

API Security for DevOps and InfoSec

Subra Kumaraswamy

@subrak

Tim Mather

@mather_tim

Apigee

@apigee

youtube.com/apigee


apigee

[Home](#) [Videos](#) [Discussion](#) [About](#) [Search](#)


[Subscribe](#) 3,610

8 in your circles subscribed


[Playlists](#) [Date added \(newest - oldest\)](#)




Favorite videos
10 videos




I Love APIs 2013
10 videos · 1 month ago




Digital Strategy
2 videos · 2 months ago




Apigee Platform
2 videos · 3 months ago




Office Hours
1 video · 1 year ago




How To Video Tutorials
9 videos · 1 year ago




Featured
14 videos · 1 year ago




Data and Analytics
7 videos · 1 year ago




Mobile
14 videos · 1 year ago




Developer Adoption
3 videos · 1 year ago




API Design
10 videos · 1 year ago




API Technology
6 videos · 1 year ago




Strategy & Business
19 videos · 1 year ago




API Product Management
8 videos · 1 year ago




API Facade Patterns - Series
8 videos · 1 year ago




About Apigee
22 videos · 2 years ago



API Talks
5 videos · 2 years ago




Free Developer Tools
8 videos · 2 years ago



API Consoles
15 videos · 2 years ago

slideshare.net/apigee



Present Yourself

Search

Upload

Go PRO


0 landlessness ▼



Free eBook: Web API Design
Crafting Interfaces that Developers Love

Download Now ▶


Apigee






Follow


36 SlideShares
78 Followers




PRO


 Palo Alto, CA, United States


 Technology / Software / Internet


 apigee.com  +1 408 343 7300

 We love APIs. Apigee is the leading provider of API products and technology for enterprises and developers. Enterprises use Apigee for visibility, control and scale of their API strategies. Developers use Apigee to learn, explore and develop API-based applications.

 Twitter  Facebook  LinkedIn

 Followers (78)



 video inside.

Big Data - Beyond the 'Bigness' and the Technology





April 26, 2012

Anant Jhingran @jhingran


<http://blog.apigee.com>

<http://jhingran.typepad.com>

Share



1 / 37







Big Data: Beyond the "Bigness" and the Technology (webcast) 506 views

Aniaee Bloa

Presentations

35

- Big Data - Beyond the 'Bigness' and the Technology
April 26, 2012
- Mobile Apps 101
April 26, 2012
- Why APIs
April 26, 2012
- Scaling APIs
April 26, 2012

Documents

0

Videos

1



@Subrak
Subra Kumaraswamy



@mather_tim
Tim Mather

Agenda

- The API security architecture framework
- DevOps in the context of API security
- InfoSec in the context of API security
- API threat protection
- Security analytics: what to expect

