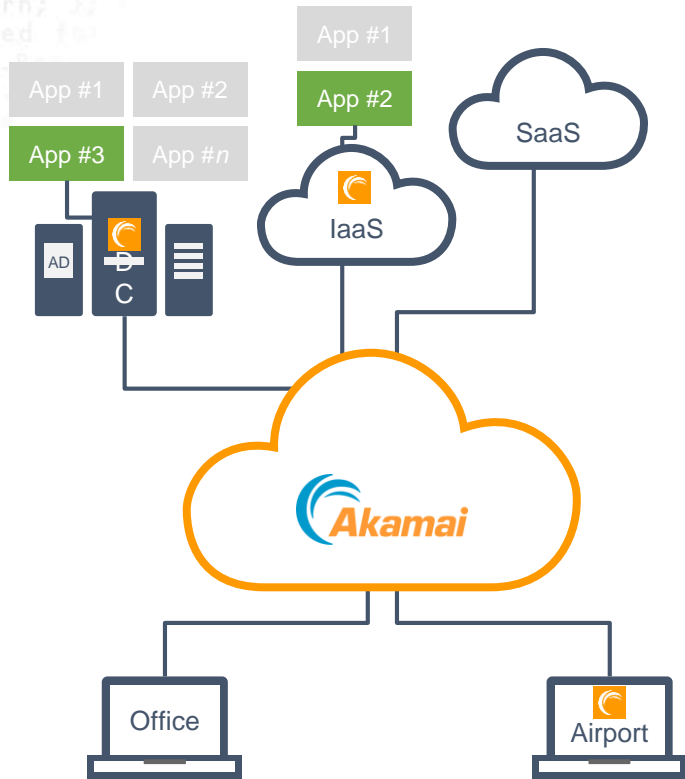


Moving Beyond Perimeter Security With Akamai



Intelligent Security Starts at the Edge

Enterprise Application Access



Adaptive app access through an Identity Aware Proxy at the Edge

- Inline app access
 - Client & clientless
 - On-prem & IaaS
- Identity & single sign-on
 - Akamai, on-prem or cloud based identity stores
 - On-prem, IaaS & SaaS
- Multi-factor authentication
 - Email, SMS, TOTP or Duo Security
- App access based on risk
 - Device security posture incl. ETP & Carbon Black

Isolated From The Internet & Always Verified

12:19
Akamai
Phone-w iPhone

- ✓ **iOS version 13.1.1 is up to date**
Great! Keeping your operating system version up to date ensures that your device has the latest security fixes.
- ✓ **EAA Client version 0.94 is up to date**
Great! Keeping the EAA Client version up to date ensures you have the latest security checks for your device.
- ✓ **Face ID is enabled.**
Great! Face ID is enabled. This keeps your device secure from others.
- ✓ **Screen lock is enabled.**
Great! A device passcode (screen lock) helps keep your device private from others.

Welcome To Akamai IDP User Portal
charlie@secperimeter.com
LOG IN

Enter authentication code
Please provide a valid authentication code from your mobile app.
Authentication code
VERIFY
Remember me
Click here to receive codes another way

Certificate Standard

10:54
portal.secperimeter.com
Akamai charli...

ATLASSIA... CONTACTS

Dropbox G Suite

DROPBOX G-SUITE

SharePoint Office 365

KERBEROS... OFFICE365

Windows Server salesforce

Launch Instance Connect Actions

search: 10.10.10.177 Add filter

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status
EAA_Connector_PrivateSubnet	i-2692630	m3.medium	us-east-1a	running	2/2 checks ...	None

Instance: [i-2692630 (EAA_Connector_PrivateSubnet) Private IP: 10.10.10.177

Description	Status Checks	Monitoring	Tags
Instance ID	i-2692630		
Instance state	running		
Instance type	m3.medium		
Elastic IPs			
Availability zone	us-east-1a		
Security groups	Cloud/PrivateSub-SPBEXM2Q8VX	view inbound rules	
Scheduled events	No scheduled events		
AMI ID	Cannot load details for ami-7bc20310. You may not be permitted to view it.		
Platform			
IAM role			
Key pair name			
Public DNS (IPv4)			vpc-ecb709d9
IPv4 Public IP			subnet-H257083
IPv6 IPs			
Private DNS			ip-10-10-10-177.ec2.internal
Private IPs			10.10.10.177
Secondary private IPs			

Public DNS (IPv4) -
IPv4 Public IP -
IPv6 IPs -
Private DNS ip-10-10-10-177.ec2.internal
Private IPs 10.10.10.177
Secondary private IPs

