SECURITY OPERATIONS IN THE CLOUD

Marc Baker

Goals & Agenda

- Learn about today's threat landscape and how these threats can affect your security operations.
- Learn about perimeter services in the cloud that can help protect your applications, without the need to re-architect.
- Learn how to meet compliance requirements easily and quickly across all applications in your organization

The Cloud Issue For Infosec

HP Enterprise 2017 App Sec and DevOps Report (1)

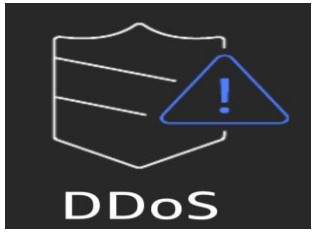
- Security leaders are not developers
  - Less than 15% of CISOs have a background in development
- Lack of application security talent
  - Organizations migrating to the cloud have an average of 900 developers for every 11 application security professionals
  - 2016 Cloud Passage Report: the top 10 US Bachelor's Computer Science programs did not require a security class for graduation
  - The survey looked at requirements for software developers in Fortune 100 companies and none specified security or secure coding experience as a required skill
- Integrating security into DevOps is difficult
  - Ninety percent of security professionals surveyed state that since their organization has started developing DevOps methodologies, integrating application security has become more difficult.

HP Enterprise 2017 App Sec and DevOps Report (2)

- Organizations averaged four application releases annually in 2010 and are projected to release an average of 120 applications annually by 2020
- The overwhelming majority of respondents cited security control application as being downstream of the SDLC with only 20% stating that secure SDLC is being done in the development cycle
- Most of the responding organizations rely on pre-production penetration testing and network security once applications are released from development
- 17% of responding organizations stated that they are not using any technologies to protect applications

Common Cloud Threats

Types Of Cloud Threats That Exist Today

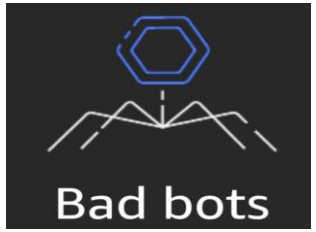


HTTP Floods

Reflection Attacks

SQL Injection

Cross-site Scripting (XSS)



