FROST & SULLIVAN

Continuous Monitoring and Threat Mitigation with Next-generation NAC

A Frost & Sullivan White Paper

COMMON GAPS IN NETWORK SECURITY STRATEGIES

Conventional security practices are becoming less and less effective. Security solutions such as antivirus (AV), encryption, data leakage prevention (DLP), patch management, and vulnerability assessment (VA) typically assume that all endpoints on a network are well-managed, contain security agents, and remain static on the network (not transient)—problematic assumptions given today's reality of bring-your-own-device (BYOD), the enterprise Internet of Things (IoT), and mobile computing.

Furthermore, the majority of traditional security tools typically operate as independent silos not designed to interoperate with each other. Traditional security tools like VA and intrusion detection/intrusion prevention systems (IDS/IPS) have very specific use cases. VA scans end points for configuration errors and exploitability from known vulnerabilities. IDS/IPS sound alarms when a suspected perimeter breach is detected. Perimeter network defenses do each individual element well. However, many of these network defenses do not share contextual information with other peer security tools and don't provide any native controls for threat mitigation. This silo approach results in security blind spots and a huge burden on security operations staff who need to manually respond to security alerts.

Network Access Control (NAC) is a technology with a nearly two decade legacy. While the technology is well-established, its impact is resurging—Frost & Sullivan forecasts global NAC market expansion at a compound annual growth rate (CAGR) of 30% from 2013 to 2018.[1] NAC engines discover and profile all endpoints connecting to the enterprise network. Part of the reason that NAC is resurging is because this visibility extends to BYOD, mobile, and IoT devices, which is problematic for traditional enterprise security platforms. After endpoint discovery, NAC is able to assess endpoints and then apply policies, which can include placing them in a narrower network segment with a small range of permissions for the end user. NAC vendors have capitalized upon this vantage point to provide insight into endpoint posture assessment and network mapping. Further, NAC's persistent surveillance of endpoints and role-based enforcement of endpoint policies are used in bidirectional integrations with other network security platforms to enhance perimeter defenses. NACs often see what eluded perimeter defenses.

This white paper discusses NAC technology and, more specifically, NAC continuous monitoring and threat mitigation. Additionally, this white paper discusses how the ForeScout CounterACT™ platform is differentiated among other NAC products in the market, requiring no agents or 802.1 X protocols.

THE NETWORK VISIBILITY SURVEY

Frost & Sullivan on behalf of ForeScout conducted a survey of IT and security professionals. The survey was conducted in August-September 2015 to assess the views of these professionals on network security visibility, tools, threat detection, and incident response practices. To get a global perspective, IT and security professionals located in the United States, the United Kingdom, and Germany and employed in large organizations participated in the survey. See below for the number of respondents and size of company criteria.

- **Germany (100 responses).** For Germany, the panel consisted of companies that had 4,000 or more employees, or were listed in the Global 2000.
- **UK (100 responses).** For the UK, the panel consisted of companies that had 4,000 or more employees, or were listed in the Global 2000.
- **US (201 responses).** For the US, the panel consisted of companies that had 10,000 or more employees, or were listed in the Global 2000.

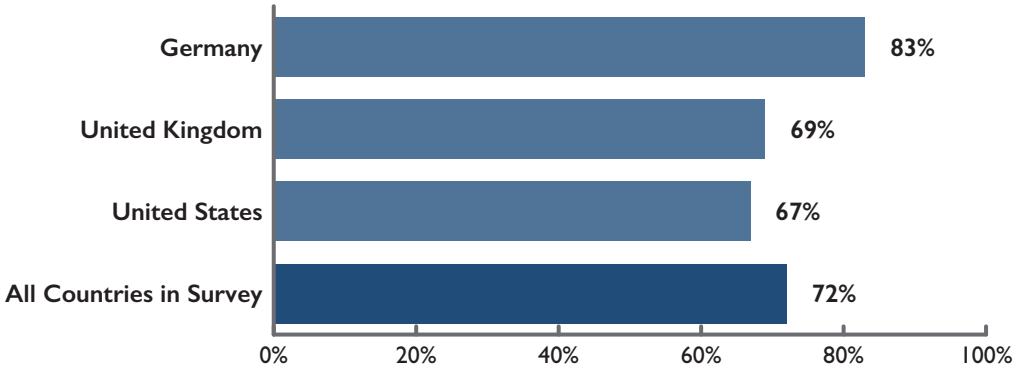
[1] From the Frost & Sullivan Report, Analysis of the Global Network Access Control (NAC) Market, December 2014

KEY RESULTS OF THE NETWORK VISIBILITY SURVEY

The survey asked questions about security breaches and the efficacy of certain network security tools. Pertaining to the breach environment, the IT professionals were asked how many security incidents their company experienced over the past 12 months by specific network components. The network components included managed end-user computers, managed servers, unmanaged BYOD, smartphones/tablets, non-computing devices (IoT), physical intrusion, and network intrusion.

