

Beyond NAC: The value of post-admission control in LAN security

By Jeff Prince

Many organizations are taking the first step toward LAN security by deploying Network Admission Control (NAC) solutions. NAC ensures that only authenticated users operating compliant computers are allowed onto the enterprise network, and it provides some security benefits.

Many organizations are taking the first step toward LAN security by deploying Network Admission Control (NAC) solutions. NAC ensures that only authenticated users operating compliant computers are allowed onto the enterprise network, and it provides some security benefits. As organizations expand globally and virtualize operations, their user bases have grown to include employees, contractors, consultants, business partners, customers, even guests. LANs are more open than ever, and enterprises need the ability to control who connects to their networks and determine whether their machines are free of infection.

However, NAC is limited, and while it is a necessary part of a LAN security solution, it is not sufficient. Threats can arise from malicious insiders, even from end-user “misbehavior” such as the failure to follow business policies or accidental disclosure of sensitive data. NAC does nothing to address these risks because they all happen after a user has been admitted onto the LAN. Enterprises need post-admission access control to reduce these threats – to limit where users can go and what they can do once they’re on the LAN.

With a post-admission control solution, IT can, for example, restrict guests to accessing the Internet from an office lobby. Similarly, IT could limit the locations and times of day when customer service staff can access customer-related applications and data; when and from where contractors can use engineering resources; and from which conference rooms non-employees can connect to the network.

NAC and post-admission access control are not either-or solutions; organizations need both for effective LAN security. Focusing on NAC alone leaves enterprises vulnerable to abuse or misuse of corporate assets. In this article we discuss the capabilities of NAC and access control solutions, highlight what to look for in each area, and

provide a roadmap for implementing post-admission access controls.

Ins and outs of NAC implementations

Network Admission Control employs user authentication to control who can access the LAN, and “host posture check” to ensure that users’ computers comply with corporate standards. For example, standards may call for running an approved operating system with current patches and fixes and an updated antivirus program. Without host posture check, authorized users could unwittingly unleash malware.

A NAC solution should be easy to deploy and use, and non-disruptive. A few NAC appliances offer basic post-admission access controls, but these controls are very limited. In evaluating the authentication capabilities of a NAC product, IT should consider whether it supports 802.1X, provides both passive and active authentication, and leverages existing identity stores.

802.1X support

A number of NAC solutions require 802.1X, a standard for port-based Network Admission Control that provides authentication at Layer 2. While it offers a standard method for authentication, 802.1X must be supported on both clients and LAN switches. Consequently, IT has to deploy or configure 802.1X supplicant software on desktops and other end stations.

While many organizations have 802.1X-enabled LAN switches already, many companies would need to replace all or some of their switches to implement an 802.1X-based NAC solution. Organiza-

tions that prefer not to use 802.1X will find good alternatives available in the market.

Passive and active authentication

Passive authentication is typically used to support employees and other known users, and operates by tracking users logging into a Windows domain or RADIUS server. Active authentication is often used for guests and other non-employees. Generally implemented as a captive portal, active authentication is important for directing visiting users to specified resources, such as Internet access. A NAC solution must support both mechanisms to ensure consistent authentication enforcement regardless of user identity or the point of entry into the network.

Identity stores

For ease of deployment, a NAC solution should work with an organization's existing identity stores, whether RADIUS servers or directory services such as Microsoft's Active Directory and other Lightweight Directory Access Protocol (LDAP)-compliant directories.

On the host posture check side, enterprises should look for a NAC solution that does not require a separate agent, but instead works with existing host software such as installed antivirus software. Sometimes implemented as dissolvable agents, these posture check systems are well suited to working with a mix of managed and unmanaged systems.

What post-admission access control should do

Network Admission Control is a good first line of defense, preventing unauthorized users and non-compliant machines from accessing the network. Post-admission access control is the next critical step in securing the LAN, protecting corporate assets by controlling users' access to applications, data, and resources.

Enterprises should look for an access control solution that provides granular visibility into – and flexible, policy-based control over – user traffic. In addition, a post-admission solution should provide threat control to identify and contain anomalous traffic.

Vendors have delivered a number of appliance-based post-admission control solutions. The architecture of an appliance determines what type of access controls the system supports. A key architectural difference is whether the appliance operates inline or out-of-band. Inline devices sit in the flow of traffic, so they can see and act on everything that goes by. In contrast, out-of-band appliances sit in a central location

and see only a user's initial entry onto the LAN. They have no visibility into ongoing LAN traffic, which limits their control capabilities.

