FROST & SULLIVAN

50 Years of Growth, Innovation and Leadership

The Business Advantages of NAC as a Service

Benefits, Requirements and Considerations for the Customer and MSP

A Frost & Sullivan
White Paper
Co-sponsored by
Forescout Technologies, Inc
and Konsultek

Rob Ayoub,
Global Program Director
and
Chris Rodriguez,
Industry Analyst

www.frost.com

ForeScout

KONSULTEK
Connected To Your Success

CONTENTS

INTRODUCTION

Best practices for securing enterprise networks and data have traditionally focused on perimeter defenses such as firewall, virtual private networks (VPNs), intrusion prevention systems (IPS), gateway anti-virus, and others. These products excel at protecting sensitive internal resources from external network-based threats. Unfortunately, these solutions fall short when defending the network from unauthorized access via Ethernet and wireless connections. This challenge is compounded by the increasing number of remote and guest end users, as well as the proliferation of personal and mobile devices touching the network. Concerns around malware, data leakage, and compliance have organizations looking for products that provide comprehensive network visibility, access control, endpoint security and policy enforcement. It may be surprising to CIOs that next-generation Network Access Control (NAC) products can address these very difficult challenges.

In order to be relevant, a next-generation NAC solution must provide capabilities beyond basic network access authentication. NAC's goal of holistic network protection necessitates the ability to identify all users and network-attached devices and to apply a broad number of role- and policy-based security services ranging from device classification, endpoint security assessment and remediation, guest networking, access enforcement, and post-admission monitoring. To achieve this goal, a next-generation NAC solution must provide real-time visibility into the network by identifying, profiling and applying security policies to every IP-enabled device.

This paper discusses the advantages and challenges facing the modern enterprise and how NAC, and especially NAC delivered as a managed service, solves many of the challenges associated with the technology. Furthermore, this paper examines the top requirements and considerations for a successful NAC-as-a-managed service investment from the customer and service provider perspective. Lastly, the paper provides an assessment of how ForeScout's CounterACT solution aligns with end user and service provider business needs.

NAC—AN ESSENTIAL DEFENSIVE AND ENABLING TECHNOLOGY

NAC solutions provide a mechanism for network access authentication, guest networking and endpoint compliance, which helps prevent data leakage, endpoint compliance violations and the propagation of malware introduced by unprotected endpoints.

Some solutions rely extensively on the 802.1x protocol for authentication and access control. With this protocol, the authenticator (an 802.1x-enabled switch or wireless access point) requires endpoints to have a managed 802.1x supplicant and submit credentials at a network connection attempt. The authenticator then checks with an authentication server for access approval. Based on these credentials, the authenticator then either grants or denies access to the supplicant. Businesses must manually add unmanaged devices or devices that do not support 802.1x to an

exception list. 802.1x can be a part of the NAC architecture, but it should not be the only security mechanism offered, given its high potential for operational impact and cost (see 802.1x Challenges). Complete NAC solutions will support a wider range of authentication, inspection, and remediation services.

While 802.1x does not enable endpoint posture assessment, a full NAC solution can define the minimum security baseline to include any combination of compliance parameters, such as operating system version, service pack or patch levels, or the presence of active security software, such as anti-virus, firewall, and anti-spyware. By determining the endpoint security posture, NAC customers can better understand and reduce their organization's operational risk.

802.1x Challenges

There exists some confusion with solely relying on 802.1x. The authentication protocol falls short of providing the rich features of NAC. Many organizations that deployed 802.1x discovered that the protocol itself does not assess endpoint health, and alone, only offers the ability to allow or block network access. The polar allow or deny mode can seriously impact operations. Furthermore, 802.1x can only manage endpoints with the requisite supplicant software, making it difficult to manage devices that do not support supplicants, are not corporate owned, or access multiple network domains. In many cases, 802.1x may require organizations to upgrade or replace their network infrastructure. In short, the larger, more dynamic or more complex the implementation, the higher the cost and greater the risk for an 802.1x approach to succeed.

