



*Sponsored by ForeScout Technologies, Inc.*

# **“Your Pad or Mine?” Enabling Secure Personal and Mobile Device Use On Your Network**

**The What, Why and How to Employ NAC to Apply Guest Networking,  
BYOD (Bring Your Own Device) and Endpoint Security Policies**

*November 2011*

**A SANS Whitepaper**

*Written by: Mark Kadrich*

**Building Guest Networking, BYOD and  
Endpoint Security Policies *PAGE 2***

**Architectural Challenges and Considerations *PAGE 6***

**Top 10 NAC Functions Enabling Guest Networking,  
BYOD and Endpoint Security *PAGE 10***

# Introduction

Many of today's endpoints are neither known nor protected. According to Gartner, enterprises are only aware of 80 percent of the devices on their network.<sup>1</sup> Those 20 percent of unknown devices are inside the perimeter of the network, are unmanaged and provide users with access. They are small, varied and highly mobile, and they are loaded with their own applications, can act as WAPs, and often contain outdated firmware or are jailbroken. Even as the devices are accessing personal applications on the web, they are also accessing corporate resources such as e-mail—all from the very same unmanaged devices, which have not been vetted by the security organization. Smartphones, notebooks, netbooks, iPads, e-readers, gaming consoles and more—the list of personal devices attempting access to employer networks seems to grow every day in what's come to be known as the BYOD (Bring Your Own Device) era in networking.

While this level of ubiquitous access produces gains in workforce productivity, it also represents new layers of risk for which traditional endpoint controls are unsuitable. As such, Gartner predicts that by 2013, 80 percent of organizations with BYOD policies will see botnet compromises increase by 100 percent inside their networks.<sup>2</sup>

Because they are small, these devices can't support the heavy artillery of firewalls and antivirus with all their signature, blacklist, whitelist and heuristics files. And, unless organizations can standardize on or control the highly mobile platforms their users are allowed to bring into the enterprise, security of these devices also becomes a problem. Intrusions and exploits can occur through many means, for example by users browsing malicious sites, clicking malicious links in e-mail and SMS messages, and installing malicious firmware updates, as well as making assumptions about the security and privacy of applications<sup>3</sup> and WiFi connections. One has only to review the ontology of Shady RAT to appreciate the impact that one user and one bad e-mail can have on your enterprise.

With the introduction of BYOD and these associated new threat vectors, Network Access Control (NAC) has emerged as an important solution for mitigating the risks of consumerization.<sup>4</sup> NAC can be used to provide secure guest networking services and management to these devices. This paper discusses policies and approaches for using NAC to support guest networking and BYOD, as well as the need to secure today's users and their new devices requesting access to the corporate network.

---

1 "Strategic Roadmap for Network Access Control," Gartner, October 2011, by Lawrence Orans and John Pescatore

2 "Predicts 2011: Infrastructure Protection Is Becoming More Complex, More Difficult and More Business-Critical Than Ever," Gartner, November 2010, by Avivah Littan, Neil MacDonald, John Girard and Ray Wagner

3 [www.wired.com/threatlevel/2011/03/android-malware/](http://www.wired.com/threatlevel/2011/03/android-malware/)

4 "Strategic Roadmap for Network Access Control," Gartner, October 2011, by Lawrence Orans and John Pescatore

# Building Guest Networking, BYOD and Endpoint Security Policies

Developed as a response to deficiencies in WiFi protocols, NAC's original function was to pass user credentials to a policy control point, where permission to connect to the network was approved and sent back to the network. NAC enables guest networking for wired and WiFi access requests coming from endpoints that don't fall within the realm of what the network considers "normal," such as traditional laptop computers or printers.

So, why not let our employees use their own devices by following similar guest networking policies? NAC enables employee, contractor and visitor choice by moving the control to the endpoint and where that endpoint connects to the network, called the port of entry for that endpoint. This *port of entry* provides the opportunity to assess a device before it's allowed entry to determine the level of trust that can be associated with the device and user requesting access.

The capability to classify network users and their devices gives the enterprise greater choices regarding how they're going to treat new devices as the industry pumps them out. Instead of making decisions on a case-by-case basis, the enterprise can now set NAC policy that states what kinds of devices can be used and what respective security policies must be in place on a device if an employee or guest wants to connect a personal device to the enterprise network in any way. Depending on the device, you can now ensure that the endpoint has the latest updates, a working firewall, and antivirus before you allow a connection or a limited connection to network resources.

