Technical Review

AI-driven Management and Security of Corporate Networks with Arista Cognitive Campus Workspaces

Date: October 2021 **Author:** Alex Arcilla and Tony Palmer, Senior Validation Analysts

Executive Summary

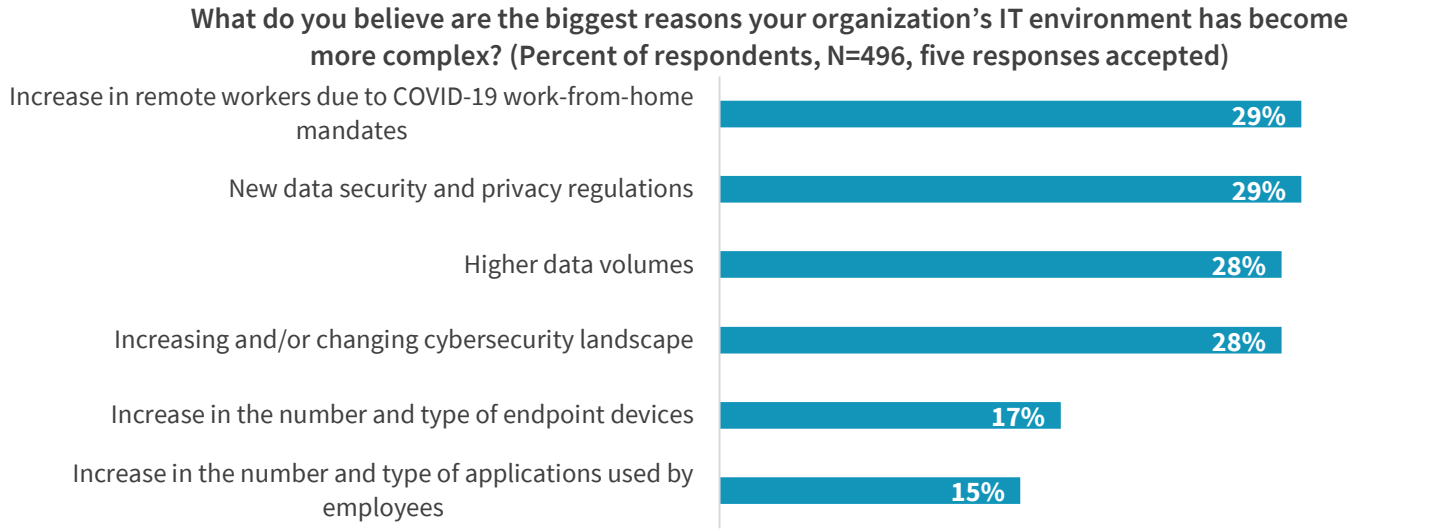
This ESG Technical Review validates the value that Arista's Cognitive Campus Workspace solution delivers to organizations. We reviewed how Arista's latest offerings help enterprises address the proliferation and security needs of expanding network infrastructures that include IoT devices, remote workers, and access to cloud-hosted applications.

ESG validated that the Arista Cognitive Campus Workspaces can help organizations to better manage and monitor their enterprise wired and wireless infrastructures with less time and operational costs. We observed how the Arista solution, via its artificial intelligence (AI)-driven engine and CloudVision portal, can decrease the time and effort in identifying and troubleshooting network connectivity issues. With increased wireless access in campus networks, the proliferation of IoT devices, and the resulting increase in network traffic, we verified that Arista's solution can improve overall network, endpoint, and IoT security. We also validated how additional Arista capabilities—such as enhanced visualization, flow monitoring, and cloud-based device provisioning—simplify corporate network deployment, visibility, and management.

The Challenges

Events over the past 18 months have prompted organizations to drastically modify existing IT networks and policies in order to accommodate the increase in remote workers. As a matter of fact, ESG research has uncovered that 72% of organizations have become more pro-work from home. Organizations are prioritizing efforts for transitioning back to a relatively "normal" working environment while keeping their employees healthy and safe, yet productive. Yet, the increase in remote workers, along with factors such as the changing cybersecurity landscape and an increase in the number and type of endpoint devices and applications used, is contributing to more complex IT environments to be managed (see Figure 1).[1]

Figure 1. Top Six Factors Contributing to Increasingly Complex IT Environments

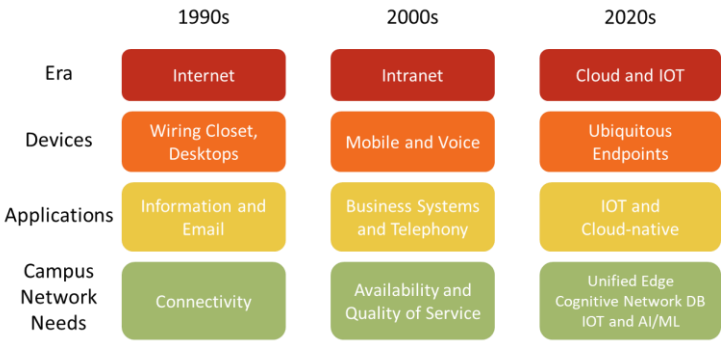


Source: Enterprise Strategy Group

[1] Source: ESG Master Survey Results, *2021 Technology Spending Intentions Survey*, January 2021.

As the return-to-work transition continues, organizations realize that the IT network boundary needs to be broader and more agile than ever before. While employees increasingly adopt a hybrid work model, it is uncertain where they will work at any given time, contributing to a constantly changing network boundary and varying degrees of end-user experience. The IT network also needs to accommodate internet of things (IoT) deployments, which are inherently less secure. Finally, with the continued consumption of public cloud services, organizations struggle in maintaining control with how employees access and connect to cloud services providers. This added IT network complexity, exacerbated by the lack of a well-defined IT network boundary, makes it more difficult for organizations to ensure that users and devices can access the corporate resources consistently without sacrificing productivity and security.

The Solution: Arista Cognitive Campus Workspaces



Arista Cognitive Campus Workspaces helps organizations to better manage and monitor their IT networks, including both wired and wireless infrastructure, by leveraging AI and machine learning on aggregated and anonymized data sets collected from all users, devices, and endpoints. With the data compiled into a unified, state-based, network-wide database, the Arista Cognitive NetDB, and the underlying AI engine, organizations can uncover and manage any connection spanning clients, corporate campuses, data centers, and public clouds. By leveraging real-time streaming data collected via standards-based APIs, organizations can conduct AI-based predictive analysis to support troubleshooting and network threat analysis (both real-time and historical) across IoT, users, and endpoint devices. Using CloudVision, network administrators can access this streaming data to understand how and when an organization's IT environment is accessed. Arista Cognitive Campus Workspaces also helps organizations to automate workflows so that users and devices can connect to their IT networks without compromising productivity and security.