Crawlers

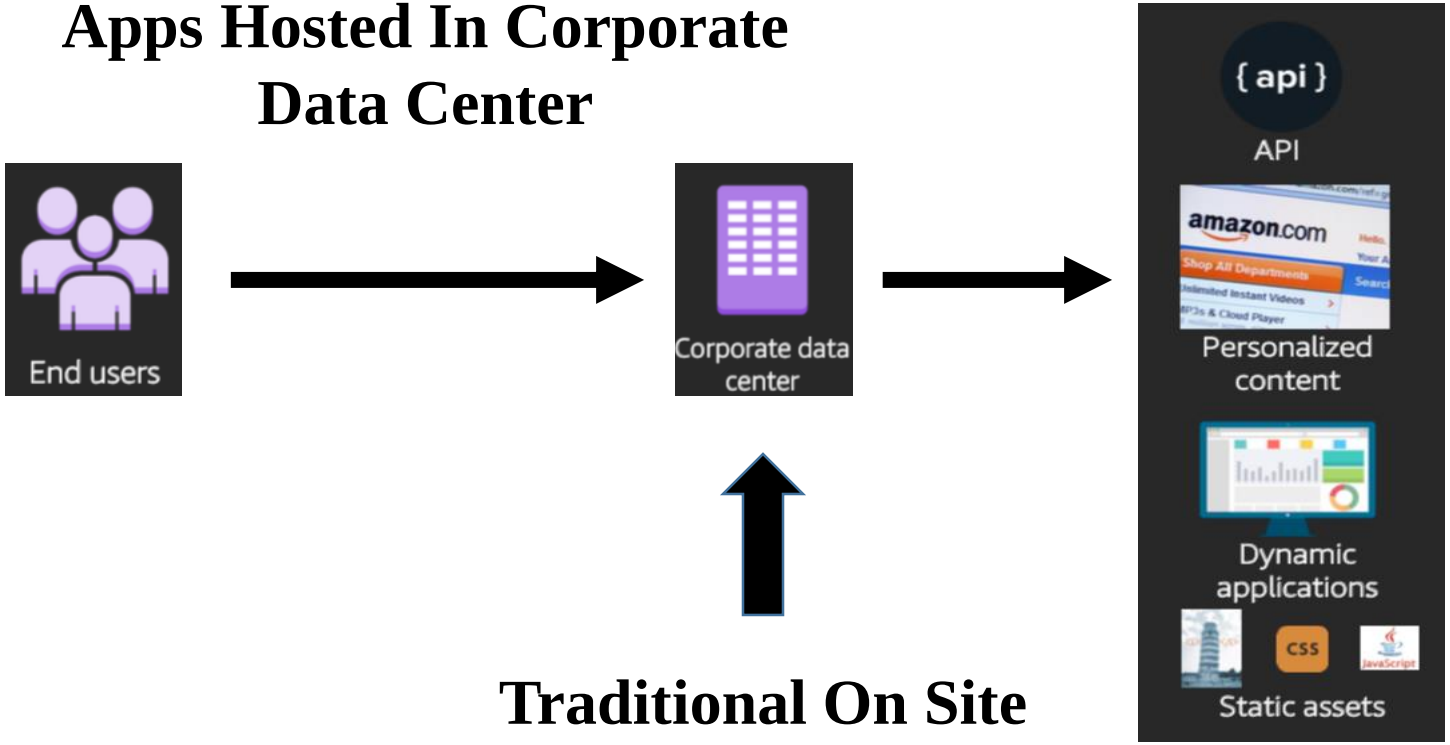
Content Scrapers

Scanners & Probes

“How can we protect our cloud applications from these threats?”