The results were troubling. If all of the network components are added together, the percentage of networks that had five or more security incidents within the past 12 months was 72%.

Exhibit 1. Percentage of Networks that Experienced Five or More Security Incidents Within the Last 12 Months



Source: Network Visibility Study, Frost & Sullivan, October 2015

Looking at the data more granularly, no network component is truly secure. Analyzing the percentage of companies that report at least five security incidents for each network component category, one clear message emerges from the survey data: both managed and unmanaged (BYOD) network components provide penetrable entry points to networks.

Exhibit 2. Security Incidents Reported Within the Last 12 Months

Network Component	Germany	UK	US	Total
Managed End-User Computers	50%	19%	31%	33%
Managed Servers	36%	19%	27%	27%
Unmanaged BYOD or Business Partner Devices	36%	17%	21%	24%
Smartphones or Tablets	42%	17%	23%	26%
Non-computing Device (Printers, IoT, etc.)	34%	19%	24%	25%
Physical intrusion (e.g. stolen media)	31%	18%	23%	24%
Network intrusion (e.g. Wi-Fi attack)	41%	23%	20%	26%

Q. How many security incidents did your organization experience within the last year involving (network component?) Responded five or more incidents in the last year.

Source: Network Visibility Study, Frost & Sullivan, October 2015

Note that the results presented are isolated to five or more security incidents. Managed end-user computers yielded high numbers of security incidents across the board, with an amazing 50% of German firms reporting five or more security incidents. While these results may be jarring, any number of factors exist that can cause security lapses to happen. Network security environments work under the assumption that servers and endpoint agents are properly configured; however, if a misconfiguration does occur, endpoints can get lost on the network unbeknownst to the security team (coming up shortly are survey results about endpoint agents).

Across the board, the results seem high; five security incidents for a single network component category in a year is a lot. Consistent with the idea that network security technologies tend to work as silos, no type of computing device is easily secured. Given the evolution of network architectures, this result is understandable. As recently as seven or eight years ago, network architectures were designed to support Ethernet-connected PCs tethered to a local network. Today, laptop PCs are semi-transient devices and tablets are almost exclusively transient devices. Private, public, and hybrid cloud infrastructures add to network complexity.

The panel was asked if their networks suffered from a "significant" blind spot caused by certain network technology platforms. The resulting data is fairly clear. Regardless of the region or the technology, IT and security administrators stated their networks have significant blind spots (please see Exhibit 2). The survey indicates that better visibility is required, and communication between technologies is needed to shore up blind spots.

Many of the questions in the survey were qualitative rather than quantitative. The scale used was a 1-7 scale. In the survey, "1" represented not significant, while "7" represented very significant ("don't know" was an option).

Exhibit 3. Networks Suffer from a Variety of Security Blind Spots

Network Security Technology	Germany	UK	US
Vulnerability Assessment	38%	32%	44%
Firewall	45%	38%	44%
Network Intrusion Prevention	38%	29%	37%
Advanced Threat Detection	46%	35%	36%
SIEM	39%	31%	38%
Mobile Device Management (MDM)	37%	30%	39%
Endpoint Protection (Antivirus)	37%	33%	35%
Patch and Configuration Management	41%	29%	34%
Does your network suffer from a significant blind spot from (network security technology)? Combined percentages of "6" and "7" on a 7 point scale.			

Source: Network Visibility Study, Frost & Sullivan, October 2015

The increasing complexity of network and information security burdens security teams that are already overtaxed. Most organizations report that they have too few information security workers. Removing manual tasks through automation would seem to make sense, but there are questions about how willing security professionals are to embrace automation. So, the question was put to the survey respondents, "To what degree would your network benefit if they could automatically invoke a set of pre-determined security controls (network security technology)? The survey results indicate a Clarion call for security vendors to add more automation to their products. (Please see Exhibit 3.) Ideally, IT and security teams would like to be able to customize settings; however, a security tool has to be effective out of the box and has to remain effective when integrated with other tools in a layered cyber defense.

