ACDN Enterprise Application Access

Competitive Assessment

4 January 2018

DR180615H

Miercom
www.miercom.com

Contents

1.0 Executive Summary

Internal Business communications contain sensitive information vulnerable to attacks from internal users accessing corporate network data. Traditionally, companies use virtual private networking (VPN), a client-server tunneling architecture to securely pass information to and from a remote endpoint. This was vital for applications hosted anywhere and for users who need to access these applications from any location. This can be useful for a handful of applications, but for an enterprise this is complex and costly. Shifting to a security model that limits lateral movement across the network significantly reduces the attack surface and can help solve the issue of complexity and security.

An enterprise application may be for employees only, developers, or for third-parties such as contractors or consultants. Third-party access is one of the largest attack vectors used for internal network data breaches. This has created a climate where the vast majority of data breaches are occurring as a result of trust being abused inside the network by actors who have gained approved access in the perimeter. Threats are moving inside the trusted network and internal applications are attacked from "trusted sources" by overly privileged access. It requires an ongoing set of security exceptions to be made, creating a demilitarized zone prone to breaches that severely impact the enterprise.

ACDN Enterprise Application Access (EAA) solves this problem by offering application access as a service in the cloud. Inbound access to the network – even with the best designed networks – requires many network and application components to accomplish what ACDN accomplishes with a globally distributed identity-aware proxy platform in the cloud. Instead of the traditional, complex setup where hardware and software components require costly and time-consuming maintenance and setup, ACDN provides an extensible cloud service for secure application access control.

AT&T engaged Miercom to independently assess and compare the ACDN EAA solution to a competitive product for application access features, user experience and performance. For the performance section only, the ACDN EAA solution was compared to both its competitor and a VPN. The following key findings from our testing highlight the features of the ACDN EAA solution.

Key Findings of the ACDN Enterprise Application Access Solution

- **Simple Deployment.** Easy setup for connecting applications, free of the complexity and configuration changes required with its competitor's product.
- **Flexible Directory Integration and Authentication Bridging.** Does not require an external identity provider, imports specific group users through a single tab and includes authentication bridging between modern and legacy authentication protocols (NTLM, Kerberos). Supports any user count; for this report functional validation is performed for 3,000 Active Directory users.
- **Abundant, Simple Configuration Options.** Unlike its competition, there are many configuration options available – including tailored default templates with simple, one-click login for advanced access control and authentication setup. EAA also offers advanced configuration options for more flexible deployment with support for multi-factor authentication.

- **Seamless Compatibility.** Excels at Single Sign-On (SSO), using a unified design that accomplishes the functionality of multiple products entirely in one solution; for example, SAML authentication can be configured to allow custom attribute mapping for versatile deployment. In addition, SSO can also be configured across on-premises, IaaS, and SaaS applications offering a centralized point of control to organizations.
- **Independence from Identity Provider.** While its competitor requires an identity provider (IdP), EAA has a native IdP, can integrate with multiple IdPs, such as Okta, and bridge with legacy authentication methods (NTLM, Kerberos).
- **Enhanced Performance.** With enhanced performance capability enabled, ACDN showed as much as 263% faster HTTP GET and 253% faster HTTP POST times for access to a US server from the US, EU and AP.
- **Innovative Load Balancing.** Round Robin and IP Hash methods actively load balance application traffic for even distribution within one percent of multiple front-end application servers.
- **High Value, Low Cost.** Eliminates the complexity and cost of VPN, providing a benefit of up to $380,475 over the course of a three-year deployment.

The ACDN Enterprise Application Access service was validated as a user-friendly, consolidated suite of robust functionality for application access control, monitoring, security and remediation – outperforming its competitor. Based on our findings, we proudly award the ACDN Enterprise Application Access product the ***Miercom Performance Verified*** certification.

Robert Smithers

CEO

Miercom

2.0 Product Overview

Most data breaches occur because of unsecured third-party network access or because the network perimeter was breached from lateral movement, and data was exfiltrated. Not all applications on the network should be accessible to every end user. Controlling access via an identity-aware proxy allows remote employees, third-party contractors, vendors and developers to gain access to necessary applications by verifying user identity and context to determine if they have the authorization to access an application. It allows granular access control on a per-app basis without allowing full network access once authorized.

ACDN Enterprise Application Access (EAA) *Summer 2018 Release*

Fortunately, ACDN understands the gravity of digital transformation and can seamlessly accommodate applications with a configurable connector for any environment.

With the Luna Control Center, the ACDN EAA solution gives customers a unique, centralized control over administrative actions, end user activity, experience and performance that goes beyond a traditional VPN solution.

EAA Admin Console in Luna Control Center

The EAA Console in Luna Control Center allows management, analysis and remediation via web, mobile and API platforms.

This self-guided service provides actionable insight through an intuitive interface, along with ACDN support to help customers access training, open tickets, and contact the technical support team for assistance.

Source: ACDN

The Luna Control Center and the EAA Admin Console include the following capabilities:

- **EAA dashboard** is a single pane-of-glass of how users and devices are accessing applications. Including multiple widgets: assets health, browser/OS, access map, activity, login failures users and activity feed.
- **Application configuration manager** allows customers to independently create, modify and deploy application configurations through a single page. It also provides rule templates, contextual help and debugging capabilities, in addition to providing a single pane-of-glass for monitoring usage and access across all applications made accessible through EAA.
- **Identity** section helps to organize directories and identity providers, built-in or third-party.
- **Connectors** allow to create/delete/monitor connectors.
- **System** allows to configure shared elements such as certificate, API/SDK access keys.
- **Reporting** is a visual, interactive display that gives customers a detailed account of access activity and an overview of metrics (e.g. traffic volume, links, errors). Reports can be exported or consumed with corresponding API for sharing with other business team members for further analysis.
- **Luna Resolve** gives real-time remediation with customizable alerts and predictive notifications based on traffic trends.