The capabilities that Arista Cognitive Campus Workspaces offers include:

- Zero-touch provisioning – Simplifies first-time switch installation and is now offered as a cloud-based service. Switches communicate with and are authenticated by the cloud. Configurations specific to corporate campus specifications are downloaded via secure handshake.
- Quality of Experience (QoE) – Provides application-level performance analytics so that network administrators can proactively monitor cloud-based collaboration applications such as Zoom and Microsoft Teams. Detects application reachability with support from the solution's AI engine.
- Remote Monitoring – Supplies comprehensive, state streaming of wired and wireless network activities including 802.1X metrics. Summarizes endpoint and interface status in real-time.
- Secured Access – Enables user authentication and end-to-end encryption, leveraging identity partners including Aruba ClearPass and ForeScout eyeSight. Simplifies security administration and end-user access management using Okta Single Sign-on (SSO) integration.
- Compliance Dashboard – Provides proactive risk assessment of both wired and wireless infrastructure via a unified interface to discover and remediate risks.
- Arista P-Tracer Contact Tracing Engine – Uses Wi-Fi association data to help identify a user's location over a given period of time, which is critical information for contact tracing by person, proximity, or position zones.
- CloudVision Studios - Abstracts complex CLI-driven provisioning workflows (e.g., EVPN, ACL's, network segmentation) to more easily understood operation tasks. Point and click workflows quickly validate Arista recommended designs.

To improve the security of networks across campus, data center, public cloud, and IoT environments, organizations can leverage Arista's Awake security platform, empowered by AI, to autonomously hunt for both insider and external attacker behaviors, while providing triage, digital forensics, and incident response. Awake models complex attacker behaviors using a

multi-dimensional machine learning approach across entities, time, protocols, and attack stages. This enables the discovery of more than just anomalous events or static indicators of compromise, but malicious intent.

ESG Tested

ESG proceeded to validate how Arista Cognitive Campus Workspaces helps network administrators to better manage both end-user and endpoint experiences so that both productivity and security are assured, regardless of connecting via wired (switched) or wireless (Wi-Fi) infrastructure in corporate campuses, data centers, or the public cloud.

ESG first audited how network administrators can use Arista CloudVision Wi-Fi to manage and monitor Wi-Fi access points (APs) in small and home offices with little manual effort. As employees opt either to work from home or from a remote office, as opposed to corporate offices, network administrators want to ensure secure, enterprise-grade connectivity without having to physically connect and deploy APs in person. Using CloudVision Wi-Fi, an administrator can deploy and configure APs remotely, regardless of where the APs are located, so that employees can connect to the corporate network automatically. Employees do not have to rely on consumer-grade APs or configure equipment without enterprise support.

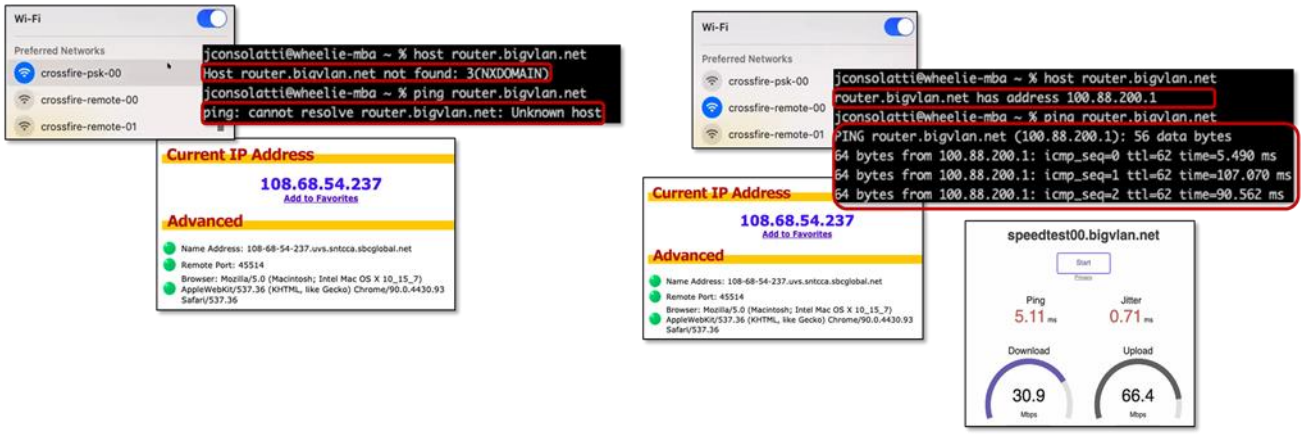
We used the following testbed for connecting remote APs to the "corporate network" (see Appendix for testbed diagram). Two Arista remote APs were deployed in a home office and sat behind a third-party services gateway. The first AP was configured to access SSIDs "*crossfire-psk-00*" and "*crossfire-remote-00*," while the second AP only allowed access to SSID "crossfire-remote-01." If connecting to the first AP, a client could access either the internet or the corporate network. With the second AP, a client could only access the corporate network. The APs were connected to the corporate network via dual IPsec VPN tunnels going through AT&T (*vpn-a.biglan.net*) and Comcast (*vpn-a.biglan.net*).

The testbed's corporate network sat behind two Palo Alto PA-220 next-generation firewalls (NGFW). Network resources were interconnected via the router named "router.bigvlan.net" and included APs, network-attached storage (NAS), a VMware server, and a printer. To access the corporate network, we used a MacOS X laptop as our client. The client was authenticated by the RADIUS[2] server in the corporate network.

ESG first verified only internet connectivity for the MacOS client connected to crossfire-psk-00. We attempted to resolve the host name router.bigvlan.net and ping it but could not reach it (see left-hand side of Figure 2). We also verified that we reached the Juniper gateway with the IP address 108.68.54.237, leading us straight to the internet. We then selected the Wi-Fi network crossfire-remote-00 and attempted again to reach the corporate network. We were successful in resolving the host name and pinging router.bigvlan.net (see right-hand side of Figure 2). We also tested the download and upload speeds and found that we achieved a maximum of 30.9 Mbps and 66.4 Mbps, respectively (as this was an ADSL connection from the home office).

