Analysis of the Global Network Access Control Market *More than Just NAC*

(Abridged Report Provided Courtesy of ForeScout Technologies,Inc.)

FROST & SULLIVAN

A Frost & Sullivan White Paper

TABLE OF CONTENTS

Executive Summary

NAC started as a solution to address a massive outbreak of malicious software (also called malware) in enterprise networks in 2003 and 2004. To combat this threat, first-generation NAC products required strict authentication practices and aggressive pre-connect device checks. By 2008, NAC became a more solid and understood technology. Vendors overcame deployment and usability challenges inherent in earlier generation products. Since 2012, enterprise mobility, inclusive of BYOD and wireless security, helped to revitalize customer interest in BYOD, which served as an introductory catalyst for customers that did not yet understand the full capabilities of NAC. The NAC vendors were among the first platform providers to see value in providing dynamic endpoint visibility and being able to apply that data to enforce access, remediate systems, and respond to threats. At the heart of the matter is NAC, a foundational network security defense—endpoints are ultimately the place where intrusions to networks happen, and the last chance to defend or detect a network breach.

- The culmination of improvements in NAC platforms, enhanced endpoint visibility, remediation, and integration with other technologies made NAC a very hot technology.
- Next-generation NAC is winning revenue (budget) that may have gone to vulnerability management, patch management, and other security product vendors.
- The NAC market is forecasted to achieve a compounded annual growth rate of 29.5% and reach $1.46 billion by 2018.

In recent years, three larger technological developments have made NAC more essential to network security. Endpoint visibility, including configuration assessment, adds value to the platform and helps provide crucial information about corporate assets, specialized devices, their location, and the security posture of endpoints. With true endpoint visibility and improved posture assessment, NAC adds "context" to controls. IT directors can establish very granular policies, and can build risk management into NAC and anticipate potential weaknesses in the network through posture assessment and visibility into configurations. NAC platforms are being bi-directionally integrated with other network and security platforms. If properly done, NAC integrated with firewall, advanced threat detection (ATD), vulnerability management (VM), security information and event management (SIEM), mobile device management (MDM), and other platforms improves the efficacy of both NAC and the integrated platforms, and allows these platforms to trigger NAC defense actions.

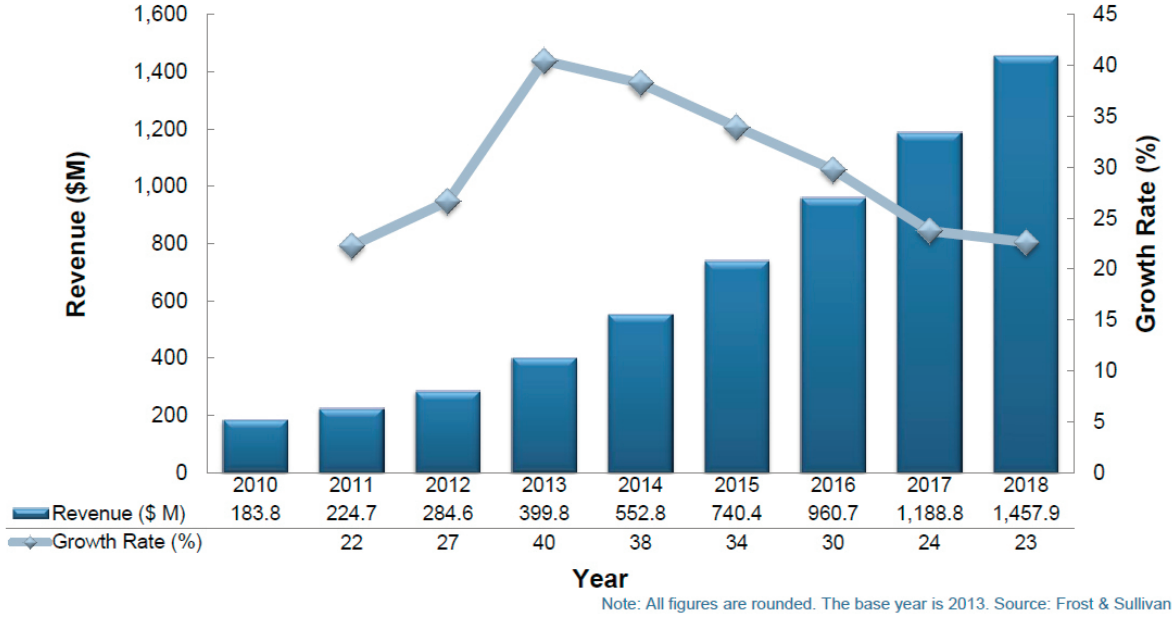
Next-generation NAC vendors can be lauded for improving the fundamentals of traditional aspects of NAC platforms and for expanding their platforms. While there are 14 visible competitors, the top three vendors—Cisco Networks, Juniper (now Pulse Secure) and ForeScout—represent 69.5% of the NAC market. Frost & Sullivan believes the market share of Cisco and ForeScout will continue to

grow through 2018, with Aruba Networks surpassing Juniper Networks (now Pulse Secure) as anticipated market leaders. Competitive factors in NAC include extent of endpoint visibility, ease of use and deployment, pre- and post-admission feature set, granular policy settings, integration with other security tools, scalability, management, global support, and pricing.

The size of NAC deployments is getting larger, mostly because in enterprise accounts, IT teams are continuing to increase the number of endpoints protected (e.g., corporate and personal mobile devices) and the level of added NAC functionality purchased in each contract renewal. Enterprise and mid-sized networks are expanding to include more devices per employee and BYOD. Beyond "greenfield" opportunities, organic growth is also happening as IT directors are dismissing first-generation NAC issues and realizing next-generation NAC capabilities and advantages. Prior installations are upgrading and expanding requirements and implementation coverage at the time of contract renewals.

In 2013, the culmination of improvements in NAC platforms, enhanced endpoint visibility, remediation, and integration with other technologies made NAC a very hot technology. NAC is winning revenue (budget) that may have gone to vulnerability management, patch management, and other security product vendors. Increase in value to the customer is evident in both small to medium-sized (SMB) and Enterprise NAC as the average selling price (ASP) is anticipated to increase, respectively, 16% and 19% over the next five years (2013-2018). Overall, the NAC market grew by more than 40% in 2013 and is anticipated to achieve a compounded annual growth rate of 29.5% and reach $1.46 billion by 2018.