Performance Features

For those applications where performance is critical, additional performance-enhancing features can be applied. ACDN has deployed a highly-distributed infrastructure with hundreds of thousands of servers in over 110 countries in 1,400+ networks. This network includes features that enable faster performance, such as Internet route optimization and edge caching, that wouldn't be possible without the breadth and scale of the ACDN Intelligent Platform. Customers can expect faster performance for applications.

Competitors

The following competitors claim to offer similar capabilities for secure enterprise access to applications and websites:

- Centrify
- Cyxtera
- Duo Beyond
- F5 Big IP Cloud Edition
- Secure Link Enterprise
- Zscaler Private Access

In this testing, the ACDN product is compared to another leading test solution. Due to End User License Agreement (EULA) restrictions, the other product will be masked from this report.

3.0 Testbed Overview

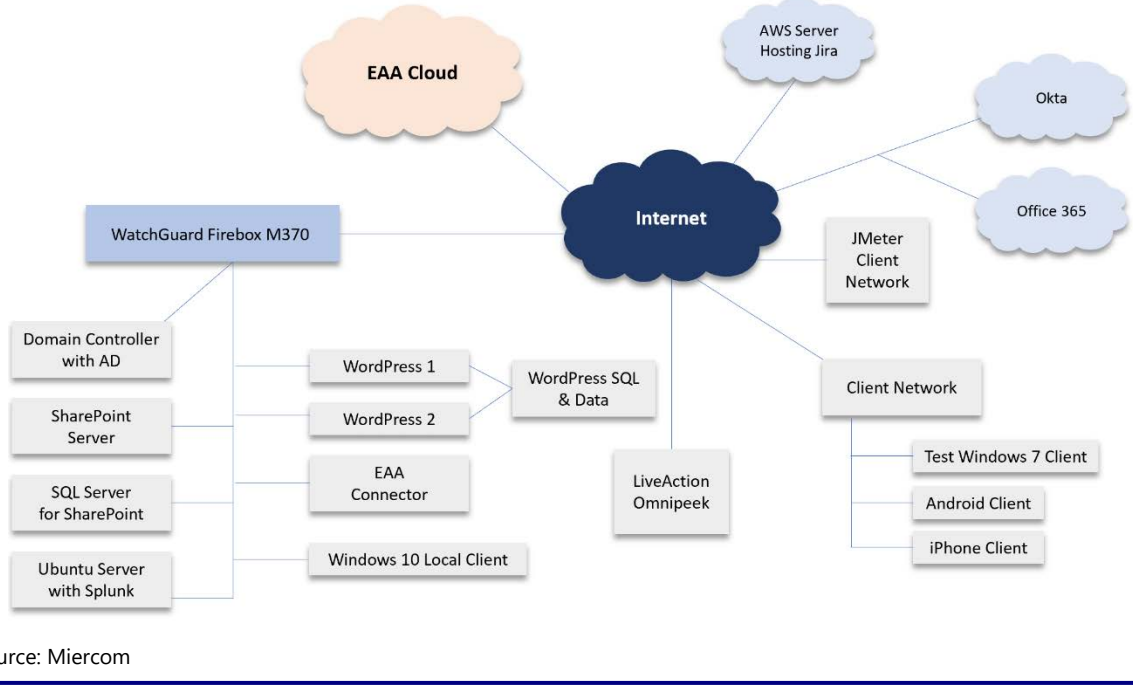
Using test case scenarios, Miercom engineers examined the ACDN EAA cloud service and compared its results to a competing vendor based on product setup, configuration, compatibility and end user experience. Functionality was observed and recorded for strengths and opportunities for improvement in future releases.

The ACDN EAA product was further examined for its product differentiators, to highlight the unique ways it outperformed a similar product in its industry. Lastly, the ACDN product was valued using a cost-benefit analysis in our Total Cost of Ownership grid. This Impact Analysis Grid weights the objective and subjective benefits of a product with respect to its cost of ownership over the course of one year. ACDN's vision is to provide the same level – or better – service as its competition for a fraction of the price.

3.1 Test Bed Architecture

Miercom's hands-on testing replicates realistic environments to challenge and provide an accurate assessment of a product's functionality. Our test methods, tools and observations of each Software Under Test (SUT) are detailed in the remainder of this report. Testing is hosted at Miercom's New Jersey lab.

Test Bed Architecture



Source: Miercom

The test bed shown above depicts the setup used to simulate a basic corporate infrastructure.

The basic functionality of the SUT was tested using the following components: an onsite Active Directory, a single instance of SharePoint, a local Ubuntu server with a single server deployment of Splunk, a local intranet site, Office 365, and an Amazon cloud server running Jira.

The server hosting the SUT connectors utilized VMware ESXi v5.5 with vCenter. The internal network is configured behind a WatchGuard M370 UTM. The VPN over SSL functionality of this product was used when comparing the SUT to a traditional VPN. The VPN access is not segmented and provides full access to the internal network.

Test Tools

LiveAction Omnipeek *Version 11.1.1*

Captures network traffic and creates packet files for replay. Statistics can help monitor changes in real-time. By baselining normal activity, changes can be observed to analyze problem areas in the network.

Apache JMeter *Version 4.0*

Java application software to test performance and behavior of web applications and product functionality.