Exhibit 4. Networks Would Benefit from Automated Security Controls

Network Security Technology	Germany	UK	US
Vulnerability Assessment	53%	58%	67%
Firewall	65%	65%	69%
Network Intrusion Prevention	56%	62%	70%
Advanced Threat Detection	62%	56%	67%
SIEM	57%	50%	66%
Mobile Device Management (MDM)	54%	48%	68%
Endpoint Protection (Antivirus)	50%	58%	73%
Patch and Configuration Management	59%	52%	65%
To what degree would your network benefit if they could automatically invoke a set of pre-determined security controls (network security technology)? Combined percentages of "6" and "7" replies.			

Source: Network Visibility Study, Frost & Sullivan, October 2015

Many network security administrators use security and management agents to track endpoints on their networks. An agent is a small piece of code installed on an endpoint that associates the endpoint to the enterprise network. The advantage to using agents is that an endpoint is more easily recognized by the network and communications such as software updates are more easily facilitated between the endpoint and the network.

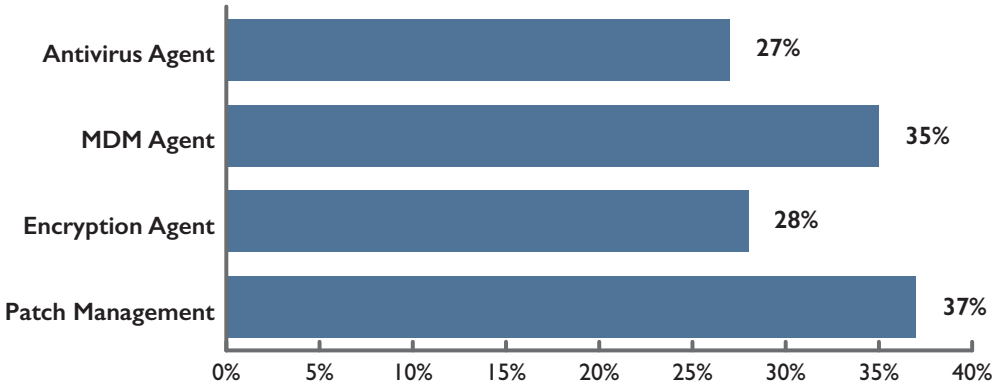
However, there are three significant problems with agents. The first problem is that the majority of cyber security tools use a "polling" type of scan technology. Commonly, in vulnerability management (VM), security information and event management (SIEM), and other cyber technologies, semi-persistent scanning is initiated. This procedure works well for static devices that are attached by Ethernet to a network. However, as networks are designed to accommodate more mobile devices, much happens dynamically between polling events. Transient devices are easily lost. The second problem is that agents can be misconfigured or disabled. An enterprise network is often a fluid environment. Endpoints are frequently reconfigured and new office locations are dropped or added. If an agent is not functioning properly, the network loses visibility into the endpoint and security can be compromised.

The second problem with reliance on security agents is that agents required by IT teams cannot be installed on the increasing number of personal (BYOD) and IoT devices on the enterprise network. Hence, reliance on agents means that the network isn't aware of the fastest growing segment of endpoints coming onto the enterprise network and reduces the organization's security posture.

The last problem with security agents is reliance on security agents brings a false sense of security. In the Network Visibility Survey conducted by Frost & Sullivan, the survey asked security professionals about the confidence levels they had about the installed antivirus, mobile device management (MDM), encryption, and patch management agents they had on their networks.

Recognizing that answers of "6" and "7" represent high or extreme confidence in agent installments, presented here are replies of 1 thru 5, which demonstrate a confidence that is less than "on point."

Exhibit 5. Low Confidence that Security Agents are Installed and Working Properly



Source: Network Visibility Study, Frost & Sullivan, October 2015

A foundational element of network security is knowing what is on the network, and how each infrastructure device and endpoint is related. The survey data suggests organizations lack true visibility to the devices connecting to their networks. Transient devices have changed the game in terms of network exposure. The long suits for NAC are endpoint visibility, network segmentation, and access and control—the fundamental security characteristics needed to provide cyber defense in today's connected reality.