Total 2013 NAC Market: Revenue Forecast, Global, 2010-2018



Note: All figures are rounded. The base year is 2013. Source: Frost & Sullivan

NAC Overview

Next-generation NAC products are essential and well regarded within network security teams. Throughout this report, the virtues of discovering and monitoring endpoints will be discussed in terms of how overall network security is improved. Ultimately, NAC is the last line of defense in network security. If perimeter network defense products represent the front door of cyber defense, NAC is the back door. NAC can be set up to simplify and automate IT operations and coordinate disparate identity, network, security, and reporting tools. The factors driving NAC sales include granular policy settings, full endpoint visibility, ease of deployment, and integration with other security tools. NAC platforms and diversity of support and services varies greatly between NAC vendors. Reliability, extent of endpoint intelligence, policy engine granularity, post-admission controls, complementing other technology platforms, and scalability features are more important than pricing when it comes to purchasing, maintaining, and expanding NAC. Several NAC platforms already have integration modules or built-in integrations with complementary security technologies (SIEM, VM, MDM, and IDS/IPS). Most NAC providers have an OpenAPI or RESTful API as a way to enable integrations with security platforms or custom applications.

NAC products have a base price plus some modular or subscription licensing costs based on the number of endpoints and desired features, including device onboarding, device posture assessment, and security tool interoperability. NAC products are delivered as a hardware appliance or a virtual appliance, with NAC appliances ideally operating out of band and not in line with network traffic. NAC empowers IT administrators to define, implement, and enforce granular access policies for connecting endpoints based on user identity, role, device type, security posture, location, and other relevant factors. To accomplish this objective, NAC products must be able to detect connecting endpoints, regardless of device type (e.g., smartphone, laptop, or wireless router) or connection type (e.g., wired, wireless, or remote).

The IEEE 802.1X is a standard protocol for port-based network access control that evolved from a subset of standards that emanated from the IEEE 802.11i wireless networking system architecture. It requires three components supporting 802.1X management: devices with a supplicant or software agent, an authenticator such as a switch, and an authentication server such as remote authentication dial-in user service (RADIUS). In the past two years, Android, IOS devices, Windows Phones, and Blackberry devices all have embedded supplicants. The device, through supplicants or other methods, can be recognized and managed by the NAC when a device is registered onto a network. With 802.1X-based NAC, a device cannot have authorized network admission unless it is authenticated or authentication has been bypassed via MAC address. The benefit of this type of architecture is that the approach prevents rogue device access as a pre-connect authentication mechanism.

Of the four leading NAC vendors—Cisco, ForeScout, Pulse Secure, and Aruba Networks—all support 802.1X port-based Network Access Control. The 802.1X-based NAC can be challenging, in terms of cost, deployment and maintenance, for users with network components whose 802.1X support varies and for those with endpoints not supporting 802.1X supplicants, such as printers and medical equipment. Additional types of network authentication approaches are: a) a multi-factored approach to device authentication and assessment supports policy-based device discovery, intelligence, profiling and response in real time; b) device profiling and network mapping; c) passive traffic monitoring; and d) the interrelation of endpoint visibility, network mapping, and passive traffic monitoring. ForeScout has a different approach. ForeScout CounterACT can be implemented as either 802.1X or non-802.1X, or in a hybrid approach.

Market Drivers

NAC platforms provide complete endpoint visibility, which is the focal point of access, policy, performance, and security. The most true and simplistic aspect of network defense is that an IT team must understand the security surface it is protecting. This includes a continuous monitoring of all users, devices, system and applications, including virtual applications and machines, and the location of the network endpoint (local, shared data center, cloud, etc.). An endpoint is an entity that has a MAC address or IP address—this includes servers, routers, switches, as well as desktop and laptop PCs, tablets, and mobile devices. Endpoint posture assessment is a nearly ubiquitous feature offered by NAC vendors. Types of posture assessments include application software versions, antivirus, patches, OS upgrades, and hard disk encryption. For example, endpoint assessment can be initiated as a way to see if an application or patch was properly applied.

Contextual awareness has become a part of NAC platforms, leading to more operational intelligence, whereby granular policy settings provide greater efficacy. NAC becomes more valuable by providing dynamic endpoint intelligence to the operator so that the IT team can make informed decisions, adjust policies, or take action from the console. NAC platforms can aggregate visibility into hundreds of thousands of endpoints onto a single console and can also be integrated into help desk, ticketing, and service management systems used by IT and security teams. Contextual awareness is largely what happens when endpoint visibility intersects with cues from other network infrastructure, applications, and security defenses.

Access policy is determined through a multi-factor derivative, which can include the authenticity of the endpoint (does it have necessary credentials to access the network), where the endpoint is located, the user and role, the use of required security software on the endpoint, and the types of applications an endpoint is running or are installed; this can all be factored and applied within a NAC policy for monitoring, reporting, and response. Monitoring, access, and response rules can be customized and weighted to provide different network access control policies based on business need. This can be applied to devices pre-admission and post-network admission.

Similarly, the granular NAC policy can be applied to the type of information not only natively obtained by the NAC, but also obtained by receiving or gathering information from the infrastructure and other systems. For example, receiving information that a MDM-managed mobile device on the network is jail broken. Many of the leading NAC providers have mechanisms that allow the network and endpoint security information to be sent to other network, application, and security platforms, and the NAC system can also receive data from these other platforms. This enhances the context and resulting controls of both NAC and other systems.

NAC is being integrated with other security platforms to enhance the efficacy of the NAC as well as perimeter network defenses. The breadth and depth of integration varies by vendor and may include advanced threat detection (ATD), antivirus (AV), virtual private networks (VPN), vulnerability management (VM), security information and event management (SIEM), mobile device management (MDM), firewalls, and Web gateways. The communications between platforms can be one way or bidirectional, depending on the implementation.