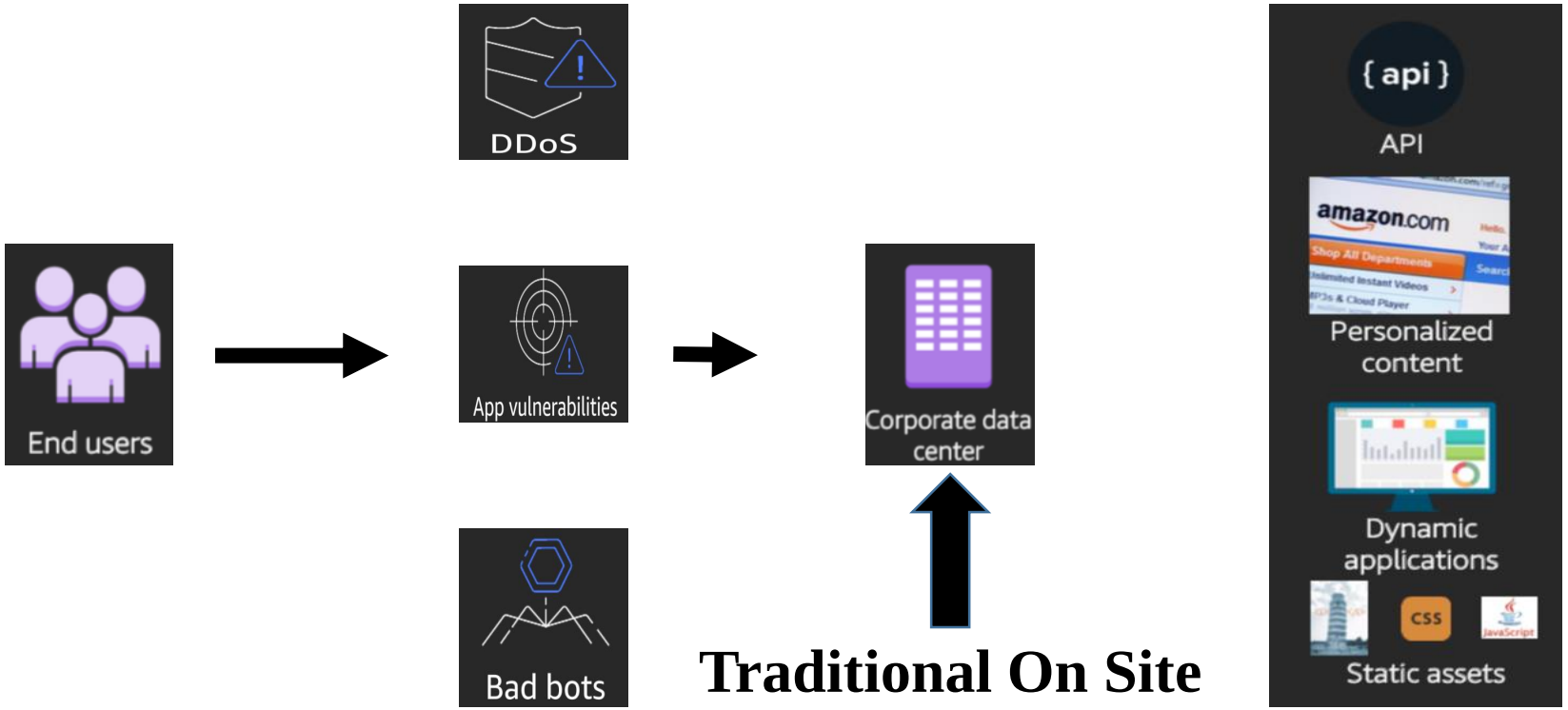
Common Applications – Traditional Build

End Users Interact With Web Apps Hosted In Corporate Data Center



Traditional On Site Security Protections

Traditional Secure Design Considerations



Security

Authentication

Encryption (TLS)