NAC integrates with directory and identity management systems to enable the creation of security policies based on end-users' identities. Businesses can ensure that employees have access to the network resources that they require to perform their jobs and prevent access to sensitive, unauthorized systems and data. This promotes productivity while preventing data leakage. Similarly, network access for guests and contractors can also be defined and limited to only specific and appropriate network resources, also based on user and device security posture.

Beyond enhanced security, NAC's features offer measurable cost savings for IT organizations. NAC solutions can minimize the level of IT intervention for a multitude of labor-intensive activities, such as: guest registration, asset management, detection and elimination of rogue systems, remediation of vulnerable systems, auto remediation of common endpoint security issues, as well as reporting and auditing processes. The ability of NAC solutions to create and enforce granular security policies also helps organizations achieve compliance with industry and government regulations. A commonly cited example of NAC solutions boosting

compliance efforts occurs with the Payment Card Industry (PCI) Data Security Standard (DSS), which has a broad range of requirements that demands a multi-layer defense strategy. Table 1 gives just one example of how NAC can help organizations meet these requirements by listing key PCI requirements and NAC capabilities that meet these needs.

Table 1: PCI Requirements and NAC Capabilities

PCI Requirement	NAC Solution
Limit access to cardholder data by job function	Role-based access control policies
Policy development and maintenance	Endpoint health assessment
Minimum password requirements	Configuration checking
Network security testing	Network inventory and auditing

Furthermore, data from the NAC solution can be integrated and recorded into log and event management, ticketing, and systems management solutions to support incident response, auditing and change validation. This reduces the time necessary to demonstrate compliance and to avoid penalties and fees associated with non-compliance.

NAC CHALLENGES

Although NAC currently provides a number of benefits, historically NAC is also known for a number of challenges related to complexity, agent requirements, interoperability, and potential operational disruption. Table 2 describes some of the key challenges that organizations face with traditional NAC deployments.

Table 2: Key NAC Challenges and Effects on Enterprise

Challenge	Organizational Effect
Complexity	Increased deployment time and costs
Lack of integration with network environment	Network upgrades or replacement required
Limited control options; 802.1x only	Weak security; reduced productivity
Agent-based solution	Decreased end-user experience

NAC vendors that failed to address these challenges have fared poorly in the market or have exited the market, while innovative NAC vendors evolved their approach and extended their functionality to meet these challenges. By doing so, these vendors not only better support customer requirements, but enable NAC-as-a-Service with significantly lower implementation costs and faster time to value for both customer and service organizations.

THE VALUE OF NAC-AS-A-SERVICE

The key value proposition for NAC-as-a-Service is an accelerated implementation cycle, improved service results with little or no capital expense, predictable operational expense, and reduced in-house expertise. For the service provider (SP) or managed security service provider (MSSP), NAC provides a way to extend security services to their existing install base and to increase business opportunities.