SIEM is great at collecting, assimilating, and analyzing events and log information. NAC can provide the SIEM dynamic endpoint intelligence with regards to network, use, configuration, application and activity details that are important in enhancing SIEM's analytics coverage and supporting forensic tasks and compliance reporting. Additionally, SIEM rules that identify security issue can result in a SIEM message being sent to the NAC platform, which, in turn, can trigger NAC policy to take action on a specific endpoint.

When NAC is integrated with MDM, enforcing policies for corporate and personal mobile device management becomes possible. NAC can enforce access policy to the network based on mobile device and user. NAC can automate the enrollment of unmanaged mobile devices into MDM controls. NAC also delivers network-based enforcement of MDM-controlled devices to trigger MDM profile checks on network requests and to take action on non-compliance devices through device notification, network reassignment, or network blocking.

NAC can also be integrated with other threat management platforms to support identifying threats and taking containment and forensics action. For example, in ForeScout CounterACT, if an endpoint is compromised, the ATD platform can send information to CounterACT to isolate the breached system from the network and even trigger other controls, such as initiating a third-party system image capture for forensics purposes. Furthermore, IOC (Indication of Compromise) properties generated by the ATD can automatically be put to use by ForeScout to check against endpoints accessing or on the network.

Drivers	1–2 Years	3–4 Years	5th Year
NAC platforms provide complete endpoint visibility which is the focal point of access, policy, performance, and security	H	H	H
NAC is being integrated with other security platforms to enhance the efficacy of the NAC as well as perimeter network defenses	H	H	H
Contextual awareness has become a part of NAC platforms leading to more operational intelligence whereby granular policy settings provides greater efficacy	H	H	H
The NAC platform has evolved to match the way that businesses have evolved network architecture and access	M	H	H
A positive secondary effect of having endpoint visibility is formal inventories and compliance reporting can be spun from a central console	M	M	M

Key market Drivers:

1) NAC platforms provide complete endpoint visibility, which is the focal point of access, policy, performance, and security.

2) NAC is being integrated with other security platforms to enhance the efficacy of the NAC as well as perimeter network defenses.

3) Contextual awareness has become a part of NAC platforms, leading to more operational intelligence, whereby granular policy settings provide greater efficiency.

4) A positive secondary effect of having endpoint visibility is formal inventories and compliance reporting can be spun from a central console.

5) The NAC platform has evolved to match the way that businesses have evolved network architecture and access.

A positive secondary effect of having endpoint visibility is formal inventories and compliance reporting can be spun from a central console. A standard component of all security compliance frameworks is the tracking of all hardware and software in an enterprise, as well as ensuring host-based security systems are in place. For example, the first three controls within the Critical Security Controls (maintained by Center for Internet Security and the SANS Institute) ensure an inventory of hardware and software, as well as ensure secure configurations. NAC capabilities address many compliance specifications directly or by integrating with other tools. NAC can see if host-based defenses are not present or active and take corrective action, such as sending alerts about unencrypted disks or missing data loss prevention (DLP) agent. NAC can integrate with vulnerability scanning tools that check for missing patches or the expiration of digital certificates. NAC supports many specifications, including:

- The National Institute of Standards and Technology (NIST) 4.0 was released April 30, 2013. For federal agencies or businesses conducting business with the federal government to be NIST-complaint, a monthly inventory of devices, applications, and OS in use is required.
- As a part of Health Insurance Portability and Accountability Act (HIPAA) compliance, patient healthcare and financial records must be secure. Additionally, the devices that doctors or admissions use to access patient records must also be proven to be secure. For breach notification safe harbor, encryption must be active.
- As part of the Payment Card Industry Data Security Standard (PCI DSS), access to payment processing systems must be segregated, and host-based defenses, patching and vulnerability scanning must be in place.

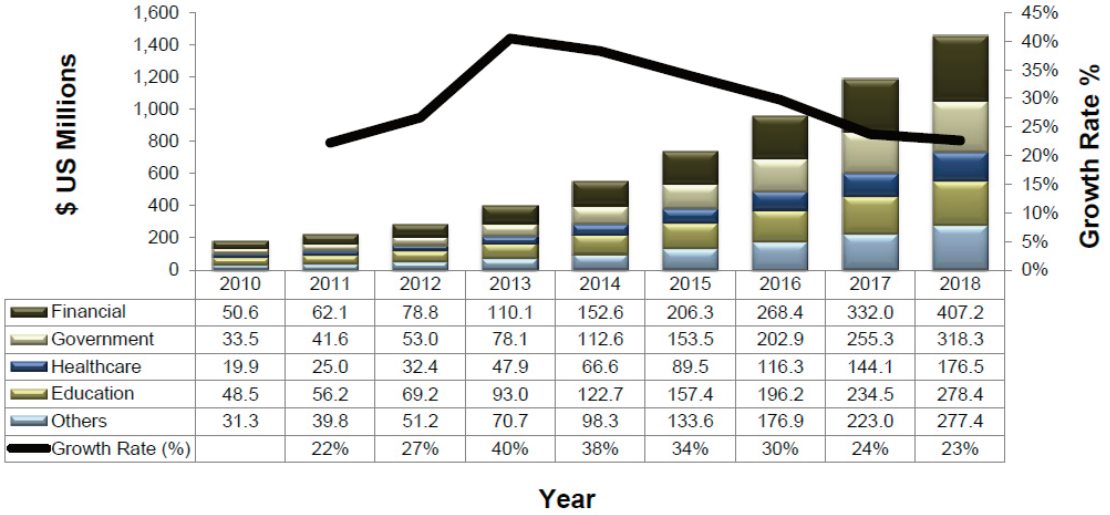
The NAC platform has evolved to match the way that businesses have evolved network architecture and access. Networks are no longer just hardwired Ethernet devices protected by a stateful firewall. Network access includes cellular and Wi-Fi. For many businesses, the network includes offsite data centers, hybrid networks, shared networks, and cloud communications. Businesses are allowing network access to BYOD devices, guest registers, as well as to contractors. In addition, Web-based applications are becoming inevitable and network security products must adapt. Profiling is used to determine what types of devices are on a network at a given time. NAC policy rules can be established for the user, types of devices that are on the network, or the type of device requesting access to the network. Tablets and mobile phones can have different policy requirements. Companies may have different requirements for Android and IOS. An IT team may want to monitor Android devices more closely because Android third-party applications may be perceived as containing malware. Or NAC policy can simply register these devices and relegate access to Internet-only.