[2] RADIUS (Remote Authentication Dial-In User Service) is a client-server networking protocol that provides centralized authentication, authorization, and accounting (AAA) management for users that want to connect to a secured network.

Figure 2. Connecting to Corporate Network with SSID "crossfire-remote-00"



We should note that the IP address did not change as the first AP was configured for split tunnel mode. However, when we connected to SSID crossfire-remote-01, the IP address changed to 108.68.54.237, indicating that traffic was now going through the Palo Alto Networks firewall via vpa-a.biglan.net (see Figure 3).

To verify that traffic was flowing from the client to the corporate network, we navigated to the CloudVision Wi-Fi interface and saw the applications accessed by the client as well as client traffic volume. We could view this user as if the client connected via a Wi-Fi network on a corporate campus.

Figure 3. Connecting to Corporate Network with SSID "crossfire-remote-01"

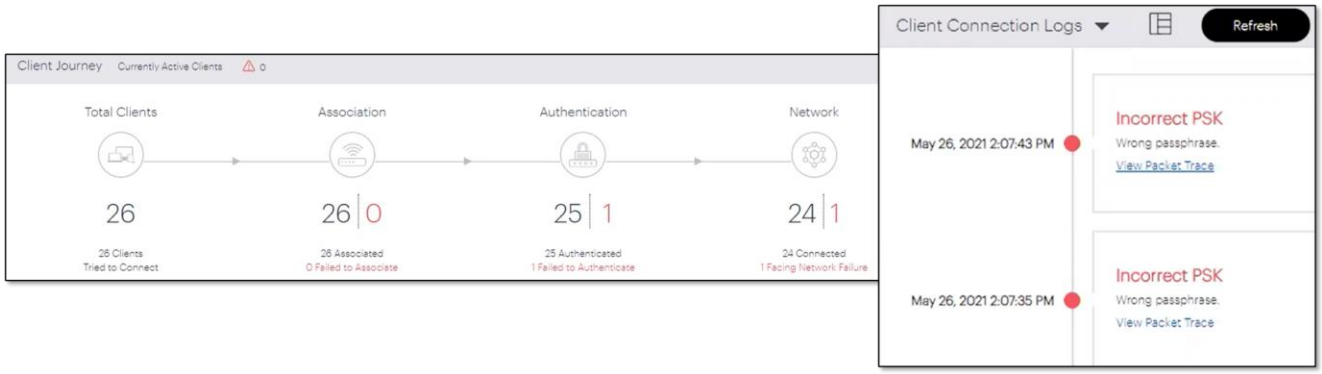
For organizations that are dealing with an increasing number of remote employees, providing enterprise-level connectivity and security is key so that productivity is not disrupted. Instead of employees configuring their own equipment and relying on other methods to access the corporate network, the Arista APs have been designed such that corporate SSIDs can be extended to any location outside of the corporate campus.

> ESG validated that organizations can extend Wi-Fi networks to any given number of locations outside an organization's on-premises network with Arista APs, providing enterprise-grade network connectivity and security.

ESG proceeded to validate how network administrators can gain full visibility of the "client journey"—the pathway for a client to access the corporate network—via CloudVision. With the CloudVision Wi-Fi dashboard, we obtained an overall summary of the number of clients that attempted to connect to our network. Details included the total number of clients attempting to connect, the number of clients that were successfully associated with an Arista AP, the number of clients that were authenticated (e.g., PSK, WPAs, or 802.1x), and the number of clients that obtained network connectivity (e.g., with DNS, DHCP, etc.) (see Figure 4). The numbers in red indicated clients that failed at each stage of the client journey. We also saw how and why a client could not

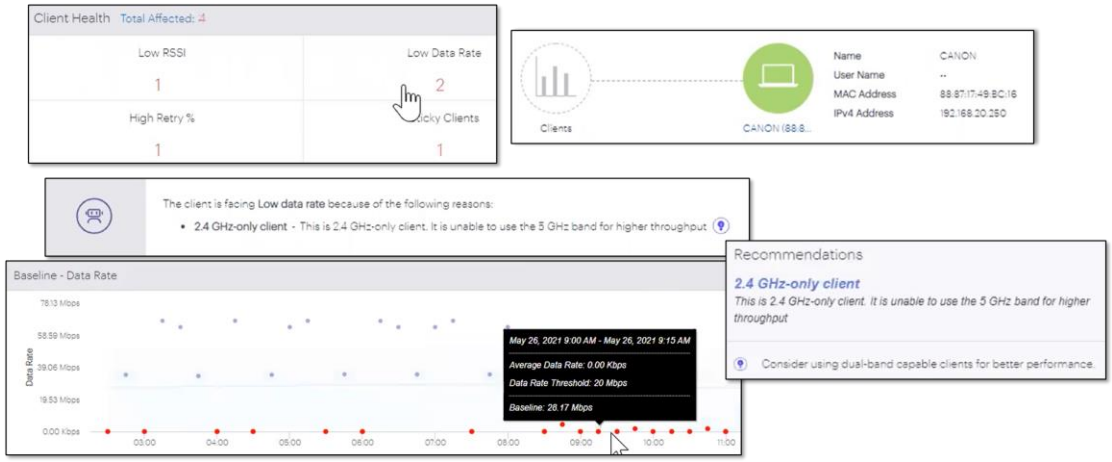
connect to the corporate network at any stage. We clicked on the number of clients that failed to authenticate and automatically found out that the failure was due to an incorrect PSK.

