Solution Brief

Trend Vision One™ – Cloud Security, an AWS Built-in Competency Partner Solution

Jump-start your cloud journey securely

As your business continues to navigate its cloud journey, moving from migration and optimization to cloud-native application development, you need assurance that the security technology protecting your environment is built from the ground up to include foundational AWS services. Working with an AWS Built-in Competency Partner like Trend Micro helps you achieve your business goals for scale, simplicity, and operational cost control in the cloud, in addition to helping you manage your cyber risk.

Our Cloud Security solution enables your organization to connect security operations (SecOps) and cloud security teams across your entire hybrid cloud environment We'll meet you at any stage of your cloud security maturity journey, helping to stop adversaries faster and take charge of risk. Our AI-powered cybersecurity platform is purpose-built to help you securely build and innovate in AWS, facilitating earlier detection, faster response, and ultimately reduced risk across your diverse range of hybrid IT environments.

AWS Built-in Solution

With Cloud Security, you can install, configure, and integrate with AWS Organizations, AWS CloudTrail, and AWS Systems Manager using a well-architected Modular Code Repository (MCR) in an automated deployment package that is validated by AWS experts. This enables you to accelerate deployment and increase the time to value of your investments in AWS and Trend solutions.

To further simplify your experience, we have embedded the AWS Built-in solution into our Trend Vision One™ platform via the Cloud Account Management app. This provides you with a streamlined, user-friendly approach to configuring the foundational elements of your cloud security using AWS services across multiple accounts.

Our AWS Built-in Solution, Cloud Security enables you to:

- Accelerate your response against vulnerability exploits via automated intrusion detection system and intrusion prevention policy (IDS/IPS) rules for workloads running in AWS
- Enhance risk insights to streamline SecOps by leveraging the power of our platform; within the Workbench app in Trend Vision One, effortlessly monitor your AWS accounts for suspicious activities by ingesting CloudTrail events and applying a threat detection model
- Gain full visibility and protection of workloads across multiple AWS accounts, enhancing threat protection; Trend Vision One™ – Workload Security agents are seamlessly deployed every time a new instance is created in your AWS accounts, via Distributor in AWS Systems Manager
- Aggregate, organize, prioritize, and automate remediation of security alerts in a centralized location; Trend Vision One™ – Container Security sends findings from runtime protection for Amazon Elastic Kubernetes Service (Amazon EKS)/Kubernetes clusters directly to Trend Vision One, giving you a comprehensive view of security posture across multiple AWS accounts
- Accelerate compliance with the AWS Well-Architected Framework and other standards with automatically secured cloud workloads

Visit the overview page to learn more

> “We love creating with AWS and the key to this co-build solution launch was not figuring out what was possible, but rather uncovering what the world needs most to protect digital assets and mitigate the advanced risks we see today. Cloud development is not only more accessible now but far more can be done with less expertise—which is invaluable to all. Innovations are only as powerful as they are secure, which is the role Trend Micro fills in all AWS competencies.”