4.0 Product Setup

ACDN EAA and its competitor were assessed for system and integration capabilities for the following:

- Connector Setup
- Active Directory (AD) Integration/Identity Provider (IdP) Assignment

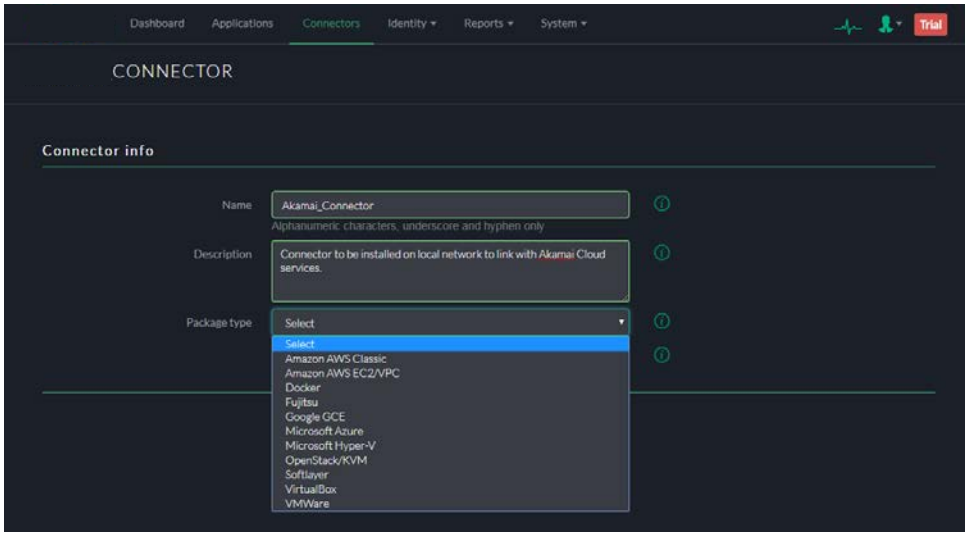
4.1 Connector Setup

ACDN EAA

One of the first required actions for setup is connector creation and installation. Installation is a similar process among products, but notable differences will be highlighted in our findings.

The ACDN EAA setup is easy, beginning in the Luna Control Center. Once the product has been purchased, this location is accessible to the end user for navigating the EAA configuration page and additional ACDN products, such as ION or the Kona Security package.

The connector requires only the user name and platform to get started, with other available platforms visible as shown below. The default connector sizing is 4 vCPU and 8GB RAM.



Source: Miercom

This image shows the setup page used when creating a connector. After entering a name, the user can choose between formats – Amazon AWS, Docker, Fujitsu, Google GCE, Microsoft Azure, Microsoft Hyper-V, OpenStack/KVM, Softlayer, VirtualBox and VMware.

The VMware connector was created, downloaded and imported into the respective host machine in New Jersey. Once the product was initialized, it automatically reached out to the ACDN Cloud to connect.

The competitor's setup is similar – the connector can be downloaded in the following formats: VMware, Red Hat Linux, Amazon AWS, Oracle Linux, CentOS, and Microsoft Azure. As with ACDN, the VMware connector download was used, but had a few extra steps, causing deployment to take 40% longer than EAA. This also added complexity to the setup as it was imported. The competitor requires an API key and basic alterations to the imported VM settings to deploy the connector. This process is well documented in VMware deployment help resources provided by the competitor. Changes include basic VM configuration alterations before initialization and entry of the API key.

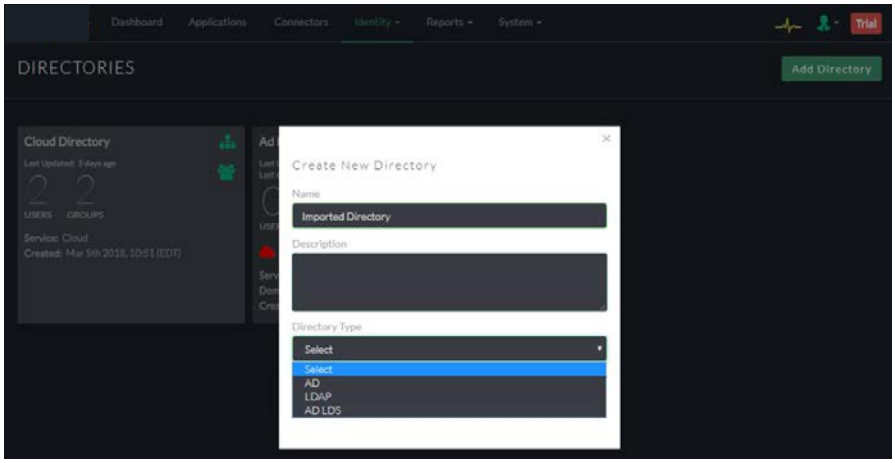
4.2 Directory Integration

ACDN EAA

ACDN can integrate with Active Directory (AD), OpenLDAP and AD-LDS base directories. The next configuration step taken for the ACDN product was the integration to the local instance of the AD. The AD integration was set up through a single tab, requiring the following:

- Host information
- Domain information
- Account information
- Login preferences for EAA application access

After configuring the AD settings, groups could be imported using the Group tab. This allows the end user to import users from specific groups.



Source: Miercom

ACDN EAA allows users from specific groups to be imported using the Group tab. Its competitor does not offer this integration ability unless it uses an external identity provider.

The competitor's software does not have the capability to integrate with a local AD in the same way as ACDN EAA. The competitor requires the use of an external IdP for authentication. This potentially increases cost, reduces authentication protocol support and introduces complexity. Of the many available options,

Miercom utilized the product's capability to integrate with Azure AD using a built-in application. This method is chosen because the Azure AD instance is linked to the same local directory used by ACDN to provide comparable user data. The test bed consisted of 3,000 users; this was not the product maximum for either product.

In terms of scalability, both products offer the capability to add users by group for application access. The competitor also offers the capability to add specific users, if only a portion of a group will utilize the remote access solution.

To confirm functionality, 3,000 users were successfully integrated with the ACDN EAA IdP using group assignments. Group assignments were confirmed to work in the Azure AD enterprise application when configuring the competitor, but the 3,000-user test bed limitation is further reduced due to licensing restrictions.

The EAA solution supports the creation of custom overlay groups internal to the management console. These groups do not require any back-end alterations to the active directory. In this use case, a custom group is created to perform user specific access rules.

