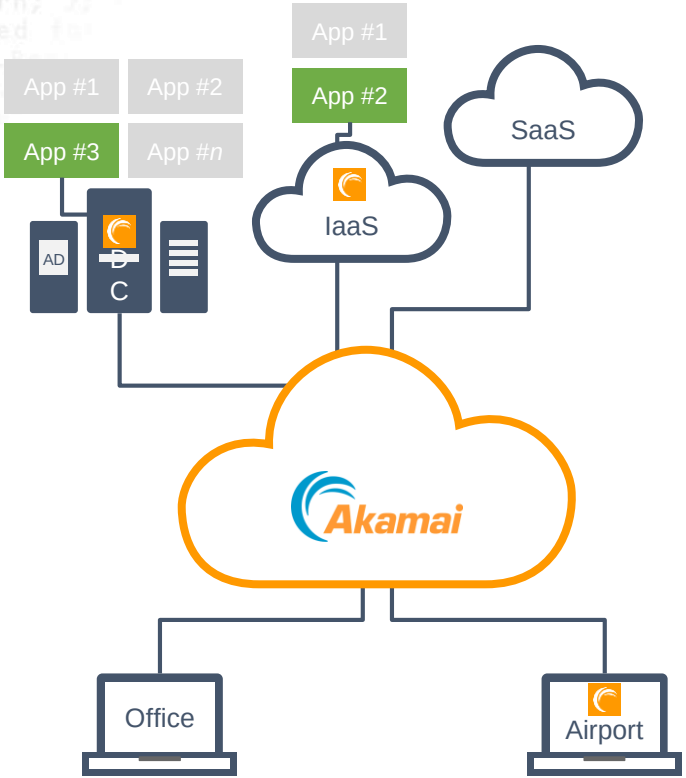
Moving Beyond Perimeter Security With Akamai