Mike Milner

VP of Cloud Technology at Trend Micro

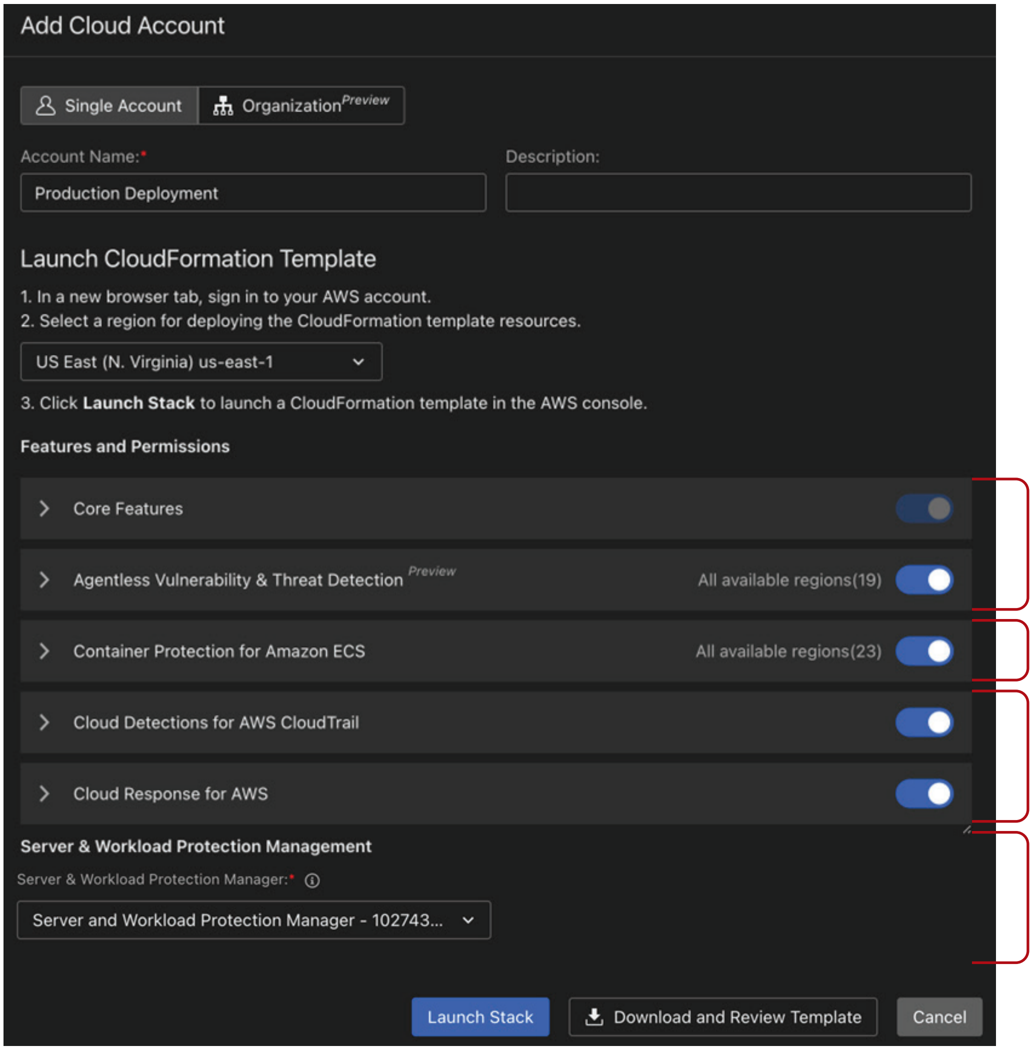
AWS Built-in Solution service integrations

AWS CloudTrail

AWS Systems Manager

AWS Organizations

Add Cloud Account menu in Trend Vision One



Add Cloud Account

Account Name:* Production Deployment

Description:

Launch CloudFormation Template

1. In a new browser tab, sign in to your AWS account.
2. Select a region for deploying the CloudFormation template resources.

US East (N. Virginia) us-east-1

3. Click **Launch Stack** to launch a CloudFormation template in the AWS console.

Features and Permissions

- Core Features
- Agentless Vulnerability & Threat Detection Preview – All available regions(19)
- Container Protection for Amazon ECS – All available regions(23)
- Cloud Detections for AWS CloudTrail
- Cloud Response for AWS

Server & Workload Protection Management

Server & Workload Protection Manager:* Server and Workload Protection Manager - 102743...

Trend Vision One™ – Attack Surface Risk Management for Cloud (ASRM for Cloud)

Trend Vision One – Container Security

Trend Vision One™ – XDR for Cloud

Trend Vision One™ – Endpoint Security (Server and Workload Protection)

Key benefits of Cloud Security

Cloud Security enables you to unify, simplify, and standardize your organization's security operations. Bringing our market-leading[1] hybrid cloud security to Trend Vision One allows you to integrate security across your entire enterprise, centralize visibility, better manage risk, and ultimately build business resilience.