Out of Band
<ul style="list-style-type: none"> • Fewer devices to deploy • Not in the flow of traffic • All equipment resides in network core
Inline
<ul style="list-style-type: none"> • Retains existing LAN • Sees all traffic, enabling stronger controls • Simplifies troubleshooting

To be most effective, an access control solution should tie LAN traffic to user names. Many systems link traffic to IP or MAC addresses, but these addresses do not equate to users, and they typically change depending on where users connect to the network and what computer they use. Access controls that resolve traffic to user names

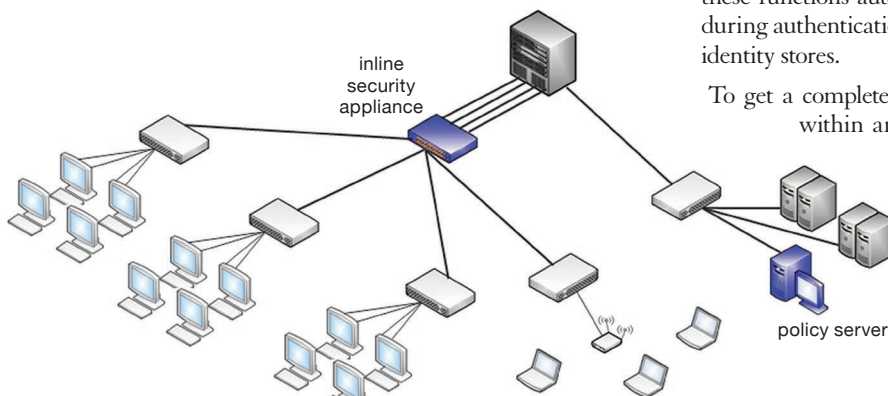


Figure 1. Inline Appliances:
Between wiring closet switches and the core, policy decision and enforcement in the same platform

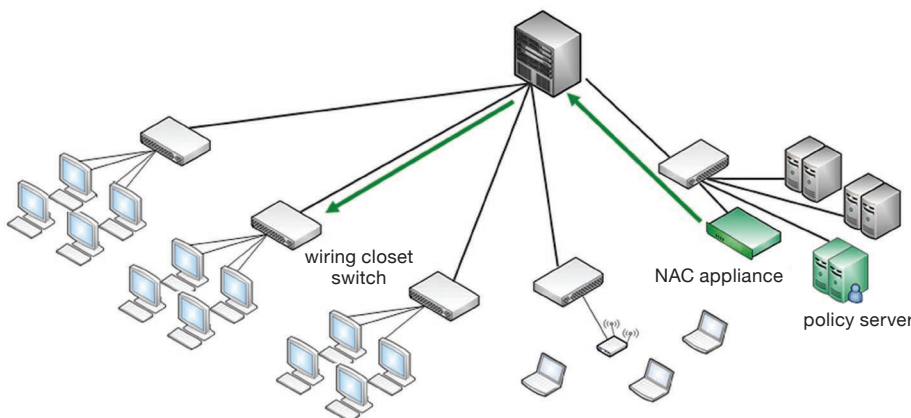


Figure 2. Out-of-band Appliances:
Policy decisions are communicated to wiring closet switches which provide policy enforcement

make it easier to define and apply control policies, identify trends and interpret security events, and respond quickly to problems.

Let's look more closely at the three components enterprises should look for in an access control solution – comprehensive traffic visibility, user-based access control, and threat control.

Visibility: Gateway to control

Visibility into LAN traffic is fundamental to both user access control and threat control – you cannot control what you cannot see. Enterprises should look for access control solutions that provide a level of visibility granular enough to support the level of control they want.

Detailed traffic visibility is the basis for role-based provisioning, enabling IT to control application access and resource usage based on a user's group association or role within the enterprise. It also allows for a range of other management activities, including incident response, auditing, and trend analysis.

In evaluating the traffic visibility feature of a post-admission control solution, IT should look for two main characteristics: the ability to tie all LAN activity back to specific users, and the ability to perform deep packet inspection on all traffic flows. Both are needed for IT to define granular policies, see policy violations, and troubleshoot problems.

To tie LAN traffic to users, an access control system must learn user name and role information and bind a user name to an IP and MAC address. Look for post-admission control solutions that perform these functions automatically, for example by learning user names during authentication and extracting role information from existing identity stores.

To get a complete picture of LAN traffic, the visibility function within an access control solution must perform full application classification through Layer 7, including expanded application details, such as a file open, copy, delete, or edit action within the Windows file-share protocol, CIFS (Common Internet File System). Sampling traffic does not deliver the visibility needed for granular control.

IT should look for an access control solution that sees all flows and user activity, including login/logout time, applications run, resources reached, and transactions performed. For very granular visibility, look for solutions that track events that occur within a flow, such as the URL, source user, and browser in use for HTTP flows; file name, source and destination IP addresses, and FTP user name for FTP flows; file transaction (read, write), user, file name, and volume name for SMB/CIFS flows; and user name, MAC address, IP address, and time for DHCP flows.