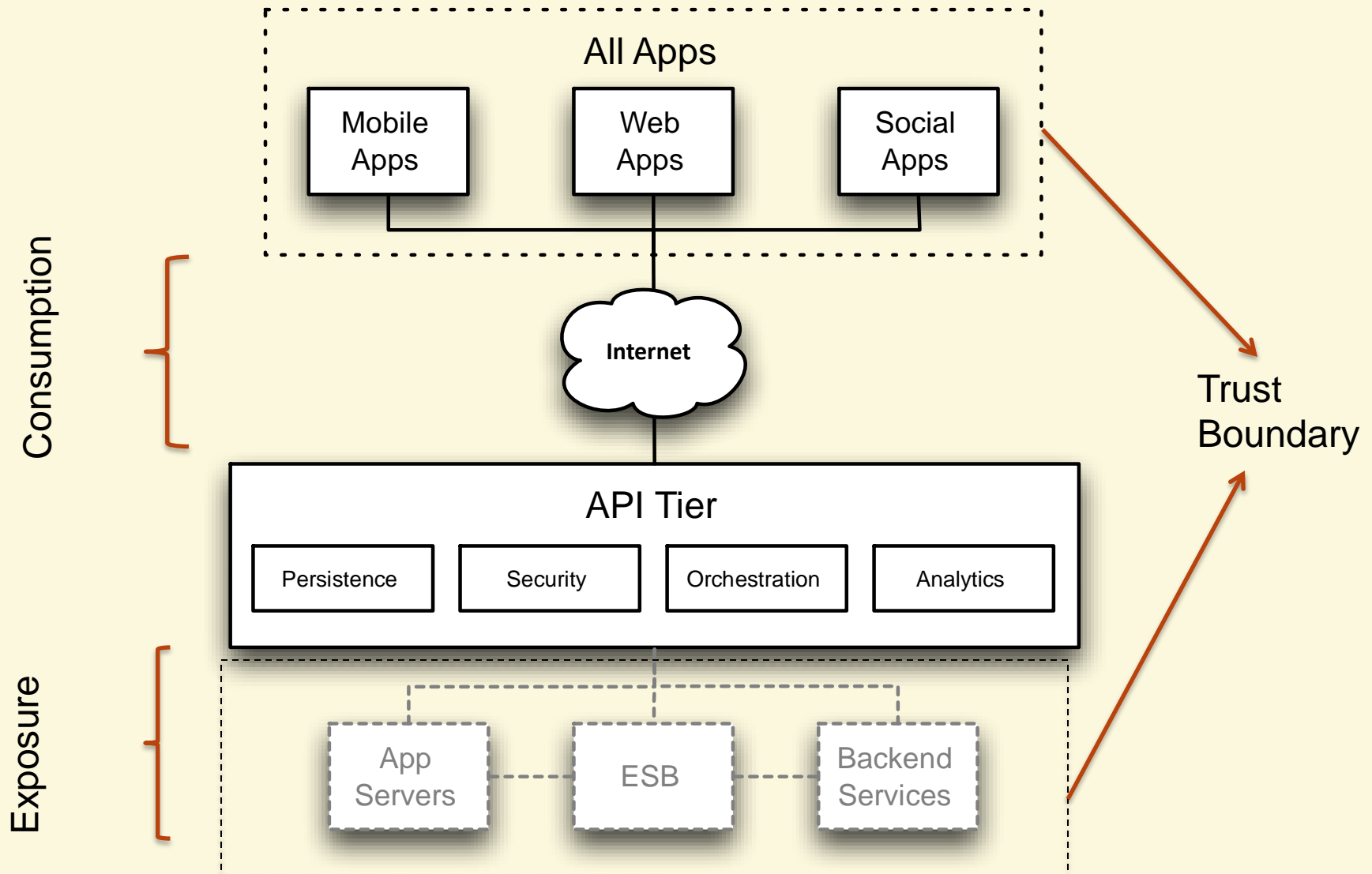
API Security Goals

- End-to-end security managed through configuration
- Security (prevention & detection) integrated into the architecture to limit attack surface
- Flexibility to integrate with external security services
- API and app-centric security for threat protection