Intelligent Security Starts at the Edge

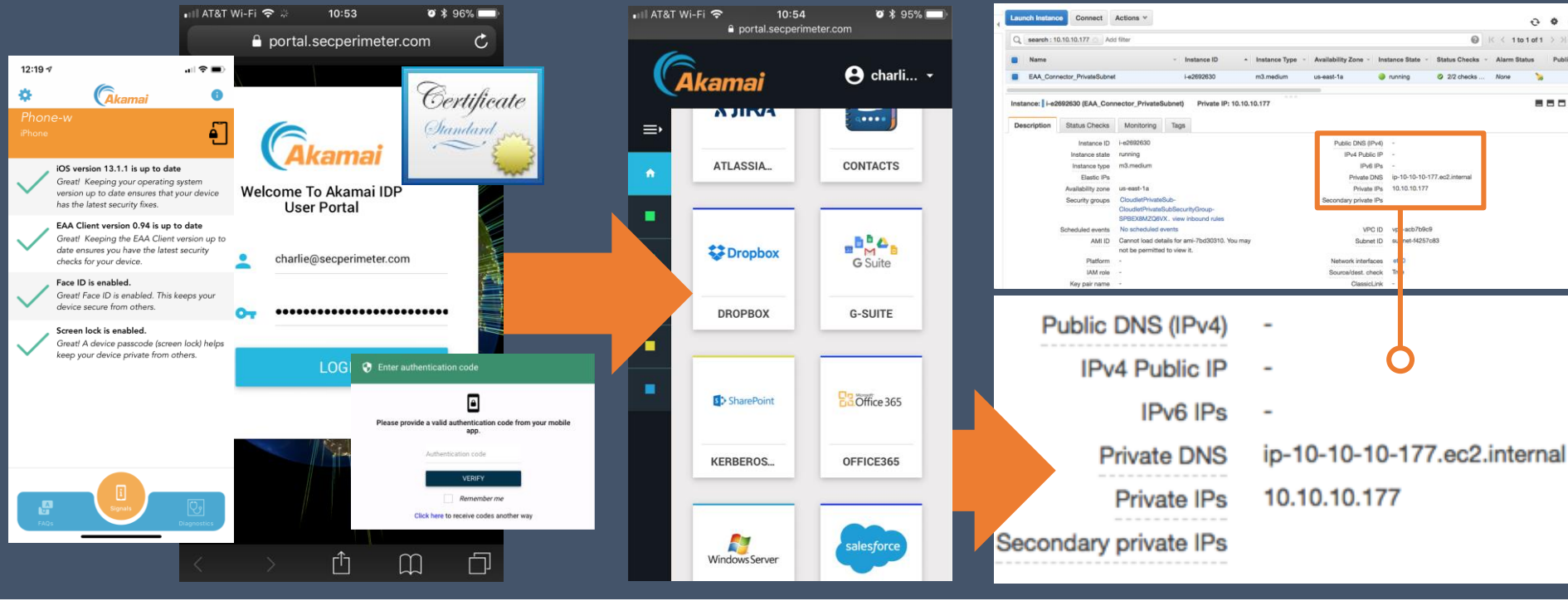
Enterprise Application Access



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



App Access & Service Insertion

Web Application Firewall

DDoS Mitigation

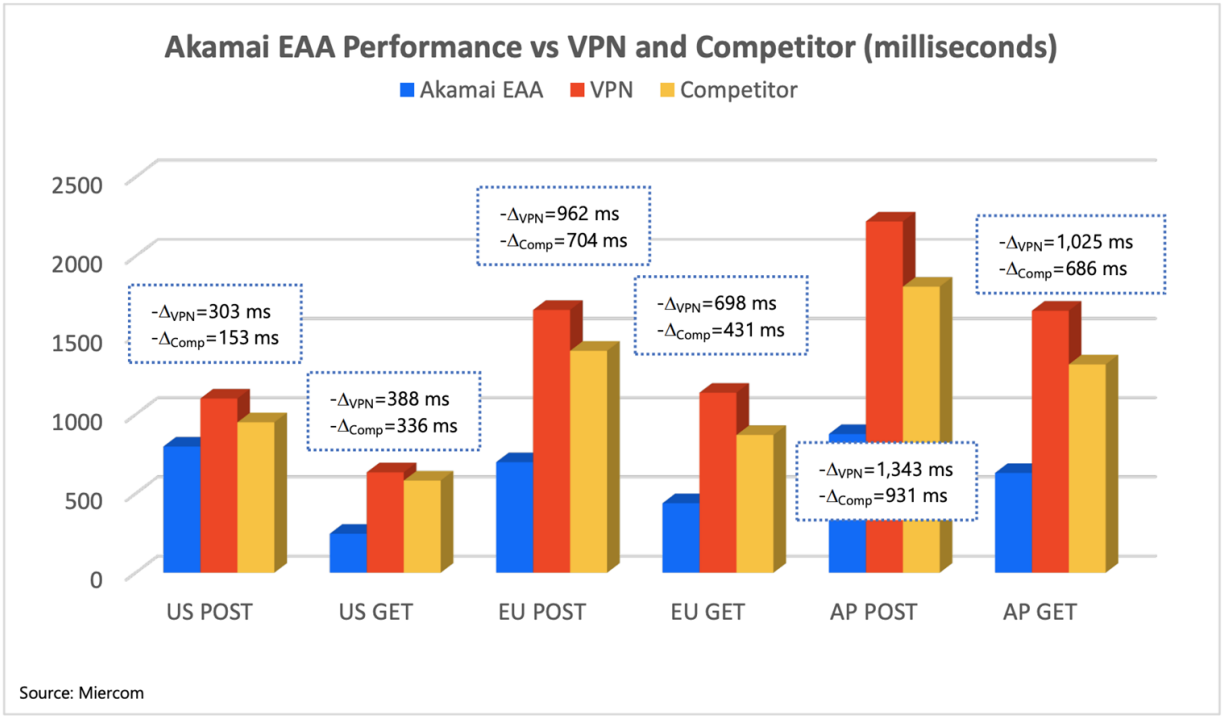
Protect apps & APIs from DDoS, exploits & misuse