Although NAC implementation may differ, there are two phases of every NAC program that provide governance telemetry: implementation and operation. At the beginning of the implementation phase, resource utilization, budget and schedule are the drivers. Functionality and policy compliance become more important as the project nears completion and enters the operational phase. After deployment, policy-compliance metrics and user productivity tend to dominate the discussion.

NAC policy begins with assessment-of-use case scenarios: What types of devices are being brought in by employees, contractors and guests; when, where and what access is being requested; what types of applications are they running; what type of access are they requesting? Once the policy identifies users and devices accessing the network, it should be used to determine what devices to allow on the network, what applications and peripherals the devices should or should not be running, and the security state they should be at before any access is granted. Policy and procedures should also include monitoring for unwanted applications or malicious activity emanating from endpoints, as well as provide remediation.

Between these policy layers are myriad subtleties to consider: What do you do with a corporate device that no longer complies with the corporate policy? How can you automate or semi-automate guest registration and remediation actions? What do you do with devices not owned by the corporation? NAC policy can address these and other questions.

### Determine Prerequisites for Granting Access

After you gather and assess the information on device usage, you can make an informed decision regarding how the device should be allowed to connect. Full, partial or guest access can be granted based on the assigned level of trust. Trust is based on the device's compliance with many policy questions: Is the device owner known (for example, corporate managed)? Does the device have the requisite security controls, such as antivirus, firewalls, encryption, and strong authentication, which you may require prior to allowing access to critical enterprise resources? In many cases, smaller, legacy and noncorporate devices may not have some of these controls available, but that is part of the decision process. After you decide on the required controls, you can move on to making decisions concerning the existence of forbidden or high-risk applications. For example, is the endpoint running an application that can probe the network or share files illegally? Are there peripheral devices being used on the endpoint requesting access and should there be?

### Consider Scalable Policy Actions

The policy should also be able to scale to include new forms of mobile devices requesting access as users continue the trend toward BYOD. A policy could be as simple as asking, "Is this an approved device?" To keep policy simple, some organizations may allow only Blackberry smartphones to connect to their networks. Ultimately, however, most small devices used for workforce applications need to be accommodated. For example, perhaps Apple and Android devices should be granted access only to a segregated guest network that allows Internet access. For more fine-grained access controls, endpoints are authenticated through Active Directory, where group assignments and other entitlements can be provisioned. Other high-level policies, such as "no device may act as a protocol bridge when connected to the corporate network," may be deconstructed into a set of controls that checks to see whether a cellular data network connection exists and, if so, to ensure that the cellular network connection is turned off prior to connecting to the corporate network.

After a level of trust is associated with an endpoint, NAC can support policy actions, including port control, guest registration, remediation or denial of access (a last resort due to its potential impact on productivity). For example, if a system is contractor owned and not employee owned, the policy would enable restricted enterprise access only after it passes a security check. If that check reveals that policies are not met, the device requesting access can be sent to remediation services, from which the user can remediate or, possibly, consent for the NAC to auto-remediate as possible.

Many organizations require contractors to load some corporate security controls onto their endpoints. Connection time is a perfect opportunity to verify not only compliance with policy, but also enforcement of any contractual agreements made between the parties on the endpoints making the connections.

If the system is employer owned and controlled, policy might include the level of access and the network segments to which the device is allowed to connect. For example, you probably don't want a developer's notebook connecting to your finance network. Another example would be restricting departments within health care administration from being able to use external mobile storage peripherals, such as thumb drives. Although security control capabilities vary, the capability to enforce these levels of action is critical as more and different types of devices connect to the network. See Case Study 1, which describes the experience of Guelph, Ontario.

### Case Study 1: How a City Enabled BYOD with Guest Networking

The city of Guelph, a community of 118,000 people in Ontario, accepts credit cards and other citizen financial information over the web. It also manages medical information with Emergency Technicians (ETs) using mobile devices in the field.