Figure 4. CloudVision Wi-Fi Dashboard Showing Client Journey

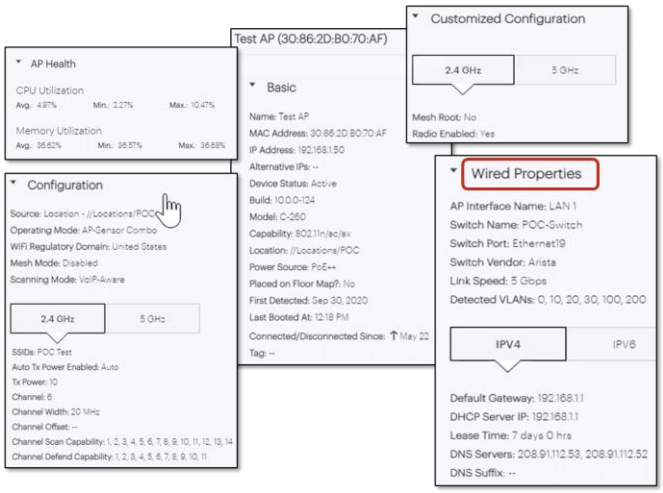


ESG then clicked on the **Performance** tab to observe how else we can determine root causes of issues affecting connectivity, such as low RSSI and low data rates (see Figure 5). We clicked on the number of clients that CloudVision detected as displaying low data rates and selected the Canon printer. Examining the performance over time (via the time-series chart), we concluded that the printer exhibiting low data rates over time is typical behavior.

Figure 5. Determining Root Cause of Low Data Rate Exhibited by Client



We noted that CloudVision also performed root cause analysis (RCA) and determined that the printer was a 2.4 GHz client, unable to use the 5 GHz band. Using machine learning, CloudVision Wi-Fi recommended a possible solution. We should note that CloudVision Wi-Fi can also perform RCA for other issues that have occurred and, with the machine learning engine, determine potential issues (e.g., quality of experience issues) when accessing applications via Wi-Fi.



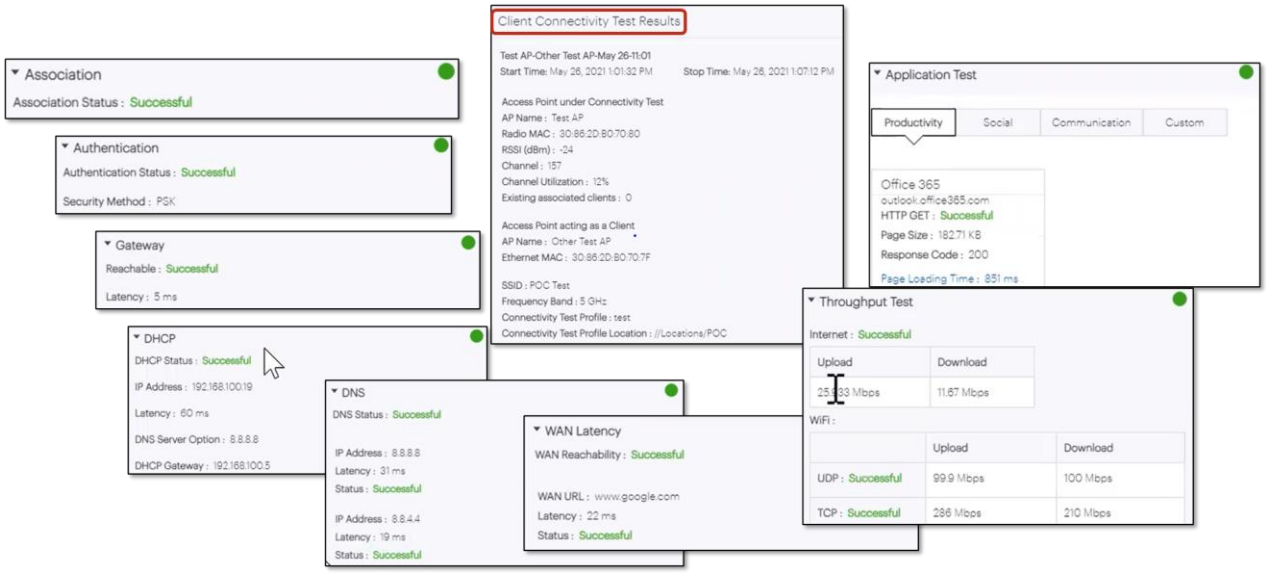
ESG continued to examine how CloudVision Wi-Fi can help network administrators gain broader visibility and better manage connectivity between switches, APs, and clients with less time and effort. From a list of APs available in our test network, we clicked on "*Test AP.*" We saw how CloudVision Wi-Fi revealed details, including standard and customer configurations and overall health, as shown in the figure to the left. We noted that these details included "Wired Properties," which revealed how an on-premises switch connected to *Test AP*, showing how CloudVision integrated information about both the wired and wireless infrastructure. There was no need to use additional tools, interfaces, or command lines to determine how an AP connects to on-premises switches for verifying connections or uncovering network-impacting issues.

ESG proceeded to conduct a Client Connectivity Test to ensure that any client could connect to the Test AP. We simulated a client connecting to a third radio designed into the Arista AP and observed how administrators could test application accessibility. After running the test, which completed in very little time, we saw the results shown in Figure 6.

> ESG validated that a network administrator could locate client connectivity issues, from the wired and/or wireless infrastructure side, using only the CloudVision Wi-Fi interface, saving time and operational costs.

ESG noted the comprehensive results that would reveal any potential client connectivity issue, from the time that a client associates with an AP to the point at which an application is accessed. Even details such as latencies were listed to help an administrator better diagnose an issue should it exist. Red dots and messages in red would flag exactly where an issue has occurred and the potential cause, helping an administrator to decide upon next steps. Less time spent on identifying client connectivity issues results in less operational cost and, ultimately, increased end-user productivity.

Figure 6. Results of Client Connectivity Test with Arista AP



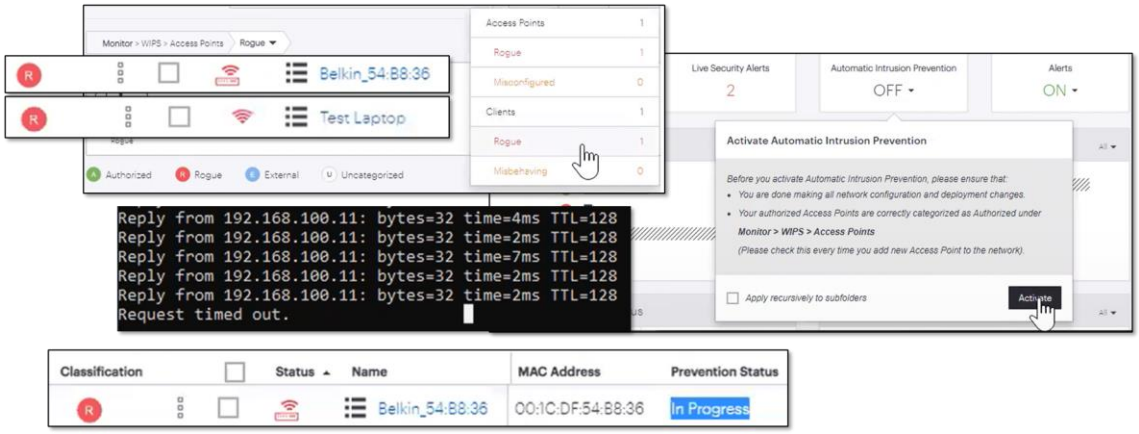
ESG then examined the wireless intrusion prevention system (WIPS) of CloudVision Wi-Fi to see how quickly rogue APs and clients could be detected and isolated. Arista's Cognitive Wi-Fi accomplished this by sending out gratuitous ARPs to all

available SSIDs and associated VLANs. When detecting an ARP that is determined to not be under control of the SSIDs, the relevant APs and their associated clients are isolated automatically.