App Access & Service Insertion



Web Application
Firewall



DDoS
Mitigation

Protect apps & APIs from DDoS,
exploits & misuse



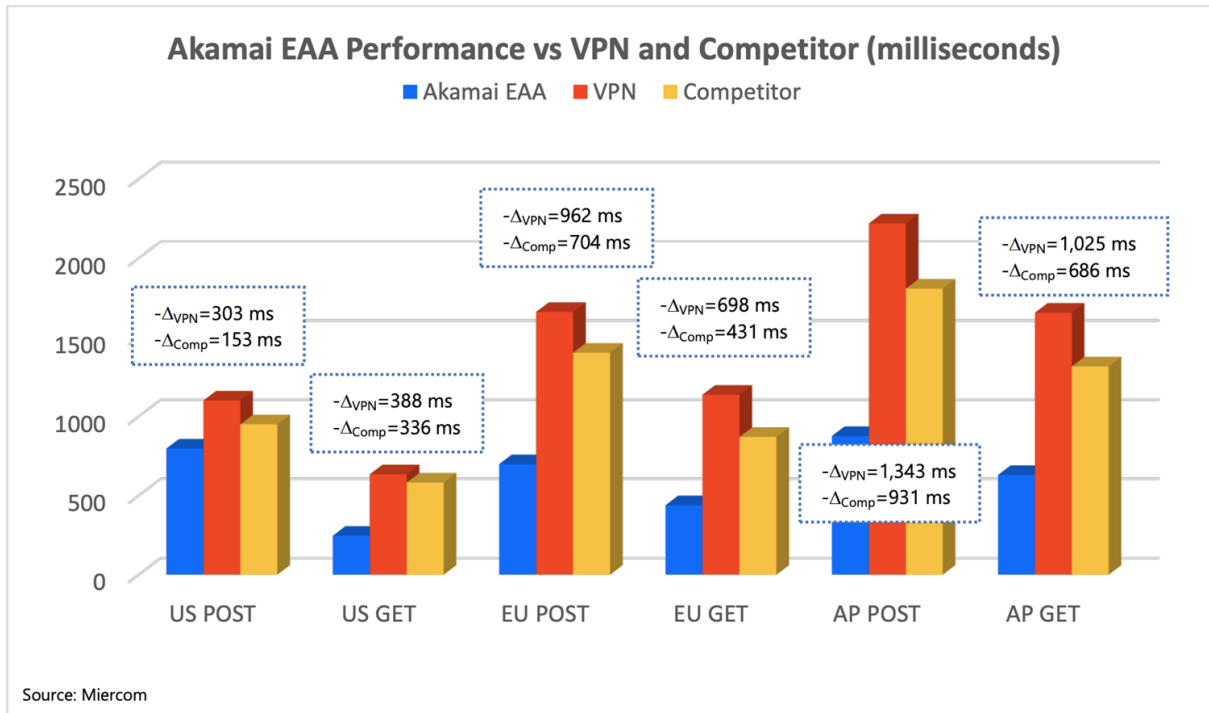
Application
Acceleration



Global Traffic
Management

Provide fast & reliable corporate apps
to end users

Better Enterprise App Experiences



App Access Use Cases



Secure access to
cloud apps



Mergers &
acquisitions



Secure 3rd party
app access



Traditional VPN
elimination



Intelligent Security Starts at the Edge

Adaptive App Access Based On Risk

Identity & contextual signals

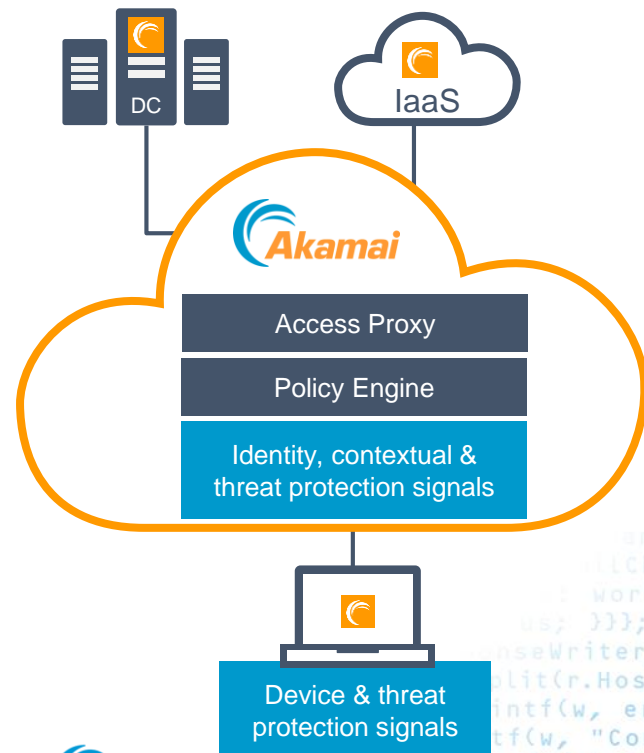
- Time of day, location, specific URL & HTTP method, user agent string, etc.
- Authentication state, group membership, etc.