To support the highly mobile BYOD needs of 2,000 city workers, while at the same time meeting PCI-DSS and HIPAA regulatory compliance, the city assembled a cross-organizational team to assess NAC solutions against its requirements, including the following:

- Visibility into all devices and the status of devices accessing the network
- Visibility into all updates—including Windows update status, which is typically hard to collect logs from
- Simplified guest networking through self-serve policies
- Means to enable noncorporate device use on guest networks
- Self-remediation and user education
- Accuracy, speed and automation

After the team selected an automated NAC tool to facilitate these processes, they brought in an outside consultant to assist in assessment and implementation. Now, with guest networking automated, city workers, contractors and VIPs can self-register and use their personal devices in courtyards, the lunchroom and other designated areas without direct access to rest of the network.

With this NAC arrangement, the organization now has full visibility into access and other activities from endpoints, giving them the ability to classify device types entering the network and put them in containers based on their profile.

For the city of Guelph, automating the process of guest networking also provided a secondary benefit of better accuracy and cost savings. This process was managed manually before, with no guarantee the devices accessing the servers were safe, and administrators had to remember to manually disable the port. The self-help features for guest networking also significantly reduced help desk costs associated with requests for manually established new connections.

### Have a Remediation Plan

Policy should also include whether and when remediation is required. Remediation can include anything from removing the malicious device from the network, to blocking the use of certain applications and peripherals, to shutting down an endpoint completely. Can you determine whether the device has a peer-to-peer or other out-of-compliance application, and can that application be turned off during the network connection? If a device falls out of compliance or shows signs of malicious activity, can it be dropped from the network and placed into a closed environment for remediation? Policy should cover when remediation is appropriate, what remediation choices are available, and whether it is integrated with the trouble-ticketing process to ensure completion. Integrating a solution with your trouble-ticket system helps you understand why devices are being remediated and provides an opportunity for you to refine your policy for improved overall security and compliance.

### Monitor for Malicious Endpoints

There are cases where your system should give careful consideration to employee or guest endpoints if they exhibit behaviors that indicate they may be hostile in nature. For this reason, give careful attention to monitoring network segments that provide guest networking services. For example, any device that launches port scans should set off an alarm.

### Monitor for Wanted and Unwanted Applications

IT organizations have made investments in endpoint protection products, such as antivirus, data leakage prevention (DLP), patch management and client VPN/IPS. Whitelist policies can ensure that the security posture of listed devices is current and active. Similarly, IT organizations may want to blacklist certain applications for various reasons, such as the use of noncorporate instant messaging applications.

### Use NAC to Enable New Services

Policy should also include ways NAC can enable new services to support BYOD use by employees, contractors and visitors that, in the past, had to be provided through physical compartmentalization (a separate physical network) or not provided at all. For example, the combination of guest networking and NAC allows guests a method to connect to the Internet from anywhere, not just specific areas such as conference rooms that have been configured to provide access to the Internet while preventing access to the enterprise network.

Guest networking can support the use of personal mobile devices by employees, contractors and visitors; it can also be used to facilitate meetings and training for employees, contractors or visitors on demand.

By setting policy and assessing resources before implementation, organizations can create NAC environments that increase trust and still allow the flexibility of BYOD in the workplace. By providing a policy-driven remediation option, many more devices can be granted access to networking resources.

# Architectural Challenges and Considerations

A well-planned system can also provide remediation processes and support visibility and governance of access from multiple types of devices. However, there will still be challenges to which the following advice applies:

- Understand your legacy networking capability and your ability to adapt to new forms of access and the NAC solution:
  - Determine whether the present network infrastructure is robust enough to support the bandwidth and authentication demands presented by the influx of mobile devices.
  - Keep in mind that everything is connected. Take the time to find and analyze those connections.
- Understand where your business-sensitive and regulated data exists, as well as who should have access to this data and under what conditions access should be granted.
- Support protocols beyond 802.1x WiFi protocols and common user directories, such as LDAP, Active Directory and more in the authentication process.
- Involve business units, support, legal, developers, architects, users and other stakeholders with development, implementation and ongoing user education.
- Keep policies well defined and up to date, because device uses and applications continue to evolve.
- Automate. You are about to introduce a very large amount of decision-critical information that must be collected, assessed and acted upon far faster than any human mind can comprehend.
- Supply consumable management metrics. If your telemetry says that nine percent of your guests are really employees with noncompliant devices, what does that mean for productivity, and what will it cost to fix it?
- Phase in policy enforcement while phasing out noncompliant devices. Start by granting BYOD access only to the guest network and only with specific device types. As capability improves, migrate more compliant guests to internal networks and so on.
- Include remediation! Make sure it works, it's painless and that you can get reliable direction from the NAC system.
- Integrate where possible. Technology should never stand on its own, so enable a flexible system that integrates and correlates well with other controls for detection, security event management, vulnerability management, forensics and optimization.