NAC-as-a-Service Advantages for Customers

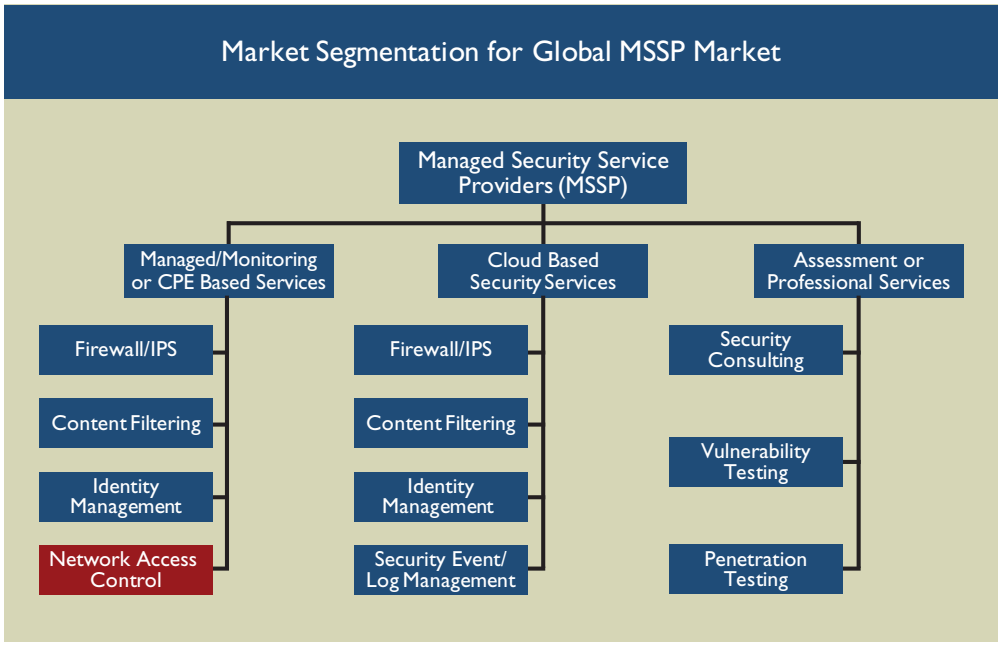
As a managed service, NAC requires minimal capital investment, as the customer is able to make regular payments for product use and services to the provider. Managed NAC services also reduce business risk as enterprises don't have to assume all capital costs (including resources and expertise) that would be necessary with an outright purchase and operation of a full NAC deployment. A managed services approach provides cost-savings by eliminating hundreds of labor hours needed to understand, deploy and manage the NAC solution, including associated costs such as training and tuning. Instead, a managed NAC service ensures that deployment and on-going management is done by highly-experienced and regularly trained security professionals.

NAC-as-a-Service ensures that businesses receive cutting-edge protection and can yield the maximum value from the investment. Ideally, the service provider will be able to draw on its previous NAC expertise to yield an optimized deployment and management that avoids pitfalls and enables customization and tuning. Additionally, because many businesses face a similar set of access control, endpoint security, and remediation requirements, as well as the need to support similar industry and regulatory mandates, managed security providers will be able to implement the NAC solution in a manner that satisfies these requirements.

NAC-as-a-Service Advantages for Service Providers

NAC also offers business advantages for managed security service providers. Since there is no one security product that can address all internal and external network-based threats, a defense-in-depth strategy requires the use of multiple security technologies. The managed security services market is growing rapidly but is very competitive, and service providers must continue to seek new strategies to differentiate their portfolio and extend value to customers. Figure 1 illustrates NAC's positioning within a MSSP portfolio.

Figure 1—Market Segmentation of Global MSSP Market



Source: Frost & Sullivan North American MSSP Market Study

By adding a NAC solution to a MSS portfolio, service providers can re-engage customers with regularly scheduled consultations and in-depth security reports. This allows the MSSP to strengthen customer relationships and demonstrate a commitment to provide comprehensive security services. Table 3 lists the service practices associated with NAC.

Table 3: Managed NAC Services

Training	Ticketing and incident response
Policy development and maintenance	Endpoint remediation
Installation and integration	Enforcement and tuning
Network inventory/device classification	Operational/compliance reporting
Guest networking	Endpoint and mobile security monitoring

PRODUCT REQUIREMENTS FOR NAC-AS-A-SERVICE

There are numerous solutions available in the marketplace today, but not all products provide the full benefits of NAC. Since there are competing approaches to NAC, customers need to understand the implications of these approaches before choosing a solution.

NAC-as-a-Service Requirements for Enterprise Users

- Out-of-band appliance architecture
- Agentless scanning and enforcement, with optional persistent and dissolvable agents
- Access authentication
- Real-time device profiling and inventory
- Flexible policy management
- Integration with broad range of network and security technologies
- Wide breadth of enforcement options and technologies, including guest account management, automated registration, user self-remediation, and auto remediation
- Post-admission monitoring

NAC-as-a-Service Requirements for Service Providers

- Virtual appliances to efficiently deploy and scale the solution
- Remote management capabilities
- Role-Based Access Control (RBAC)
- Payment options, training, marketing and technical support
- Ongoing product and feature development

FORESCOUT'S NAC-AS-A-SERVICE PLATFORM

Frost & Sullivan believes that service providers and enterprises both should shortlist ForeScout's CounterACT platform when considering NAC-as-a-Service. As a platform for a managed NAC service, CounterACT offers versatile and enterprise-grade capabilities that provide tremendous customer value and service opportunity. From a non-intrusive, interoperable and scalable product architecture to a complete, integrated feature set, ForeScout's CounterACT provides all the key elements of a solid managed service offering.