In addition, security teams do not have access to all the virtual systems and tools that the IT network operations team uses, yet security policies for virtual systems need to follow similar specifications as physical systems. There is value in NAC being able to provide operational oversight to the security team. Not all NAC vendors have made accommodations to fully integrate into virtualized network technologies like VMware or Microsoft Hyper-V.

Next-Generation NAC Industry Adoption

All types of businesses benefit from NAC. The financial sector, government, healthcare and education are the top four industries purchasing NAC and represent approximately 82% of sales. Others industries, which represent 18% of NAC markets, are commercial businesses, including retail, manufacturing, technology, telecommunications, and utilities. The financial sector is the largest NAC vertical market in terms of revenues. The education market vertical is the largest in terms of unit shipments but has the most confining budgets of any of the vertical markets in this study.

Total Global NAC Market: Revenue Forecast by Vertical Market, 2010–2018



	2010	2011	2012	2013	2014	2015	2016	2017	2018
Financial	50.6	62.1	78.8	110.1	152.6	206.3	268.4	332.0	407.2
Government	33.5	41.6	53.0	78.1	112.6	153.5	202.9	255.3	318.3
Healthcare	19.9	25.0	32.4	47.9	66.6	89.5	116.3	144.1	176.5
Education	48.5	56.2	69.2	93.0	122.7	157.4	196.2	234.5	278.4
Others	31.3	39.8	51.2	70.7	98.3	133.6	176.9	223.0	277.4
Growth Rate (%)		22%	27%	40%	38%	34%	30%	24%	23%

Year

Note: All figures are rounded. The base year is 2013. Source: Frost & Sullivan

Financial Institutions

Financial institutions will continue to be high-priority targets by cyber criminals. Attempting to steal money or monetary assets has been and will always be a constant. Financial markets tend to purchase the most progressive NAC platforms as the consistent improvement in NAC, including granular policy settings, endpoint visibility, and integration with other security platforms, has provided value.

Government

Federal government agencies have strict security requirements and often invest in NAC solutions to prevent unapproved user and device connections. More so, there is a trend to reduce security risks and increase threat response through continuous diagnostics and monitoring programs. State and local agencies are also strong adopters of NAC solutions. For example, in the US, for businesses hoping to do business with the federal government, compliance with NIST 800.53 standards is a requirement. NIST 4.0 requires agencies of the federal government to provide an inventory of devices, applications, and OS every month.

Healthcare

With the rapid adoption of eHeath initiatives, so increases the potential risk to personal identifiable health information and the respective penalties for unauthorized data use and disclosure. As such, there are numerous compliance areas that hospitals must account for, including HIPAA, HITECH, and the Affordable Care ACT. Beyond the challenge of managing employees, contractors and guests, and their BYOD devices, hospitals have been expanding their use of connected medical devices, as well as the deployment of hotspots and distributed antenna systems.

Education

NAC in the education market, both K-12 and higher education, has the most application with school-issued and personal mobile devices with the requirement to on-board both faculty and students. College students are technically savvy and network access is a crucial part of the academic experience. As such, user experience is key in terms of intuitive registration, and reducing time to register, access resources, and re-authenticate. The primary use cases are malware detection, guest management, inventory, and preservation of bandwidth. This market also has material compliance considerations for PCI, FERPA, HIPAA, and copyright laws. Installments with educational institutions can reach 20,000 endpoints or higher; realistically, these NAC deployments have lower management and scale requirements.

Case Study—Financial Sector

A large and familiar provider of financial services has used ForeScout NAC for approximately four years. The corporation is US-based, but has a global footprint. ForeScout emerged as the preferred NAC vendor for several reasons. The IT director was reticent to use competing solutions due to modest pre-connect and post-connect functionality, limited degree of visibility, lack of broad integration, scalability concerns, and fear of vendor lock; his feeling was ForeScout was the best NAC for the company's heterogeneous and large distributed network. Not only did ForeScout provide heterogeneous network support, the solution also supported centralized management of multiple CounterACT appliances. Also, several network visibility protocols were supported by CounterACT, including 802.1X, agentless, MAC address routing, SNMP, etc. Endpoint visibility turned out to be the single feature that most impressed the IT director. The endpoint intelligence provided many important capabilities toward network diagnostic capabilities:

Endpoint visibility does not apply just to the endpoint; visibility is available on the switches and ports that the devices are connected to (and are active). Endpoint visibility can instantly detect unknown, rogue, and unmanaged devices, and take informed action.

Visibility includes the applications that are installed and active on each device. In this specific deployment, the financial institution prohibited Skype, but nonetheless found systems with Skype installed. The institution integrated CounterACT to McAfee ePO via ForeScout ControlFabric.

Patch management validation is an added capability. Patching happens through the patch management app on the endpoint. In one update, the network engineering team changed some device auto duplexing rules in the network. The patch was properly pushed out, but the MAC routing was mismatching the switches and environments. CounterACT was able to show that the devices simply had not accepted the patches. CounterACT is now part of the validation process.