To demonstrate this capability, ESG used a testbed that represented a small corporate Wi-Fi network with SSID "*POC Test*" containing VLAN 100 (see Appendix for testbed diagram). Our network consisted of two Arista APs connected to an Arista switch via trunk ports. A rogue Belkin AP named "Bad Guy" was also connected to this switch. We employed a test laptop to act as a client attempting to access the POC Test. All elements were contained within VLAN 100.

We first verified the rogue elements under the WIPS tab of CloudVision Wi-Fi (see Figure 7) and saw that the AP and client had already been flagged. We also pinged the AP to see if we could reach it. We then activated "Automatic Intrusion Prevention." Almost immediately, we found that we could no longer ping the AP.

Figure 7. Isolating Rogue AP from the Corporate Wi-Fi Network



ESG validated that CloudVision Wi-Fi can automatically identify and isolate rogue APs and associated clients before they cause any significant security breaches.

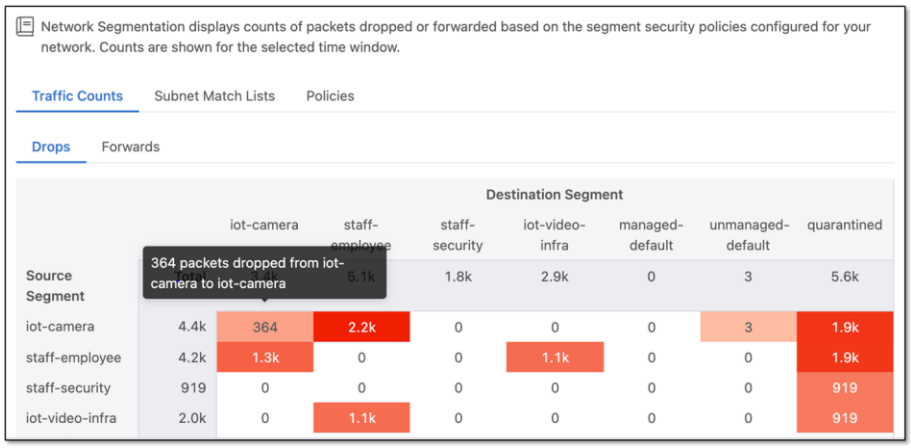
We also saw that the Prevention Status of the AP was noted as "In Progress" shortly after activating "Automatic Intrusion Prevention." In addition, ESG noted that the associated laptop was also isolated from VLAN 100. With CloudVision Wi-Fi, once a rogue AP is isolated, all associated clients would automatically be isolated, as any policy is applied globally in a hierarchy within a Wi-Fi network managed by CloudVision Wi-Fi. We also noted that the WIPS can work with APs of other vendors aside from Arista APs. Securing the Wi-Fi network can be done automatically, while freeing up an administrator's time to ensure that the network is running smoothly.

ESG then reviewed enhanced capabilities to Arista's wired networking infrastructure and monitoring. One notable addition included Arista Multi-Domain Segmentation Services - Group (MSS-G), previously reviewed by ESG.[3] Approaches to group segmentation have been limited in managing the proliferation of security attacks brought about by IoT deployments and increased usage of the public cloud. Arista MSS-G offers a simpler, efficient method of group segmentation enforcement and policy management by leveraging the forwarding decisions applied to incoming packets at the switch level, as opposed to via VLANs and subnets. With CloudVision Studios, we observed how an administrator could abstract complex segmentation configuration commands into easily understood tasks rather than CLI knowledge. CloudVision also works with third-party authentication and security platforms via API exchanges, including ForeScout, for endpoint discovery and device type analytics.

[3] For more information about Arista MSS-G, refer to ESG First Look, *Reinforcing Zero Trust Posture with Arista Multi-Domain Segmentation Services – Group*, February 2021.

Figure 8 shows the results of applying segmentation rules on the Arista switch "bri267." With the policy "*camera-video-infra,*" we assigned the IP address "222.100.0.120" to the group "*iot-camera*" and specified that any traffic from *iot-camera* can be sent to any IP address within the group "iot-video-infra." The only exception was that traffic from TCP port 139[4] would be denied. After generating traffic from TCP port 139, we saw that traffic was quarantined.