ForeScout's NAC-as-a-Service Innovation

ForeScout offers many innovative features in its CounterACT managed solution that further increases the value for customers and service providers. A few of these innovations are highlighted below.

Integration and Interoperability

ForeScout CounterACT is an integrated platform that provides real-time network asset discovery, 802.1x and non-802.1x access enforcement, device classification management, policy management, guest registration management, self-assessment and remediation management, policy-based enforcement, and remediation. This NAC solution is delivered in one physical or virtual appliance, which makes the solution significantly more efficient to deploy and manage. Although the system ships with support for a wide range of network and security infrastructure, ForeScout also offers 24x7 technical support services and a portal with plug-ins for leading network, security and identity vendors. This NAC platform integrates with third-party tools such as Microsoft NAP, McAfee ePO, eEye Retina, BigFix, Aruba, Xirris, VMware, ArcSight, Nitro Security and Lumension for additional policy and security management. For consideration of government clientele, CounterACT is also certified against Common Criteria standards EAL 4+, which at the time of this publication is the highest certification achievement among NAC products.

Agentless Discovery with Device and User Monitoring

CounterACT's agentless endpoint discovery and monitoring technology gives it the ability to identify, auto classify, and assess all network-attached devices in real time without requiring agents. This pre-admission and post-admission assessment can be handled without an agent, or with dissolvable or persistent agents called ForeScout SecureConnector. Sophisticated device fingerprinting capabilities leverage identified attributes from multiple sources, including NMAP, WMI, HTTP, RPC, directory service and SMB, to identify and classify new and known devices. CounterACT maintains an active asset inventory, including device type, owner, user, location, time, device type, hardware details, applications and security posture, which it presents in the management console and portal. CounterACT can manage users and enforce their network access based on the role in the organization. User management can be done internally or via integration with common directory services, including Microsoft Active Directory, RADIUS, TACCAS, Novell e-directory, SUN One and any user-defined LDAP server.

Mobile Security

CounterACT agentlessly classifies all wireless corporate and personal mobile devices, such as smartphones, netbooks, notebooks, tablets, and WAPs by brand and user in real time. Using HTTP redirection, mobile users can be forced to register their devices for access. Mobile device security policies can deny access or limit access to VLANs and network resources. ForeScout has introduced mobile applets, such as for Android, for even greater mobile control.

Flexible and Powerful Policy Creation

CounterACT further expedites implementation by providing numerous, extensible policy templates and a policy creation wizard. Policies cover a broad number of control processes, including guest networking, wireless, security agent status such as anti-virus, application whitelisting and blacklisting, external storage device use and more. The policy interface is intuitive and advanced, supporting simple to nested logic. Access policies are applied to user and device types and can provide monitoring, escalated response or full enforcement. This flexibility allows organizations to conveniently apply progressive policies, as well as to easily manage exceptions.

Broad, Advanced Enforcement

CounterACT supports numerous enforcement options, including 802.1x, VLAN assignment, port blocking, layer 3 ACL, HTTP re-direction and MACFF. ForeScout can interface with popular VPNs to execute compliance checks on endpoints post-connection to the VPN gateway. The solution's advanced ACL enforcement capabilities allow CounterACT to dynamically update ACLs on a customer's existing switches, routers and firewalls, and routers at either layer 3 or access layer with device-by-device or port-by-port level enforcement. A virtual firewall enables a TCP reset mechanism, whereby a connection can be terminated before a handshake is completed—isolating a device from network resources. This enables enforcement where VLANs are not available or too many VLANS would be arduous to manage. Beyond integrated guest management and end user self-remediation management capabilities, CounterACT offers background endpoint security remediation, including re-activating, installing and updating anti-virus client software or executing appliance-hosted scripts. Automated guest registration, enforcement and remediation capabilities enable companies to optimize resources and defenses.