Application Acceleration

Global Traffic Management

Provide fast & reliable corporate apps to end users

Better Enterprise App Experiences



Source: Miercom

App Access Use Cases

Secure access to cloud apps

Mergers & acquisitions

Secure 3rd party app access

Traditional VPN elimination

Adaptive App Access Based On Risk

Identity & contextual signals

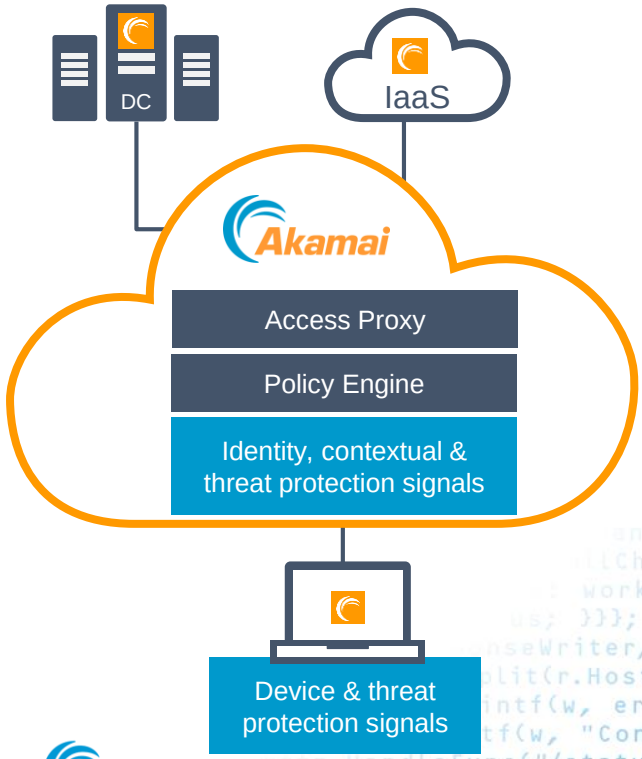
- Time of day, location, specific URL & HTTP method, user agent string, etc.
- Authentication state, group membership, etc.