### Access and Endpoint Security: Agent, Agentless or Hybrid?

NAC architectures include network, client and hybrid (agent and network) controls for assessing endpoints and establishing access based on results of those assessments. Policy depends on a number of questions: Should you rely on the network to make all the decisions? Can you offload some of those decisions onto trusted endpoints? How do you determine if an endpoint is trusted? How can you monitor and enforce policy, and tie into existing access control structures? Under what conditions is it difficult or impossible to either manage or support agents? Ultimately, to achieve a comprehensive and flexible level of endpoint control and guest networking, most organizations resort to using network and endpoint agents, or they adopt an agentless approach for reasons explained shortly.

In network-based NAC, packets and flows associated with specific devices are routed, switched or relegated to the bit bucket based on rules enforced by network infrastructure devices as discussed previously. VLAN capability can also be employed in a NAC architecture in order to provide security segmentation. By assigning guest devices to a separate VLAN, you can put untrustworthy devices in a network that does not have access to the corporate network. In some advanced cases, dynamic VLANs can be employed in order to stratify traffic based on user, data or resource sensitivity.

Other networking methods, such as the use of DHCP (Dynamic Host Configuration Protocol) and the ARP (Address Resolution Protocol), as well as Active ACL modification, TCP reset and other networking protocols, can support a NAC architecture.

Organizations with little control over the network devices, such as personal mobile devices, yet with significant control of the endpoints, clients and servers, can implement an active NAC-like solution at the endpoints as they request access. Agents can be persistent or nonpersistent (meaning they are placed on the endpoint during each session request). An active agent on an endpoint can assess the status of the endpoint, gather information, report, take action based on instructions provided by a management server and, most importantly, take proactive steps to ensure that the endpoint remains compliant with pertinent security policies. See Case Study 2, which discusses how Wellington College managed the influx of personal devices and visitor devices using active NAC agents and scanning.

### Case Study 2: Facilitating a BYOD Explosion with Agentless NAC

School and higher education IT departments were the first organizations, by nature of the environment, to manage guest networking and BYOD policies. To protect against an ever-increasing amount of Trojans, bots and other malware attempting to get into the network, the director of IT services and development at the prestigious Wellington College in the United Kingdom began a NAC overhaul in 2010. The system needed to regulate student network use and protect against malware emanating from any device attempting access into the network, not just internally managed computers.

Wellington was experiencing an explosion of mobile devices among the 1,000-member student body. Now, many students have three devices each, all used for accessing the network, including a smartphone, tablet and laptop. The campus must monitor 4,000 devices belonging to employees and students for guest-access compliance and violations. The campus also hosts open nights for parents and visitors to access school resources, at which point up to 2,000 additional guest devices might attempt to access the network.

In this environment, a persistent agent solution wasn't practical on endpoints, so the director of IT services made the decision to go with an active scanning (agentless) solution to enforce policy from the network. The school was able to take advantage of their new NAC tool's built-in policy templates to address the diversity of the student population and its devices connecting to the network. Active scanning occurs against the devices wanting access. Those devices that don't meet policy are quarantined until they can be remediated. The system can also monitor for suspicious and unwanted postconnection behavior, for example, if one of the shared bank of printers begins to operate as a Windows machine or if a new personal rogue WAP connection appears.

The tool leveraged the school's VMware investment to provide rapid scalability for occasions such as parent night. The solution eliminated most rogue traffic on the network, reducing latency, and managed malware and other risks. Now, the organization can handle the need for on-demand guest networking with reduced latency, manual cycles and costs.

For those devices without agents, an intelligent scanning approach from the network is the first step in determining the security posture of the device requesting access. Detailed network scans of an endpoint can provide a wealth of information, including the type and number of services running and the type of operating system and processor installed. A network scan might reveal the presence of services that can provide more detailed information, such as the Windows Management Instrumentation (WMI), which itself can provide significant levels of detail with respect to system configuration, update and patch status, user information and security posture. The client scan, on the other hand, can tell more information—for example, what user is attached to the device, what applications are loaded, and verification of external scan and fingerprint information.