Continual Network Protection

CounterACT provides post-admission monitoring to block threats originating from inside the network. This capability utilizes behavior-based detection technologies to provide ongoing, real-time threat prevention. Automated post-connection monitoring is extensive to identify and stop suspicious activity, unwanted actions and propagating threats. This capability enables organizations to monitor for devices that represent threats through the following behaviors:

- change their profile (for example, a printer which now acts as a Windows system)
- use blacklisted software (peer-to-peer or instant messaging) or devices (USB storage)
- attempt to interrogate network resources

By comparison, competing NAC solutions do not monitor endpoints after network admission and therefore cannot address these threats.

NAC-AS-A-SERVICE SUCCESS

An MSSP Customer Perspective

With 28,000 employees, one of North America's largest transportation companies must lock down more than 8,500 endpoints in 300 offices around the world. The company outsources its IT program to two different managed security service providers. Despite a full security architecture that includes firewalls, intrusion prevention and anti-virus systems, the company recognized a gap in its security architecture. Rogue users could easily connect their devices to the wired or wireless network without the company's knowledge. In addition to closing this threat vector, the company also wanted real-time visibility into all the devices on its network to be able to allow access only to authorized users, by policy, as well as to provide guest-user access.

The Selection Process

ForeScout CounterACT was shortlisted during the first stage of their product evaluation process along with three competing solutions, including McAfee, Cisco, and Juniper. The company then determined that CounterACT best met its criteria in terms of cost, interoperability, manageability and ease of implementation, as compared to competing solutions. In particular, the company has a varied, complex and distributed network where attempting to implement and manage a pure 802.1x approach would be disruptive and not effective.

The company selected the ForeScout CounterACT solution; however, the company's security service provider, a large national provider, at that time was not familiar with this solution. The service provider, which also provides a competitive NAC solution, analyzed the product at the company's request. The provider concluded that it indeed would be a valuable addition to its solution set. The service took advantage of ForeScout's professional services to train and certify its experts to be able to implement and managed the solution.

Putting NAC into Practice

The company utilized a phased deployment, which included proof-of-concept testing, beta deployments, appliance deployment, and network mapping. The service provider deployed the CounterACT solution, which consisted of five appliances in the company's two data centers, and was centrally administered by a CounterACT Enterprise Management appliance. CounterACT was able to integrate with a variety of endpoints, the network and systems, including directory services, and quickly accommodate exceptions where the company assets were managed within a third-party network or by multiple providers. In less than six months, CounterACT was fully deployed and provides complete network monitoring.

CounterACT enables the customer to identify and monitor all endpoints on the network in real time, including guest devices, and determine device compliance with security policies such as anti-virus and patch-level requirements. When a device is

unknown or violates policy, notification is provided and a trouble ticket is automatically issued. Within the ticket, CounterACT provides identity, location, and endpoint configuration details to streamline problem resolution. This IT organization plans to complete additional device categorization and finalize response and remediation requirements to enable broad NAC enforcement and automated mitigation by early 2012.

Project Results and Analysis

CounterACT has already elevated the customer's security policies and will soon automate the respective controls by blocking rogue users, devices, and wireless routers. The company has also identified tangible cost savings by limiting end-user access to productivity applications, reducing help-desk tickets, and eliminating dedicated DSL services for guest access. Additionally, CounterACT enables this company to embrace the trend of mobile devices on the enterprise network. End users will be able to access limited network resources from their own mobile devices, and the company will improve connectivity by providing staff with tablet computers.

