Forcepoint

Solution Brief

Forcepoint Next Generation Firewall with Amazon Web Services

The most secure and efficient enterprise firewall—centrally managed, always on & relentless

Challenge

- Businesses and organizations need to maintain the same level of security over their cloud and hybrid environments as they did with traditional on-premises infrastructures
- Building and maintaining a secure cloud or hybrid infrastructure can be expensive and pose a technical challenge
- Regulatory compliance can be difficult to navigate and time consuming

Solution

- Forcepoint Next Generation Firewall (NGFW) software-based solutions are designed to deliver maximum security with minimum cost and complexity
- Forcepoint NGFW Security Management Center (SMC) is a unified platform that streamlines processes and provides visibility and control
- Forcepoint NGFW SMC enables IT administrators to streamline compliance efforts across virtual and physical networks, including easy access to audit reports

Outcome

- Maximum cloud and hybrid security with minimum complexity
- Faster incident response
- Simplified regulatory compliance, implementation, and management
- Lower cost for network infrastructure and security

Forcepoint Next Generation Firewall (NGFW) connects and protects people and the data they use throughout the entire cloud or hybrid enterprise network—all with the greatest efficiency, availability and security. Trusted by thousands of customers around the world and available through the AWS marketplace, Forcepoint network security solutions enable businesses and organizations to address critical issues efficiently and economically.

Forcepoint Security for Public Cloud Environments

Cloud-based services and virtual deployments are transforming businesses of all shapes and sizes. Traditional on-promise hardware is rapidly disappearing because organizations need greater efficiency, agility and cost control without the burden of maintenance and overhead, in order to stay competitive. This widespread adoption of cloud architectures puts added responsibility on security professionals and IT leaders to ensure that these new environments are just as secure as their physical predecessors.

Forcepoint Next Generation Firewall (NGFW) software-based solutions are designed to deliver maximum security with minimum cost and complexity. The Forcepoint NGFW Security Management Center (SMC) is a unified platform that gives you unmatched visibility, control and consistent policy enforcement to help ensure regulatory compliance in physical infrastructure as well as virtual and cloud environments.

AWS Cloud Security

To secure cloud environments, Forcepoint brings leading next-generation firewall technology to AWS with proven scalability, operational efficiency and strong security. Easily and safely extend your organization's network—from data centers and network edge through your branch offices and remote sites—into your AWS cloud environment through a secure Virtual Private Network (VPN) gateway. Our centralized management enables you to create and deploy policies swiftly and consistently across all of your systems. You can quickly zero in on what's happening in both your AWS environment and your physical network.

Customers who switch to Forcepoint NGFW report an 86% drop in cyberattacks, 53% less time burden on IT, and 70% decrease in planned maintenance.

Maximum Security, Minimum Complexity

The software-based architecture of Forcepoint's security for solutions such as advanced threat protection, deep packet inspection, and application-level control is designed for easy deployment to help ensure maximum security without all the complexity and additional costs. The software-based Forcepoint security platform provides a comprehensive and integrated, defense-in-depth protection that can be tailored to the specific needs of each person, place or asset including firewall, VPN, IPS, URL filtering protection. This software platform offers all the existing capabilities in hardware-based appliances, including stateful inspection, granular policy and access control and redundant ISP connections – but without the box.

Real-Time Visibility and Control

Forcepoint NGFW delivers complete visibility and control over the traffic flow within the virtual as well as cloud environment that traditional management consoles can't. The SMC provides rapid reporting on the amount of traffic passing between virtual systems and alerts administrators if a system is about to go down. Manage any number or combination of physical or virtual Forcepoint devices or clusters as well as softwarebased versions running on standard x86-hardware. The SMC also enhances virtual system security via a holistic monitoring dashboard with full stack application visibility and granular control.

Simplify Regulatory Compliance

Maintaining compliance with the latest regulatory requirements such as PCI DSS, HIPAA, Sarbanes-Oxley and FISMA in the physical world is difficult, but remaining compliant in the virtual world is even more challenging. Traditional controls around each application are not present in a virtual environment. This makes determining which information was accessed by whom and when nearly impossible and is likely to raise a red flag with auditors. The SMC gives you the level of monitoring, analysis and reporting you need to help ensure compliance across virtual and physical networks. It gathers comprehensive data on all network events and presents them in clear and easily read audit logs. The SMC also lists security settings, reports system changes and provides the accurate audit reports you need, all at the press of a button.

