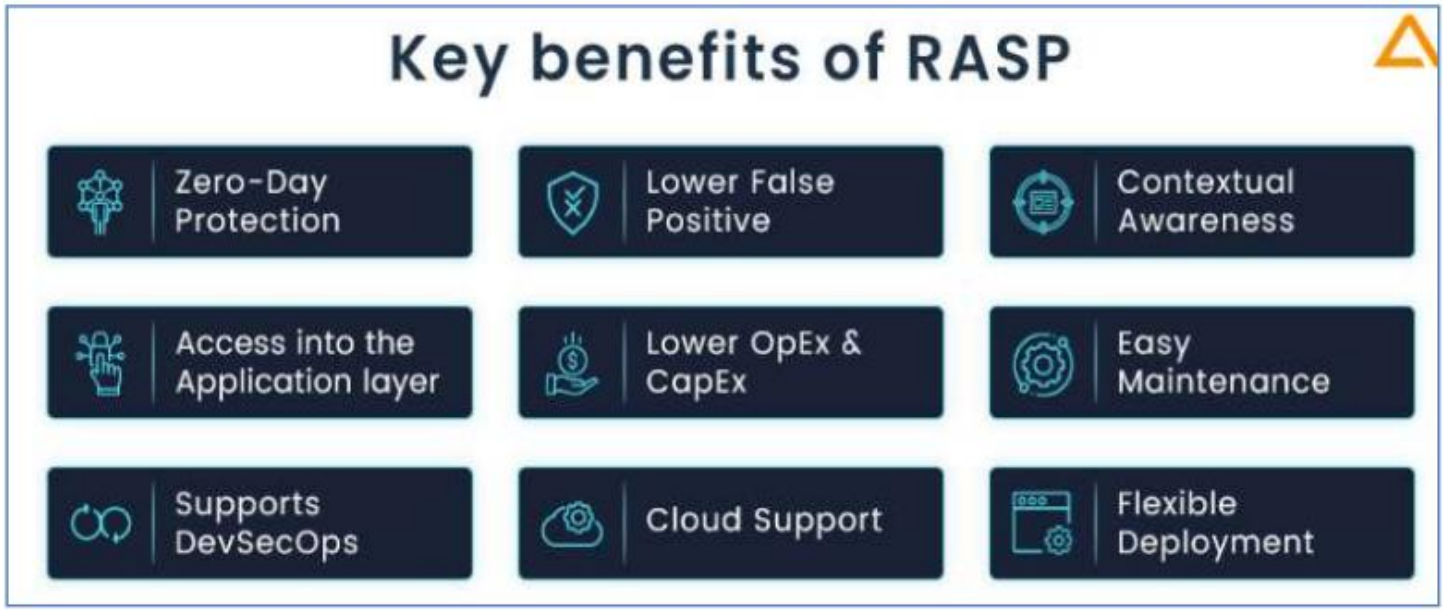
Explain Run Time Application Self Protection – Contrast Security or Microfocus Fortify Software can be used as an example.

Runtime Application Self Protection (RASP) is a security solution designed to provide personalized protection to applications. It takes advantage of insight into an application's internal data and state to enable it to identify threats at runtime that may have otherwise been overlooked by other security solutions.

How RASP Works

RASP wraps around and protects a particular application, rather than a general network-level or endpoint level defensive solution. This more targeted deployment location enables RASP to monitor the inputs, outputs, and internal state of the application that it is protecting. By deploying RASP, developers can identify vulnerabilities within their applications. Additionally, the RASP solution can block attempts to exploit existing vulnerabilities in deployed applications.

RASP's focused monitoring makes it capable of detecting a wide range of threats, including zero-day attacks. Since RASP has insight into the internals of an application, it can detect behavioral changes that may have been caused by a novel attack. This enables it to respond to even zero-day attacks based upon how they affect the target application.



Contextual Awareness: When a RASP solution identifies a potential threat, it has additional contextual information about the current state of the application and what data and code is affected. This context can be invaluable for investigating, triaging, and remediating potential vulnerabilities since it indicates where the vulnerability is located in the code and exactly how it can be exploited.

Visibility into Application-Layer Attacks: RASP has deep visibility into the application layer because it is integrated with a particular application. This application-layer visibility, insight, and knowledge can help to detect a wider range of potential attacks and vulnerabilities.

Zero-Day Protection: While RASP can use signatures to identify attacks, it is not limited to signature-based detection. By identifying and responding to anomalous behaviors within the protected application, RASP can detect and block even zero-day attacks.