- Proactively identify cloud threats, visualize risk, and prioritize vulnerabilities
- Quickly respond to security threats and mitigate breaches
- Manage agent/agentless and run-time/on-demand services
- Reduce complexity and create a viable path towards tool consolidation
- Gain richer insight to asset discovery, security policy management, licensing, and more
- Easily roll up operational metrics for executive reporting and compliance requirements
- Support orchestration, automation, and cloud best practices
- Protect, investigate, and remediate security incidents via connected platform workflows

[1] - Trend Micro Industry Recognition: trendmicro.com/en_sg/about/industry-recognition.html

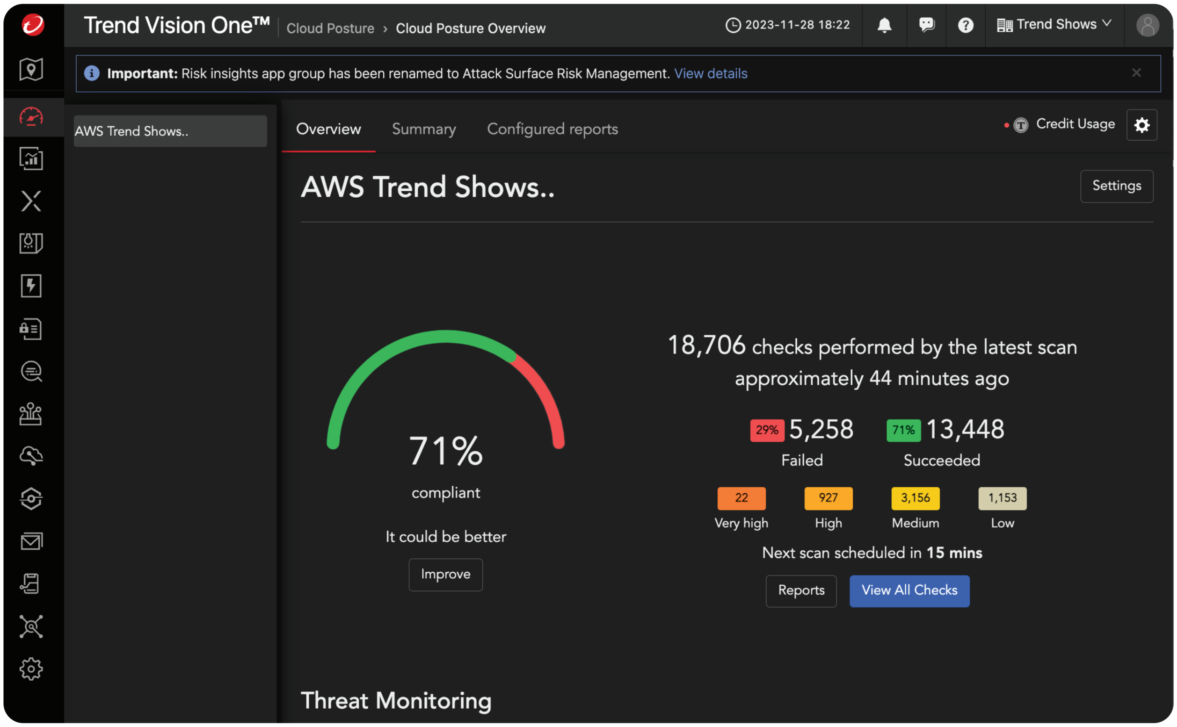
ASRM for Cloud

Take charge of your cyber risk with cloud-focused internal and external attack surface discovery, assessment, risk prioritization, and remediation. ASRM for Cloud delivers bespoke hybrid cloud telemetry correlation, facilitating faster detection and response while empowering cloud and security teams to consistently uncover, identify, and prioritize risks. These capabilities enable you to take swift, data-driven actions to proactively mitigate risk and reduce your attack surface.