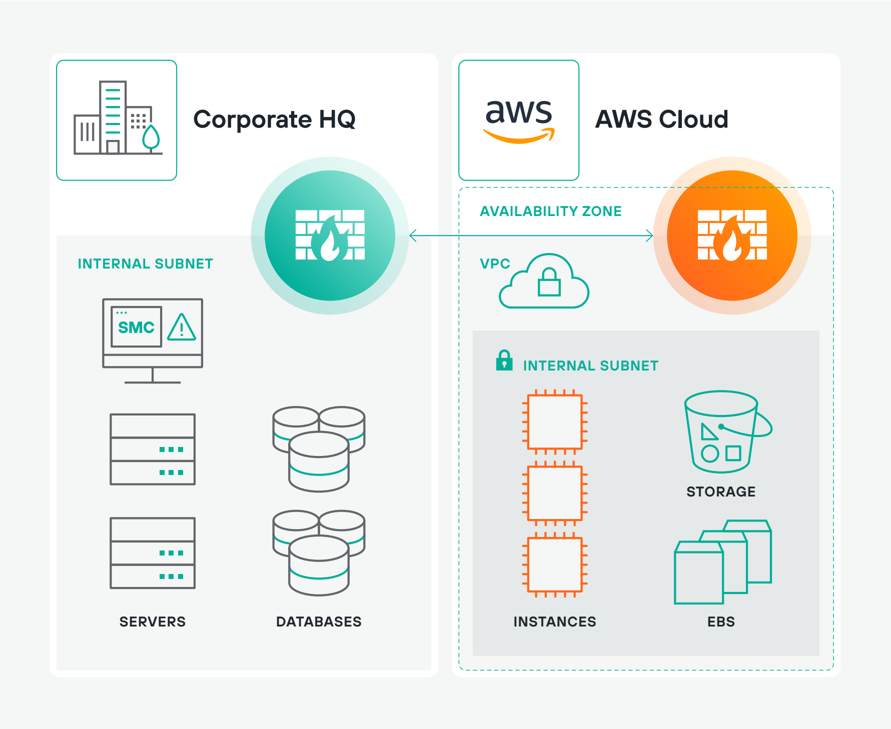
Quick & Elastic Deployment

To quickly deploy Forcepoint software-based architecture security in your AWS environment, simply choose one of the available options in the AWS marketplace

→ Visit Marketplace

Forcepoint NGFW + AWS Solutions

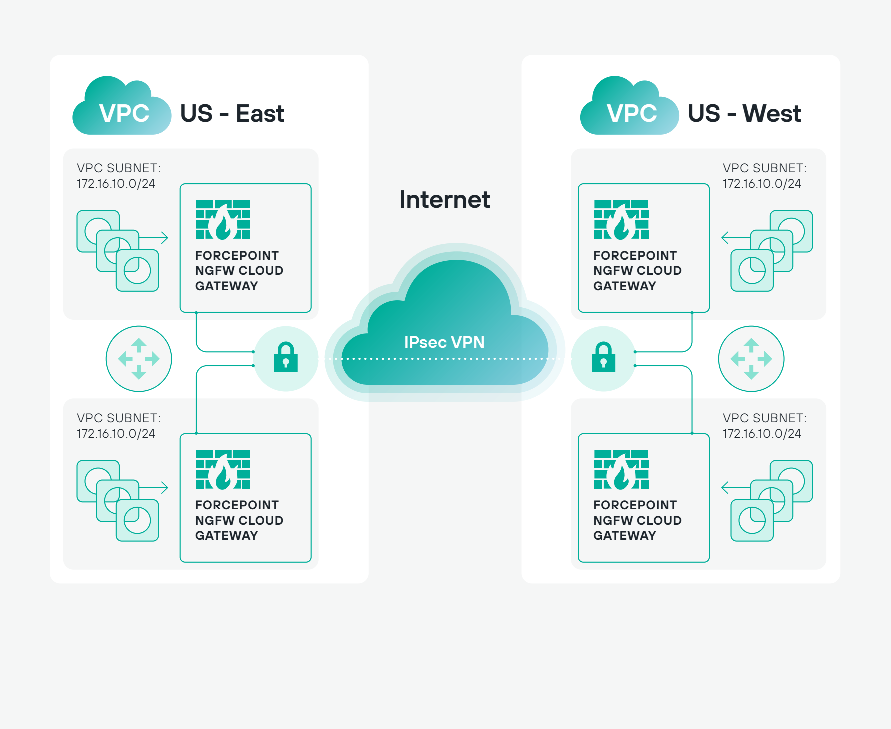
Securely extend corporate networks and leverage the power of AWS with Forcepoint NGFW