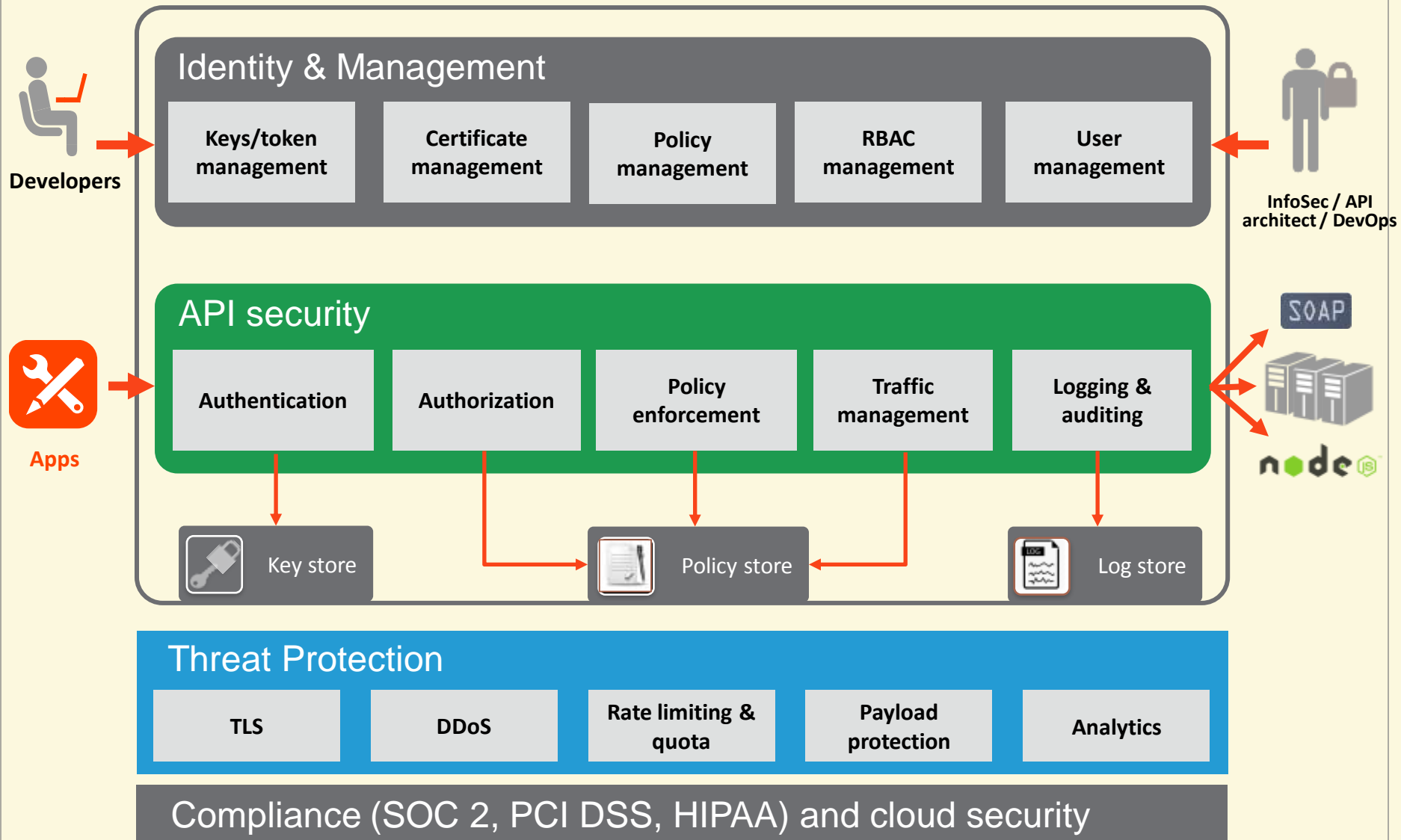
Architecture

Security has to be approached from the API
consumption and exposure perspectives

Security Architecture: Consumption vs. Exposure



Security Architecture



So how does this manifest from an API security capability standpoint?

API management solutions must address the security considerations of various stakeholders and consumers of API

Stakeholders	API Exposure Security	API Consumption Security
DevOps	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
App Developers		<input checked="" type="checkbox"/>
InfoSec	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
API architects	<input checked="" type="checkbox"/>	
Business owner	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
End users		<input checked="" type="checkbox"/>