NEXT-GENERATION NAC SOLVES THE PROBLEM OF BLIND SPOTS INSIDE THE NETWORK

Next-generation NAC dynamically identifies, inspects, and controls all network-connecting devices, including wired, wireless, and remote endpoints, as well as ensures that managed endpoints are compliant with security policies. As a result, the value of next-generation NAC has moved beyond the simple access authorization offered by earlier NAC solutions. NAC reduces the risk of exposure by minimizing the attack surface represented by insecure devices, compromised or rogue devices, unauthorized users, and unwanted applications.

NAC provides visibility and can begin the remediation process for endpoints that agent-based solutions cannot, such as personally owned devices and IoT devices. This latter category includes printers, industrial equipment, security systems, and healthcare devices—anything on the enterprise network that cannot be managed with an agent. NAC solutions categorize these devices and place them on differentiated-access network segments. The segmentation to cordon off sections of the network reduces the security risks of compromised devices to the rest of the network. Once a device is compromised, an attacker can spoof credentials to access sensitive data or launch attacks. Some next-generation NAC systems include traffic monitoring capabilities, which can detect suspicious activity from unmanaged and IoT devices and quarantine them from the rest of the network to prevent threat propagation.

Similarly, bring-your-own-device (BYOD) is a top concern for many enterprise organizations that need to enable employee mobility, while maximizing flexibility of device selection and minimizing security risks. Mobile device management (MDM) systems require software to be installed on each mobile device, which introduces additional complexity and effort on behalf of end users and IT staff. The combination of NAC and MDM provides the visibility, management, and granular control of all connecting devices necessary to secure a BYOD strategy.

In the *2015 ISC² Global Information Security Workforce Study*, prepared by Frost & Sullivan, 13,930 security professionals were surveyed. Two questions were asked that give perspective about the challenges of integrating new technologies into the framework of network security:

1. Does securing the use of emerging technologies adopted by your organization (e.g., BYOD, social media) consume a significant amount of time? **50% of the participants responded yes.**

2. In which areas of information security do you see growing demand for training and education within the next three years? **47% of the participants responded BYOD will require additional training.**

While the most apparent value proposition of next-generation NAC is in access controls, network visibility, continuous monitoring, and endpoint posture assessment, there may be more than meets the eye. A good platform with self-intuitive dashboards can help cut down future costs in personnel training and development, as well as in maintenance and monitoring.

NEXT-GENERATION NAC SOLVES THE PROBLEM OF TRANSIENT DEVICES

As stated previously, most existing IT security and management systems were designed to work best with static endpoints. Because traditional network security systems assume static endpoint networks, semi-persistent scanning/monitoring seems like a reasonable option. For example, vulnerability assessment systems are typically operated periodically, such as once a month or once a week. The problem with periodic scanning in today's world is intervals between scans are likely to miss seeing a laptop computer that is only present on the network for short periods of time.

IT organizations can utilize NAC's real-time endpoint intelligence capabilities to continuously monitor all connecting devices, ensuring that corporate devices and approved guest devices meet a required security posture on a continuous basis. This monitoring and checking ensures required security software, patches and configuration software are present, running, and up to date.

NAC policies are flexible and can be set to instantly notify the user, helpdesk or security professionals on known issues and violations; quarantine non-compliant endpoints; or initiate the remediation processes directly on the endpoint. This instantaneous security response and policy-based remediation capability is essential to minimize exposures and rapidly respond to a broad range of security issues. Next-generation NAC offers flexible, policy-based, network-based endpoint inspection and control mechanisms to enforce security policies at the time of network connection and after. These advanced technologies are used to protect enterprise networks in the following ways:

- **Agentless endpoint identification.** Without agents, a next-generation NAC can identify, profile, and monitor in real time all network-attached endpoints, including employee devices, guest devices, and IP-enabled devices that cannot support a software agent such as printers and CCTV systems.

- **Discovery.** Next-generation NACs can discover and remove unauthorized devices, rogue wireless access points, and unmanaged legacy systems.

- **Access control.** Access control policies allow an IT team to manage corporate-owned mobile devices and reassign employee-owned mobile devices to guest VLANs.