Lastly, the company is exploring expanding the use of the system internally to support PCI-DSS compliance and other auditing initiates. Overall, the customer considers the NAC deployment a success, and CounterACT has enabled the company to extend their security architecture and business practices to be more competitive and efficient.

MSSP Perspective #1

"To me [the ForeScout NAC deployment] is a success…this is the right product; it just does everything we want."
—Manager of IT Security

A large IT service provider that operates in Canada and the United States is considered the incumbent solution provider for many large businesses looking to outsource their IT strategy. The service provider recognized the need for a NAC solution when a customer requested the ability to provide guest network capabilities, as well as endpoint posture security capabilities.

After considering multiple vendors, the service provider preferred ForeScout's ability to apply identical security policies to every access point supporting the user's existing network and security environment. This solution would be able to effectively control all devices requesting network access, whether wirelessly or wired. This solution also recognized and allowed the customer to apply controls to any device, managed or unmanaged—in real time.

The service provider required a non-intrusive solution to meet its static SLA requirement to not impact business productivity. The SLA allowed for solutions to be offline for a given period of time, but to not reduce end-user productivity or resource availability. Therefore, the service provider was able to eliminate solutions that represented a single point of failure or increased network latency. The ForeScout solution met these requirements and provided vendor-agnostic support for a wide range of network and security technologies. Additionally, automated remediation simplified the management process and helped reduce the window of exposure.

After extensive testing to ensure that the solution would meet its current and future needs, the service provider decided to deploy the solution in three major stages. The service provider allotted six months for each stage to tweak policies and to introduce end users to the process. First, the service provider did a pilot deployment and then deployed the NAC solution deeper in the network. The organization is now moving into deploying advanced features such as NAC enforcement and mobile device strategies.

The service provider considered ForeScout's management console to be user-friendly, which improved the company's ability to deploy and manage the solution. It also required a solution capable of integrating with other management tools since the same team would be responsible for managing several different technologies.

The service provider had company-level criteria besides product features and management capabilities and sought partners that demonstrated dedication to ongoing product and strategy development. In this regard, ForeScout has a long history of product innovation and demonstrated the ability and willingness to anticipate and support the service provider's requirements throughout the deployment process. ForeScout met many of the service provider's product and company-level requirements and contributed to a successful NAC deployment.

MSSP Perspective #2

A service provider with facilities in the United States and Central America sells a range of different security capabilities and technologies, with the goal of mitigating risk for its customers. Despite a strong portfolio of Web security, e-mail security and encryption capabilities, the service provider identified the need for a solution that could address the "insider" threat. Insider threats ranging from fraud to malware, whether committed maliciously or unintentionally, are a leading concern for the service provider's customers.

The service provider required a solution that offered low implementation times, ease of use and administration, scalability, and support for many different platforms. ForeScout met these criteria and helped the service provider efficiently increase its business. For example, one of the provider's customers had a time-sensitive requirement to meet regulatory requirements within 60 days. After assessment, testing and staging, the service provider was then able to deploy ForeScout in 16 days—only two days for each data center.

For the service provider, ForeScout's open platform enhanced its ability to be easily deployed. CounterACT integrated with the customer's network environment, including firewalls, anti-virus, and switches, regardless of vendor or brand. ForeScout also supported its deployment effort by offering policy creation wizards and policy templates. These product features enabled the service provider to reduce its deployment and training costs.

These features helped the service provider meet its SLA obligations and provide solutions that address its customers' security requirements without negatively impacting business productivity. Specifically, the service provider is required to respond to and resolve security issues ranging from access violations, rogue device detection, malware outbreaks to other policy problems within two days. In addition, the service provider must resolve failed systems within two hours. CounterACT's role-based access control and policy management features enable the service provider to easily manage these deployments remotely, while high availability options are available to insure against operational failures.

Most importantly, ForeScout enables the service provider to solve multiple challenges for its customers. With CounterACT's integrated functions, the service provider can offer a variety of packaged solutions for mobile device control, USB device control, guest control, regulatory compliance, endpoint security, remediation and even automatic inventory. This allows the provider to increase the value of its services, enhance customer relationships, and increase its business.

