



What is a next-generation firewall (and why does it matter)?



Matt Bromiley

SANS Analyst
SANS Institute



Geoff Sweet

Sr Security Solutions Architect
AWS

Today's Agenda

- Starting Out
- NGFW Basics & Implementation
- NGFWs in Action: Use Cases

Starting Out

Will a legacy firewall help defend modern applications?

Why/why not?

Starting Out

- Legacy firewalls offered capabilities needed in their time.
 - Mostly operating at Layers 3 and 4
 - Little to no application awareness
 - Detection capabilities, if present, were atomic and user-generated and –input.
 - Management may be per-device or site, hard to scale.

Starting Out

Do these legacy capabilities stop
adversaries?

Why/why not?

Starting Out

- Modern attacks require modern defenses
 - Advanced threat protection
 - Application awareness and control
 - Improved visibility
 - Compliance requirements
 - Business continuity
 - Central management capabilities

NGFW Basics & Implementation

Advanced Threat Protection

- Perhaps the most common use of NGFW - advanced threat detection and handling capabilities.
- Malware detection, IDS/IPS capabilities, threat intelligence, etc.

Application Awareness & Control

- NGFWs inspect and categorize traffic at the application layer (and lower), allowing for specific actions & control.

Improved Visibility

- Deeper insight and profiling of network traffic.
- Security team can "see" more.

Compliance Requirements

- NGFWs help keep compliance in place by satisfying multiple regulatory requirements.

Business continuity

- Simply put - less risk == less business impact,








NGFW Basics & Implementation

AWS includes a multitude of cloud-based NGFW options.

Research and compare!