5.0 Configuration

The next portion of analysis documents a comparison in configuration settings for essential operations, such as adding an application. The following actions were assessed for end user experience and configuration flexibility:

- Application Configuration
- Group Access Rules

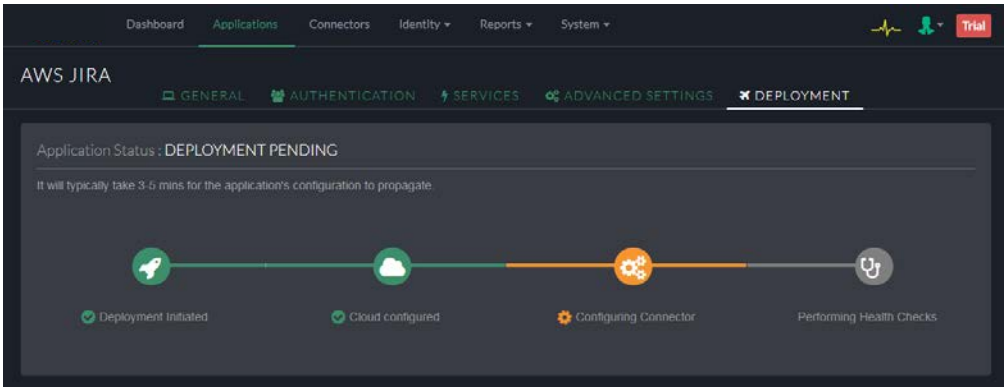
5.1 Application Configuration

The application configuration consisted of two categories – local and cloud applications.

Local Applications

The local application configuration settings are not complex for either SUT. Applications used for performance testing with ACDN EAA utilize the US East cloud zone.

The ACDN EAA product provides an abundance of configuration options, and default applications can be used as a starting point. This default template can save time by including tailored configurations of applications such as Jira or Salesforce. Each application can be modified under its respective tab, which maps the application to a location and connector, and allows for end user authentication setup, addition of services (e.g. access control, advanced authentication settings) and deployment. The advanced authentication settings allow for flexible customization of various authentication types (e.g. NTLM, Kerberos, SAML) and methods (e.g. cert-only, form-based, header-based).



Source: Miercom

This is the first tab of options available when configuring an application for use with the ACDN EAA. The application server location and other access options are configured in this page.

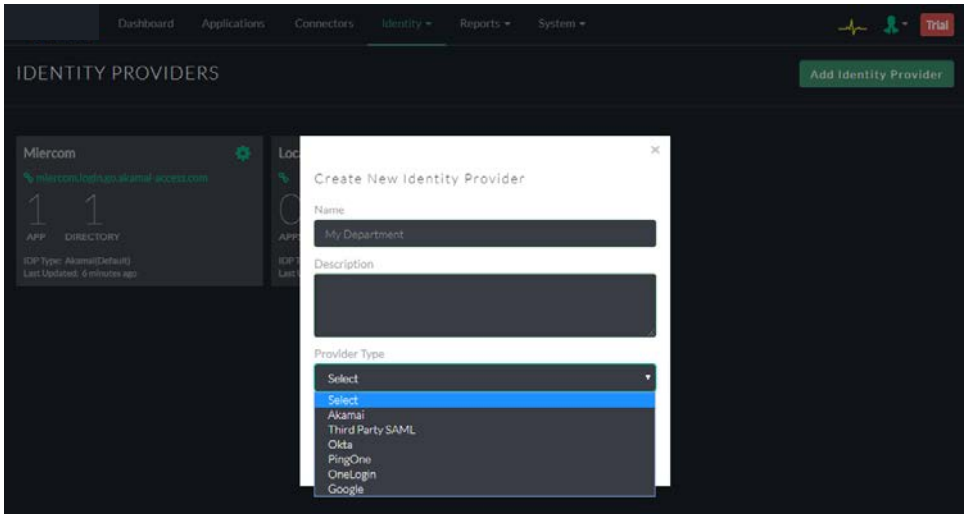
While the competitor's simplistic user interface requires less configuration, it does not offer the same amount of options as the ACDN EAA. This difference in end user experience is discussed in further detail in Section 7.0.

There are fewer steps required to configure the competitor's software. When comparing, each process begins with similar settings and information; basic settings are created which include application location, ports and a few additional settings. For the competitor, all that is required to complete the setup is the assignment to groups and servers.

Cloud Applications

When assessing cloud applications, an instance of Jira on an AWS server was utilized to confirm functionality. In this case, the cloud application configuration was only applicable to ACDN. Individual cloud applications were not accessible through the competitive product's cloud infrastructure in this test scenario.

With a more complex cloud network configuration, both ACDN and the competitor offer the option to utilize a connector in the cloud to access a Virtual Private Cloud (VPC). Using ACDN EAA, the cloud application configuration is easily accomplished with the same setup as a local application. After a connection to the cloud is established, application access is provided via the centralized user interface.



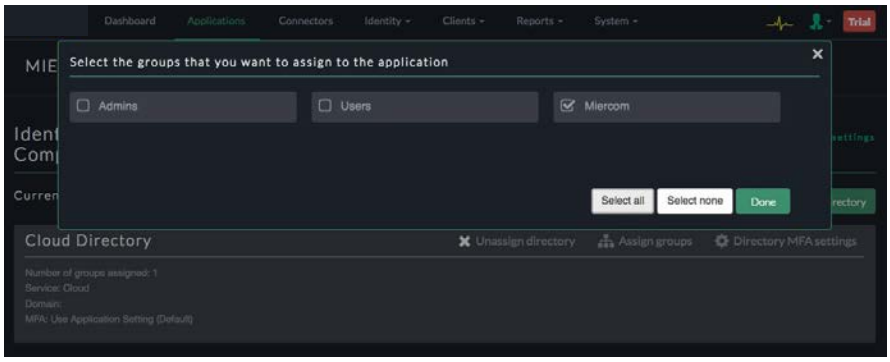
Source: Miercom

As with local application setup, the ACDN EAA can provide cloud application access from a centralized interface by creating a new identity provider.