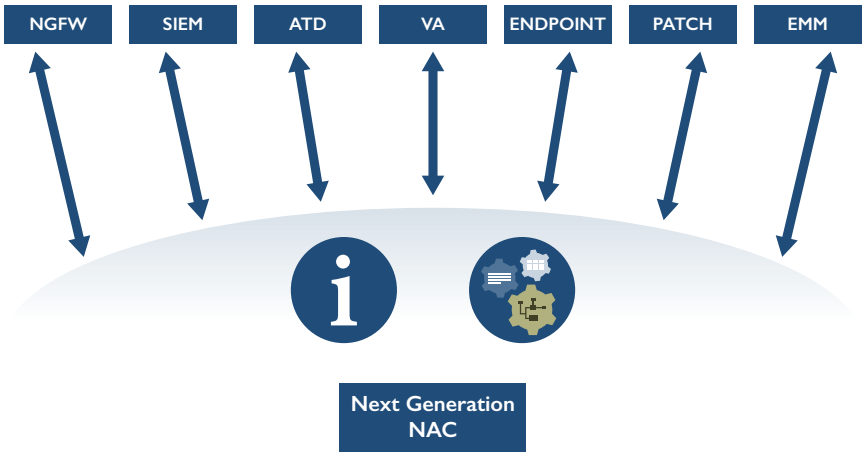
- **Network awareness.** As next-generation NACs have comprehensive network visibility, the NAC can inventory devices and systems in real time. Not only are next-generation NACs application aware, they can terminate unwanted or unauthorized applications, such as Instant Messaging and Peer-to-Peer (P2P) file sharing running on a system.
- **Security Agent Validation.** Next-generation NACs provide a double check in ensuring that security agents such as antivirus, patch management, encryption, and system update tools are installed, enabled, and up to date.
- **Continuous monitoring for security and compliance.** One of the main benefits of next-generation NAC is the ability to continuously monitor endpoints to identify signs of compromise or non-compliance.
- **Alarms and alerts.** Next-generation NAC is a highly proactive tool. A security team can respond to policy violations: logging, alerting, limiting access, blocking, and quarantining. The NAC can then be used to begin endpoint remediation.
- **Platform integrations.** Next-generation NACs are able to interoperate with VA, MDM, security information and event management (SIEM), advanced threat detection (ATD) systems, and other tools to improve a company's overall security posture.

NEXT-GENERATION NAC SOLVES THE PROBLEM OF SECURITY SILOS

The ability to integrate bidirectionally with systems such as next-generation firewalls (NGFW), vulnerability assessment, mobile device management, data leakage prevention, antivirus, configuration management, and security information and event management (SIEM) is an essential and differentiating factor for NAC solutions. After gleaning information about endpoints on the network, NAC can send this information to other security tools. NAC can also receive information from these tools. As a result, the policy engines of both the NAC and other security tools are greatly enhanced with shared intelligence. For example, NAC can identify devices that do not have required patches and inform a desktop management system of the non-compliance. Alternatively, a vulnerability scanner or advanced threat detection solution can identify vulnerable or breached devices and inform NAC to remediate or isolate said devices.

Bidirectional integration also allows NAC to perform as a trusted third party, monitoring and verifying the security of systems to ensure that controls and desired changes are active. IT teams report that a NAC management console presents far more accurate and comprehensive information than the management consoles offered by network security platforms as well as configuration management systems. Most importantly, integration with directory services, wireless and MDM systems enables the NAC platform to automate identification, enrollment and mitigation of personal and mobile devices. Therefore, bidirectional integration mechanisms allow next-generation NAC to form a symbiotic relationship with customers' existing security tools to accomplish a broad array of monitoring and risk mitigation tasks.

Exhibit 6. Next-generation NAC Integrations with Security Technology



Source: ForeScout, Frost & Sullivan

NEXT-GENERATION NAC ALIGNS TO IT-GRC FRAMEWORKS

The powerful and flexible controls offered by a next-generation NAC platform not only fortify dynamic protection, but can also be used to satisfy compliance requirements. Continuous endpoint intelligence and remediation are germane to achieving and substantiating compliance with a wide variety of IT Governance, Risk Management, and Compliance (GRC) requirements, including federal and industry standards such as Federal Information Security Management Act (FISMA), Continuous Diagnostics and Mitigation (CDM), Payment Card Industry Data Security Standard (PCI DSS), North American Electric Reliability Corporation (NERC), Health Insurance Portability and Accountability Act (HIPAA)/Health Information Technology for Economic and Clinical Health (HITECH), and Defense Information Systems Agency Security Technical Implementation Guide (DISA STIG). These regulations define required security practices such as authorized access and network segregation, endpoint configuration integrity and compliance monitoring, threat remediation, and event logging. Enterprise IT organizations can utilize next-generation NAC solutions to support a number of IT-GRC frameworks and regulatory requirements by leveraging the following next-generation NAC capabilities:

- **Host-based system security (HBSS).** NAC endpoint intelligence and integration with vulnerability assessment and HBSS suites addresses the requirements that devices are configured properly, are scanned and protected against vulnerabilities, and are utilizing active HBSS suites as outlined by PCI DSS, HIPAA, and DISA STIG.
- **Endpoint remediation.** Automated endpoint remediation supports PCI DSS, National Institute of Standards and Technologies (NIST), and Gramm–Leach–Bliley Act (GLBA) requirements for remediation and endpoint security.
- **Access control requirements.** Port-based access control requirements, outlined by PCI DSS, DISA STIG, GLBA, and NERC, are fulfilled by NAC's support for 802.1X authentication as well as additional authentication mechanisms for network environments that lack 802.1X support.
- **Support for audit trails.** Integration with SIEM and log management tools will help satisfy PCI DSS, GLBA, and NERC requirements for strong audit trails and monitoring of user access to sensitive data and systems.

- **Systems controls for data and devices.** NAC enables IT organizations to fulfill other requirements such as mobile device control, rogue access point removal, and a data leakage prevention program that are common to multiple regulatory standards.

Next-generation NAC also enables controls for a wide variety of other IT-GRC frameworks and security best practices. For example, NAC functionality can be applied to the Critical Security Controls (CSCs) maintained by the Council on CyberSecurity. CSCs are designed to guide the implementation of effective network security architecture. These CSCs include security best practices, such as inventory of authorized and unauthorized devices and software, secure hardware and software configurations, continuous vulnerability remediation, wireless device control, malware defense, boundary defense, and maintenance and monitoring of audit logs.

The ability to demonstrate to auditors the means to validate compliance at all times is valuable when considering the severity of fines and penalties that these organizations may face for non-compliance. NAC's real-time and continuous monitoring of these controls and devices, as an external verification system, provides a complementary control to support audit and assessment processes.

HOW FORESCOUT COUNTERACT™ SUPPORTS DYNAMIC ENDPOINT INTELLIGENCE AND REMEDIATION

ForeScout is an innovative leader in the NAC market. The company's next-generation NAC solution, ForeScout CounterACT™, is designed to be an enterprise-class solution. CounterACT addresses many security risks facing customers, including employee and guest access control, real-time network visibility, mobile security, and endpoint compliance and remediation.

The CounterACT platform can be used by businesses midsized and larger; however, CounterACT is optimized for large enterprises. Large enterprises and government agencies have specific needs in terms of added functionality and managerial requirements. ForeScout has many significant integration partners and in many cases a plug-and-play solution in an existing cyber defense. CounterACT is quickly deployed in the field, and its dashboards are easy to use. ForeScout enhances its security products with frequent software upgrades and strong customer support.

AGENTLESS OPERATION PROTECTS ALL DEVICES, ALL THE TIME

ForeScout CounterACT operates without agents, collecting important security data about all network-attached devices. This feature allows CounterACT to apply policies to devices that cannot support an installed agent or that are not managed by the IT organization. This includes employee-owned devices as well as enterprise IoT devices.

REAL-TIME FUNCTIONALITY AND LEADING AUTOMATION

ForeScout CounterACT provides rapid time to value, enabling IT administrators to gain a comprehensive and real-time inventory of all attached network devices and important attributes. CounterACT can then be used to create and enforce a number of security policies and responses for non-compliant devices. The automated responses offered by CounterACT can be used to enforce high-security policies or to streamline IT help desk workflows.

FORESCOUT CONTROLFABRIC™

ForeScout ControlFabric enables ForeScout CounterACT to integrate with other IT solutions to exchange information and more efficiently mitigate security risks. These integrations help solve the problem of security silos mentioned previously.

ForeScout ControlFabric includes open interfaces such as SYSLOG, SQL, Lightweight Directory Access Protocol (LDAP), and Web Services API to enable secure, bidirectional communications. These interfaces, which allow vendors and customers to develop their own integrations, complement other integrations that ForeScout has developed with common infrastructure components such as directories, virtual private networks (VPN), next-generation firewalls, antivirus systems, and patch management systems, as well as integrations with IT security technologies such as VA, MDM, ATD and SIEM systems. As of the date of this writing, ForeScout is able to integrate with over 70 different IT security products and services.