Figure 8. Forwarded and Dropped Traffic Displayed in CloudVision

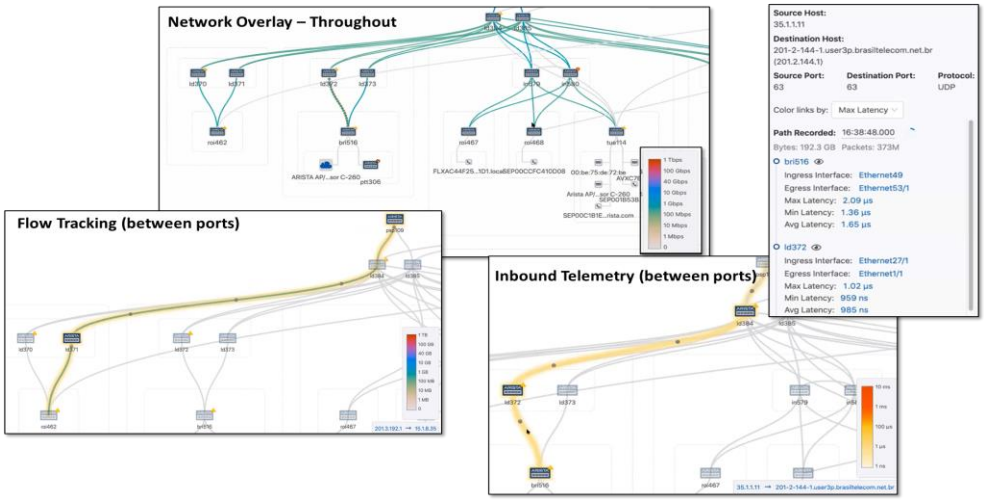


In addition to revisiting features already validated in previous reports, such as flow monitoring, endpoint identification, and compliance status (shown in Figure 9), ESG reviewed additions that can further help in decreasing time to issue identification and resolution such as colors and animation to highlight traffic characteristics of specific connections, on a hop-by-hop basis, within network topology views (see Figure 10). ESG saw how network administrators can better visualize these characteristics, such as total throughput, flow tracking (showing traffic flowing between the spine switch and specified endpoints at port level), and inbound telemetry (between the same ports but monitoring inbound traffic to the spine switch). In addition, metrics, such as latency, related to flows and inbound telemetry could also be visualized using other filters such as specified hosts, network protocol, user, or virtual routing function (VRF).

Figure 9. Endpoint Identification, Flow Monitoring, and Compliance Management

[4] TCP port 139, an open port to the internet, can become a security risk when the service listening to the port is misconfigured, unpatched, vulnerable to exploits, or has poor network security rules.

Figure 10. Enhanced Network Topology Views with Color Coding



To close out our review of the most current wired networking infrastructure capabilities contained within Arista Cognitive Campus Workspaces, we observed how Arista's Power over Ethernet (PoE) switches can better manage power distribution amongst multiple devices. Instead of relying upon class-based usage, using classified power limits to determine available power, organizations can employ usage-based limits that employ real-time usage to determine power made available. Balancing power usage amongst multiple network devices, especially with the increased deployment of IoT devices and higher power requirements for switches, has emerged as another issue to monitor. We observed how available power was reallocated and adjusted to match real-time usage, thus decreasing the required overall power budget.

(Class-based)

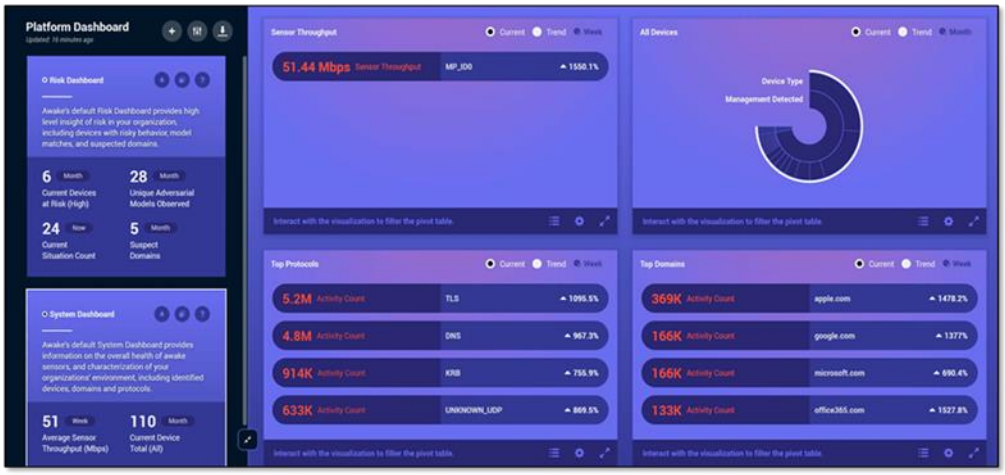
Device Name	Consumed Power
Ethernet2	7.0W
Ethernet3	9.9W
Ethernet4	7.0W
Ethernet20	60.0W
Ethernet21	60.0W
Ethernet22	60.0W
Ethernet23	60.0W
Ethernet24	60.0W
Ethernet25	60.0W
Ethernet26	60.0W
Ethernet27	60.0W
Total	503.9W

(Usage-based)

Device Name	Consumed Power
Ethernet2	3.8W
Ethernet3	3.6W
Ethernet4	3.1W
Ethernet20	1.0W
Ethernet21	1.1W
Ethernet22	1.1W
Ethernet23	1.0W
Ethernet24	1.1W
Ethernet25	1.0W
Ethernet26	1.1W
Ethernet27	1.1W
Total	18.9W

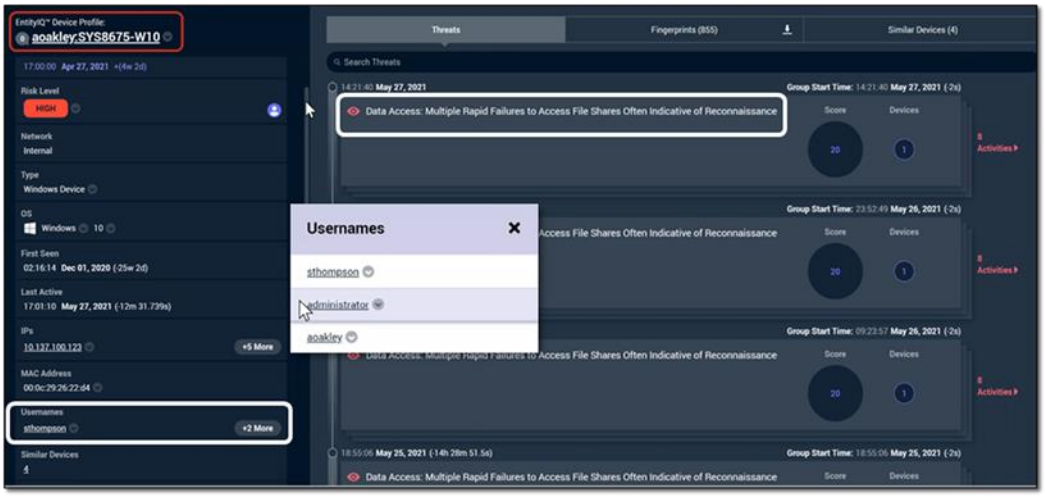
ESG then examined how organizations can use the Awake security platform to secure IoT networks. We first looked at the Platform Dashboard, which summarizes real-time information about network activity. Figure 11 shows activity in our test environment. The environment contained virtual machines running typical activities plus multiple packet capture (PCAP) replays to emulate traffic in a production network environment. The dashboard presented a high-level overview of network throughput using widgets, showing types of devices and whether they are managed, where the traffic is going (Top Domains), and how the traffic is getting there (Top Protocols).