Extend Corporate Networks into AWS Environments

Forcepoint NGFW applies application-specific threat prevention polices to stop exploits, malware and zero-day vulnerabilities from compromises attempting to exfiltrate data from an organization's AWS environment(s). AWS Security Hub brings centralized visibility to the actions and conditions that triggered the policy enforcement alerts.

- → Extend your organization's network into AWS
- → Enable hybrid IT efficiently and simplify data transfer to and from AWS
- → Easily manage both ends of multiple VPN connections in one place



Inter-regional VPC-to-VPC Routing

Connect VPCs across multiple AWS regions securely. You can manage, control and enforce security policies using the Forcepoint industry-leading network security technology.

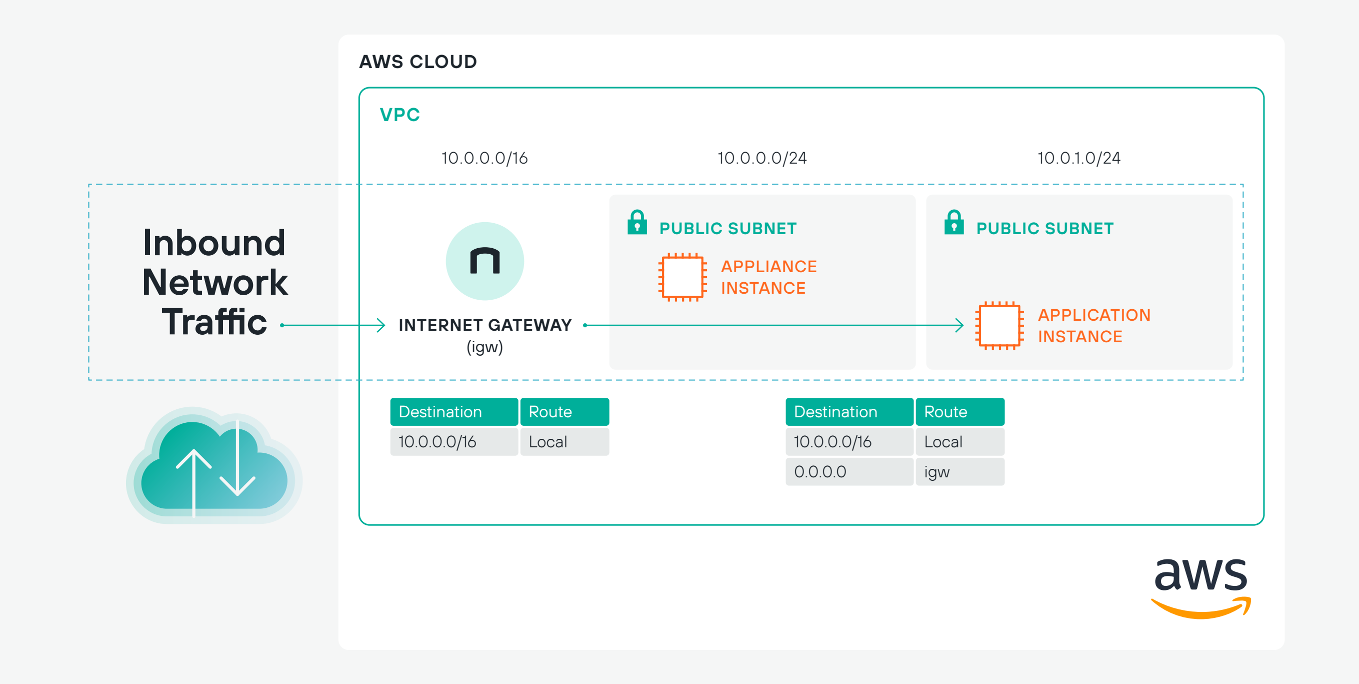
- → Secure information that flows between regions
- → Apply consistent security policies across regions

An energy company saved 90% on their WAN costs by implementing NGFW with SD-WAN from Forcepoint and moving to the cloud—all with a zero-touch deployment.