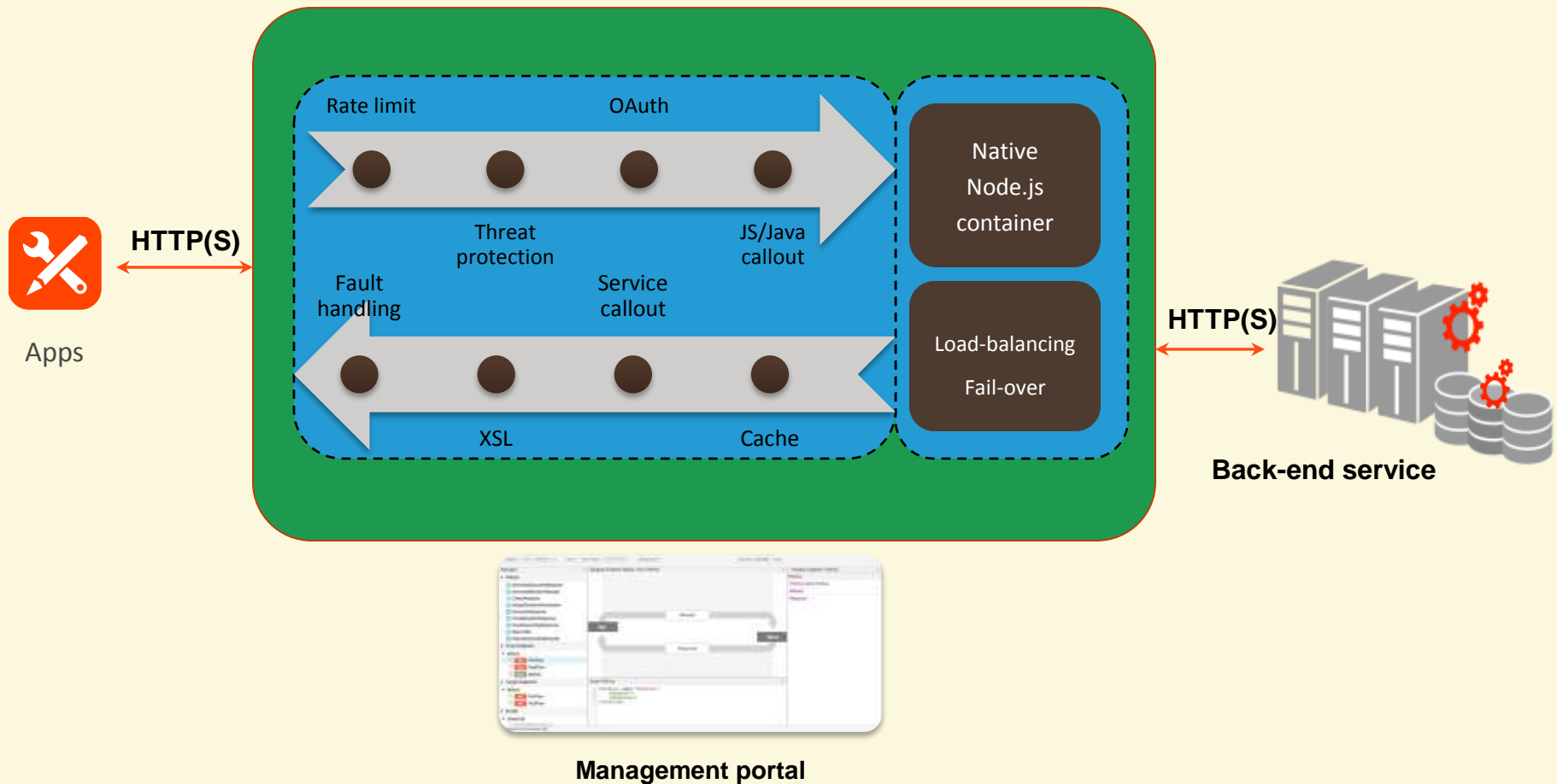
DevOps and Security

The developer (DevOps) needs to create and deploy apps and configure security (not code)

API Security considerations:

- Authentication of developers, apps, and end users
 - API Key protection, Token management
- Fine-grained authorization for apps using API keys, OAuth, and SAML authentication
- Sensitive data in XML / JSON payload protected with encryption
- Self-service capabilities for DevOps function - testing security prior to deployment, promoting code and verifying security configuration

API Service Runtime View



DevOps must be able to choose the authentication and authorization schemes to support app security needs

Authentication & Authorization

Use Case	Authentication	Authorization
B2B	Two-way TLS, API key	OAuth v1 and OAuth v2 policies <ul style="list-style-type: none">Client credentials grant (<i>two-legged OAuth</i>)
Trusted Apps	API key (client credentials), Basic Authentication, IP address	OAuth v1 and OAuth v2 policies <ul style="list-style-type: none">Resource owner password grantImplicit grant with limited permissions
Untrusted Apps	Two-way TLS, OAuth token with Scope OpenID Connect SAML 2.0 Bearer assertion	OAuth v1 and OAuth v2 policies <ul style="list-style-type: none">Authorization code grant (<i>three-legged OAuth</i>)
Identity tracking	Identity-based access tracking policy <ul style="list-style-type: none">Verify API key	

InfoSec

The API architect must be able to securely expose the back-end services with necessary authentication, authorization, message security, and traffic management.

Security considerations:

- Authentication of API services: LDAP, active directory, SAML, OAuth, two-way TLS
- Fine-grained authorization of APIs
- Quota management
- Message security

The information security administrator needs to manage security of data-at-rest and data-in-transit for both API consumption and exposure layers.

Security considerations:

- Configurable security policies to meet organizational standards
- Transport-layer protection using TLS
- Protect sensitive data stored and processed in the API gateway and mobile devices
- User and role management
- Threat management (DoS, spikes, injection attacks)
- Logging and auditing

Information security must be able to manage users (developers, API architect, business users) and privileges (roles) to in turn manage multiple levels of trusted users.