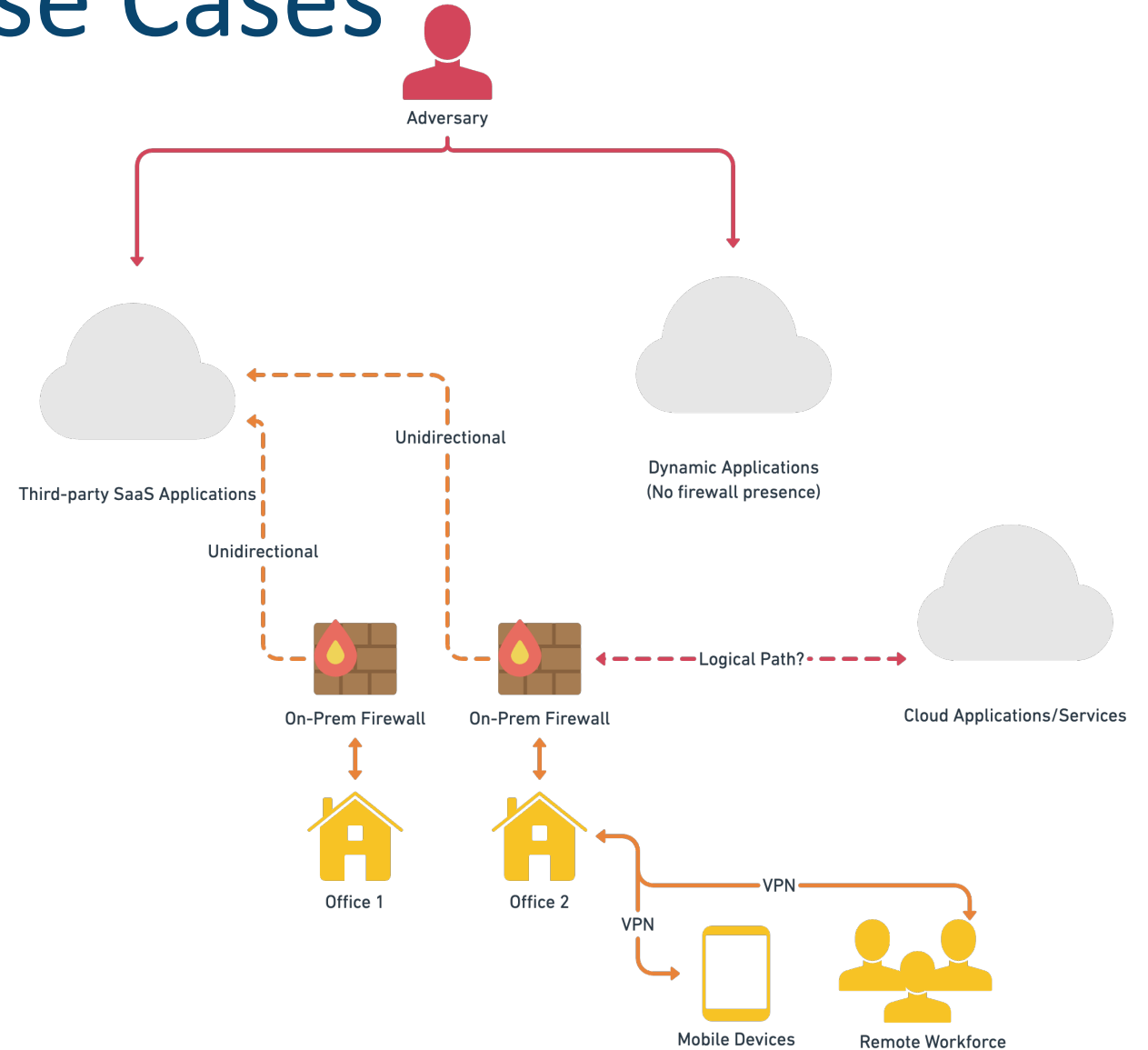
Solutions

The NGFW solutions available in AWS Marketplace help you boost your network security posture and defend against cybersecurity threats. These NGFW platforms combine multiple integrated security functions, such as intrusion detection systems (IDS), intrusion prevention systems (IPS), virtual private network (VPN) gateways, antivirus and anti-bot controls, application control, secure sockets layer (SSL), transport layer security (TLS) inspection, and web filtering.

 Check Point SOFTWARE TECHNOLOGIES LTD CloudGuard Network Security NGFW delivers advanced, multi-layered threat prevention for AWS cloud, and protects cloud assets from threats. Learn more > See how it works: Video Datasheet	 CISCO Cisco Firepower NGFW Virtual delivers unified policy management, application control, threat prevention, and advanced malware protection from network to endpoint. Learn more > See how it works: Video Datasheet	 Forcepoint Connect, automate and orchestrate tools across development, operations and shared service teams to optimize software delivery. Learn more > See how it works: Datasheet	 FORTINET Fortinet FortiGate NGFW protects your apps and data in AWS by mitigating known and unknown threats with an efficient policy structure and automation. Learn more > See how it works: Video Datasheet
 JUNIPER NETWORKS Juniper vSRX delivers a complete cloud-based virtual firewall with advanced security, secure SD-WAN, robust networking and built-in	 paloalto NETWORKS VM-Series augments AWS native network security with real-time application layer visibility and next-generation threat and data theft	 SOPHOS Sophos Firewall protects AWS VPCs and web facing apps from advanced threats, with centralized management from Sophos complete	