Amazon VPC Ingress Routing

Amazon VPC Ingress Routing simplifies the integration of network security with your Amazon Virtual Private Cloud (VPC) infrastructure, making it simpler for you to apply security policies uniformly across the entirety of your enterprise network—both in the cloud and on-premises—to effectively protect your AWS workloads.

- → Gain flexibility to treat any traffic destined to Amazon VPC with the same level of scrutiny as is used in accessing the enterprise network
- → Enforce network security policies uniformly across the entire enterprise network, without additional latency
- → Gain maximum security with minimum cost and complexity



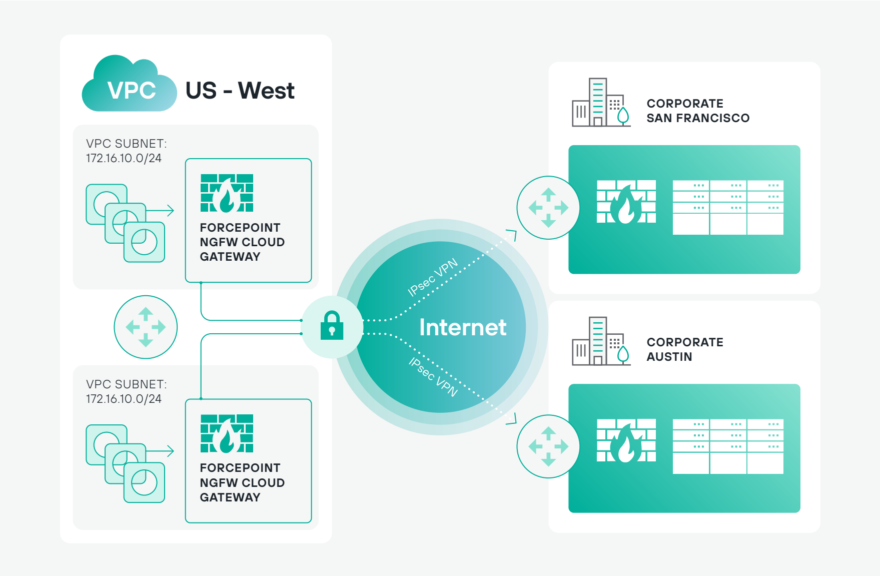
Destination	Route
10.0.0.0/16	Local

Destination	Route
10.0.0.0/16	Local
0.0.0.0	igw

AWS VPN CloudHub

Connect VPCs across multiple AWS regions securely. You can manage, control and enforce security policies using the Forcepoint industry-leading network security technology.

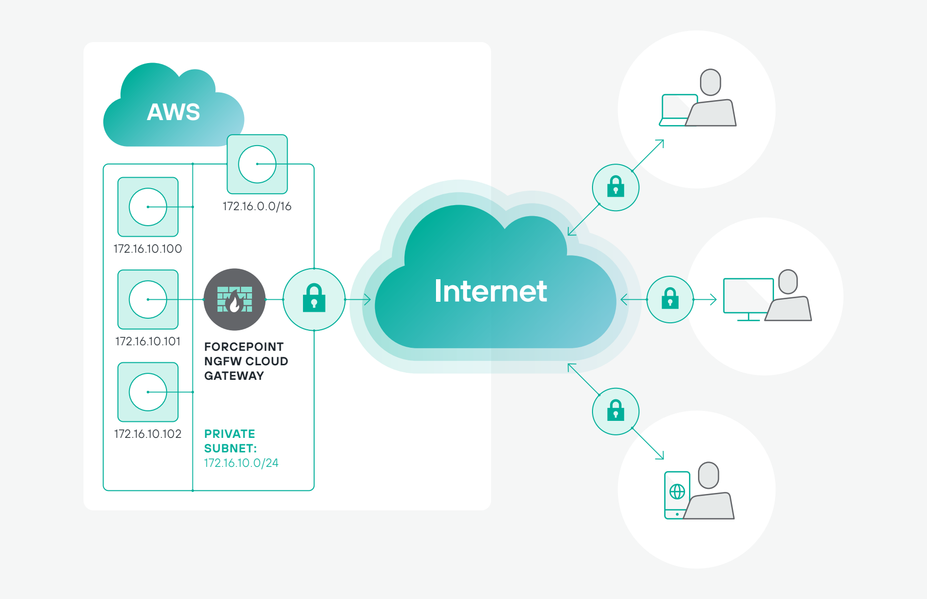
- → Secure information that flows between regions
- → Apply consistent security policies across regions