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

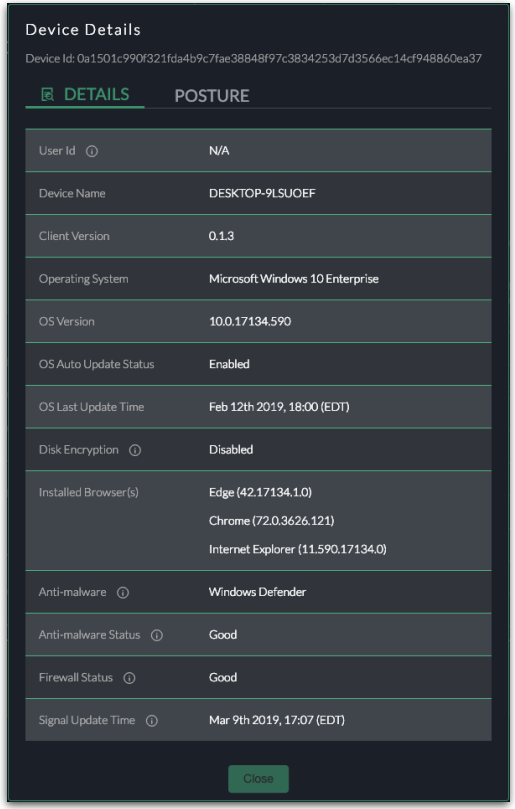


Contextual & Adaptive Access Protection

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

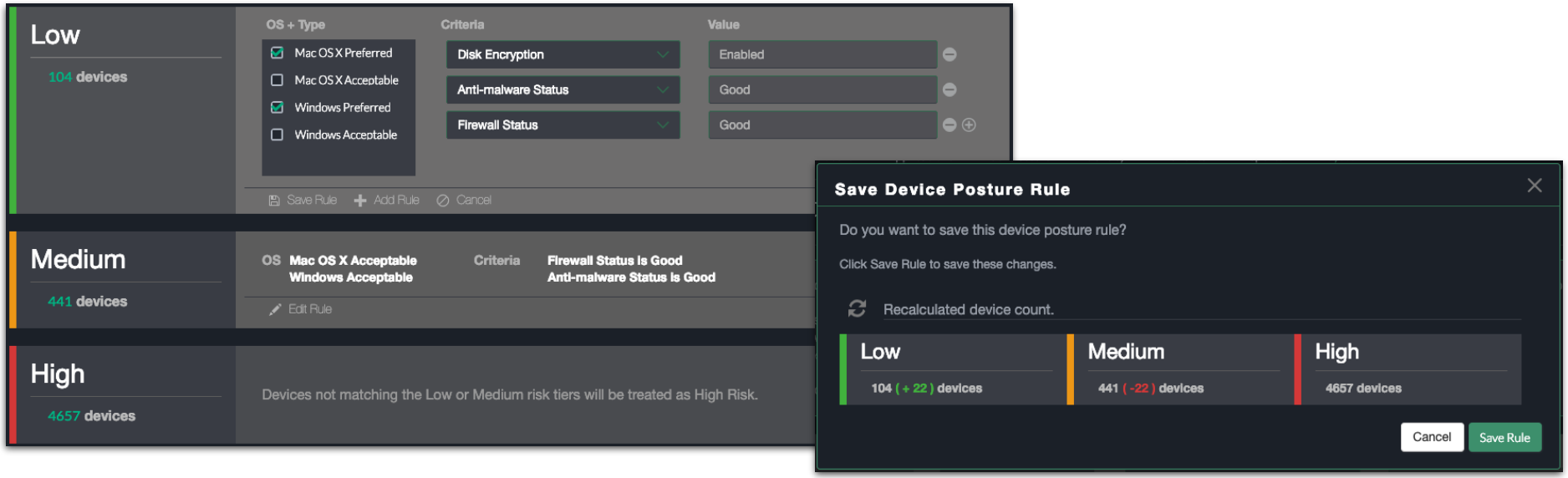
Device Signal Details



- 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

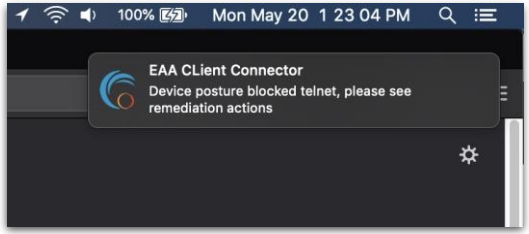
- Low, medium, high risk
  - Hierarchical (if not low, checks med, etc)
  - Select OS and signal criteria
  - Total device count per tier (clickable to display details)
- Config Preview
  - Tiers re-calculated before saving
  - Evaluate impact on devices before saving