5.2 Group Access Rules

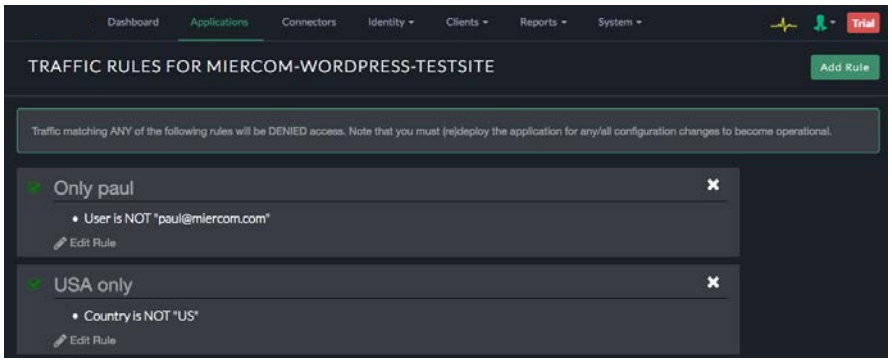
When an application is created, group access rules must be assigned to the application to ensure proper access. At a basic level, each product's application access is only granted to users in the respective IdP. Each SUT had noteworthy advantages and disadvantages, but both allow for rules to specific user groups to access applications.

When creating an application in ACDN EAA, the groups that are allowed access are selected.



Source: Miercom

Immediate selection of group access options is provided upon application creation.



Source: Miercom

The Access Rule policy editor provides adaptive options, based on more specific criteria (e.g. time, client's geolocation).

For the competitive solution, all users in a group are allowed access to an application until access rules are created. Unlike ACDN, this default configuration – unless modified – increases risk and is open to unauthorized access. Multiple access rules must be created, based on different IdPs; the chosen setup resembles a flexible firewall ruleset of multiple applications with centralized management.

6.0 Compatibility

This section reviews compatibility and design for the following functionality:

- Single Sign-On (SSO)
- IdP Test Case
- Bring Your Own Device (BYOD) Test Case

Both products were capable of VPN Coexistence, wherein VPN is still available while the remote user access SUT is deployed.

6.1 Single Sign-On

The ACDN EAA excels at single sign-on (SSO) with its unified design and seamless compatibility to deliver functionality that typically requires multiple products to achieve. When configuring the EAA, ease of access via single-click login was observed for the following methods and applications:

- NTLM with SharePoint
- SAML with Jira and WordPress
- Office 365 SAML for Control Interface (Luna Control Center for ACDN)
- RDP
- Kerberos

Single-click login was confirmed for all test cases, showing seamless compatibility and ease of use for each scenario. When using SAML authentication, EAA provides a flexible configuration that allows users to create custom attribute mapping for versatile deployment.

Authentication Bridging

The competitive product is designed to work in a different way and cannot be directly compared to ACDN EAA in this instance. EAA is an identity-aware proxy (IAP) that provides native IdP, integrations with multiple third-party IdPs, and can bridge identities to legacy applications to break down identity silos.

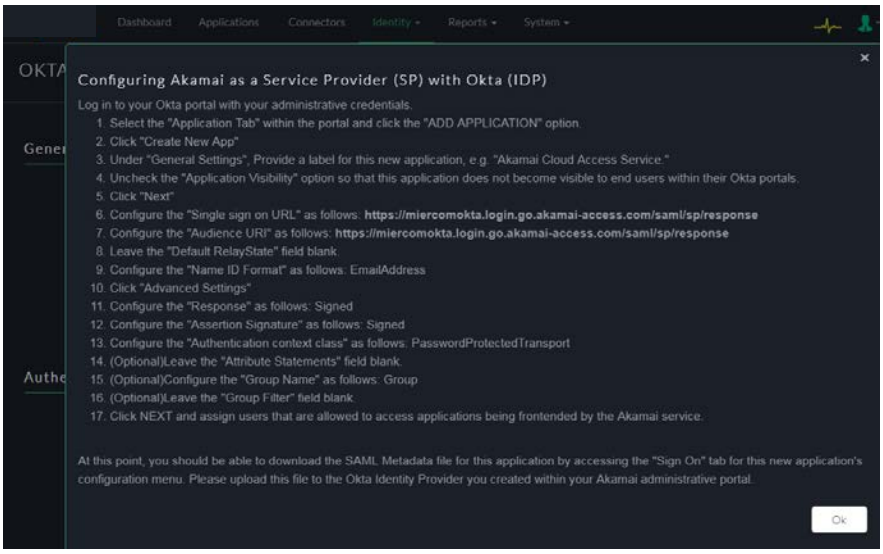
Authentication bridging is critical to enabling SSO and application control and experience across applications, even if the application uses native authentication methods, such as Kerberos or NTLM. EAA can translate and bridge authentication methods, such as SAML 2.0 to Kerberos, because EAA is based on an identity-aware proxy architecture – as opposed to the network tunnel-based architecture of the competitive product.

6.2 Identity Provider (IdP) Test Case

Many companies make use of pre-existing IdP solutions such as Okta, OneLogin or Active Directory Federation Services (ADFS). In this test, each SUT's compatibility with the Okta solution was confirmed.

The configuration inside of the Okta interface was very similar; both require the configuration of a built-in application for the respective product. After this application is configured, the setup on the SUT can be completed. Finally, the local applications can be added to the Okta interface for quick access. If the product requires a local application for traffic tunneling, this will need to be connected before accessing the internal application links configured in Okta.

EAA does not require use with an IdP such as Okta; however, EAA can be integrated if a third-party IdP is already in use by the customer, or if a more mature IdP is desired.



Source: Miercom

Although not required, the ACDN EAA can be integrated with Okta using the list of simple steps above.

ACDN EAA allows Okta to have access to internal applications through a single connector, providing seamless integration. User verification through EAA/Okta is automatic and smooth. The browser application works well and allows for an SSO end user experience. Specific application access can be managed through the Okta application for centralized control. Feedback for users attempting to access unauthorized applications is specific and useful.

6.3 Bring Your Own Device Test Case

The Bring Your Own Device (BYOD) test case was performed using Linux, Windows, iOS and Android systems.

The versatility of the EAA was demonstrated through the BYOD scenario; it allowed any device with a web browser to become a mobile workstation for the user. In the analysis, the solution was confirmed as working on all operating systems tested. There is a mobile site design/re-flow that makes EAA easy to navigate on either Android or iOS.