VPC
US - West
VPC SUBNET: 172.16.10.0/24
FORCEPOINT NGFW CLOUD GATEWAY
VPC SUBNET: 172.16.10.0/24
FORCEPOINT NGFW CLOUD GATEWAY
Internet
IPsec VPN
IPsec VPN
CORPORATE SAN FRANCISCO
CORPORATE AUSTIN

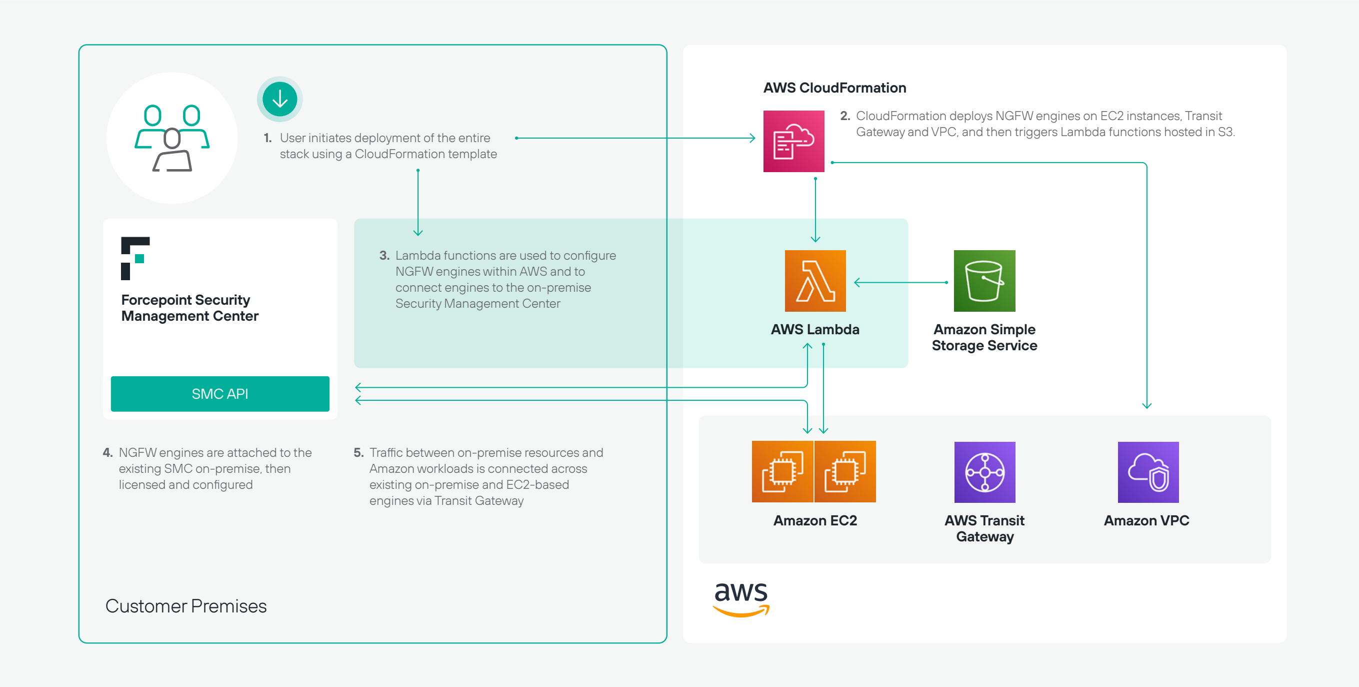
Remote Access Connectivity

Forcepoint NGFW can be used as a cloud edge gateway to connect your remote users to Amazon Virtual Private Cloud (VPC). The Forcepoint NGFW cloud gateway can be deployed in an Amazon Elastic Compute Cloud (EC2) instance, offering advanced firewall features to protect your EC2 instances for all inbound and outbound access, such as:

→ Application awareness
→ User identity capabilities



Forcepoint NGFW + AWS Service Integrations



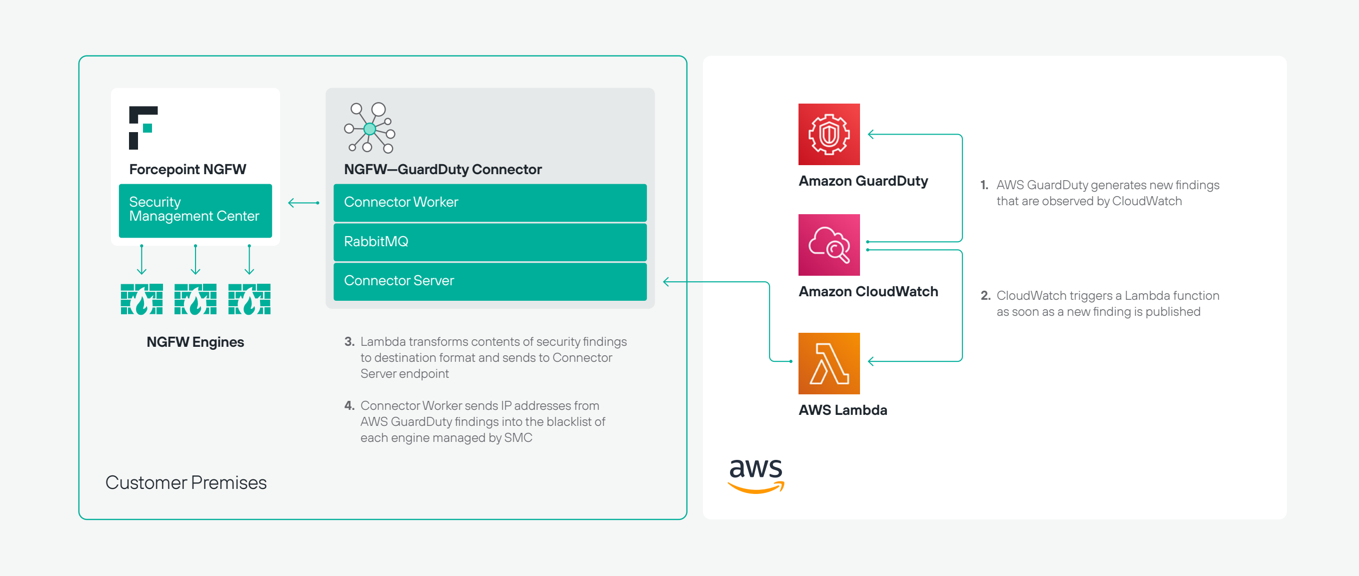
1. User initiates deployment of the entire stack using a CloudFormation template
2. CloudFormation deploys NGFW engines on EC2 instances, Transit Gateway and VPC, and then triggers Lambda functions hosted in S3.
3. Lambda functions are used to configure NGFW engines within AWS and to connect engines to the on-premise Security Management Center
4. NGFW engines are attached to the existing SMC on-premise, then licensed and configured
5. Traffic between on-premise resources and Amazon workloads is connected across existing on-premise and EC2-based engines via Transit Gateway

Transit Gateway Integration

Deploys a redundant set of Forcepoint Next Generation Firewalls as EC2 instances, and an AWS Transit Gateway, and connects the NGFW engines to an existing Forcepoint Security Management Center using AWS Lambda functions. Redundant IPSEC tunnels are set up between the in-the-cloud NGFW engines and the Transit Gateway, and security policies managed by Forcepoint Security Management Center can be applied to the NGFW engines in AWS to secure the traffic flowing to and from the Transit Gateway.