Device signals

- Presence/validity of client certificate
- OS details (version, auto update, disk encryption, firewall status, etc.)

Threat protection signals

- 3rd party signal from EDRs like Carbon Black
- Akamai signal from Enterprise Threat Protector



Contextual & Adaptive Access Protection

Adaptive access per app based on identity, threat protection & device signals

- Time of day
- Location (from IP seen by IAP)
- Specific URL & HTTP method
- User agent string from browser
- User authentication state
- Group membership of user
- Presence/validity of client certificate
- Device posture including OS APIs & 3rd party client signals (e.g. Carbon Black)
- Advanced threat detection signal from Akamai Enterprise Threat Protector



Device Signal Details

Device Details

Device Id: 0a1501c990f321fda4b9c7fae38848f97c3834253d7d3566ec14cf948860ea37

DETAILS POSTURE

User Id	N/A
Device Name	DESKTOP-9LSUOEF
Client Version	0.1.3
Operating System	Microsoft Windows 10 Enterprise
OS Version	10.0.17134.590
OS Auto Update Status	Enabled
OS Last Update Time	Feb 12th 2019, 18:00 (EDT)
Disk Encryption	Disabled
Installed Browser(s)	Edge (42.17134.1.0) Chrome (72.0.3626.121) Internet Explorer (11.590.17134.0)
Anti-malware	Windows Defender
Anti-malware Status	Good
Firewall Status	Good
Signal Update Time	Mar 9th 2019, 17:07 (EDT)

Close

- Identifiers
 - Akamai unique device ID
 - Logged in user ID, machine name
- OS details
 - Platform and version info
 - OS auto update enablement status and last OS update time
- Disk encryption
 - Encryption status of the OS partition user is logged in to
- Installed web browser versions
 - Chrome, Firefox, Safari, Internet Explorer, Edge
- Firewall and anti-malware status
 - Status of OS built in firewall
 - Anti-malware as detected by Windows, or predefined software list on macOS
- Signal update time
 - Timestamp of last signal update from the device posture client
 - Expected 30 minute update interval for an online client
 - More often if signal changes are detected

Risk Tiers

- Low, medium, high risk
 - Hierarchical (if not low, checks med, etc)
 - Select OS and signal criteria
 - Total device count per tier (clickable to display details)
- Config Preview
 - Tiers re-calculated before saving
 - Evaluate impact on devices before saving

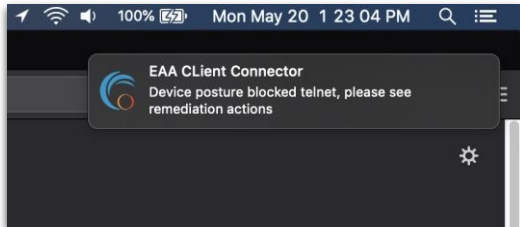
The screenshot displays the Risk Tiers configuration interface. It is divided into three horizontal sections: Low, Medium, and High risk tiers. The Low tier is currently selected and shows 104 devices. The Medium tier shows 441 devices, and the High tier shows 4657 devices. A dialog box titled 'Save Device Posture Rule' is overlaid on the right side, asking if the user wants to save the rule and showing the recalculated device counts for each tier: Low (104 + 22 devices), Medium (441 - 22 devices), and High (4657 devices).

Risk Tier	Device Count
Low	104 (+ 22) devices
Medium	441 (- 22) devices
High	4657 devices

Remediation - Client Apps

- Remediation info for client connector apps
 - Why was access denied?
 - Basic remediation steps
 - OS notifications
 - Enable self service for end users
 - Reduce support burden

- Client signal status
 - Reflects latest values
 - Last update time to EAA

A screenshot of the EAA Client Connector Settings web interface. The page title is "EAA Client Connector Settings". The user is logged in as "device-posture@akamai.com". The device is identified as "9d00f...2075c" on a "Mac" OS. The status is "Connected". The "Remediation" tab is active, showing a list of blocked applications. Below the list, there is a table with columns for "Timestamp", "Process", "Hostname", and "Signals that require attention".