Figure 11. The Arista Awake Platform Dashboard



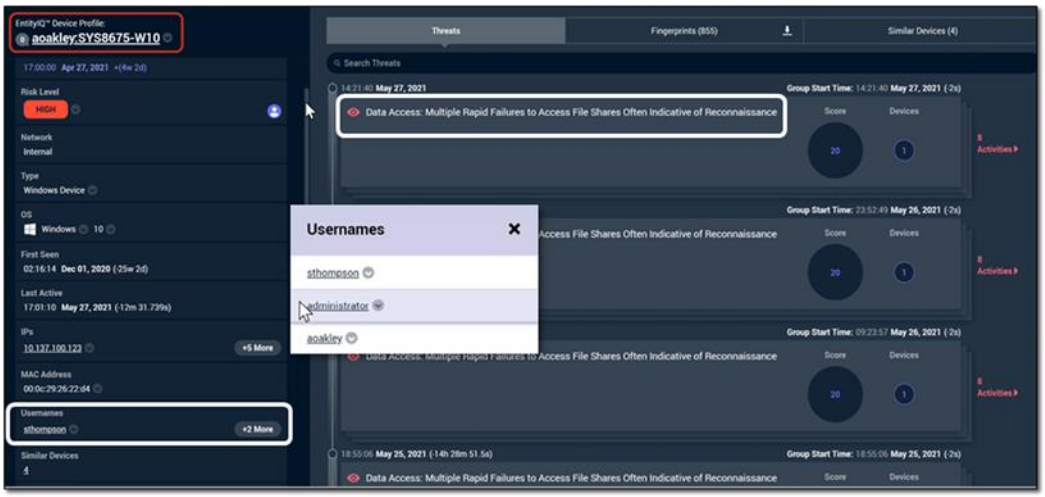
We proceeded to drill down into any widget to learn more detail, as a security operations (SOC) analyst would when investigating potential malicious activity. We clicked on the device type widget and selected managed Windows devices from the drop-down list. Figure 12 shows the Entity IQ screen, with details for the device "*aoakley*." In addition to standard device attributes like IP address and associated usernames, the Awake platform listed other details such as detected threats, fingerprints—AI-generated identifying unique and shared attributes a device has compared to others across the network based on encrypted traffic analysis—and a list of other devices exhibiting similar activity and traffic.

Figure 12. The Arista Awake Platform—Entity IQ Device Details



To illustrate how the Awake platform can identify an attack that was launched using an unauthorized IoT device, ESG observed a simulated investigation of a situation modeled after an attack that Awake had exposed at an actual Arista customer, where an attacker attached a hardware keylogger to a system kiosk to monitor and exfiltrate all input going through that system (see Figure 13). From the Risk Dashboard, we opened the Situation Overlay that detailed the timeline of activities in this attack on the left, from initial access to the execution of the attack (in this case, the exfiltration of data). We noted how the Situation Overlay was completely interactive and how this could help analysts to drill down into any step of the attack. With one click, we could see the source device, its hostname, IP address, the destination it was communicating with, and the time of first access. Another click took us deeper into the details, including access to the original PCAP.

Figure 13. The Arista Awake Platform—Situation Overlay

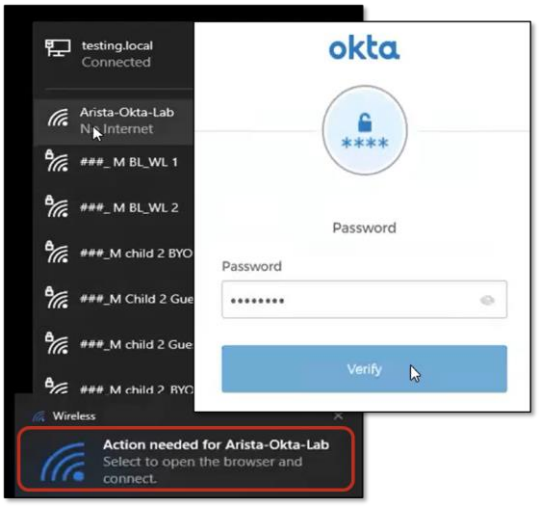


Clicking on the device and selecting View Artifact Details pivoted back to the Entity IQ device details screen (Figure 10). From here, we were able to determine that this device was of an unknown type, a red flag. At the top of the threats list, we saw that the adversarial model for exfiltration had been triggered. Clicking on that model opened up a detailed listing of activities. The first entry showed that this unknown device was communicating with smtp.gmail.com using TLS. In short, it was sending encrypted email to an unknown destination, another red flag. Fingerprints showed that this device was responsible for 100% of traffic on the network using a specific version of TLS and similar devices confirmed that this activity was unique to this device.

ESG was able to leverage Arista Awake to identify an attack that was launched using an unauthorized IoT device. We verified how Awake completely automated the collection of key device and activity data with context, identified the attack, and enabled neutralization and remediation of the attack in minutes, with just a few clicks.

> ESG validated that the Awake platform can help organizations to quickly identify and remediate IoT security issues.

Finally, as more companies are decentralizing with the rise of remote work, Arista recognized the need to provide a more seamless end-user experience while improving both productivity and security. For remote and on-site employees, a typical workday involves accessing a Wi-Fi network and then accessing multiple applications via individual browser windows. These tasks involve entering and authenticating a number of usernames and passwords. However, accessing these resources and authenticated them consumes time and introduces potential security gaps.



The Okta integration with Arista Cognitive Wi-Fi enables employees, regardless of where they are located, to access both corporate Wi-Fi networks and applications with Okta's cloud identity provider (IdP), as shown in the figure to the right. The underlying architecture uses API calls to exchange information and is agentless. No 802.1x is employed; it is an https redirect that enables end-users to access the corporate network and be authenticated by Okta. End-users also gain access to applications as defined by an Okta administrator.

Why This Matters

The corporate network boundary is no longer fixed as the number of remote workers increases, IoT expands, and more public cloud services are consumed. Managing and controlling such a boundary while maintaining end-to-end visibility of the related wired and wireless infrastructure is required.