The competitor's solution for BYOD requires application installation, which in turn assumes full control or management of the device, which is often not available particularly in BYOD or third-party scenarios. It is confirmed to work on each operating system, with the exception of Linux.

7.0 End User Experience

ACDN EAA was competitively assessed for its user experience for the following situations:

- Application and Access
- Base Performance
- Logging and Visibility

7.1 Application and Access

This test assessed how easy applications could be accessed and interfaces be made available to the end user. Functionality was observed using the same applications referenced in Section 6.1.

Application ease of use was another great differentiator for the EAA solution. The end user has a browser link showing all available applications and opens them in a new tab when accessing the link. The end user can switch between applications without being logged out. Also, the EAA product can be configured to make use of multiple SSO solutions that allow single-click login.

The competitor's product provides application access in a manner that feels very similar to the end user experience when on the local network. The applications are accessed via the same means as a local user. The competitor product seamlessly links the end user to the local application.

7.2 Base Performance Analysis

This test assessed the performance of the EAA in comparison to a typical VPN connection over SSL and a competitive solution to determine the difference in the end user experience. This is not a stress test or analysis of resource usage under heavy load.

The test bed consisted of a Windows endpoint which accessed the New Jersey corporate network from three global locations: New Jersey, Frankfurt and Tokyo. These locations are intended to simulate the performance differences observed when accessing a US-based network from the US, Europe (EU) and the Asia-Pacific (AP). The endpoint accessing the network using WatchGuard's VPN Client through a WatchGuard Firebox M370 UTM. The Mobile VPN with SSL option was used in the M370. The testing is completed using Apache JMeter over the course of one week. Hundreds of datapoints are collected for each of the products from the three geographic regions.

The speed of HTTP GET and POST requests is compared between each of the products. This comparison is intended to benchmark the end user experience when accessing a local application. When accessing the application, the load time in which a page can be received and the time in which content can be posted to a page is expected to be quick. The navigation of a local application should never slow down the end user.

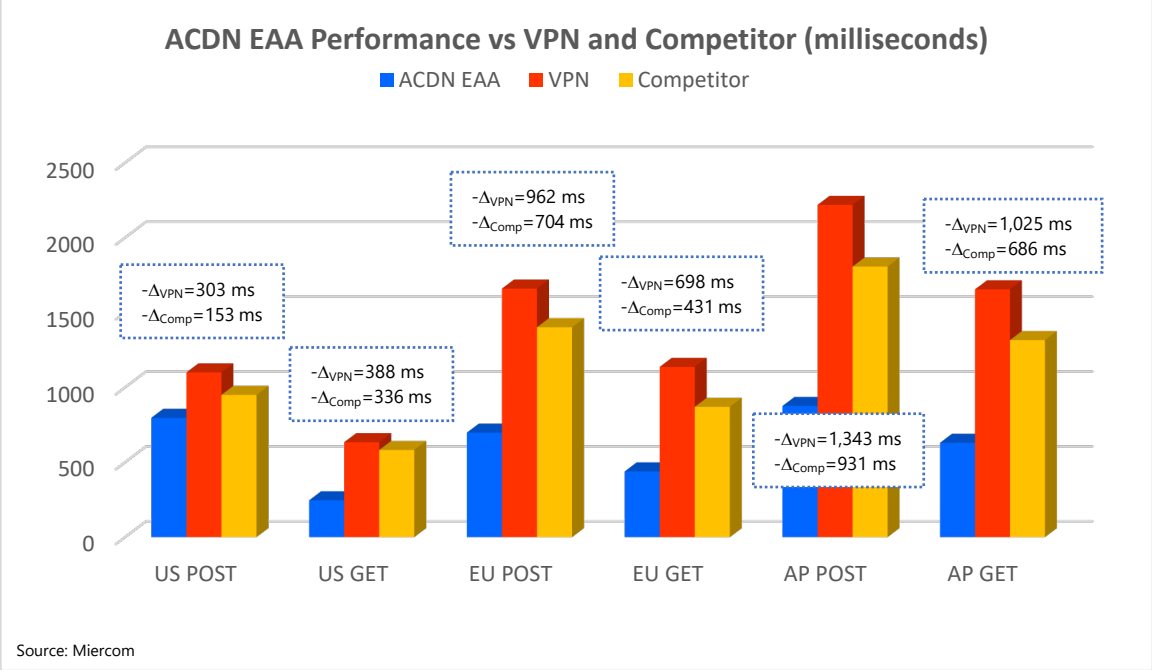
Throughout the testing, two simultaneous clients performed a series of automated actions on an intranet site – a basic WordPress site acting as a static endpoint for data collection. These two sessions were repeated ten times to obtain a larger sample set. This test was run every hour each day, to ensure that no temporary

issues impacted results. After logging in and reaching the application, the average time in which the end user could load a specific page and post a standardized comment are recorded. These times are used as a benchmark of the end user experience. An average time of less than a half second is considered good performance. Any navigation times taking over 1.5 seconds is considered average, and any reported time over four seconds is considered slow. This test was repeated for the ACDN EAA product with performance features enabled, the standard VPN, and the competitor product.

The following table shows the results of each product on user experience. ACDN EAA had the lowest latency in comparison to VPN and the competitor, proving the best performance.

Comparative HTTP POST/GET Time

POST/GET Time (ms)	ACDN EAA	VPN	Competitor
US POST	797	1100	950
US GET	246	634	582
EU POST	698	1660	1402
EU GET	439	1137	870
AP POST	876	2219	1807
AP GET	630	1655	1316



Source: Miercom

7.3 Logging and Visibility

The quality and thoroughness of a system's feedback is critical to a smooth user experience. Some items are essential – a dashboard with customizable feedback, detailed logs, log filters, log sorting, and data export.