Turn visibility into decisions

- Obtain a high-level view of your organization's overall security posture, scanning against over 600 AWS rules
- Identify, prioritize, and remediate high-risk violations, misconfigurations, overly permissive identity and access management (IAM) policies, and compliance risks
- Gain contextual visibility into your cloud assets with attack surface discovery, facilitating a clearer understanding of the assets posing cloud risks, empowering you to proactively take action, swiftly reduce risks, and prevent potential data breaches and major attacks within your AWS environment
- Customize regular infrastructure checks and directly apply them to over 30 compliance regulations and best practices, complete with exportable reports for audits
- Use infrastructure as code (IaC) template scanning to shift security and compliance checking left, improve code, and enable innovation
- Graph asset connections to one another to analyze potential attack paths, helping to mitigate potential breaches
- Integrate with Amazon API Gateway, achieve application program interface (API) visibility across multiple cloud accounts, identifying risk factors linked to issues such as authentication deficiencies and other API-related risks

Cloud posture overview in Trend Vision One



Important: Risk insights app group has been renamed to Attack Surface Risk Management. View details

AWS Trend Shows..

71%
compliant

It could be better

18,706 checks performed by the latest scan approximately 44 minutes ago

29% 5,258	71% 13,448
Failed	Succeeded

22	927	3,156	1,153
Very high	High	Medium	Low

Next scan scheduled in **15 mins**

Threat Monitoring

Trend Cloud Security Posture Assessment

Utilize our free assessment to scan your organization's AWS infrastructure to identify misconfigurations, compliance, and security risks based on common standards and practices including the AWS Well-Architected Framework.

XDR for Cloud

Stop adversaries faster with a broader perspective, improved contextual awareness, and the ability to hunt, detect, investigate, and respond to threats from a single platform. XDR for Cloud extends detection and response to your customer cloud accounts by examining user, service, and resource log activity for suspicious behavior and by providing remediation and response actions.

Enhanced by our global threat intelligence, this solution is the perfect complement to XDR for Endpoints running either on-premises or in AWS. In addition, you can detect, track, and investigate suspicious container activity and cross-layer threats with Container Security.

Streamline hybrid cloud investigations

Benefit from an expanding list of advanced cloud security models and response action across all your AWS environments. Integrate XDR for Cloud with CloudTrail logs to gain insights into all user, service, and resource activity, including:

- Who or what took which action
- Which resources were acted upon
- When the event occurred

In addition, stay in front of privilege escalation attempts, policy rollbacks, master password modifications, Amazon Simple Storage Service (Amazon S3) data exfiltration attempts, multi-factor authentication (MFA) deactivations, and more.

CloudTrail detection models include:

- AWS IAM privilege escalation through policy rollback
- Amazon Relational Database Service (Amazon RDS) master password modification
- Amazon S3 bucket data exfiltration
- AWS IAM user login MFA deactivation

Empower analysts with automated response actions through:

- CloudTrail alerts, which trigger workbench activities for investigation and response
- Response actions that can be automated via playbooks to revoke access to AWS resources under attack

Protection in the Cloud

Quickly identify, mitigate, and block security threats across your hybrid cloud environment by leveraging on-demand and runtime protection techniques for virtual machines (VMs), containers, storage, databases, and APIs.

Trend Vision One – Workload Security

A market-leading solution, Workload Security is purpose-built for servers and cloud workloads like Amazon Elastic Compute Cloud (Amazon EC2). Integrating advanced threat protection, detection and response, and threat intelligence, it enables you to streamline IT and security operations, reduce complexity, and achieve optimal security outcomes across your on-premises, cloud, multi-cloud, and hybrid environments.

Trend Vision One – Container Security

Container Security delivers container image security, admission control policy, runtime protection, and detection and response capabilities, ensuring the security of your containers from build to termination.

Trend Vision One™ – File Security

Get instant scanning capabilities for any file size or type. File Security protects your downstream workflows from malware, integrating into your custom cloud-native processes, and providing broad cloud storage platform support.

Trend and AWS

Trend and AWS share a strong commitment to customers, and together we strive to help them securely build in the rapidly evolving landscape of the cloud. This shared commitment is underpinned by a dedication to continuous innovation, as Trend and AWS work together to stay ahead of emerging threats and challenges, delivering advanced solutions that align with the dynamic nature of cloud technology. Our commitment to AWS customers is demonstrated through our support of over 80 AWS Services, our acquisition of 10 AWS Competencies, and over 2,000 successful customer launches in AWS Marketplace.

Get started

Trend Vision One is available in AWS Marketplace.

For details about what personal information we collect and why, please see our Privacy Notice at trendmicro.com/privacy