The following case studies illustrate how ForeScout has helped large IT organizations advance their security monitoring and risk management programs.

FINANCIAL SECTOR INSTITUTION CHOOSES FORESCOUT COUNTERACT TO AUGMENT ITS SECURITY PRACTICES

In the financial sector, a provider of financial services worked with ForeScout and its CounterACT platform for approximately four years. The corporation is a large US-based corporation with a global footprint.

CounterACT can be used for many different purposes, but the major focus for this financial institution was enhancing its security posture. The financial institution integrates NAC with different categories of security solutions. For its security measures, the institution has a next-generation firewall (NGFW), SIEM, and an advanced threat detection system. For greater visibility and application control, the institution integrated CounterACT with the McAfee ePolicy Orchestrator (ePO) via ForeScout ControlFabric.

Large enterprises have the advantage of having dedicated response teams. NAC, when integrated with a SIEM, for example, can use baseline measurements to determine if a change has happened on an endpoint. If the change is outside the realm of established traffic patterns, an alarm can be sounded. If a verified alarm occurs, the desktop response team can isolate the incident, and quarantine the affected device and ports within 5-10 minutes. (Worth noting, while the corporation's cyber defense grid combined many different technologies and dashboards, the IT director felt he gained value from the risk management analytics in CounterACT.)

COUNTERACT FOR ENDPOINT VISIBILITY AND POSTURE ASSESSMENT

One place where ForeScout is differentiated from other NAC solutions is that it does not rely on 802.1X protocols; although 802.1X is a more commonly used protocol and ForeScout is proficient there as well. In regard to the financial institution, endpoint visibility does not apply just to the endpoint; visibility is needed on switches and routers that the devices are connected to on the network. The financial institution had a hybrid network using several different protocols. CounterACT had no problem in the heterogeneous network as it supports 802.1X, agentless discovery, MAC address routing, and simple network management protocol (SNMP), among others.

Aspects of endpoint visibility include continuous monitoring and isolating endpoints on various server and OS environments. The financial institution has security teams responsible for compliance and endpoint posture. For instance, unique security considerations are given to UNIX and Windows environments. The NAC is capable of immediate endpoint discovery and assessment of configuration details; for example, checking Windows registry settings to ensure endpoint compliance.

Toward assuring that the endpoint postures remain healthy (or signal an alarm if a posture is compromised or starts to degrade), in this installation, CounterACT™ could:

- Re-assess each endpoint every few hours.

- Offer redundancy for patch management and configuration. In one case, a patch was pushed out to endpoints, but the patch installation was incomplete as the MAC routing was mismatching the switches and environments. While patch management suggested the patches were installed, a cursory check of the endpoints showed the patches never got to the endpoints.
- CounterACT informs a vulnerability assessment tool to run a scan when a new device comes onto the network.
- CounterACT provisions devices to different parts of the network. Laptops issued to employees are pre-loaded with security settings and posture alignment. BYOD devices are diverted to a different part of the network.

> *"Some NACs, when scrutinizing endpoints, provide insight into OS and software updates, patches, and vulnerability management. To some degree, this creates a backup (redundancy) to patch management, VM and SIEM."*

COUNTERACT™ IMPROVES COMPLIANCE

With the possible exception of healthcare, United States banking and financial companies have the most compliance requirements. Large financial institutions are subject to a broad range of regulations. This means proving compliance auditing and reporting. Compliance involves regulations established by governments, specific industry standards, and legal entities. Compliance standards can be onerous. For instance, the National Institute of Standards and Technology (NIST 800 Rev 53.4) requires that government agencies initiate a monthly inventory of all devices, operating systems, and applications on their networks.

The financial institution sends NAC information to the SIEM for the purpose of compliance reporting and forensics. Network visibility is a key here. The NAC can relay to the SIEM what user groups an end user/endpoint belongs to, which switches and ports an endpoint/device has tried to access, and what applications are on each endpoint. Compliance reporting is then primarily generated by SIEM and log management tools.

The NAC helps to inform compliance platforms, but the NAC is not the main instrument of compliance reporting. SIEM tools are predominantly used to demonstrate compliance in heavily regulated industries. Notably, synching up endpoint visibility for devices, infrastructure, network mapping, endpoint posture assessment, and applications emanating from an endpoint with SIEM creates redundancy.