ACDN provides an exceptional user experience in these categories with easy navigation and intuitive setup. When comparing the built-in logging capabilities of the two products, both were able to filter results based on specified criteria. Detailed logs are one of the first locations analyzed when troubleshooting an issue. ACDN EAA can save and export these detailed logs to CSV or another format, while its competitor cannot. In addition ACDN has full integration with SIEM tools, such as Splunk - https://learn.ACDN.com/en-us/webhelp/enterprise-application-access/enterprise-application-access/GUID-B6C8EAFE-8D6A-48C7-9892-A4674A9AB9F1.html

The following compares the ACDN EAA product to its competitor for Dashboard and Logging features.

Administrative Dashboard Features

Dashboard Feature	ACDN EAA	Competitor
User Activity *Relay user activity to the administrator*	Yes	Yes
Per App Breakdown *Refine information by application or direct the administrator to location of this information*	Yes	Yes
Health Reporting *Relay network health information (e.g. connector, application, server)*	Yes	Yes
Active User Reporting *Relay number of active users and specific user activity information (e.g. logins, application access)*	Yes	Yes
Error Reporting *Relay error information*	Yes	Yes
Smooth End User Experience *Intuitive, easy interface*	Yes	Yes
In-Depth Detail Entry *Drill-down view of overview elements via links or tooltip text*	Yes	Yes
Bandwidth Breakdown *View of application usage separated by bandwidth to show most used applications*	Yes	Yes
Display Rule Violations *Allows administrator to view access rule violations or settings*	Yes	Yes
Customization *Customizable user portal and/or landing page*	Yes	No

Logging Features

Logging Feature	ACDN EAA	Competitor
Smooth End User Experience *Practical, simple log viewer with few transitions between log pages*	Yes	Yes
Chronological Order/Filter *Logs presented by date with option to filter or retrieve results for a specific time period*	Yes	Yes
Log Export *Detailed log reports, granular access information with per session/per request visibility*	Yes	No
Detailed Logging *Visibility into granular aspects of user sessions and actions*	Yes	Yes
Error Isolation *Filtering of all logged errors*	Yes	Yes
Application Filter *Simple filtering of all applications*	Yes	Yes
Connector Filter *Filtering of all connectors (e.g. by status)*	Yes[1]	Yes
User Filter *Simple filtering of specific user(s)*	Yes	Yes
Basic Overview *Broad display of information*	Yes	Yes
In-Depth Detail *Drill-down view of overview elements via links or tooltip text*	No	Yes
Administrative Logs *View of administrative activities*	Yes	No
Server Command Query *View of SSH commands to servers*	Yes	No
SIEM Integration *Integration with third-party SIAM: Splunk assessed and available on Splunkbase*	Yes	Yes

[1] *Must export reports to CSV to accomplish customer-preferred filtering*

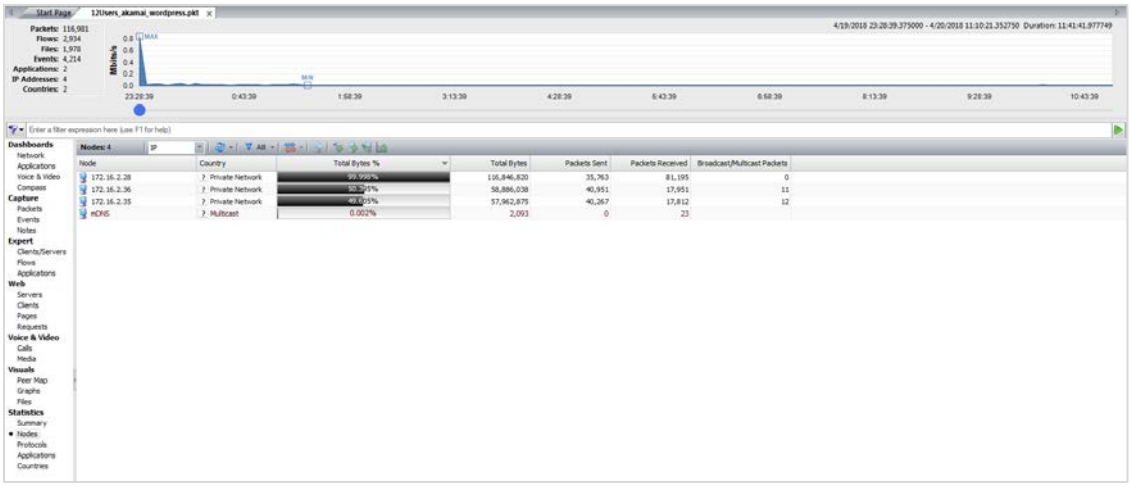
8.0 Product Differentiators

ACDN EAA outperforms its competition with several unique features discussed in the following sections:

- Load Balancing
- Embedded Identity Provider
- Advanced Network Configuration Options
- Multi-Factor Authentication
- Performance Features
- Client or Clientless Implementation

8.1 Load Balancing

A beneficial product differentiator when considering EAA is the ability to load balance applications. Round Robin and IP Hash are two load balancing methods available in the ACDN dashboard. In this test, Round Robin is configured using a LiveAction Omnipeek traffic capture. Using a portion of the JMeter performance test, twelve users accessed the application through the EAA product. With the built-in analytics provided by Omnipeek, load balancing was easily observed between the two servers.



Source: Miercom

The LiveAction Omnipeek tool provided nodal statistics. Traffic coming from the public (first node) was distributed almost evenly between the two application endpoints. Observed traffic was actively load balanced by the EAA product within one percent.