User and Role Management

Scenario	Identity services
User provisioning	Configure fine-grained control of user access to data features and functionality; flexible provisioning and management of users
RBAC management	Employ RBAC at every layer to protect sensitive information, including API keys, TLS certificates, OAuth tokens, and audit logs
Manage groups	Group users based on any number of criteria, including location and interests, to create fine-grained authorization
Identity provider	<p>In general, an API platform must be able to integrate with any identity provider that:</p> <ul style="list-style-type: none">• has an API• supports SAML• supports LDAP v3 (for on-premise only)

Information security must be able to meet governance requirements and manage compliance when handling PCI DSS or HIPAA use cases

Infrastructure & Compliance

Scenario	Infrastructure Security & Compliance
European Data Protection Directive	Safe Harbor program <ul style="list-style-type: none">Registered with U.S. government; Apigee meets the requirements of the European Union Data Directive
SOC 2	Apigee has completed a SOC 2 Type 1 , and will be completing a SOC 2 Type 2 in 2014
PCI-DSS, HIPAA	PCI DSS certified and HIPAA compliance <ul style="list-style-type: none">API in-cloud offering must be PCI DSS Level One certified to protect credit card informationAPI gateway in-cloud must meet a third-party attestation to HIPAA “compliance” to protect personal data and security requirements
API health visibility	Round-the-clock monitoring <ul style="list-style-type: none">Real-time and historic API health visibilityAPI security and compliance trackingComponent and process monitoring

Threat Protection

Types of API Threats

- Spoofing of identity
- Network eavesdropping
- Man-in-the-middle attacks
- Velocity attack using legitimate API calls
- Elevation of privileges by applications and developers
- Data tampering and injection attacks that lead to information disclosure
- Disclosure of confidential data stored and processed in mobile, API, and back-end services
- Theft of credentials: API keys, tokens, or encryption keys

Threat Protection

Scenario	Threat Protection
Denial-of-service (DoS) attack (both inadvertent and deliberate)	Spike arrest <ul style="list-style-type: none">• Protection against instantaneous bursts of traffic Access control <ul style="list-style-type: none">• Imposing limits on who can access your API
Injection and scripting attacks	Configurable protection <ul style="list-style-type: none">• Allows payload scanning for SQL, JavaScript, etc.
XML/JSON threats	XML and JSON threat protection <ul style="list-style-type: none">• Keep malformed payloads out of your system

Example: JSON

Error Code	Message
ExceededContainerDepth	JSONThreatProtection[{0}]:Exceeded container depth at line {1}
ExceededObjectEntryCount	JSONThreatProtection[{0}]: Exceeded object entry count at line {1}
ExceededArrayElementCount	JSONThreatProtection[{0}]: Exceeded array element count at line {1}
ExceededObjectEntryNameLength	JSONThreatProtection[{0}]: Exceeded object entry name length at line {1}
ExceededStringValueLength	JSONThreatProtection[{0}]: Exceeded string value length at line {1}
SourceUnavailable	JSONThreatProtection[{0}]:: Source {1} is not available
NonMessageVariable	JSONThreatProtection[{0}]: Variable {1} does not resolve to a Message
ExecutionFailed	JSONThreatProtection[{0}]: Execution failed. reason: {1}

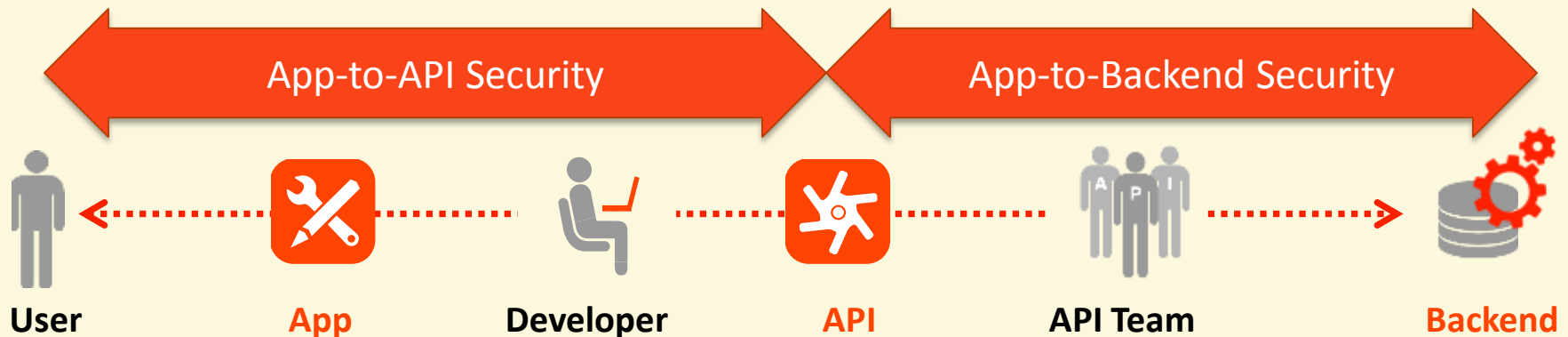
Security Analytics

Security Analytics

- Start with operational events such as runtime events
- Correlate against volume information such as quotas and spikes
- Correlate with threat protection information, such as attempted poisoning and injection attacks
- Correlate against security sensor data; effectively using your API management platform as a security sensor unto itself