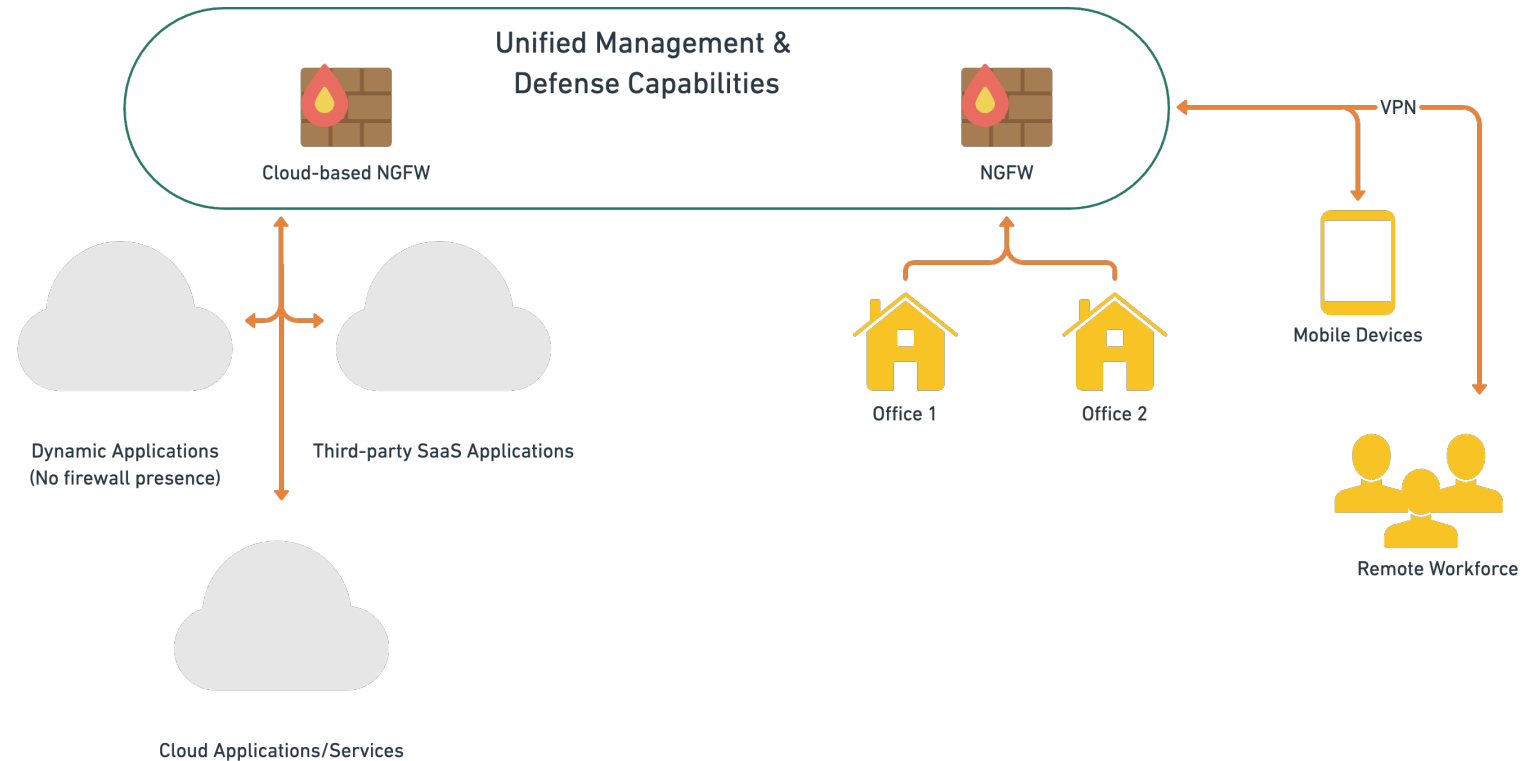
NGFWs in Action: Use Cases

- Do legacy firewalls even assist in protecting cloud assets?
- How can they stand up against adversaries, targeted or opportunistic?