With Arista Cognitive Campus Workspaces, organizations can manage, monitor, and secure their corporate campus networks regardless of where end-users or endpoint devices are located. Throughout our testing, ESG saw how Arista's solution can help network administrators control and manage the reach and security of its network, beginning with the "client journey," which reveals how an end-user or endpoint device is associated and authenticated to a corporate Wi-Fi network. We validated how an administrator can trace, test for, and identify root causes for any connectivity or application access issue encountered automatically, leveraging both real-time capture of network device data and machine learning. We also saw how network administrators can gain end-to end visibility by viewing how all wired and wireless devices are interconnected and tracking compliance status. With the Awake platform, network administrators can also manage and monitor their IoT networks. Finally, we viewed how Arista Cognitive Campus Workspaces simplifies end-user network and application access and authentication via integration with Okta SSO. By automating network access, device management and monitoring, and issue resolution, organizations can ultimately use Arista Cognitive Campus Workspaces to decrease overall management and operations costs without sacrificing employee productivity and network security.

The Bigger Truth

As organizations deal with a "new normal" of how and where employees will work, they are prepared to allocate more IT dollars to accommodate this as well as other business-impacting events that marked the past 15 months. While ESG research uncovered that 40% of respondents will increase technology spending to enable employees to effectively work from home, 53% of those same respondents will increase spending to implement long-term strategies for enabling a resilient IT infrastructure in the event of future major business disruptions.[5] Dealing with an increased number of remote workers, as well as handling the continued adoption of IoT and increased usage of public cloud services, requires a solution that can maintain end-user productivity and security in light of a constantly changing network boundary, as resources are no longer confined in a fixed perimeter.

With Arista Cognitive Campus Workspaces, organizations can manage and monitor their wired and wireless infrastructure via aggregated and anonymized datasets collected in real time from any user or endpoint. Once the data is compiled into a unified, state-based, network-wide database, the Arista Cognitive NetDB, organizations use the CloudVision portal to locate, diagnose, and determine solutions for issues that can impact end-user productivity and security. Organizations can also automate workflows so that users and devices can connect to corporate networks, thus decreasing operational costs without compromising productivity and security.

Through demos conducted with Arista, ESG validated that organizations can:

- Extend the reach of any corporate Wi-Fi network to accommodate remote users or endpoint devices.
- Show the client journey, which reveals how an end-user or endpoint device is associated and authenticated to a corporate Wi-Fi network and identifies immediately when connectivity issues arise.
- Trace, test for, and identify root causes for any connectivity or application access issue uncovered automatically, leveraging both real-time capture of network device data and machine learning.
- Gain end-to end visibility by viewing how all wired and wireless devices are interconnected and tracking compliance status.
- Bolster overall network security with the use of Arista's MSS-G capabilities.

[5] Source: ESG Master Survey Results, *2021 Technology Spending Intentions Survey*, January 2021.

- Improve means for securing IoT networks within the Arista Awake platform.
- Simplify end-user network and application access and authentication via integration with Okta SSO.

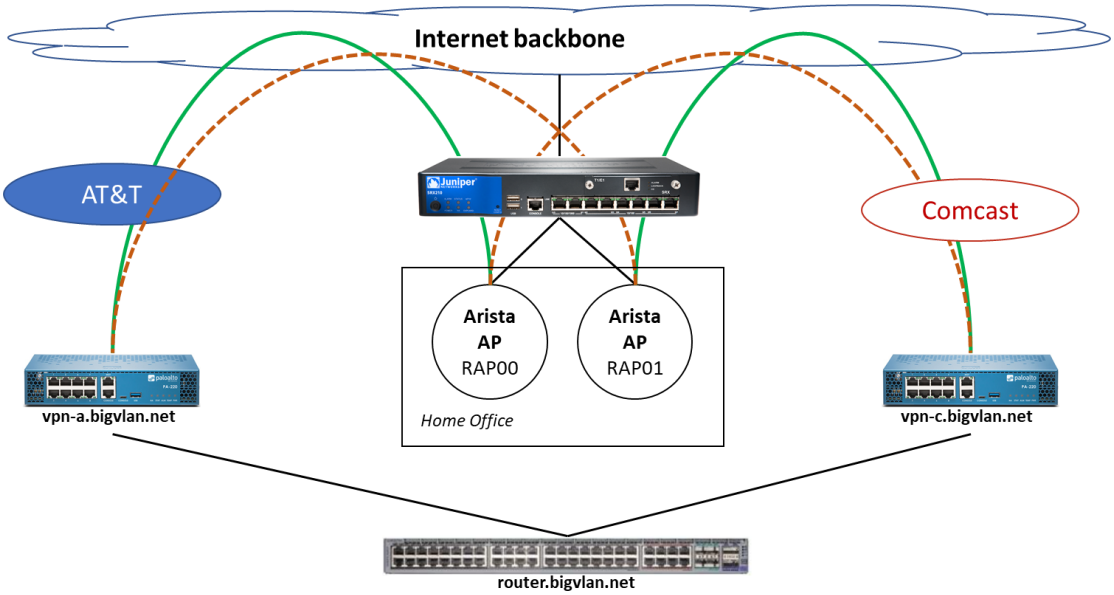
Throughout our observation of the conducted tests and demos, ESG noted how Arista Cognitive Campus Workspaces employs its data-driven model to locate and diagnose network-impacting issues in less time than using separate sets of tools and interfaces to gather information from both wired and wireless infrastructure. With Arista Cognitive Campus Workspaces and CloudVision, real-time data from all wired and wireless devices are gathered and integrated to provide a unified and comprehensive view to automate real-time analytics to support issue identification and resolution. Less time spent on daily operations translates into lower costs, leading to both increased end-user productivity and security.

While Arista has delivered solutions to increase the efficiency and effectiveness of IT network deployment and management, ESG suggests that you consider how much the overall network size and footprint will change and evolve over time. We believe that Arista's solution will gain more mileage out of corporate campuses that anticipate a number of end-users and endpoint devices to be dispersed over a significant geographic area.

If your organization is looking to unify the visibility of your corporate network and automate the location and resolution of issues impacting productivity and security, then ESG believes that you should consider the advantages of using the data-driven model underlying Arista Cognitive Campus Workspaces.

Appendix:

Testbed Diagram 1: Connecting to Corporate Network via Remote Arista APs



Testbed Diagram 2: Isolating Rogue AP from the Corporate Wi-Fi Network