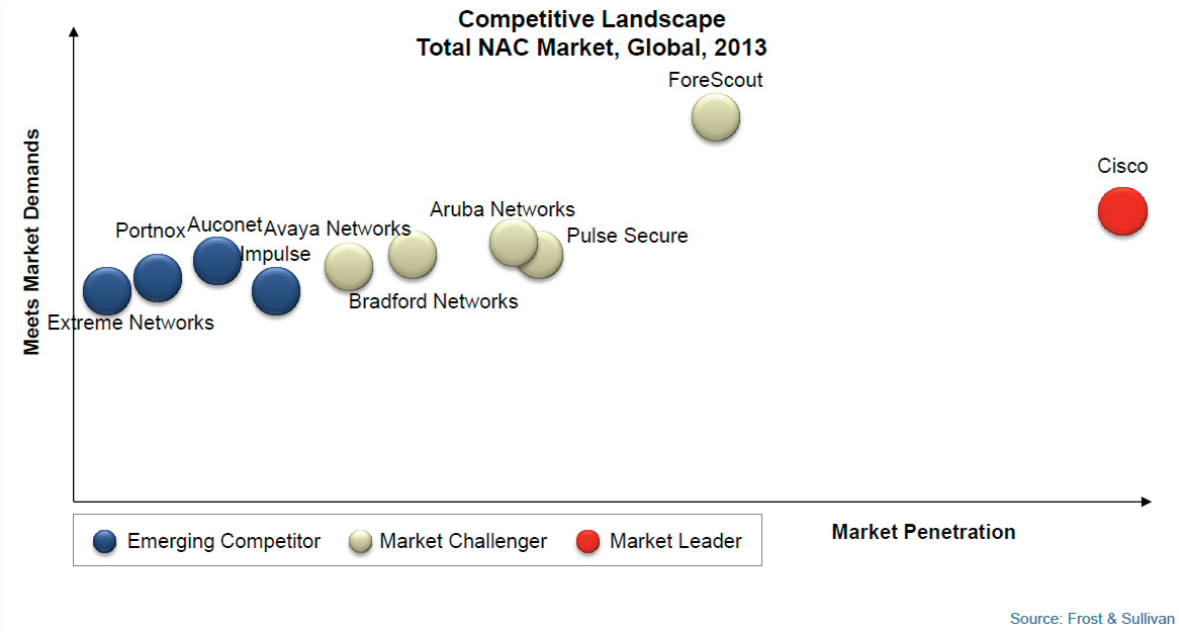
To complement vulnerability scans, CounterACT also does an assessment of endpoints (evaluating

against CounterACT security policies) every few hours or as defined by the administrator to assess security posture. Additionally, when a new device comes onto the network, ForeScout can also inform the vulnerability assessment to run a scan based on the last time a scan was performed. While a vulnerability management scan will check for configuration errors, CounterACT can check for endpoint compliance. In essence, integrating NAC with VM offers a good level of redundancy.
The IT director is convinced CounterACT makes other security tools better, such as firewall, SIEM, VM and ATD—reducing false positives and enabling faster response to issues.
The financial institution was impressed with the risk management analytics in the CounterACT platform, and this helps it make better-informed decisions and reduces analysis effort.

The institution can block rogue devices and do guest networking. The next priority the financial institution had was network blocking based upon non-compliance endpoint configuration settings.

- Wireless was not overly problematic for the financial institution. The internal network made extensive use of two-factor authentication.
- Laptops issued to employees were already pre-loaded with security settings and posture alignment.
- BYOD devices are diverted to a different part of the network.
- Endpoint activity is also an indicator of a potential security breach. Seeing an alert about an endpoint plugging into an unexpected port is common. Also common is an endpoint trying to engage with several ports at once. The CounterACT IPS feature detects these instances and monitors MAC address-bypassed devices.

Market Share and Versatility of NAC Solution



The graphic above plots NAC market penetration against the ability to meet market demands of the NAC solution. Frost & Sullivan believes ForeScout has the most versatile platform and the largest deployments in terms of endpoints protected. ForeScout is noted for:

1. Heterogeneous networking with support for 802.1X and non-802.1X platforms.
2. A highly scalable platform that is especially beneficial to enterprise-sized deployments.
3. ForeScout has the most security platform integration partners. ForeScout NAC can become an integral part of a company's perimeter defense architecture.
4. Excellence in traditional NAC services, including accurate NAC alarms, granular policy settings, and integration of wired, wireless, and VPN into common policy control and monitoring.

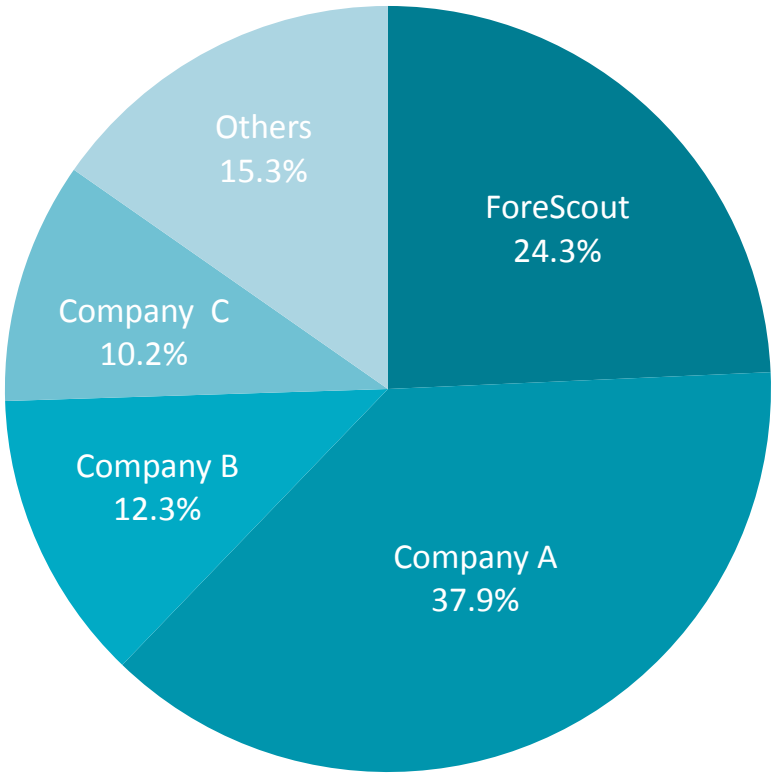
Enterprise Market

The enterprise market NAC is highly lucrative and highly competitive. Enterprise network security teams are looking for a NAC platform that is extensible and self-intuitive. A NAC must be able to quarantine or divert suspicious and non-compliant endpoints. The network security team must then be able to immediately identify the risk and be able to take policy-based or on-demand action. To authenticate the endpoint and validate configuration, the network security team must have complete intelligence about the endpoint (understanding where the endpoint is, its OS, applications, etc.), and its security posture (status of certificates, antimalware, etc.). The enterprise NAC market is more features-oriented than price-sensitive. Endpoint visibility teamed with other control information

gathered from external network and security infrastructure helps improve the overall defense capabilities of NAC. Integrating NAC with existing network security defense products, as well as with directories, increases the value of NAC with enterprises.