FORESCOUT COUNTERACT USED BY A MIDSIZED MANUFACTURER TO UNIFY COMMUNICATIONS

A midsized manufacturer has been a ForeScout customer for three years. The manufacturer has a large distribution channel. The manufacturer's products can be found online as well as in stores that sell appliances.

The midsized manufacturer had specific needs. The NAC had to provide sufficient protection advantages for its large manufacturing plants, regional offices, corporate human resources and administration, and an additional 70 satellite offices. The network had subtle nuances. For instance, employee PCs and Cisco VoIP phones used the same Ethernet port. If access is shut down to the port, it will shunt access for the PC and the phone. The customer also required access control lists (ACL) and VLAN controls.

The company wanted a NAC solution that would be useful for VPN, wired, and wireless considerations. While 802.1X was an option, this manufacturer did not pursue it because a non-802.1X deployment had advantages in

terms of ease of deployment, offered greater visibility, and the platform provided more flexible and granular control afforded by an agentless approach.

One problem that stymied the growth of NAC is that if badly implemented, a NAC can inadvertently shut down a network. Of course, if there is a loss of access to the network, the problems can range from a mild nuisance to an absolute catastrophe. As a manufacturer, the company intimated that in a contest of unacceptable outcomes it would risk a network breach against any shutdown in production.

COUNTERACT™ POLICY ENFORCEMENT

When comparing ForeScout CounterACT to other NACs, the manufacturer felt the CounterACT policy engine was the strongest. The network engineer was able to configure alerts and had several options toward directing devices onto alternative VLANs or shunting access. The network engineer wanted to write policies with contingencies and felt that CounterACT gave him the greatest flexibility.

> *"ForeScout CounterACT was up and running within a week with an option for more tuning if needed."*

The manufacturer produces a commercial product sold through online distribution and in stores, and this meant that part of what the company had to prove was that its practices were PCI-DSS compliant. Compliance reporting was becoming problematic for the manufacturer. The ForeScout CounterACT platform handled this requisite.

Security and endpoint visibility was not a top priority for this manufacturer. However, the manufacturer found added value when the NAC was installed. The NAC provided not only the visibility to all of the endpoints, but also provided visibility into the network, all of the ports, operating systems and applications. The extent of CounterACT's ability to do endpoint posture checking was unanticipated but welcomed, as it could be applied to support other potential security issues.

Often lost in the discussion about NAC (and in other enterprise security and software products) is how long the physical deployment will take. In bids by competing vendors to ForeScout, the competitors scheduled an installation cycle that would take at least three weeks and the platform would need tuning every six months. ForeScout was up and running in less than a week with an option for more tuning if needed.

Scalability was also a concern. ForeScout was winning with its policy engine, compliance reporting, and comparatively quick installation times. The manufacturer saw that comparative NAC systems required various workarounds or extensive configurations to apply security policy correctly to VPN connections. CounterACT was simply a more fluid platform.

CONCLUSION

The NAC value proposition has expanded at a rapid pace in recent years. NAC is no longer limited to basic network admission decisions that include binary "block or allow" outcomes. Instead, Next-generation NAC provides comprehensive, real-time asset intelligence of all network-attached devices. This intelligence is not attainable with conventional network security and endpoint management solutions. Next-generation NAC is already being used in large organizations with thousands to hundreds of thousands of devices and distributed networks to more effectively manage security risks, enable BYOD adoption, and support IT-GRC framework specifications.

Next-generation NAC allows enterprises to transform disparate security technology silos into a more unified and automated system. The bidirectional information sharing that next-generation NAC facilitates helps individual security systems become aware of unmanaged devices, transient devices, dynamic risks and threats. Lastly, next-generation NAC provides a significant amount of automation for incident response and remediation.

FROST & SULLIVAN

Auckland
Bahrain
Bangkok
Beijing
Bengaluru
Buenos Aires
Cape Town
Chennai
Dammam
Delhi
Detroit
Dubai
Frankfurt
Herzliya
Houston
Irvine
Iskander Malaysia/Johor Bahru
Istanbul
Jakarta
Kolkata
Kotte Colombo
Kuala Lumpur
London
Manhattan
Miami
Milan
Moscow
Mountain View
Mumbai
Oxford
Paris
Pune
Rockville Centre
San Antonio
São Paulo
Seoul
Shanghai
Shenzhen
Singapore
Sydney
Taipei
Tokyo
Toronto
Valbonne
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 SW1W 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?