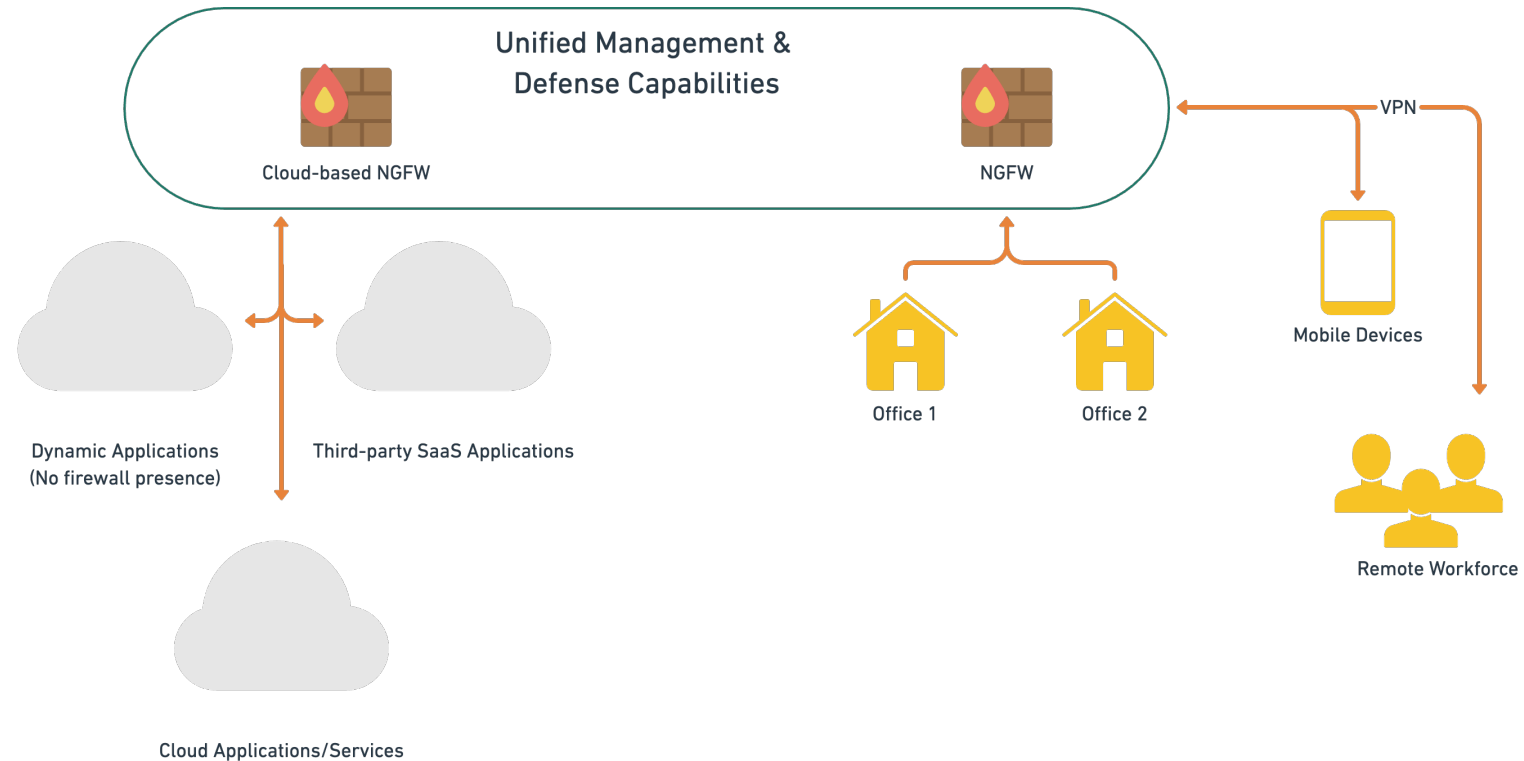
NGFWs in Action: Use Cases

- Do legacy firewalls even assist in protecting cloud assets?
- How can they stand up against adversaries, targeted or opportunistic?



NGFWs in Action: Use Cases

- NGFW implementations allow for centralized management and scaled defense capabilities.
- NGFWs can integrate with larger plants (ZTNA, SASE, etc.) to better protect networks.



NGFWs in Action: Use Cases (1)

Behavioral Analysis

- Analyze behavior of traffic for anomalous patterns.
- Can be used with ML/AI approaches to create a baseline of "normal".

Machine Learning

- Advanced analysis capabilities, relying on machine learning and trainable algorithms to learn nuances of your environment.

Deep Packet Inspection

- Identify and blocks threats, even ones that are hidden inside packet contents
- Detect malicious activity based on data and metadata.

NGFWs in Action: Use Cases (2)

Application Awareness

- Understand "what" and "how" applications should behave to find anomalous behavior.

Malware Sandboxing

- Detonate malware in a "safe" space, outside of production, to identify key characteristics and determine severity.
- Sandboxing can also be used to develop additional detections and hone heuristics.

Third-party support team

- Most NGFW vendors have analysis and threat intelligence teams that can provide additional support and/or context around threats.



What is a next-generation firewall (and why does it matter)?



Geoff Sweet

Security Solutions Architect
AWS

Various resources available



NGFW Solutions in AWS Marketplace
Enhance network security through stateful, application aware, deep-packet inspection and intrusion prevention and detection using third-party software

<https://aws.amazon.com/marketplace/solutions/security/next-generation-firewalls>



ebook: The value of next generation firewall (NGFW) tools

<https://pages.awscloud.com/awsmpebook-sec-firewall-lob-ebook.html>



Learn more about AWS Security Partners and gain access to exclusive content on security solutions addressing security use cases on behalf of our customers

<https://aws.amazon.com/security/partner-resources/>



Cloud NGFW for AWS Blog

<https://aws.amazon.com/blogs/aws/new-cloud-ngfw-for-aws/>

Customer success stories



paloalto[®]
NETWORKS

Software NGFWs: Best-in-class network security



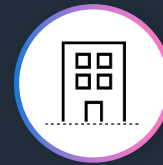
Internet



Private Cloud/DC



Public Cloud



Remote Location
(Virtual Branch)