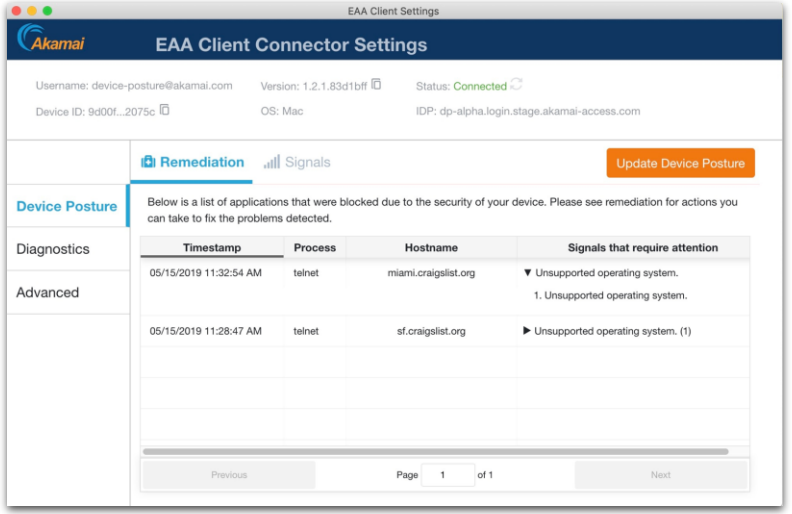


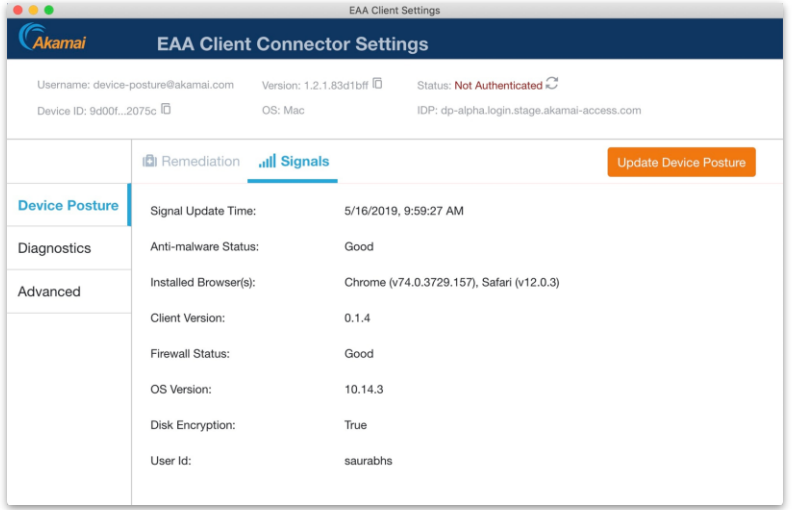
Remediation - Client Apps

- 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

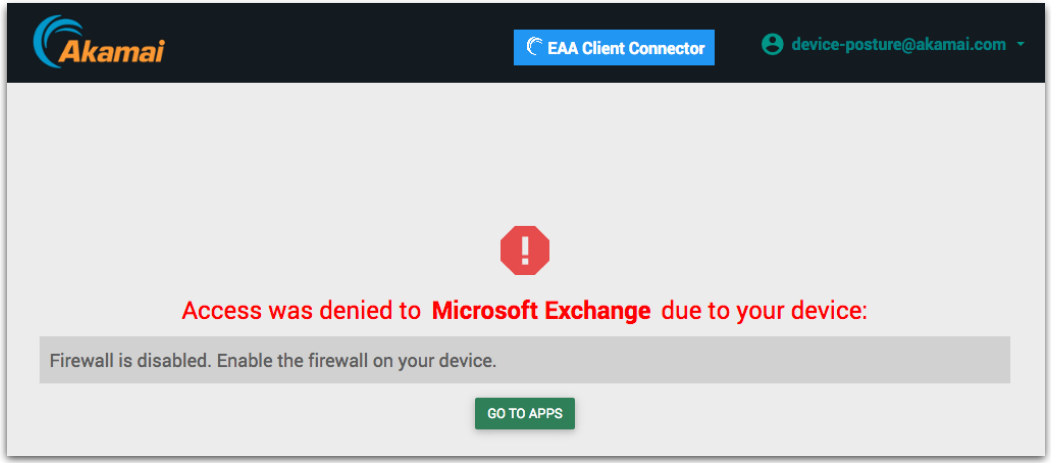


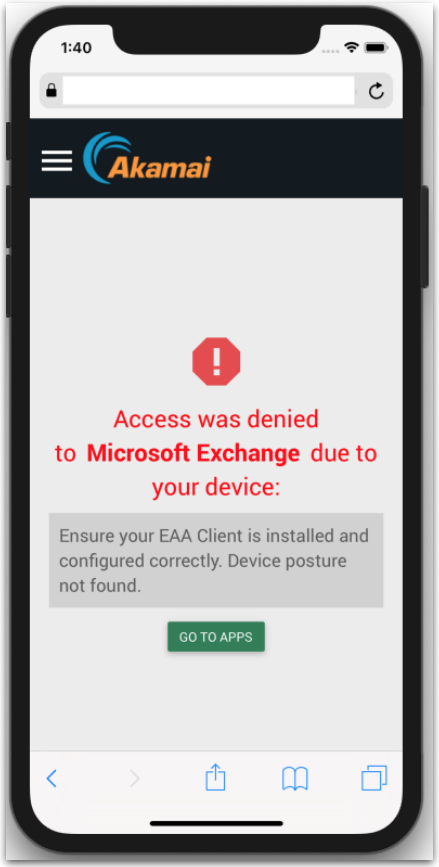




Remediation - Web Apps

- 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