Lower False Positives: RASP has deep insight into an application's internals, including the ability to see how a potential attack affects the application's execution. This dramatically increases RASP's ability to differentiate true attacks (which have a true negative impact on application performance and security) from false positives (such as SQL injection attempts that are never included in an SQL query). This reduction in false positives decreases load on security teams and enables them to focus on true threats.

Lower CapEx and OpEx: RASP is designed to be easy to deploy yet is able to make a significant difference in an application's vulnerability to attack and rate of false positive alerts. This combination reduces both upfront expenses (CapEx) and the cost of effectively protecting the application (OpEx) compared to manual patching and web application firewalls (WAFs).

Easy Maintenance: RASP works based upon insight into an application, not traffic rules, learning, or blacklists. SOC teams love this reliability and CISOs appreciate the resource savings. Applications become self-protected and remain protected wherever they go.

Flexible Deployment: While RASP is typically based upon HTML standards, it is easy to adapt its API to work with different standards and application architectures. This enables it to protect even non-web applications using standards like XML and RPC.

Cloud Support: RASP is designed to integrate with and be deployed as part of the application that it protects. This enables it to be deployed in any location where the protected applications can run, including in the cloud.

DevSecOps Support: RASP solutions are designed to be integrated into a DevOps continuous integration and deployment (CI/CD) pipeline. This makes RASP easy to deploy and supports DevSecOps operations.

Microfocus Fortify:

Using Microfocus' Fortify Application Defender, you can analyze and safeguard your applications in realtime against risks and typical cyberattacks. It protects operational applications against zero-day attacks by distinguishing between valid requests and harmful threats in .NET and Java applications. Its end-to-end application protection services encompass every stage of the programming process.

In complement to line-of-code data, Fortify provides logs transparency. For privacy transparency and regulation, it also enables you to submit attack and record data to a log administrator or SIEM without needing to update the code base.

Key Features:

You will be provided with a multi-layered protection system.

It has 32 different protection rule categories to safeguard you from security breaches.

With adaptable and fast installation, you may get immediate protection.

You can control your security from a single, easy-to-use administration interface.

Cost: You can request a quote through their website.

Contrast Security:

Contrast Security Is an output App and API Security That Helps Developer Players Utilize Security Vulnerabilities Additional Source by Blocking Threats and Reducing False Positives. Without Needing New Versions, Contrast Security Can Prevent the log4j Issue in Your Production Environments Right Now. Contrast Protect Also Protected the Apps from the Fundamental Issue. This Indicates Contrast Was Defending You From Log Injections.

Key Features:

Unparalleled Accuracy

Extensive Forensics

Features Software Development and Maintenance Apps

Cost: The pricing starts from $2,800 per year.

Define Web Application Firewall. Demonstrate using a tool.

- A WAF or web application firewall helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. It typically protects web applications from attacks such as crosssite forgery, cross-site-scripting (XSS), file inclusion, and SQL injection, among others.
- A WAF is a protocol layer 7 defense (in the OSI model), and is not designed to defend against all types of attacks. This method of attack mitigation is usually part of a suite of tools which together create a holistic defense against a range of attack vectors.
- By deploying a WAF in front of a web application, a shield is placed between the web application and the Internet. While a proxy server protects a client machine's identity by using an intermediary, a WAF is a type of reverse-proxy, protecting the server from exposure by having clients pass through the WAF before reaching the server.
- A WAF operates through a set of rules often called policies. These policies aim to protect against vulnerabilities in the application by filtering out malicious traffic. The value of a WAF comes in part from the speed and ease with which policy modification can be implemented, allowing for faster response to varying attack vectors; during a DDoS attack, rate limiting can be quickly implemented by modifying WAF policies.

Types of Web Application Firewalls There are three primary ways to implement a WAF:

- Network-based WAF—usually hardware-based, it is installed locally to minimize latency. However, this is the most expensive type of WAF and necessitates storing and maintaining physical equipment.
- Host-based WAF—can be fully integrated into the software of an application. This option is cheaper than network-based WAFs and is more customizable, but it consumes extensive local server resources, is complex to implement, and can be expensive to maintain. The machine used to run a host-based WAF often needs to be hardened and customized, which can take time and be costly.
- Cloud-based WAF—an affordable, easily implemented solution, which typically does not require an upfront investment, with users paying a monthly or annual security-as-a-service subscription. A cloud-based WAF can be regularly updated at no extra cost, and without any effort on the part of the user. However, since you rely on a third party to manage your WAF, it is important to ensure cloud-based WAFs have sufficient customization options to match your organization's business rules. Demonstrate using a tool: AWS WAF Best For Scalable use for businesses of all sizes as long as they are AWS clients.
  Price:
- The Amazon AWS web application firewall is a robust website security solution. However, AWS WAF is only available to customers who just use the company's Web Services.
- The solution is just an add-on to an existing subscription to cloud services such as the Amazon content delivery network and Application Load Balancer. Features: ¬ Agile protection against web attacks ¬ Improved web traffic visibility ¬ Ease of deployment and maintenance ¬ Cost-effective web application protection ¬ Security integrated with how you develop applications. Verdict: AWS Amazon Web App Firewall is a highly robust and scalable solution facilitated with countless useful security features that ensures that your website remains safe against different types of cyberattacks.