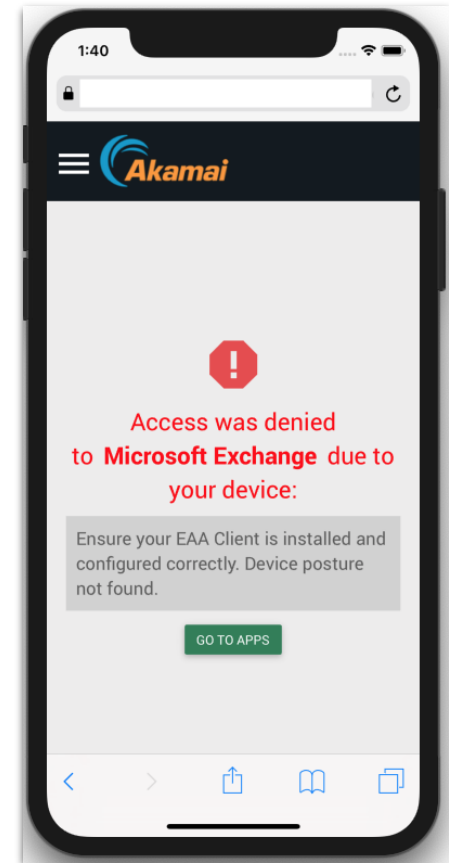
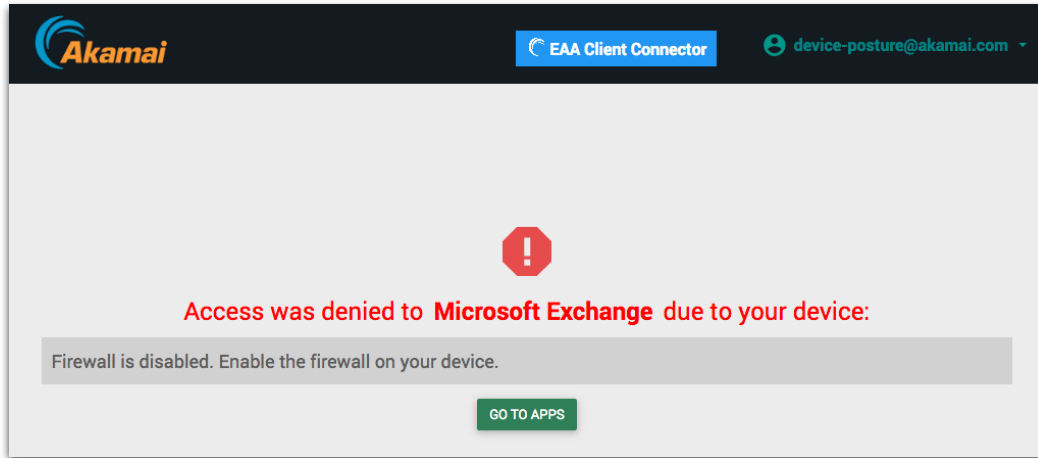
Timestamp	Process	Hostname	Signals that require attention
05/15/2019 11:32:54 AM	telnet	miami.craigslislist.org	▼ Unsupported operating system. 1. Unsupported operating system.
05/15/2019 11:28:47 AM	telnet	sf.craigslislist.org	▶ Unsupported operating system. (1)

A screenshot of the EAA Client Connector Settings web interface. The page title is "EAA Client Connector Settings". The user is logged in as "device-posture@akamai.com". The device is identified as "9d00f...2075c" on a "Mac" OS. The status is "Not Authenticated". The "Signals" tab is active, showing a list of system signals. The "Signal Update Time" is "5/16/2019, 9:59:27 AM".

Signal Update Time:	5/16/2019, 9:59:27 AM
Anti-malware Status:	Good
Installed Browser(s):	Chrome (v74.0.3729.157), Safari (v12.0.3)
Client Version:	0.1.4
Firewall Status:	Good
OS Version:	10.14.3
Disk Encryption:	True
User Id:	saurabhs

Remediation - Web Apps

- Remediation info for web apps
 - Why was access denied?
 - Basic remediation steps
 - Enable self service for end users
 - Reduce support burden



Device Posture Dashboard

- Device risk & activity at a glance
 - Device activity based on signal updates from device posture client
- Device signal breakdown
- Interactive graphs
 - Clickable to view device inventory details

