ESP FAQ

Q: What is the Evident Security Platform (ESP)?
A: The Evident Security Platform is the first and only cloud-native infrastructure security solution providing full coverage of all AWS accounts, services, and regions, in addition to all Azure subscriptions, services and standard regions.

ESP combines the detection and analysis of misconfigurations, vulnerabilities, and risk – with guided remediation and audit capabilities to meet compliance requirements – all in one solution. ESP was designed specifically to help modern IT, DevOps and Risk/Compliance teams implement and maintain security within the cloud shared responsibility model.

ESP enables IT, Security, Engineering, and Operations with a continuous global view of security risk and compliance, with the actionable intelligence needed to rapidly remediate and secure their entire AWS and Azure Infrastructure.

Q: How Does ESP Work?
A: ESP gathers the AWS and Azure services configuration data, CloudTrail and Log data, and other information from each AWS account or Azure subscription via the Amazon and Azure APIs. This data is then input into the ESP risk analysis engine which generates a detailed assessment of the security risks, misconfigurations and vulnerabilities it detects.

Q: Does ESP Work Like An Active Vulnerability Scanner for the Cloud?
A: No. ESP is neither an active or passive vulnerability scanner in the traditional sense. Unlike traditional, on-premise / virtual vulnerability scanners that use active scanning technology, ESP does not directly "scan" cloud assets to identify OS or Application layer vulnerabilities running inside instances – as it cannot view the actual contents of AWS nor Azure services like EC2, S3, VMs or Storage.

ESP operates at the control plane layer of AWS and Azure and uses a passive methodology to collect vulnerability and configuration data via the APIs, providing a detailed security assessment of the underlying cloud infrastructure.

Q: Does ESP Help Me Meet Requirements of the Shared Responsibility Model?
A: Yes. Amazon manages security of the AWS cloud; Microsoft manages security of the Azure cloud; while the security of the assets stored in the cloud is the responsibility of you, the customer. The customer is responsible for ensuring the security and configuration of the services running in AWS or Azure in addition to the applications and OSs that are implemented.

7901 Stoneridge Dr., Suite 150, Pleasanton, CA 94588 • (855) 933-1337 • sales@evident.io • support@evident.io

Q: How Does ESP Gather Security Information From My AWS Accounts?
A: The ESP Platform leverages Cross-Account IAM Roles with read-only access to your AWS services using the Audit IAM role. ESP uses the AWS assume role function and generates a secure, one-time AWS STS token each time it communicates with the Amazon API when gathering configuration information on your infrastructure. This is significantly more secure than other solutions that require you to provide API keys to assess your security posture.

Q: How Does ESP Gather Security Information From My Azure Subscription?
A: Customers must create components in their Azure subscription to enable the streaming of configuration change events through Azure Event Hub or Storage Hub mechanisms, into a Function App, that sends the event to ESP via the API. ESP never has the ability to alter or change your environments, as it maintains read-only access to this near real-time feed of relevant security events.

Q: What Data Does ESP Collect From My Cloud Accounts?
A: ESP operates at the control plane layer of AWS and Azure and gathers the accessible infrastructure configuration metadata about your resources.

Q: Do I need to install agents anywhere?
A: No. ESP is agentless, non-intrusive, and does not modify or actively change any of your AWS or Azure deployment configurations.

Q: Does ESP impact the performance of my cloud deployment when collecting vulnerability and configuration data?
A: No. Because ESP is interacting directly with the API at the control plane, it does not impact the performance of any instances or services running in your cloud environment.

Q: How quickly can I get ESP up and running?
A: A 14-day free trial is available to evaluate the Evident Security Platform. Once signed up and configured with your Amazon Account or Azure Subscription information – which takes approximately 5 minutes – ESP will start providing actionable security and risk information within approximately 5 minutes. You can follow the instructions in the external account onboarding wizard in ESP or here to get started.

7901 Stoneridge Dr., Suite 150, Pleasanton, CA 94588 • (855) 933-1337 • sales@evident.io • support@evident.io

Q: How Does ESP rank cloud risks?
A: The configuration information from your cloud accounts are analyzed by a risk engine that determines the severity of risk to help organizations prioritize their remediation efforts. Each vulnerability of misconfiguration is tagged with a specific severity status indicating:

> High: High severity alerts pose the most significant risk to your cloud deployment and should be examined and remediated as soon as possible.
>
> Medium: A medium severity alert identifies issues that should be tracked and scheduled for remediation.
>
> Low: Low level alerts may not be applicable or local business rules have determined that it is not a threat.

You have the ability to change the risk level for each security control check to match your organization's security policy.

Q: Does ESP integrate with other secure authentication mechanisms?
A: Yes: ESP provides Multi-factor Authentication (MFA), Single Sign-On (SSO), and other secure authentication capabilities to further secure access to the platform. We strongly encourage you use this added level of security.

Q: Does Evident.io Encrypt my Data?
A: Yes. Customer data is always encrypted during collection, in transit when inside our VPCs, and at rest in our data stores. At account termination your account and any data used to identify your infrastructure will be purged from our systems.

Q: How many AWS accounts and Azure Subscriptions can I view at one time?
A: Evident.io has many customers that have hundreds of accounts and subscriptions running in ESP — providing a single, consolidated view of their cloud deployments. The information for each separate account can be accessed from this global view with detailed drill down into specific services and vulnerabilities based on risk.

Q: What are custom signatures?
A: Signatures, or control checks, validate conditions that trigger alerts to potential security vulnerabilities. While ESP uses default signatures to evaluate the most common security vulnerabilities and misconfigurations, custom signatures provide organizations with the flexibility to extend the ESP platform to meet individual business needs.

Q: How many custom signatures can I create?
A: Customers can create an unlimited number of custom signatures. However, the number of custom signatures is restricted based on the ESP plan purchased. The Professional Plan allows for five (5) custom signatures, and the Enterprise Plan has unlimited custom signatures.

Q: How are users defined within ESP?
A: Users are named individuals who can view security reports and configure alerts, signatures, suppressions, and accounts monitored by the platform. More information on users can be found in the blog post Segregation of Duties with ESP Organizations.

Q: Does ESP provide a daily report?
A: Daily Risk Summary Reports are emailed to ESP users identifying new risks from the last 24 hours and summarizing the previous alerts per account and service.

Q: What are the different deployment models available?
A: ESP is available as a SaaS-based solution. You can also license ESP Private SaaS to operate in your own AWS instance to ensure data privacy and data sovereignty. Please contact an Evident.io sales representative to help you identify the solution that is right for you.

Q: Where can I find out more information about ESP Private SaaS?
A: Please contact a local sales representative. Documentation about ESP Private SaaS is available at https://docs.evident.io/#psaas.

7901 Stoneridge Dr., Suite 150, Pleasanton, CA 94588 • (855) 933-1337 • sales@evident.io • support@evident.io