8.2 Embedded Identity Provider

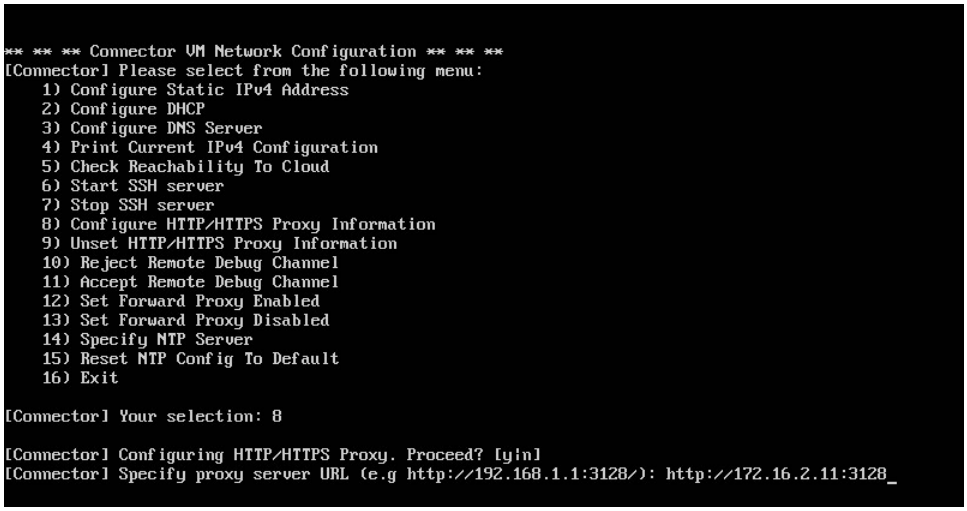
One of the biggest differentiators ACDN EAA has from a traditional VPN or its competitor is consolidation. This standalone product does not require additional products during deployment. The EAA solution has a built-in IdP.

The competitor requires the use of an external IdP and other programs, such as Remote Desktop Connection, to access local RDP instances. While it is likely a corporate environment already makes use of an external IdP and applications on employee devices, the flexibility of ACDN's built-in version eliminates obstacles related to integration with its consolidated solution.

8.3 Advanced Network Configuration Options

ACDN EAA

The ACDN EAA connector provides advanced settings for use in complex network environments. These settings can be used by an administrator when configuring a forward proxy for the connector's outbound traffic and can be designed for easy access through the connector interface.



Source: Miercom

By selecting #12 from the Connector VM Network Configuration menu, the Forward Proxy feature can be enabled. Setup is easy, and feedback is instantly available.

8.4 Multi-factor Authentication

ACDN also has a built-in Multifactor Authentication (MFA) feature for an extra layer of protection. MFA ensures the access is granted only when two of three identity components are satisfied. MFA policies can be set for all users of any application, including administrators attempting to access the EAA Management Portal.

8.5 Performance Features

EAA's performance-enhancing features:

- Route optimization and content caching at the edge to ensure speed and availability across devices, networks, browsers, and locations
- 75 percent faster DNS resolution via Zone apex mapping
- More intelligent routing decisions for users of distributed DNS solutions
- Automatic Push and Preconnect, Resource Optimizer, Script Adaptive Single Point of Failure
- Adaptive Network Optimizations, API Acceleration
- Advanced Caching & Compression
- Machine learning to determine ideal optimizations

8.6 Client or Clientless Implementation

EAA supports different types of applications:

- On-premise web-applications, SSH servers, and RDP desktops accessible throughout the browser, fully client-less.
- SaaS based, connect apps like Office 365 or Salesforce
- Any other TCP and UDP applications: EAA supports client-based applications like Outlook/Exchange, SAP GUI, databases or even Remote Desktop clients. The EAA Client software can be deployed on workstation and laptops, along with existing VPN or endpoint solutions, and will open access to these applications securely.

9.0 Total Economic Impact Analysis

Managing application availability to a highly distributed global workforce is a key factor to an organization's productivity and can have a significant impact on the bottom-line. EAA removes the cost and complexities around securing access to applications. It is a SaaS service that delivers simple, secure and convenient access to applications without providing users access to the entire network. Limiting access to the full network can dramatically reduce the risk associated with data exfiltration from internal users. Applications are accessible to your remote workers while being hidden from the Internet and from public exposure.

Miercom conducted an independent audit for Total Economic Impact (TEI) analysis, in combination with information provided by a report ACDN had commissioned Forrester to create on Enterprise Application Access, published in September 2018. This report associated the quantified benefits of the solution within three years at a value of $380,475 (NPV $315,395). The effective monthly per user benefit is $30.20. Additionally, the Forrester report pointed out that the Return on Investment (ROI) is approximately three months. These calculations are based on 350 active monthly users.

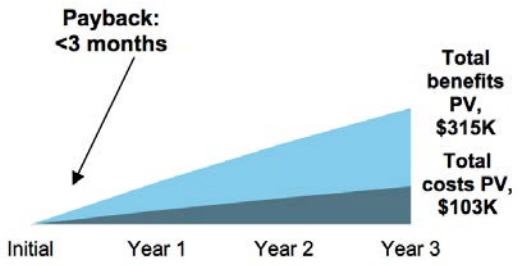
QUANTIFIED BENEFIT DATA AS APPLIED TO THE COMPOSITE

Total Benefits

REF.	BENEFIT	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Atr	Reduced effort by desktop support team	$91,800	$91,800	$91,800	$275,400	$228,293
Btr	Reduced effort by security team	$24,225	$24,225	$24,225	$72,675	$60,244
Ctr	Avoided cost of physical assets for remote access	$10,800	$10,800	$10,800	$32,400	$26,858
	Total benefits (risk-adjusted)	$126,825	$126,825	$126,825	$380,475	$315,395

Source: ACDN

Forrester's interviews with existing customers and subsequent financial analysis found that an organization experienced benefits of $315,395 over three years – versus costs of $103,211 – adding up to a net present value (NPV) of $212,184 and an ROI of 206%. EAA payback was less than three months after integration.



About Miercom

Miercom has published hundreds of network product analyses in leading trade periodicals and other publications. Miercom's reputation as the leading, independent product test center is undisputed.

Private test services available from Miercom include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Interoperable™, Certified Reliable™, Certified Secure™ and Certified Green™. Products may also be evaluated under the Performance Verified™ program, the industry's most thorough and trusted assessment for product usability and performance.

Use of This Report

Every effort was made to ensure the accuracy of the data contained in this report, but errors and/or oversights can occur. The information documented in this report may also rely on various test tools, the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the vendors that were reasonably verified by Miercom but beyond our control to verify to 100 percent certainty.

This document is provided "as is," by Miercom and gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained in this report.

All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.