Elaborate on Standard Operating Procedure for Operations, Secure Provisioning, deployment and decommissioning

- Imagine you are starting a new job at a car dealership and a customer walks in asking for your latest hatchback. How would you cater to the customer?
- Most likely, your manager must have given you proper training along with a set of documents to study the basics of how to deal with customers. These sets of documents and training guides are often known as standard operating procedures or SOPs.
- A standard operating procedure (SOP) document guides new as well as current employees on how to carry out routine tasks and maintain consistency and quality throughout business operations.
- Since SOPs are crucial documents, we decided to uncover everything there's to know about standard operating procedures and provide a tool to create SOPs with ease.

What are Standard Operating Procedures (SOP)? (Definition)

- A standard operating procedure (SOP) is a step-by-step instructions guide to help an employee in performing specific operations smoothly. The main objective of SOP is to ensure uniform and quality output, while simultaneously reducing miscommunication and ambiguity.
- SOPs are detail-oriented documents and provide step-by-step instructions as to how employees within an organization must go about completing certain tasks and processes.

Types of Standard Operating Procedures (SOP)

1. Checklists
   - A checklist or the to-do list is one of the simplest methods of writing a standard operating procedures (SOP) document. A checklist can be created on an online note-taking app like Bit or can be printed out and handed over to employees.
2. Step-by-Step List
   - Similar to checklists, a step-by-step bullet list works in the same way where you describe a procedure in relevant, easy-to-follow steps.
3. Hierarchical Lists
   - If your procedures are more complex and need additional info, you can create hierarchical checklists or bullet lists. If you are unable to explain a task in a single step and at the same time, don't want to make the SOP lengthy, adding hierarchical steps can be beneficial.

Process Flowchart

- Flowcharts are a wonderful way to represent how a process works visually and help give better context around the workflow.
- A flowchart also shows how one step is related to another, helping employees conceptualize the whole concept and have a better understanding of the work they are doing.

Why do you Need Standard Operating Procedures (SOP)?

- Some of you may be wondering- If we are already training our employees to do the tasks they are hired to do, why take on this extra work of documenting operating procedures? We understand your dilemma, which is why we are going to look at some of the reasons why every business should create standard operating procedures (SOP) no matter what…
  1. Time-saving
  2. Ensure the safety of employees
  3. Ensures compliance standards are met
  4. Improved communication
  5. Enhanced accountability
  6. Provides consistency
  7. Maintains Organizational Knowledge
  8. Provides a guiding hand 9. Onboarding and training

Steps for Writing a Standard Operating Procedure (SOP)

- Now you know what a standard operating procedure is and why your organization needs to create one, it's time to actually get down to business and create one. Standard operating procedures require a ton of effort and planning before you can even begin to document your procedures.
- Here are the key steps you need to follow to create a robust standard operating procedure document:

Step1: Generate a list of your business processes

- The first thing you need to do in order to create an SOP is to find out which tasks, processes, or workflows, you need an SOP for. Conduct a survey or ask your employees to fill out a form defining what tasks they do on a regular basis.

- This will form the basis of your list for the standard operating procedure (SOP) document. Once you have gathered a list, you can review it with other managers and look for any repetitions.

Step 2: Start with why

- Once you have your list ready, it's time to note down your objectives. Having a clear answer to why you are creating the SOP document should be your number one priority. Asking yourself questions like "how will this document help the employees?" or "how will the SOP impact our bottom line?" are great starting points.
- For a more granular approach, identify the pain points or challenges your employees face in their day to day and create your SOP around it. This gives you a solid "why" to go through all that hard work of creating an SOP and also improves employee's buy-in in the whole process.

Step 3: Choose a format

- Chances are that your organization already has some SOP documents written for past procedures. You can refer to those documents as templates and guide your current SOP.
- If not, then refer to our "types of SOP documents" section above and decide whether you want to write a list of steps, create a checklist, create workflow diagrams, or a mixture of everything!

Step 4: Identify your audience

- Knowing your audience is key in creating an awesome SOP document. Ask yourself the following questions in order to get an idea about your audience: ¬ Are they new employees? ¬ What's the size of the audience? ¬ What prior knowledge do they have? ¬ Does an SOP already exist?
- The more information you have on your audience, the better you can understand their points of view and create an SOP that will be relevant to them.