Layered Protection

Availability

Resiliency / Fault Tolerance

Request handling capacity

Blocking bad traffic

Performance

Routing

Throttling

Alerting & monitoring

AWS Building Blocks For Baseline Defense

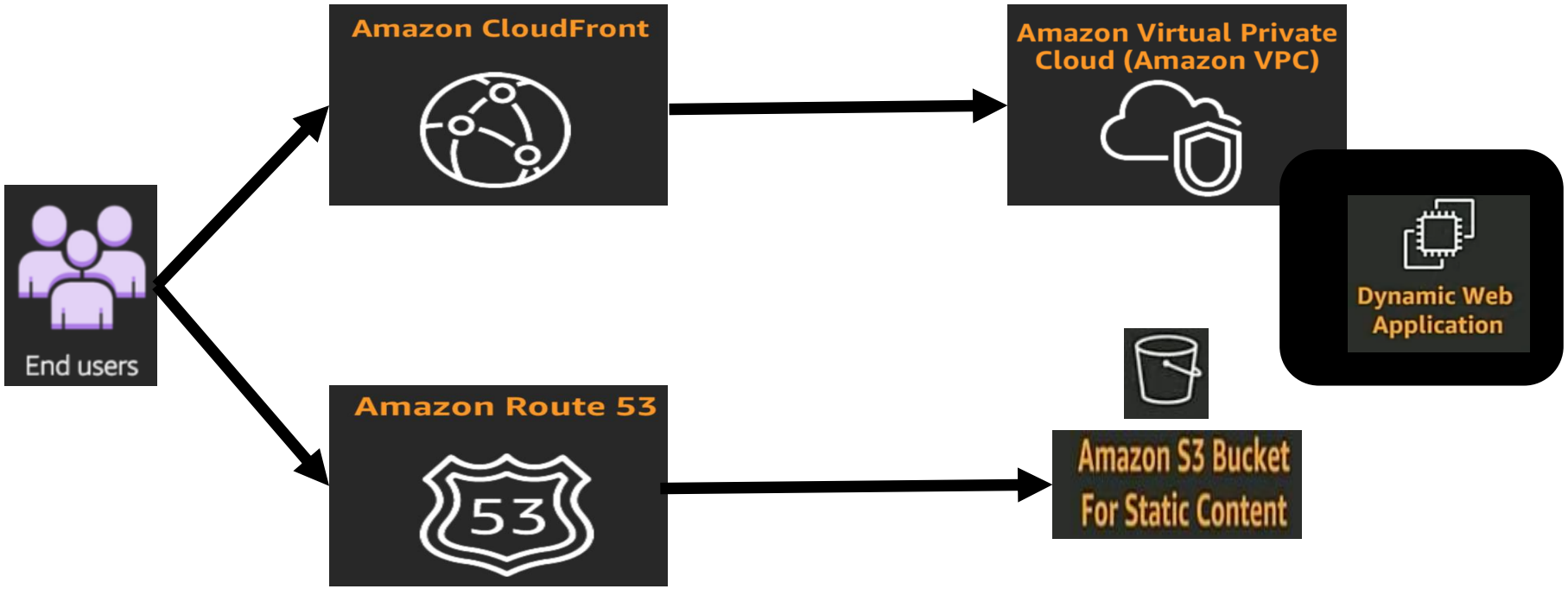
- Security groups
- Network ACLs

- Global presence
- SSL/TLS
- Origin shielding
- Resilience (TTL)

- DNS header validations
- Priority-based traffic shaping

Setting Up Your Baseline Defenses

End User Interaction Moved From Corporate Data Center To Cloud Edge Network



DDoS Mitigation on the AWS Edge Network

- Fully inline packet inspection blocks known bad traffic, scores suspicious traffic
- Sub-second latency to detect and mitigate attacks
- SYN proxy challenges illegitimate connections without maintaining state
- Anycast routing and DNS-based traffic direction

Tools For Security Operations In The Cloud

Web Application Firewall (WAF)

- Customize security to your applications using custom rules
- Utilize Managed Rules for hassle-free protection and deployment
- Monitor using custom metrics from built in services (i.e., CloudWatch) or third-party log processors
- Automate using built in security automations like AWS Lambda or Azure Functions

WAF Capabilities

Malicious Traffic-Blocking

SQL injection conditions

XSS conditions

Cloud service edge location security automation

Managed rules

Web Traffic Filtering

- Rate-based rules
- IP-match & Geo-IP filters
- Regex & string match conditions
- Size constraint conditions

Visibility and Debugging

- AWS: CloudWatch metrics and alarms
- Log sampling automation
- Comprehensive logging

Logging For Auditing, Compliance, And Analytics

Send logs to multiple destinations using AWS WAF logging features

- Formatted in JSON
- Include every request, all request headers, along with AWS WAF metadata
- Provide for redaction of sensitive fields

Capture request logs for internal auditing and other compliance requirements (e.g., PCI, HIPAA)

AWS Cloud Trail

What Can You Do?

- Simplify compliance audits and incident response by automatically recording and storing activity logs for your AWS account.
- Log API calls made to AWS services
  - 90-day event history on by default
- Can operate log “trails” stored to Amazon S3
  - Optional AWS KMS encryption
  - Optional log file integrity validation
- Optional data-level event logging for Amazon
- Can route events to Amazon CloudWatch

AWS CloudTrail Events

- Each record in a CloudTrail log file represents a single file
- All records will contain the following common files:
  - Timestamp
  - Region
  - Event name (i.e., API calls)
  - Event source (i.e., the service)
  - Source IP address
  - User identity
- Event specific request and response parameters may also be included for some events

Amazon Guard Duty

- Continuous monitoring to rapidly detect threats (needle) to your environments in the sea of log data (haystack)
- Processes AWS CloudTrail logs, Amazon VPC Flow Logs, and DNS Logs
- Analyzes billions of events across your AWS accounts for signs of risk
- Identifies unexpected and suspicious activity, such as privilege escalation, exposed credentials, and communication with malicious IP addresses
- Can send findings to CloudWatch Events

GuardDuty Data Sources

- VPC Flow Logs
  - Flow Logs for VPCs do not need to be turned on to generate findings
    - Data is consumed through independent duplicate streams
  - Turning on VPC Flow Logs will provide means of augmenting data analysis
- DNS Logs
  - DNS Logs are based on queries made from EC2 instances to known questionable domains
  - DNS Logs are in addition to Amazon Route 53 query logs
    - Route 53 is not required for GuardDuty to generate DNS based findings
- CloudTrail Logs
  - CloudTrail history of AWS API calls used to access the AWS Management Console, SDKs, AWS CLI, etc.
  - Identification of user and account activity including source IP addresses used to make the calls