→ Enables consistent application of security policies across on-premises and AWS
→ Automates the deployment of the entire technology stack using a single AWS CloudFormation template, with customizable parameters to allow for tailor-made deployments

Get the Guide



1. AWS GuardDuty generates new findings that are observed by CloudWatch
2. CloudWatch triggers a Lambda function as soon as a new finding is published
3. Lambda transforms contents of security findings to destination format and sends to Connector Server endpoint
4. Connector Worker sends IP addresses from AWS GuardDuty findings into the blacklist of each engine managed by SMC

Amazon GuardDuty Integration

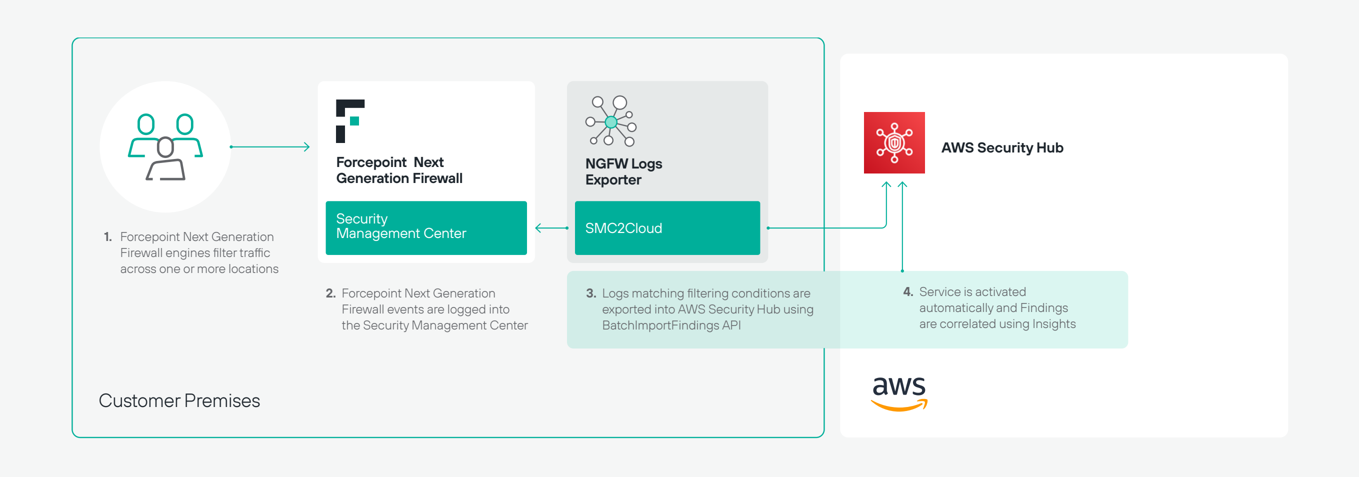
GuardDuty gives AWS customers an intelligent and cost-effective option for continuous threat detection in the AWS Cloud. The service uses machine learning, anomaly detection and integrated threat intelligence to identify and prioritize potential threats. The Forcepoint NGFW integration automates real-time import of security findings from Amazon GuardDuty.

→ Users, applications and services hosted on-premises and protected by NGFW benefit from the increased visibility of threat actors targeting the AWS footprint of an organization

→ Malicious source-IP addresses identified by Amazon GuardDuty are subsequently blacklisted into an entire fleet of NGFW engines deployed across the organization sites

→ Effectively delivers increased protection as a result of the shared intelligence

Get the Guide



1. Forcepoint Next Generation Firewall engines filter traffic across one or more locations
2. Forcepoint Next Generation Firewall events are logged into the Security Management Center
3. Logs matching filtering conditions are exported into AWS Security Hub using BatchImportFindings API
4. Service is activated automatically and Findings are correlated using Insights

Interoperability with AWS Security Hub

AWS Security Hub provides a consolidated view of your security status across AWS accounts. Forcepoint integration with AWS Security Hub provides visibility of how users are interacting with your most sensitive data, wherever it resides.

→ Automatically export log events from Forcepoint NGFW into AWS Security Hub in real-time to accelerate response time

→ Correlate security findings with other sources to enhance visibility across all locations protected by NGFW

→ Easily curate data through grouping by a variety of fields, such as severity and type, to prioritize what matters most to your organization

Get the Guide Schedule A Demo

[Forcepoint Next Generation Firewall with Amazon Web Services Solution-Brief-US-EN] 1DEC2020