a glossary of terms, service level agreement, vendor code of conduct, sustainability policy, non-disclosure agreement (NDA) and any other applicable elements

PRO TIP: Our successful clients tell us that after you've drafted the RFP, you may want to pause for a moment and objectively review the RFP before you issue it. Read the RFP as if you were an outside company who had no prior knowledge of your organization and your intended operations. If anyone in your organization has worked for a security or IT vendor previously, consider tapping into their knowledge.

What about an RFQ?

A request for quotation (RFQ) is a request for pricing and payment information about a highly- specific solution. You will use this format once you have narrowed your selection to a few vendors. We will cover this in the "Select the right solution" section below.

Invite solution providers to respond to your RFI or RFP

The process, of course, does not start and end with a written document. The RFP needs to get into the hands of the right people at your prospective IDS upgrade solution partner.

This step is typically as simple as sending an email to your existing contacts asking if their company would like to participate. Of course, In that introductory email, it is important to clearly describe your project and share your deadlines.

NOTE: Because these documents are created by your team with an intimate understanding of your environment, the vendors who are responding may have questions. Here it is helpful to provide a means for vendors to submit questions or request clarification. To keep things equitable, you will want to provide the list of questions and your responses to them for all potential respondents to review. This can be done through a password-protected website or email distribution.

EVALUATE TOP CANDIDATES "ON PAPER"

Now that you have collected information on the most viable solutions from each vendor, it's time to review their responses, create a short list of the top candidates and begin your due diligence in preparation for making your final decision.

If you went through a formal RFI and/or RFP process, you should have a wealth of similar data in response to your questions. That said, as you work through the proposals, you may encounter complications. That is because each of the responses will be slightly different, each focusing on slightly different requirements, offering different price points, and highlighting each solutions' unique strengths as well as highlighting their weaknesses and a few limitations.

Confirm your evaluation criteria

Hopefully, you established your evaluation criteria and scoring system earlier in the process. That said, it may make sense to review your evaluation criteria in light of the responses to make sure you have considered the most important aspects of your overall solution.

And if you haven't established that criteria, now is certainly the time to do so.

Once you are happy with your evaluation criteria and the scoring system you will use, it's time to review the proposals and compare the results.

Review each proposal and rank each solution

At this point, it's usually a good idea to share the vendors' proposals with your stakeholders, so that they can review each response and begin to form their thoughts about each solution. Many organizations choose to hold a team meeting in which all the stakeholders discuss each proposal, review the evaluation criteria, and score them.

For many organizations, it is critical to document this process thoroughly. At these organizations, strong internal controls are in place for selecting vendors. And in highly-regulated industries like pharmaceuticals, insurance and government contractors, there are external auditors to consider as well.

Create your shortlist

After reviewing, evaluating and ranking the IDS/IPS upgrade proposals you've received from a number of vendors, you will want to make a shortlist of the best prospective solutions. These are the vendors you want to perform due diligence on. This might include an in-person meeting, a live demonstration and possibly a network trial or proof-of-concept.

Sometimes this involves simply ranking the top candidates and calling them up. But in many cases, there will be internal debate and disagreement among key stakeholders about which vendors should actually be at the top of your list. Be sure your shortlist includes only highly ranked solutions that are a good fit with the unique concerns and needs of your stakeholders.

Begin detailed due diligence

The potential solutions that ranked highest in your "on-paper" evaluation and made it through to your shortlist show the most potential, but it's likely you will want to dig deeper.

Here, you will want to confirm the validity of their technical responses, look more closely at the vendor's ability to deliver on their promises, determine if your organizational culture aligns with theirs, and of course get more specific about the pricing of the solution for your particular environment.

Here are a few steps that our customers have found to be helpful:

Live demonstration - If you have not already done so, you will want to engage your vendor in a live demo tailored to your particular use cases and environment. When requesting the demo, be sure to let your potential solution provider know that you are not looking for a generic product overview, but instead that you need to get a feel for how this might fit into your network, environment, workflow, tech stack, etc.

Proof of concept (PoC) - If you have time and the resources to do so, consider bringing the solution into your network and performing a hands-on evaluation via a PoC. This will give your team a chance to live with the system, assess its ability to detect a wide variety of threats in your environment, and get an idea of how you might integrate the system into your existing IDS/security operations workflow. In a PoC you will also be able to evaluate the system's performance in your network and understand how difficult or easy it is to deploy.