Growth opportunities exist in current enterprise NAC deployments. Currently, the largest NAC deployments are with multi-divisional and multinational companies, with headquarters in the United States. In enterprise NAC, enterprises frequently experience organic growth driven by new employees and new devices entering networks. When enterprises renew their NAC licenses, Frost & Sullivan estimates the renewal rates have been at 10%–12% higher year over year. Integration modules, endpoint visibility, posture assessment, and vulnerability assessment capabilities are ways for NAC vendors to monetarily improve NAC licenses. **ForeScout is making the most gains with enterprises, Cisco remains steady, and Aruba Networks is leveraging NAC within its wireless install base. ForeScout has 24.3% of the Enterprise NAC Market.**

Percent of Revenue
Enterprise NAC Market Segment
Global, 2013



Vendor Profile - ForeScout

Based on our research, ForeScout was distinguished as offering the most versatile platform, possessing the largest deployments in terms of endpoints detected and being competitively rated the highest to meet market demand.

Overview

Founded in 2000, ForeScout is a privately held company based in Campbell, Calif. ForeScout has regional offices in London, Tel Aviv, and Hong Kong. ForeScout has a significant focus on large enterprise, mid-tier customers and government. The company reports that as of January 1, 2014, it has more than 1,800 customers in 62 countries and over 200 channel partners.

Company Strengths

- ForeScout's CounterACT delivers continuous monitoring and mitigation based on integrated Network Access Control technologies.
- The network security platform addresses numerous visibility, access, BYOD/mobile security, endpoint compliance and threat management risks. Customers cite cost-savings, resource optimization and improved return on security investments.
- Reasons vocalized by enterprises for why they chose ForeScout CounterACT: rapid and easy deployment, 802.1X support, agentless and agent options, robust functionality, scalability and interoperability. The policy engine is flexible and offers granular pre- and post-admission control using extensible policy templates.
- CounterACT has been designed to work with a variety of legacy and heterogeneous infrastructure: wired, wireless and virtual. It has solid mobile security/BYOD capabilities, including guest management, onboarding, mobile NAC functionality and MDM interoperability.
- ForeScout leads the pack with advanced interoperability, using its standards-based ControlFabric architecture open to vendors, integrators and customers. ForeScout pioneered bidirectional integrations such as EPP, SIEM, MDM, VA, NGFW and ATD.
- ForeScout's breadth and certifications give it a strong footing in government accounts; they are well positioned for continuous diagnostics and monitoring programs.

Product Line

ForeScout CounterACT is an integrated network security platform that offers access control, endpoint compliance, mobile security and threat management. The CounterACT platform, delivered on an out-of-band appliance with foundation and add-on software modules, offers core NAC capabilities and demonstrably distinctive pre-admission and post-admission asset intelligence, network enforcement and endpoint remediation capabilities via a centralized console, high-performance correlation engine, and extensible integrations and policies. These are some key elements of the CounterACT platform:

- Multi-factor network, user, device and application classification and profiling that does not require agents or, where agents are necessary, support for persistent and non-persistent agents.

- Authentication, on-boarding and control flexibility; supports 802.1X, non-802.1X and hybrid mode.
- ForeScout ControlFabric Architecture enables extensive infrastructure interoperability through open standards and APIs to support switches, firewalls/VPN, wireless controllers, directories, patching, and databases; used to exchange control context and enable policy-based mitigation.
- ForeScout Integration Modules. ForeScout-developed advanced integrations: endpoint protection, mobile device management (MDM), security information event management (SIEM), vulnerability assessment (VA), advanced threat detection (ATD), and next-gen firewall (NGFW).
- ForeScout BYOD functionality. Built-in guest management, BYOD device on-boarding, network-based mobile device controls, broad MDM integration, and a Mobile Security Module—offers MDM-lite functionality, such as device intelligence, configuration and application policy enforcement, and jailbroken/root detection (no containerization).
- Noteworthy: Extensive capturing of endpoint properties and security state pre- and post-network admission. Mobile security functionality is broad and can run independently or can be combined with MDM.

Next-Generation NAC Capabilities

- Diverse endpoint classification and intelligence enables more flexible and granular security policies.
- Solid corporate and personal mobile device on-boarding, policy management and enforcement.
- Continuous monitoring with advanced threat mitigation as an integral part of the platform.
- Dynamic software and hardware inventory, virtualization integration, and compliance reporting.
- Comprehensive integration with other network, security and management systems to enhance and fortify a company's oversight, overall security posture and threat mitigation capabilities.

CounterACT Installation

- CounterACT is installed as an out-of-band physical or virtual network appliance connected to a span or mirror switch port or network traffic aggregator. CounterACT has extensive infrastructure support.
- Different models and interfaces are available, which manage as little as 100 and up to 10,000 concurrent network devices. It is highly scalable, has high availability options, and offers an enterprise manager appliance to manage up to 250 appliances, which provide the administrative console means for visibility and dynamic policy management for 500,000 devices (an enterprise director is planned).
- CounterACT is deployed at core, access or distribution switch layers, and supports centralized and decentralized network architectures. Central management is managed in various ways, such as DHCP, DNS, and MLPS, to negate an appliance per network segment. It performs application-layer inspection and integrates with LAN, VLAN, RADIUS, directory services, FW/VPN, etc.

- CounterACT binds into the authentication process and captures broad user, network, device, system and application properties used for visibility, classification, profiling, reporting and policy-based actions, such a guest management (captive portal), network enforcement and endpoint remediation.
- ForeScout CounterACT can be implemented without an agent and supports a broad array of network and security infrastructure. Therefore, the platform can be implemented relatively faster and with nominal network re-architecture (as evidenced through customer interviews and testimonials).
- ForeScout offers a persistent or dissolvable SecureConnector agent, which establishes a secure tunnel between the client and the CounterACT appliance for dynamic inspection and policy enforcement of devices where CounterACT does not have credentials.