Software Next-Generation Firewalls

Consistent services are cloud delivered across all products



Intrusion
Prevention



URL
Filtering



Sandboxing



DNS
Security



Data Loss
Prevention



SaaS
Security



IoT
Security



CASB



AIOps



VM-Series Firewalls



CN-Series Firewalls



Cloud NGFW



AI/ML Powered



Software Automation



Unit 42 Threat Research

Best-in-class security
for all users and
applications

Deep integrations
with clouds and
virtualization
technologies

Automated DevOps
deployment and
scaling

Centralized
management for
all private and
public clouds

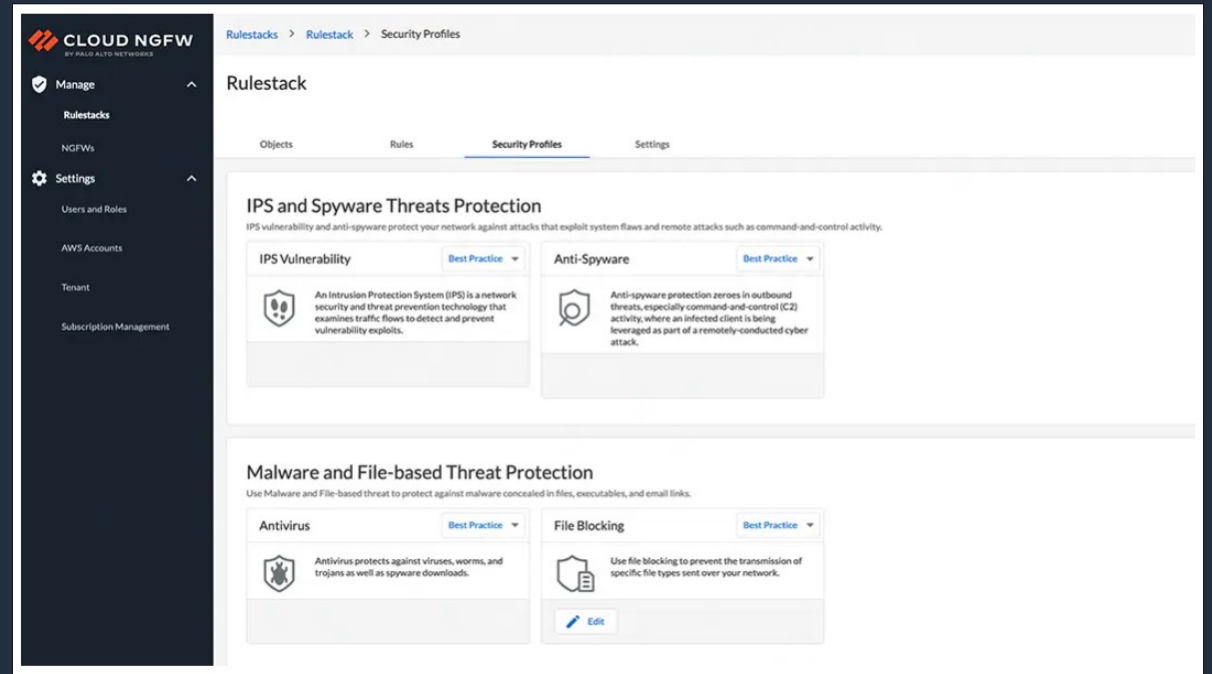
Case study: Barrett Steel

Challenge

Barrett Steel needed to maintain strong information security across its on-premises and cloud assets to prevent business disruption triggered by COVID-19. Barrett also needed to pursue lucrative defense contracts while simplifying administration for the company's lean IT team. However, Barrett was challenged by performance limitations in its legacy security infrastructure and required a more robust, easier-to-manage solution.

Solution

Barrett opted to build a Zero Trust security posture and used Palo Alto Networks solutions as the foundation. The Palo Alto Networks NGFW suite and the Prisma Cloud platform control traffic based on application type and user role, as well as intelligently detect and disrupt cyberthreats. GlobalProtect network security for endpoints enabled employees to securely work from home, and Panorama centralizes all network security management.



Case study: Barrett Steel

Business Impact



Automatic detection and prevention of phishing attacks



Enabled Zero Trust security posture on-premises and in the cloud



Support of tenfold increase in remote workers quickly and securely



Assurance that cloud applications conform with security policies



Simplified security management for a lean IT team

“The fact that we have been able to run and grow our business without any major issues is in large part because of the strong security posture we’ve taken by investing in solutions from Palo Alto Networks.”

Sam Ainscow

Head of IT Operations and Chief Information Security Officer,
Barrett Steel



CHECK POINT™

Case study: Hallmark

Challenge

Hallmark needed to develop and use new features and functionality on a day-to-day basis. However, the company had deployed multiple security gateways across several regions within several different cloud environments. This led to time, effort, and complex management issues for employees. Hallmark needed to scale security dynamically and increase its ability to develop and enhance new software products securely under tight timelines.

Solution

Hallmark collaborated with a third-party security company that worked with Check Point to build a secure cloud infrastructure that matched the needs of its applications. Check Point CloudGuard Network Security for Gateway Load Balancer enabled Hallmark with autoscaling capabilities that brought in many of the different abilities from an east-west traffic perspective, a northbound traffic inspection, and an egress traffic inspection.



Case study: Hallmark

Business Impact



Ability to produce products in a secure manner



Enabling east-west, north-south, and egress traffic protection in the cloud



Autoscaling with dynamic security elasticity to ensure capacity when and where needed

“As we work to create new features and functionalities the R&D team is able to work with a third party—or us directly—to help find quick solves. Having that immediate contact with Check Point really is a life saver.”