Step 5: Collaborate with employees

- Standard operating procedures (SOP) are written with the end-user, i.e, the employees in mind. Having employees collaborate with you in this process is a no-brainer.
- You cannot really understand their pain points and challenges unless you talk to your employees and ask for their honest feedback and suggestions. We recommend using collaboration software like bit.ai to bring your entire team inside a common document and collaborate effectively.

Step 6: Get down to writing

- Once you have spoken to your employees and have enough data points to start, immediately move to your document editor and start adding your notes. Once done creating the document, you can go through the document with your employees and management and ask for their feedback and input.
- This is also a great time to specify who would be responsible for updating and maintaining the standard operating procedures and when will you be conducting a periodic review to gauge engagement.

Step 7: Make it interactive

- While SOP documents are text-heavy and boring, they don't have to be. Add screenshots, screen recordings, images, flow charts, videos- anything that's relevant to the step being talked about.
- Media like these can help make your SOP's pop while providing a visual aid to otherwise bland steps. Making your standard operating procedures interactive will boost your engagement levels as employees are surely going to find them more useful and even entertaining!

Step 8: Distribution

- After you are done creating the SOPs, you've come to the most essential part of the process: distributing them to your employees. It's crucial to find a place to store all your standard operating procedures (SOP) and other training material in one place for employees to access as and when they like.
- This is why we recommend using Bit to store all company documents in one place and store company assets like videos, images, PDFs, and more in Bit's content library. You can quickly create a workspace in Bit, invite your employees, and share SOPs and more in a robust and safe environment.

Step 9: Make them "living documents"

- While many organizations view creating SOPs as a one-time process, that's hardly the case. As processes and workflows are often changing and ever-evolving in the hopes of making them more efficient, standard operating procedures quickly become outdated.
- This is why SOPs should be converted to living documents that get reviewed periodically (ideally after every six months) so that they don't get out of sync with the process or workflow they are describing.

Standard Operating Procedures (SOP): Best Practices

Here are some tips to keep in mind while writing your SOP document:

- **Be clear and concise:** Since standard operating procedures are text-heavy, it helps if they are written in simple language for your audience to go through it quickly. Avoid technical jargon, wordiness, and ambiguity, and remember to keep it simple.
- **Make it scannable:** Make your SOP's scannable so that employees can quickly go through them and find what they are looking for. Don't go on and on in a paragraph and make sure the length of every paragraph doesn't exceed 3 lines.
- **Take input:** Take input from your employees and understand their pain points before you begin writing your SOP. What are the areas they need help with? What processes are complex and require a lot of time? Focus on challenges and write an SOP that helps them overcome those challenges.
- **Choose your tool wisely:** While there are many editors on the market, using a collaboration platform like Bit makes sure you have a single place to write, store, share, and track all your SOPs and workplace documents easily.

Secure Device Provisioning.

- Protect your device secrets throughout the manufacturing process. We revolutionize secure provisioning by offering the simplest secure way of injecting secret identity data to a device.

How Secure Device Provisioning works

- Secure Device Provisioning (formerly from Inside Secure) ensures that secrets are not exposed or manipulated when provisioned at manufacturing time, and the innovative code protection and whitebox technology ensures that these secrets remain protected for the rest of the device's lifetime. The solution doesn't require any hardware security resource available on the device, however if available, it can be easily adapted to variety of common hardware and software architectures.
- With the Secure Device Provisioning solution, device makers can also remotely monitor the manufacturing process and even control it, without setting foot at the manufacturing site. It simplifies provisioning and makes it affordable to all device makers. The client environment can be further secured through the application of secure boot, code protection and whitebox technologies.

Features & Benefits

- Cost effective to meet your budgetary needs (light configuration, low maintenance)
- Flexible provisioning to meet your device specific needs (single or two-stage provisioning)
- Over 425 millions devices provisioned successfully
- Over 75 licensed customers, from chipset makers to service providers
- The world's first independent provisioning service

Deployment:

- An automation process workflow must be deployed to send it to the server. From server, the deployed process is assigned to a robot for execution.
- The Deployment tab allows you to deploy the published processes in Automation Studio. It also enables you to decommission the current version, restore the previous version and add a process as a processbot. Published as well as deployed processes are available in this tab. You can view details related to the process such as name of the process, its type, assigned profile, and version and so on.
- The version of the process displayed in the Deployment tab is the version that gets created while publishing the process. If you edit a deployed process, save and publish the deployed process again. The version of the saved and published process post deployment gets incremental by 1. Every version of the saved process that you publish is available for deployment.