Security Policies

- Passive and active monitoring capabilities provide comprehensive visibility into user, device, system, application, network, security posture and authentication diagnostic details. The system displays the operational state in a well-designed GUI. Any endpoint property can be used in a policy.
- CounterACT has built-in policies for device, system and application classification, and templates for endpoint compliance and security posture monitoring. These are completely extensible. The policy engine allows for simple to complex logic with granular and flexible response: monitor-only, network enforcement and endpoint remediation.
- Customers start in monitor-only mode to refine rules and exceptions before phasing in strong policy response. Policies can be administered centrally and locally to align to business requirements.
- CounterACT also monitors device behavior to address MAC spoofing and advanced threat activity.
- Network enforcement is broad and includes captive portal, DNS hijack, HTTP browser hijack, guest management, alert/report-only, allow, limit, terminate, VLAN reassign, switch ACL, WAP assign, 802.1X block and more. Endpoint remediation includes informing user to self-remediate, install/activate/terminate applications, and more. Actions can be on demand via GUI or automated within the policy.
- CounterACT offers "Virtual Firewall" device isolation via manipulating network communications.
- ControlFabric open and standard interfaces, such as REST API, Syslog, CEF, and SQL, allow CounterACT to send intelligence and control data to other systems or receive such information. This can trigger CounterACT policy-based actions for network enforcement and direct endpoint remediation.

Endpoint Visibility and Compliance

- Integral to CounterACT is real-time network asset intelligence. The system dynamically identifies and classifies users, device types, and network, system, hardware and application details. Integration with directory services and other applications allows for other properties to be associated with a device.
- CounterACT captures device properties using passive and active techniques via network integration, including switches, DHCP, DNS, FW/VPN and more. This allows for the identification of managed and unknown devices, including wired, wireless, PC, mobile, embedded, printers and virtual.
- CounterACT can directly inspect a device without requiring an agent by providing credentialed access, such as admin rights to Windows domain PCs. Optionally, organizations can employ agents, which provide a secure tunnel between the device and CounterACT.
- Advanced device fingerprinting technology allows for the identification and classification of more uncommon or custom devices, such as medical, surveillance and industrial, and applications.
- CounterACT captures a vast array of device properties (too numerous to list). Discovered properties can be used in policies to determine the security posture of endpoint pre-admission and post-admission—essentially identify what is on your network, as well as what is wanted and unwanted.
- Endpoint details are available in the console GUI tactical map, tables, alerts and reports, and policy engine. This dynamic information can be shared with other systems via ControlFabric interfaces.
- CounterACT offers extensive information for VMs running on VMware ESXi (or under vCenter) to include OS, device classification, hardware inventory, VM settings, connected peripheral devices, etc.

Facilitation of Mobile Security/BYOD

- The CounterACT platform can identify and apply policy for personal and corporate-issued mobile devices, such as laptops, smartphones and tablets, personal WAP, and portable storage.
- The platform integrates with popular wireless infrastructure, including Cisco, Aruba and Motorola, and provides network enforcement, wireless LAN assignment, user/device on-boarding and more.
- CounterACT has comprehensive guest registration capabilities, including captive portal with DNS and HTTP hi-jack, as well as employee-sponsored guest management. ForeScout also offers mobile device on-boarding with certificate management.
- ForeScout offers a Mobile Security Module (MSM), which offers some mobile device management functionality such as identity, inventory and endpoint compliance, password and encryption verification, jailbreak detection and more. This is delivered as a CounterACT licensed module plug-in as well as mobile device app for Android, and for Apple iOS as an app and profile via Apple's Live Push Technology (only Android and iOS are supported). No containerization is offered.

- CounterACT MDM Integration module supports multiple mobile device management tools, such as MobileIron, IBM FiberLink MaaS360, VMware AirWatch, Citrix XenMobile and SAP Mobile Secure.
- MDM interoperability helps organizations automate the enrollment process into MDM controls, gain on-access MDM posture scanning, and enables on-demand or policy-based network enforcement. Once the module is installed, the console displays mobile device status and compliance.
- When a device connects to the network, CounterACT can queue the MDM to do a real-time compliance assessment. If a device is complaint, the device is granted access. If a device in non-compliant, it can be quarantined until the issue is resolved

Integration with Other Security Platforms

- A compelling reason for an organization to work with ForeScout is that CounterACT can be used with other network, security and systems products to improve an organization's overall security posture and to enable IT to respond to a broad number of compliance, security and IT management issues.
- ForeScout currently has integrations with 60 vendors and numerous products based on the company's ControlFabric architecture comprised of open and standard interfaces, such as SYSLOG, LDAP, CEF, SQL and REST API.
- CounterACT base integrations support a good number of infrastructure devices, such as popular switches, firewalls, VPNs, RADIUS, wireless network controllers, ESX and more. Users with CounterACT appliances under maintenance can download base integration plug-ins as available.
- Extended integrations developed by ForeScout, in the form of licensed CounterACT Modules, offer more advanced interoperability with different popular vendors by category, including endpoint protection suites (ePO), SIEM, MDM, NGFW, advanced threat detection (ATD) and vulnerability assessment (VA).
- CounterACT can send and receive information with other systems to enhance control context and invoke policy-based response. For example, CounterACT can send endpoint posture details to a SIEM, and a SIEM rule can send data to CounterACT to invoke a response such as to isolate a system, initiate MS-SCCM patching, request a VA scan or send a log of activity for each task.
- Organizations that we have interviewed have expressed the value of different integrations and the flexibility with which the CounterACT platform can be integrated with commercial and custom systems.

Advanced Threat Response

- CounterACT offers advanced threat response through direct network monitoring and response capabilities, and also by integrating with other Advanced Threat Detection (ATD) systems.