## Architectural Challenges and Considerations (CONTINUED)

Whenever it is possible to implement, an agented response is the best choice because of the depth of information it can gather for most endpoints. If devices cannot support an agent, active scanning of the device from the network may be sufficient. The most practical and often implemented approach is the hybrid approach that relies on both agent and agentless scanning of endpoints. Figure 1 depicts this hybrid approach from a networking standpoint.

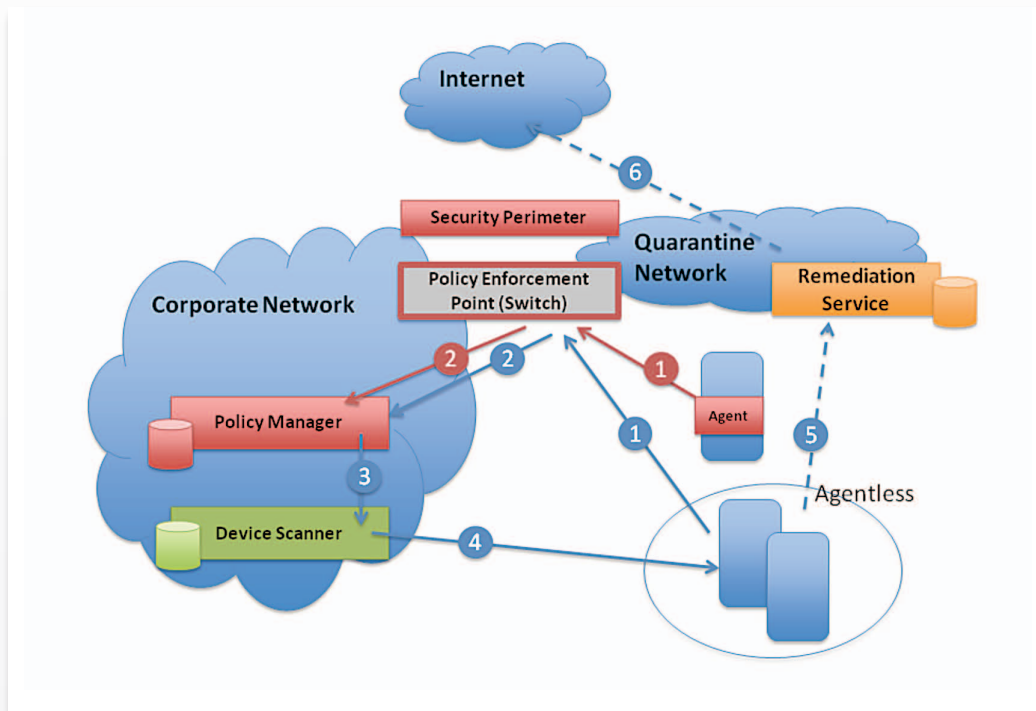


Figure 1: The Hybrid Approach

The hybrid model provides the flexibility to cover both of these scenarios and gives the network portal, with the help of the endpoint, the capability to decide whether the presented system should be given full enterprise access, provided remediation, connected to a guest network or denied access.

# Top 10 NAC Functions Enabling Guest Networking, BYOD and Endpoint Security

Inherent in the NAC process is the capability to capture, store, manage and act upon policy through the following functions that enable guest networking, BYOD and endpoint security controls:

- 1. Device Fingerprinting**—Device fingerprinting is the process of scanning a network device and capturing detailed information regarding device responses to various protocol requests. Information about how long it took the device to reply to a request to set up a network session, or how long it took for the device to time out on a specific request is captured, correlated and compared to known device fingerprints. Information such as the operating system, processor and model number of the device can be inferred from this type of testing.
- 2. Handling Applications**—Blacklisting and whitelisting should enforce what types of applications are allowed to operate on these devices and what types should not be allowed to operate. You must determine the rules to apply if peer-to-peer and other risky applications are found.
- 3. Exception Handling**—If a new driver skews scan results, other means must be employed, such as redirecting the device to a remediation server that uses a transient agent to check the device. Ideally, this exception would terminate access after a predetermined period of time, and log and note the associated session information.
- 4. Alternate Means of Identification**—Some devices don't support clients, are unmanaged and won't allow any type of agent to be installed. Sometimes the security software on the system prevents it from being enumerated. For these and other reasons, you need a reliable method of identifying the device so it can connect to the network securely. This identification can be conducted from network scans of the endpoint, as discussed previously.
- 5. Access Controls and Restrictions**—Comparing a user's authorization level and the posture of the system making the request is a good foundation from which to make further access-related decisions. For example, if John Smith presents valid credentials, but his notebook doesn't meet the minimum requirements for system configuration (it's not at the latest patch level), then John's access should be restricted until the system can be remediated.
- 6. Guest Registration**—NAC should require a guest to register with the network in order to obtain the required agents or be subjected to an enumeration scan. The registration process should be self-service and as minimally intrusive as possible, similar to how services are provided to travelers who use hotel networks. For use on corporate systems, users might need to install a permanent or transient agent, depending on the level of access required. As outlined earlier, these events should be logged and made available for review.

