Proofpoint Solutions and Amazon Web Services

How Proofpoint provides AWS customers with people-centric security and compliance

Products

- Adaptive Access Controls
- Cloud App Security Broker
- Cloud Security Posture Management
- Email Fraud Defense
- Emerging Threats Intelligence
- Enterprise Data Loss Prevention
- Insider Threat Management
- Threat Response Auto Pull
- Zero Trust Network Access

Key Benefits

- Simplify multiregion AWS security and compliance with centralised management
- Identify and classify sensitive data in cloud storage repositories
- Blocks suspicious logins and prevent account takeover of AWS resources
- Get visibility on user and data activity across AWS EC2 instances and Amazon Workspaces
- Enable secure remote access for your team
- Automatically quarantine malicious emails that bypass perimeter solutions

Cloud platforms like Amazon Web Services (AWS) have transformed the way business is done. Modern employees use them to work in the cloud remotely, and organisations use them to lower costs, become more agile and innovate faster. With this change, threat actors have shifted their focus from the old network perimeter to people and the data, systems and resources that the people access. In this changing landscape, you must secure access to AWS resources, prevent data loss and stay compliant. Proofpoint fields a collection of products that can help you do just that.

Our solutions help you with:

- Shadow IT
- Compromised accounts
- Compliance violations
- Email spoofing
- Unauthorised access
- Data loss and exfiltration
- Insider threats
- Suspicious network activity

Discover AWS Resources and Accounts

Proofpoint Cloud App Security Broker (CASB) combines people-centric controls with compromised cloud account detection, DLP and cloud and third-party apps governance. It helps you secure cloud platforms like AWS. Our multimode CASB supports both API and proxy-based deployment models.

Proofpoint CASB simplifies multiregion AWS security and compliance with centralised management. You get visibility on all of your software as a service (SaaS) apps and infrastructure as a service (IaaS) resources across AWS.

It helps you:

- Visualise resource creation trends. Look for anomalies such as excessive resource creation or deletion.
- Drill down into discovered resources. Ensure accounts are provisioned according to regulations and best practices.
- Audit network traffic logs. Discover cloud apps and AWS accounts that access your network.

Cloud Threat Prevention

Proofpoint CASB's adaptive access controls enable real-time security measures based on risk, context and role. They automatically block access from known threat actors, risky locations and networks. And they apply risk-based controls to high-risk and high-privilege users. Risk-based controls can include step-up authentication, managed-device policy rules and VPN enforcement.

Adaptive access controls block suspicious logins. They prevent account takeover of your AWS resources.

They help you:

- Block access to highly attacked user accounts from suspicious logins
- Create a blocklist of countries where your organisation does not have a presence

Identify Misconfigured Services

Cloud security posture management (CSPM) is offered as part of Proofpoint CASB. CSPM helps you govern posture in your cloud environment. With it, you can organise, configure and maintain your cloud resources. This helps you to better adhere to compliance standards.

It helps you:

- Discover configurations and settings that deviate from published baselines
- Recommend best practices to fix identified misconfigurations that present a security risk
- Simplify cloud security and compliance with centralised governance for cloud resources across accounts and regions

Protect Sensitive Data

Proofpoint Enterprise Data Loss Prevention (DLP) brings together our solutions for email, cloud and endpoint DLP. It combines content, behaviour and threat telemetry from these channels. This allows you to address the full spectrum of people-centric data-loss scenarios.

Proofpoint Enterprise DLP helps you identify and classify sensitive data in cloud storage repositories.

It helps you:

- Monitor file activities for DLP violations.
- Monitor S3 buckets for excessive sharing.
- Build data security policies. The product uses 240 built-in DLP classifiers. These include built-in smart identifiers, dictionaries, rules and templates that are shared with other Proofpoint DLP products.

Protect Your AWS Accounts

Amazon GuardDuty uses Proofpoint Emerging Threats (ET) Intelligence to protect AWS instances.

ET Intelligence is the industry's most timely and accurate source of threat intelligence. It combines a database of globally observed threats and malware analysis with up-to-the-minute IP and domain reputation feeds. It gives your security teams the intelligence and context they need to investigate and stop malicious attacks.

We provide next-generation products and solutions for security, compliance, digital risk and response. Our ET IP address and domain reputation intelligence is based on one of the broadest footprints of protective technologies. It spans email, mobile, social, SaaS and network environments.

Manage Insider Threats

Proofpoint ITM is part of the Proofpoint Information and Cloud Security platform. It protects you against data loss, malicious acts and brand damage involving insiders. Proofpoint ITM defends against authorised users who might act with malice or negligence. And it correlates user activity and data movement to protect you from insider-led data breaches.

Proofpoint ITM delivers visibility on user and data activity across AWS EC2 instances and Amazon Workspaces.

It helps you:

- Get a complete view of endpoint-based activity. Get full context around user-driven incidents.
- Visualise threat context around unique user groupings. This helps you to better manage user risk.

Secure Remote Access to Cloud Apps

Proofpoint ZTNA is a people-centric, zero-trust alternative to VPN. It secures remote access to any enterprise application; and it does not matter where the application is located. Proofpoint ZTNA gives your users microsegmented secure access to hundreds of cloud instances. You can automate cloud-to-cloud connectivity. And you can enable hybrid cloud networking between on-premises servers and public clouds.

Proofpoint ZTNA enables secure remote access for employees, contractors, partners and customers to apps hosted on AWS.

It helps you:

- Manage remote access policies to all enterprise resources in your data centre or AWS cloud from a single console
- Get a zero-trust alternative that offers segmented, verified and audited access for every user

Improve Email Trust

Proofpoint Email Fraud Defense (EFD) protects your organisation from email fraud. It provides full visibility into look-alike domains and emails sent using your domain. It also mitigates risks that your suppliers may pose. It identifies your suppliers as well as look-alike domains that third parties register.

Proofpoint EFD secures emails coming from Amazon SES. It gives you the visibility, tools and services needed to authorise legitimate email.

It helps you:

- Address misconfigured email sending systems and deliverability challenges related to broken email authentication validation checks
- Identify and report email spoofing
- Expose DKIM signing and SPF problems as seen by email receivers

Automatically Quarantine Malicious Email

The Proofpoint Threat Response Auto Pull (TRAP) appliance can be hosted on AWS. It lets your security teams analyse emails and automatically removes malicious messages. It also moves unwanted emails to quarantine from user inboxes after they've been delivered.

Proofpoint TRAP helps streamline your email incident response process. You get a powerful solution that reduces the time needed for your security teams to clean up email.

It helps you:

- Monitor mailbox automatically for threats
- Reduce time exponentially for security and messaging teams when going through mail security orchestration and response
- Quarantine messages forwarded to individuals or distribution lists

To learn about Proofpoint's partnership with AWS, visit **proofpoint.com/us/partners/aws**.

LEARN MORE

For more information, visit **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organisations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data and make their users more resilient against cyber attacks. Leading organisations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media and the web. More information is available at **www.proofpoint.com**.