- CounterACT's built-in intrusion prevention technology, called ActiveResponse, monitors for anomalous and malicious behavior to detect internal zero-day and targeted threats.
  - As post-admission IPS technology, active response can identify and respond to anomalous and malicious behavior on a monitored network segment. For example, it can identify and terminate propagating worms or breached systems that perform network interrogation activity.
  - It can also determine when a system has changed, such as a printer that is attempting to perform a communication associated with a Windows system. CounterACT's post-admission monitoring capability addresses NAC Mac-spoofing risks due to use of MAC exception lists.
  - Honey pot-like technology also identifies systems attempting to take advantage of known but fake system and application exposures, and therefore helps reduce the risk of targeted attacks.
- CounterACT has an ATD Integration Module that enables interoperability with leading ATD systems, such as those from Palo Alto Networks, FireEye, Bromium, Damballa and Invincea. CounterACT can identify systems that require ATD host protection, and can also enable ADT defense enrollment.
  - CounterACT can receive information from an ATD system and insulate the breached system.
  - CounterACT can also extract the ATD-provided IOC (indication of compromise) and put the signature into a CounterACT IOC repository. CounterACT's IOC scanner can then look for the same advanced threat signature on devices attempting to access or operate on the network

Continuous Monitoring

- Essentially, continuous monitoring means that security blind spots and risks are largely reduced through dynamic and poll-based methods that occur on network access request and post-admission.
- CounterACT delivers continuous monitoring via synchronous and asynchronous infrastructure and system integration. CounterACT interfaces with switches, firewalls, VPN concentrators, wireless network controllers, RADIUS, directory services, endpoint protection suites and VA systems.
  - CounterACT can monitor 802.1X requests to an existing RADIUS server (or its RADIUS service), as well as Dynamic Host Configuration Protocol (DHCP) requests.
  - The system monitors SPAN ports to inspect network traffic, such as HTTP traffic and banners. Network mapper (NMAP) scans discover where hosts reside in the network.
  - CounterACT can read user and device groups and policies within directory services. It can also send SQL queries and writes to external databases.
- CounterACT can assess the configuration and security state of an endpoint, including installed applications, connections and network activity, and take action based on policy.
  - Policies can be used to install or terminate applications or to trigger patch management systems.

- CounterACT can trigger a vulnerability scan on devices at connection via VA Integration Module.
  - CounterACT obtains VA details, such as last scan, vulnerability, severity and risk, which can be applied to policies for reporting, to initiate scans, and to invoke endpoint remediation actions.
- Extensive post-connection monitoring and IPS differentiates ForeScout from competition.

Inventory and Compliance

- Maintaining control over all network hardware, software and applications is a foundation of all popular IT security frameworks. Enterprises should also verify that security defenses are properly installed and active; for example, having the means to prove that device encryption is active. Network complexity, consumerization and endpoint configuration dynamics often result in operational gaps.

- In the course of a deployment, ForeScout reports that many of its clients underestimate the number of devices on their networks, as well as adherence to security policies.
  - For instance, a company may suspect that it has 10,000 devices, when is it not uncommon for CounterACT to discover 12,000 devices—a 20% gap or more depending on company size and network distribution. This common observation was verified through multiple customer interviews.
- ForeScout enables enterprises to maintain accurate network asset intelligence, including hardware, installed and running software, and network location, reducing previously mentioned operational gaps.
  - Endpoint visibility, compliance and remediation capabilities details were described earlier.
- Among NAC vendors, ForeScout CounterACT has achieved the US government's highest security certification; the National Information Assurance Partnership Common Criteria (NIAP CC) gives CounterACT version 7 an Evaluation Assurance Level (EAL) score of 4+.
- ForeScout CounterACT is on the United States Army Information Assurance Approved Products List (US AI-APL).
- ForeScout CounterACT is also Federal Information Processing Standard Publication 140-2 (FIPS 140-2)-certified.

Revenue Breakout

- ForeScout had considerable growth across vertical and regional markets, demonstrably in government, financial services and healthcare, as well as manufacturing, education, retail and energy.
- Growth rates are strongest for deployments of 10,000 endpoints or greater; more than half of bookings were from mid-tier enterprises. The company sells its product through a network of global, national and specialized channel partners, and there is an array of training and professional services.

- ForeScout is winning new accounts and achieving expansion in existing accounts.
  - Account expansion occurs in many forms, such as expanding deployment coverage from wired to wireless; adding divisions, regions and acquisitions; enabling BYOD policy; and through integrations such as augmenting MDM and ADT investments or maturing SIEM capabilities.

New Since January 2013

- Numerous endpoint monitoring and remediation enhancements, as well as extensive VMware ESXi/vCenter monitoring, virtual network enforcement, and endpoint compliance enhancements.
- ControlFabric enhancements: new Advanced Threat Detection and Vulnerability Assessment vendor interoperability, and Open Integration Module WebAPI baseline inquiry (custom integrations).
- Console, endpoint monitoring and reporting enhancements such as portal additions for guest registration and management, and support for Asset Reporting Format (ARF).
- Additional infrastructure support such as DHCP classification enhancements and IPv6 support.

Auckland
Bahrain
Bangkok
Beijing
Bengaluru
Buenos Aires
Cape Town
Chennai
Colombo
Delhi/NCR
Detroit
Dubai
Frankfurt
Houston
Iskander Malaysia/Johor Bahru
Istanbul
Jakarta
Kolkata
Kuala Lumpur
London
Manhattan
Miami
Milan
Mumbai
Moscow
Oxford
Paris
Pune
Rockville Centre
San Antonio
São Paulo
Seoul
Shanghai
Shenzhen
Silicon Valley
Singapore
Sophia Antipolis
Sydney
Taipei
Tel Aviv
Tokyo
Toronto
Warsaw

Silicon Valley
331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041
Tel 650.475.4500
Fax 650.475.1570

San Antonio
7550 West Interstate 10,
Suite 400
San Antonio, TX 78229
Tel 210.348.1000
Fax 210.348.1003

London
4 Grosvenor Gardens
London SWIW 0DH
Tel +44 (0)20 7343 8383
Fax +44 (0)20 7730 3343

877.GoFrost
myfrost@frost.com
www.frost.com

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?

For information regarding permission, write:
Frost & Sullivan
331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041