Greg Smith
Director of Cyber Security, Hallmark

FORTINET®

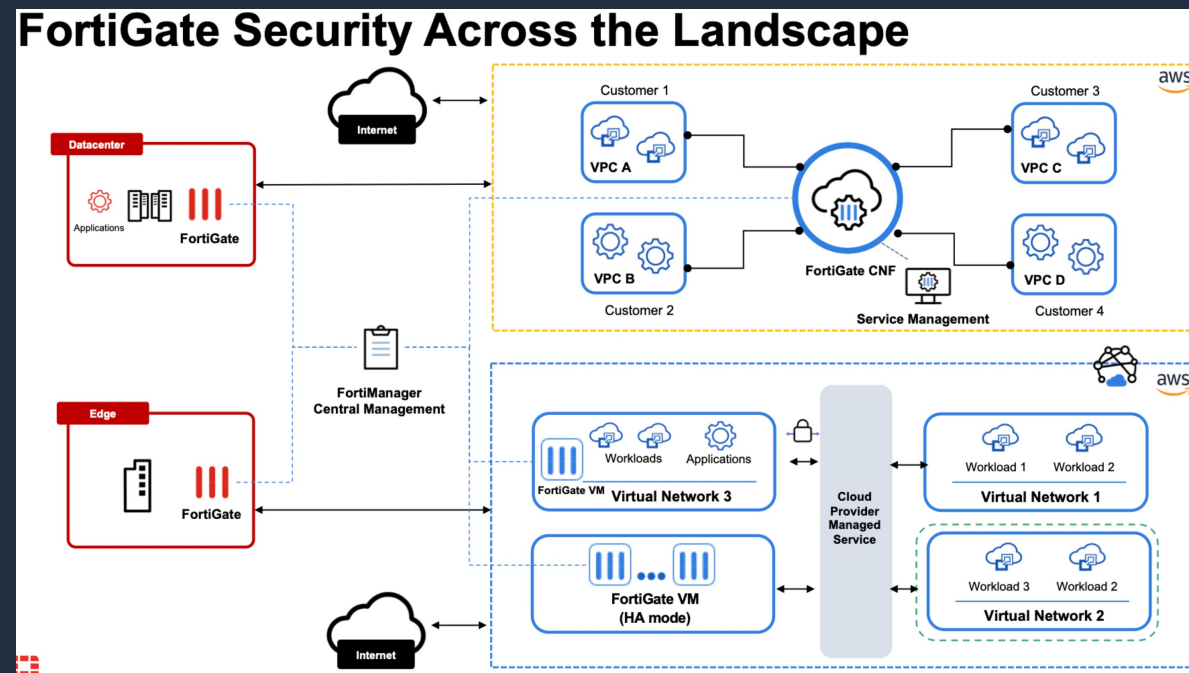
Case study: BK Bank

Challenge

BK Bank needed to protect its critical applications by minimizing or eliminating fraudulent requests—up to 80,000 every five minutes. The bank used a disparate mix of tools that detected specific security concerns, but couldn't provide a complete view of the bank's network and applications. In addition, to meet regulatory security standards, BK Bank used manual processes that added time and complexity.

Solution

BK Bank selected Fortinet to leverage automated tools to block malicious activity, balance workloads, and protect its communications. The bank now runs network and applications traffic through FortiGate next-generation firewalls (NGFWs) to detect known and unknown threats and vulnerabilities. While FortiAnalyzer provides advanced log management, analysis, and reporting to help it proactively prevent attacks.



Case study: BK Bank

Business Impact



Integrated information security ecosystem that provides full visibility into its network—both on-premises and in the cloud



Reduced time to comply with Payment Card Industry Data Security Standard (PCI DSS)



Single policy management



Access to Fortinet NGFWs in AWS Marketplace as a VM or SaaS, and as Graviton EC2 instances

“Integrated Fortinet solutions give us broad visibility, which provides for far easier and more proactive network management. This helps us improve all business processes.”