THE LAST WORD

NAC solutions provide comprehensive means to monitor and enforce network access and endpoint security policy. More recently, interest in NAC has grown considerably as IT organizations face increasingly sophisticated security threats, operational risks from personal mobile devices on corporate networks, and the desire for automation to optimize security resources. Correspondingly, NAC solutions have become easier to implement and more effective so as to enable service providers to consider NAC to complement their security portfolios.

As a platform for a managed service, NAC can enable service providers to reconnect with and increase their value to customers. Service providers should seek a NAC solution that offers broad, integrated functionality, flexible implementation and assured results that not only enhances their customers' defenses, but also represents a low-risk, high-value service addition.

ForeScout CounterACT is a proven, enterprise-class solution that addresses many security risks for customers—from employee and guest access control, to real-time network visibility, mobile security, and endpoint compliance and remediation. This platform reduces service provider risks regarding complexity, integration, impact, scalability and service delivery that have challenged competing solutions. Therefore, customers and managed security service providers should consider the ForeScout CounterACT platform when evaluating a NAC-as-a-Service strategy.

APPENDIX—LIST OF ACRONYMS

ACL	Access control list
CIO	Chief Information Officer
CPE	Customer premise equipment
DSL	Digital subscriber line
DSS	Data Security Standard
EAL	Evaluation Assurance Level
ePO	ePolicy Orchestrator
HTTP	Hypertext Transfer Protocol
IP	Intrusion prevention system
LDAP	Lightweight Directory Access Protocol
MSSP	Managed security service provider
NAC	Network access control
NAP	Network Access Protection
NMAP	Network Mapper
PCI	Payment Card Industry
RADIUS	Remote Authentication Dial-In User Service
RBAC	Role-based access control
RPC	Remote procedure call
SLA	Service level agreement
SMB	Small- to medium-size business
SP	Service provider
TACACS	Terminal Access Controller Access-Control System
TCP	Transmission Control Protocol
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VPN	Virtual private network
WAP	Wireless access point
WMI	Windows Management Instrumentation

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, Texas 78229-5616
Tel 210.348.1000
Fax 210.348.1003

London
4, Grosvenor Gardens,
London SWIW ODH,UK
Tel 44(0)20 7730 3438
Fax 44(0)20 7730 3343

877.GoFrost • myfrost@frost.com
http://www.frost.com

ABOUT KONSULTEK

Since 1994 Konsultek has been delivering technology solutions that connect, protect, inform and manage the information of mid-tier and large enterprises. The company offers a suite of infrastructure lifecycle management, application traffic management, security management and technical support services that maximize their client's efficiency and secures their most critical information. With offices in greater Chicago, England and Singapore, Konsultek offers depth and breadth of expertise to solve problems and implement solutions quickly and with optimum results. For more information, visit www.konsultek.com or call 847.426.9355

ABOUT FORESCOUT TECHNOLOGIES, INC.

ForeScout enables organizations to accelerate productivity and connectivity by allowing users to access corporate network resources where, how and when needed without compromising security. ForeScout's automated solutions for network access control, mobile security, endpoint compliance and threat prevention empower IT agility while preempting risks and eliminating remediation costs. Because the ForeScout CounterACT platform is easy to deploy, unobtrusive, intelligent and scalable, it has been chosen by more than 1,300 of the world's most secure enterprises and military installations for global deployments spanning 37 countries. Headquartered in Cupertino, California, ForeScout delivers its solutions through its network of authorized partners worldwide. Learn more at www.forescout.com

ABOUT FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, partners with clients to accelerate their growth. The company's TEAM Research, Growth Consulting, and Growth Team Membership™ empower clients to create a growth-focused culture that generates, evaluates, and implements effective growth strategies. Frost & Sullivan employs over 50 years of experience in partnering with Global 1000 companies, emerging businesses, and the investment community from more than 40 offices on six continents. For more information about Frost & Sullivan's Growth Partnership Services, visit http://www.frost.com.