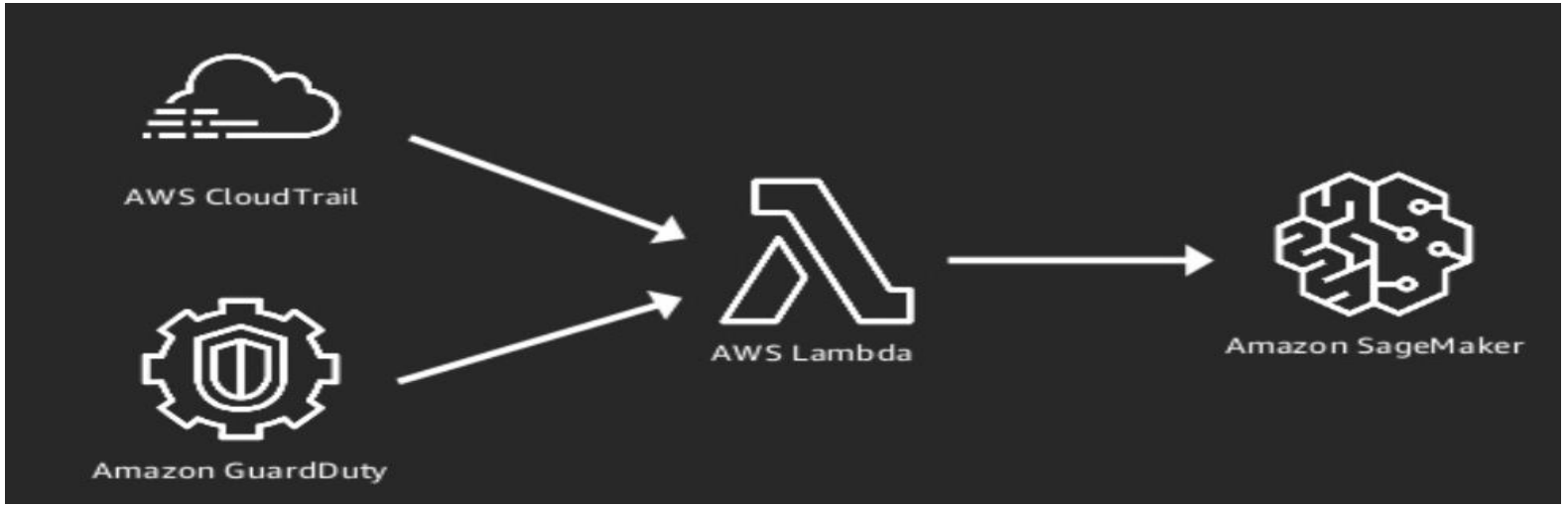
GuardDuty Trusted IP and Threat IP Lists

- Guard Duty uses AWS developed threat intelligence and threat intelligence feeds sourced from CrowdStrike and Proofpoint
- You can expand findings by adding Custom Trusted IP Lists and Known Threat Lists unique to your environment
  - Trusted IP Lists are whitelisted for secure communication with infrastructure and applications
  - No Findings will be presented for IP addresses on trusted lists
  - Threat lists consist of known malicious IP addresses
  - GuardDuty generates findings based on threat lists

SageMaker

- Rapidly build, train, and deploy machine learning models
  - Automated model for training and tuning is available
- SageMaker supports all algorithms and frameworks
  - Includes many built in optimized algorithms
  - Include MXNet, TensorFlow, and others
- You can experiment by using hosted interactive notebooks
  - Jupyter notebooks support multiple languages like Python and Scala
- SageMaker includes A/B testing capabilities

Putting This Into Practice



- Tuning: Parameters and training sets
- Use IP Insights on different classes of behavior (e.g., monitoring apps, bastion hosts)
- Think bigger – build additional detectors and models by leveraging tools like AWS GuardDuty and AWS Macie