Review the product roadmap - because your organization will likely be living with the solution for 5 or more years, you will want to make sure you are not investing in a solution without a future. One of the most effective ways to assess the long-term viability of a solution is to review the solution's 18-month roadmap. Look for evidence that the vendor plans to invest in the future of their solution offering - especially over the course of the next couple years.

Invite vendors in for a live presentation - a live presentation will give you a chance to engage with the vendor's team, ask questions, gauge their responses, assess their cultural alignment, and determine if they really understand your application environment.

Evaluate the pedigree of the team - especially if you are considering a younger, more innovative startup, you will want to meet the principals of the organization and review their backgrounds. Here you are hoping to assess their subject matter expertise and ability to execute. For example, do they have demonstrable experience in the underlying technology, do they possess prior end-user operational experience in security or network engineering, are they regularly engaged in industry exercises or forums to sharpen their skills or share their knowledge?

Check with references - if you are unsure about anything in the responses or the process, you may wish to discuss those concerns with a current customer of your shortlisted companies. Most vendors will happily connect you with one of their customers. While

vendors rarely offer up references that are not happy customers, you should be able to spot any red flags and confirm or dismiss any suspicions that you might have.

Request a quotation (RFQ)

As we described above, an RFQ is a request for pricing and payment information about a highly-specific solution. You will use this to get very specific quantified information from each vendor built around your needs.

Here, you already know the exact number and type of IDS/IPS upgrade system you desire and can explain exactly what you need.

The typical items included in an RFQ are:

- A detailed list of products, features and functionality required
- The quantity needed
- Expected delivery dates
- Expected payment terms

As with all supplier partner communications, you will want to be clear about your intent to purchase and the timeline of your decision.

Once you have the quotations from your shortlisted suppliers, you can fully evaluate the responses and make a selection.

Do you plan to purchase directly or through a reseller?

Also, if you prefer to work through a distributor or reseller, it is important to share this with your prospective vendors at this stage so they can engage their resellers in the process. This should help reduce any supply chain issues that might come up as you get closer to your selection.

SELECT THE SOLUTION FOR YOUR ORGANIZATION

Using your selection criteria and the results of your due diligence, you are now armed with enough information to make the final selection of your IDS upgrade solution.

After seeing all the demos, shortening your list of candidates to a few top vendors, executing a PoC and answering all of those last-minute due diligence questions, it's time to make the final selection.

The way a final selection will be made is different for every organization, but it often involves
Reengaging the stakeholders in a meeting to compare prices, debate details and work through any items that may impact your project
Reaching out to your shortlisted vendors to answer any final questions.

NOTIFY THE VENDOR, AND PLACE THE ORDER

Now that you've completed the selection process, it is time to notify your preferred vendor, place the order and begin preparing for delivery, installation and onboarding.

While you may be tempted to further negotiate with your vendor, at this point the focus should be on ensuring you have a successful deployment.

Also, during this phase, you may want to

- Schedule an onboarding kickoff meeting with your solution provider
- Meet with your internal team to create a project plan for installation and training
- Procure any necessary hardware required

SUMMARY

Stamus Networks is pleased to share the insights we have gathered from our work helping many organizations around the world migrate from their legacy IDS/IPS to a modern alternative.

We hope you found it useful.

We intend this document to be a living repository of fresh insights, so please visit the Resource Library on our website to make sure you have the latest version available

ADDITIONAL RESOURCES

If you are interested in exploring this topic further, we recommend the following resources:

- 3 Key Questions to Ask your Team (and answer) before Migrating from your Legacy IDS/IPS
- Evaluation Criteria for Migrating from Legacy IDS/IPS
- 10 Technical Considerations when Migrating from Legacy IDS/IPS
- 10 Business Considerations when Migrating from Legacy IDS/IPS
- Project Management Checklist for Legacy IDS Migration

All may be found on the Stamus Networks website.

ABOUT STAMUS NETWORKS

Stamus Networks believes in a world where defenders are heroes, and a future where those they protect remain safe. As defenders face an onslaught of threats from well-funded adversaries, we relentlessly pursue solutions that make the defender's job easier and more impactful. A global provider of high-performance network-based threat detection and response systems, Stamus Networks helps enterprise security teams accelerate their response to critical threats with solutions that uncover serious and imminent risk from network activity. Our advanced network detection and response (NDR) solutions expose threats to critical assets and empower rapid response.

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

Copyright © 2021