Caio Hyppolito
CTO, BK Bank



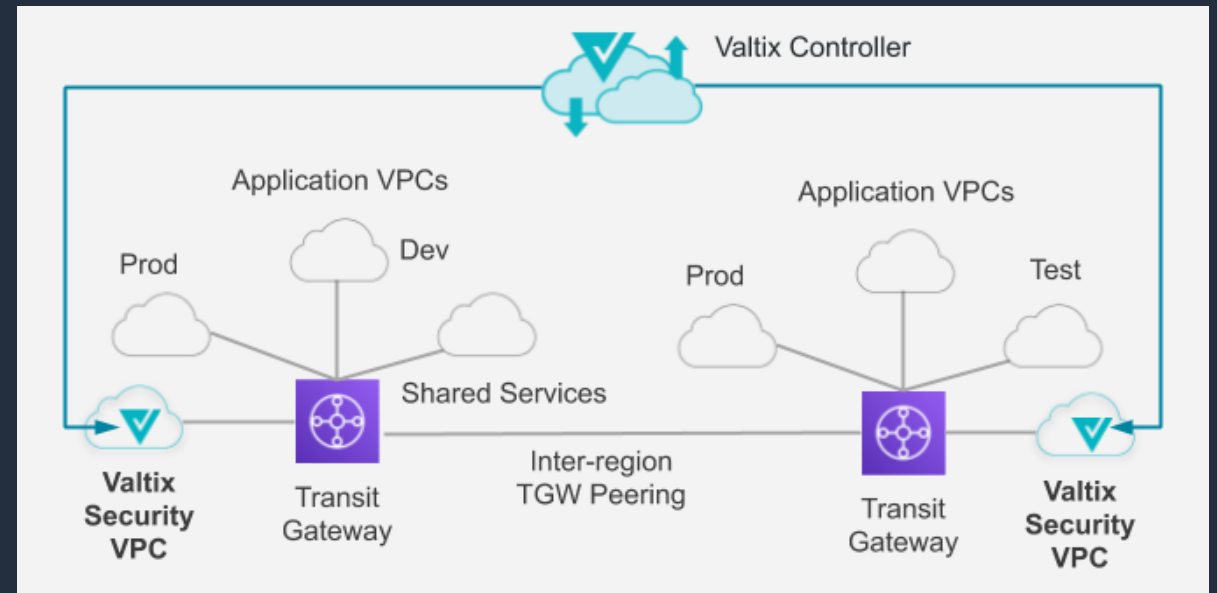
Case study: FHL Bank

Challenge

FHL Bank was migrating its application infrastructure into a modern, cloud-native stack running in AWS. The bank needed agility in the fast-changing environment, support for multiple virtual private clouds (VPCs) that grew and shrank according to workload, and protection against data exfiltration. FHL was challenged by next-generation firewalls (NGFWs) that lacked automation, ease of use, autoscaling, and a cloud-native approach.

Solution

FHL Bank used the Valtix cloud-native NGFW to enable cloud migration and centralize its security tasks. Valtix Controller continuously discovers and updates all the assets in the customer's multi-account AWS environment in near real time. An autoscaling fleet of Valtix gateways provides security against cyberattacks for both web and non-web applications, preventing data exfiltration when instances connect outbound for software updates or partner systems. This includes WAF, IDS/IPS, Application ID, URL Filtering and DLP.



Case study: FHL Bank

Business Impact



Lower total cost of ownership (TCO) with a consolidated network of security, including NGFWs, web application firewall (WAF) with OWASP Top 10, and Advanced Rule Set



No complex templates or scripting



Stronger security posture due to ease of deployment, cloud visibility, and discovery-based security policies and built-in auto scaling

“Valtix uses a SaaS controller to enormously simplify deployment of network security in our public cloud. Life is easier with Valtix and we can now focus more on business outcomes.”

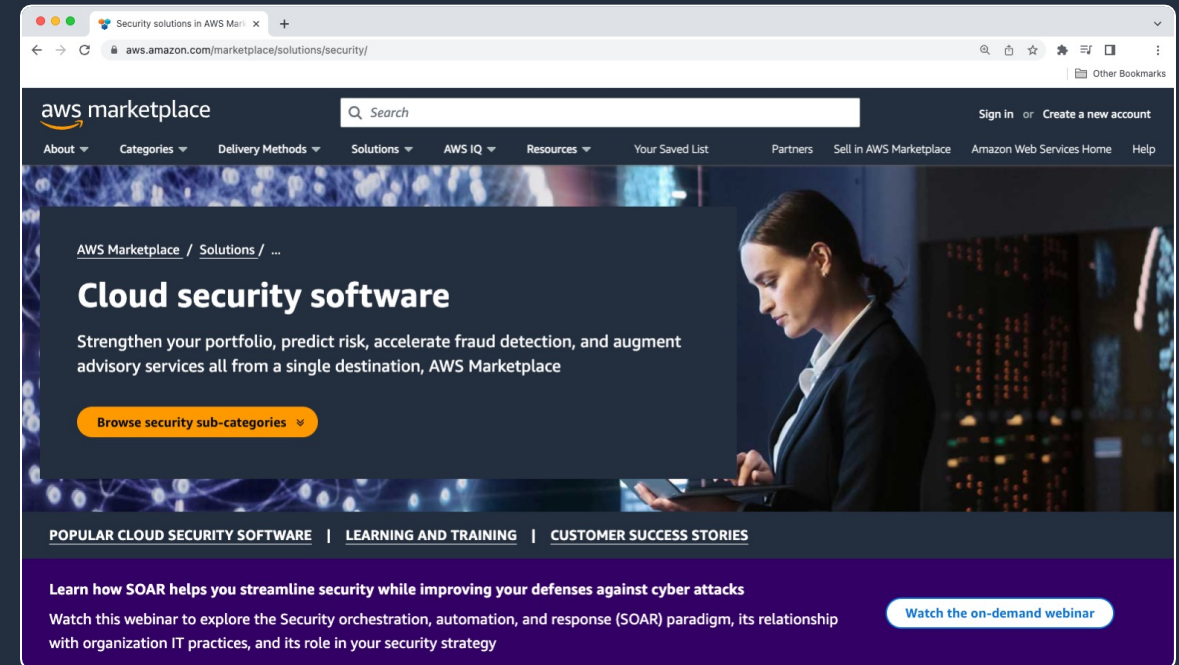
Director of Public Cloud Architecture
FinServ bank

What is AWS Marketplace?

AWS Marketplace makes it easy to **find, try, buy, deploy,** and **manage** software that runs on AWS.