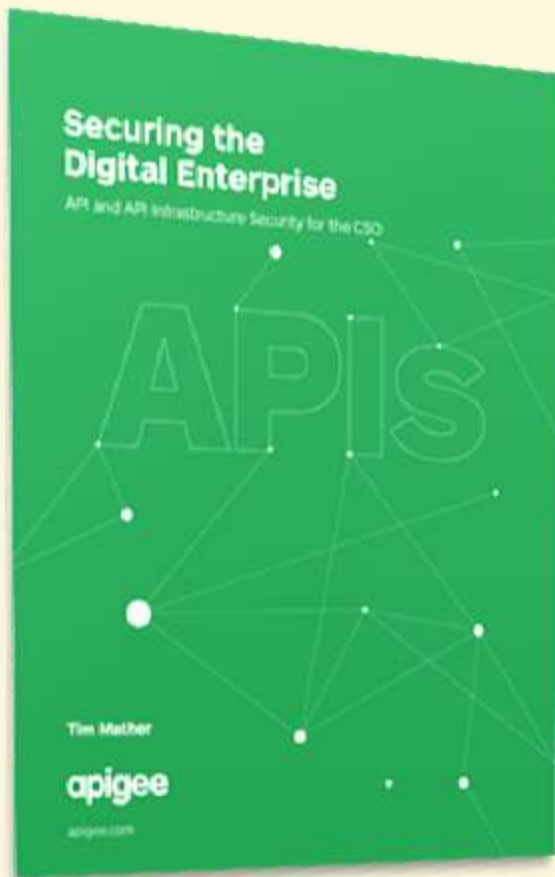
Top considerations and takeaways

- End-2-end security architecture includes consumption and exposure of APIs
- DevOps (need for speed, flexibility) and InfoSec (need for consistent protection) go hand in hand
- Agility, speed, and scale with security through configuration, not coding



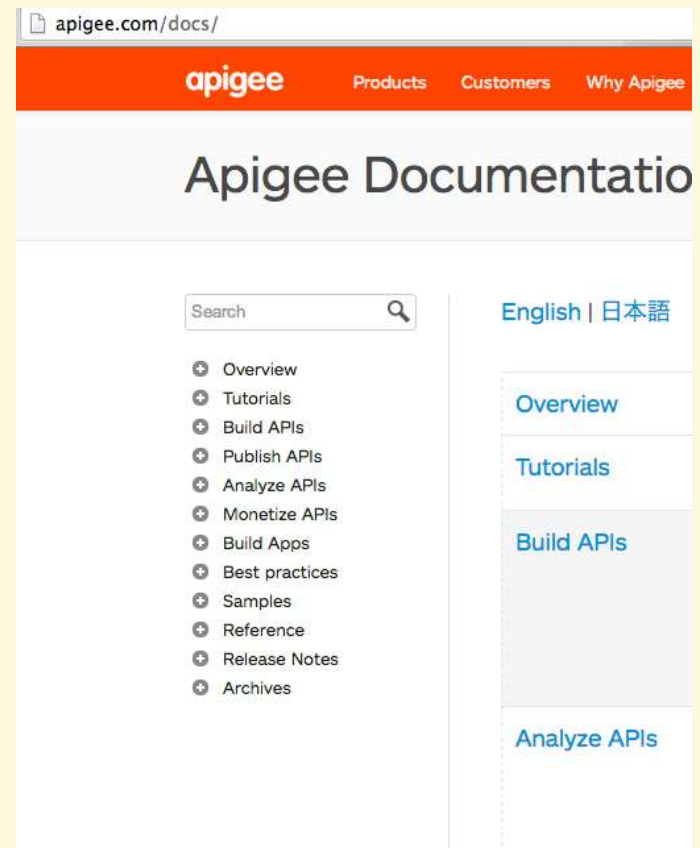
Download eBook:

<http://bit.ly/1hxcavY>



See Apigee docs:

<http://apigee.com/docs>



Questions?



@Subrak
Subra Kumaraswamy



@mather_tim
Tim Mather

Thank You