## Top 10 NAC Functions Enabling Guest Networking, BYOD and Endpoint Security (CONTINUED)

- 7. Self-Remediation**—A well-defined self-remediation process integrates with a guest access system in such a way that guest users are able to engage the remediation process for the purposes of the visit. It should also offer advice on security violations and means for resolution. Depending on the persistency of the agent, they may need to sign an acceptance clause. In cases in which endpoint security policy issues can be resolved by the end user, the NAC system can redirect the user to a self-remediation site either inside or outside the corporate network.
- 8. Auto-Remediation**—Ideally, remediation should be automatic and transparent. In many cases this is possible with corporate-provisioned systems only, because local laws may prevent you from changing the configuration of a system without the user's knowledge or permission. This process determines whether the system is a corporate asset or not, enumerates the system, identifies any deficiencies, queries the user (where required), attempts to resolve the remediation issue, continues with the NAC process, and then connects the user to requested network resources.
- 9. Trust Verification and Reporting**—In many cases, data privacy laws require a record of activity on systems handling sensitive data. The capability for NAC information to tie into reporting is critical. At a minimum, NAC reporting should be able to provide a record of the following:
  - Timestamps
  - All requests to connect
  - Connection request results and status
  - All systems that contain policy deficiencies and the status of those deficiencies
  - All remediation events
  - User names
  - System IDs
  - MAC addresses
  - IP Addresses (if applicable)
  - Operating system types
  - Locations
  - Exception requests

The reporting function should also be trustworthy and employ a secure method for verifying and validating log entries and log sequences.

- 10. Policy Enforcement**—Organizations also need to consider flexibility and scalability in their policies to facilitate exceptions and changes in employee and partner access, such as adding new users and groups. A process should be established to ensure that desired policies are in place and verifiably functional.

## Conclusion

Clearly, the world is moving toward mobility, and the technologies that go with it are being carried in the pockets and purses of users. In a couple of years, we'll be referring to anything with a network cable as legacy technology. It isn't a matter of if we should integrate personal mobile technology into our networks, but how fast and how effectively we can do it.

Employees are bringing in their own devices, and IT organizations must enable their use while managing the associated security risks. A typical corporate employee spends an ever-increasing portion of the work day in collaboration with various other people, guests and contractors, many of whom may not be a part of the organization, but with most of whom the employee is expected to share presentations, exchange calendar invites, collaborate on documents and, in general, exchange information as if they were a part of the corporate team.

Yes, there is a risk, but that risk can be managed with published policies, proper process and a network design that enable a diverse and mobile workforce. Solutions to BYOD are available in the form of NAC-enabled guest networking. Depending on the flexibility and intelligence of device interrogation, the comprehensiveness of the policy engine, the degree of interoperability with the operating environment and the means for remediation, NAC solutions can further enable trusted devices to join the corporate network based on business needs and predetermined levels of acceptable risk. As NAC solutions enable the use of more diverse devices on the network, organizations should take the time to develop architectures, design for desired outcomes and close the loop to build a trustworthy foundation for both known and unknown personal mobile devices requesting access to the corporate network.

## About the Author

**Mark S. Kadrach**, author and security policy evangelist, has been working to change how information security is executed for a number of years. His book *Endpoint Security* (Addison Wesley) discusses why security continues to fail and postulates a proven engineering approach to solving the problem. Presently, Mark is working in the health care industry as a principal enterprise security architect. Mark was founding president and CEO of The Security Consortium (TSC), whose mission was to provide security testing, research, counsel and leadership to their customers. Prior to TSC, Mark was the senior manager of network and endpoint security for Symantec and a senior scientist with Sygate Technologies.

**SANS would like to thank its sponsor:**