Customers can launch pre-configured solutions in **just a few clicks** in both Amazon Machine Image (AMI) formats and Software-as-a-Service (SaaS) subscriptions, with entitlement options such as hourly, monthly, annual, and multi-year contracts.

AWS Marketplace is supported by a **global team** of solutions architects, product specialists, and other experts to help IT teams connect with the tools and resources needed to streamline migration journeys to AWS.



Why AWS Marketplace?

Security teams use AWS-native services and seller solutions in AWS Marketplace to help build automated, innovative, and secure solutions to address relevant use cases and further harden their cloud security footprint.

Reduce licensing costs by **10%** with flexible pricing models.

Save **\$2 million** by consolidating steps and increasing visibility into procurement practices.

Cut time spent invoicing processes in **half**.

Reduce time spent researching and comparing vendors by **66%**.

Recapture **25%** of at-risk committed spend with Amazon and attain discounts.

Reduce vendor onboarding processes by **75%**, leading to time savings worth more than **\$62,000**.

Realize payback in less than **six months**.

Amazon Web Services (AWS) Marketplace surveyed 500 IT decision-makers (ITDMs) and influencers across the US to understand software usage, purchasing, consumption models, and compared savings.

How can you get started?

Find



A breadth of security solutions including:



And more:

<https://aws.amazon.com/marketplace/solutions/security/>

Buy



Through flexible purchasing options:

- Free trial
- Pay-as-you-go
- Budget alignment
- Bring Your Own License (BYOL)
- Private Offers
- Billing consolidation
- Enterprise Discount Program
- Private Marketplace

Deploy



With multiple deployment options:

- SaaS
- Amazon Machine Image (AMI)
- CloudFormation Template
- Containers
- Amazon EKS/Amazon ECS
- AI/ML models
- AWS Data Exchange

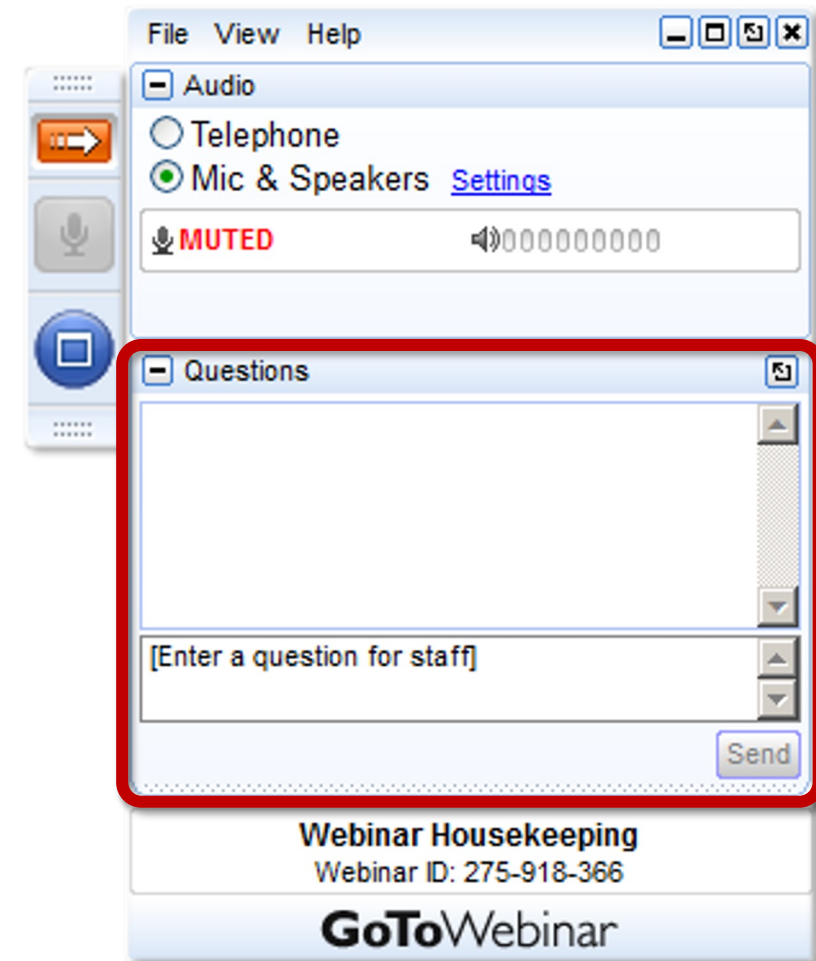
Webinar summary

- Starting out
- NGFW basics and implementation
- NGFWs in action: Use cases
- Customer success stories
- Solutions in AWS Marketplace

Q&A

Please use **GoToWebinar's** Questions tool to submit questions to our panel.

Send to “Organizers” and tell us if it’s for a specific panelist.



Acknowledgments

Thanks to our sponsor:



To our special guest: Geoff Sweet

And to our attendees, thank you for joining us today!

aws marketplace

Thank you!