Traffic visibility is needed to tie LAN activity back to specific users and is the foundation for user-based access control. Traffic visibility also allows for threat control. Enterprises should look for a visibility capability that tracks security incidents such as those relating to host posture check, authentication failures, policy violations, and malware

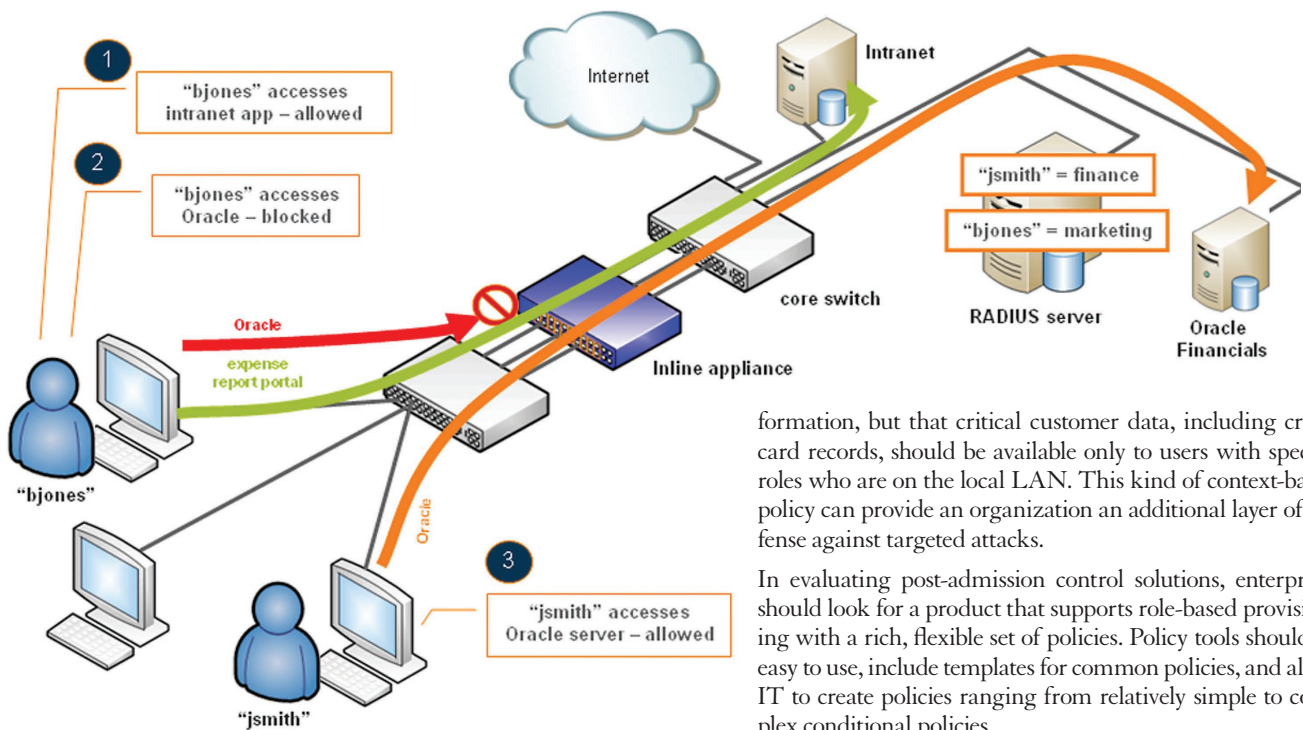


Figure 3. Role-based Access Control: Effective appliances must control access to applications and servers based on user roles

events. Look for solutions that provide real-time as well as historical data and retain flow-related statistics needed for regulatory compliance and accounting.

User-based access control

With the right level of traffic visibility, a post-admission control solution can provide role-based provisioning. Having a user's role information enables IT to easily segment employee, guest, and contractor traffic. For example, IT could define rights, permissions, and enforcement actions based on a user's group association or role within the enterprise.

If role-based provisioning encompasses network connectivity information, IT can define universal or location-based access control. For some organizations, having a single policy that applies the same access rights – regardless of a user's access medium or location – may be the desired approach. For example, the same set of access rights would apply whether a user accessed the LAN via a wired or a wireless connection; and whether he or she attached locally, or remotely via a VPN.

Other organizations, however, might want to tailor access rights based on location or medium. For instance, a company might decide that VPN users can access email and basic intranet in-

formation, but that critical customer data, including credit card records, should be available only to users with specific roles who are on the local LAN. This kind of context-based policy can provide an organization an additional layer of defense against targeted attacks.

In evaluating post-admission control solutions, enterprises should look for a product that supports role-based provisioning with a rich, flexible set of policies. Policy tools should be easy to use, include templates for common policies, and allow IT to create policies ranging from relatively simple to complex conditional policies.

Conditional policies are useful for managing highly sensitive content and applications, and for accommodating users with multiple roles. For example, a user may belong to several groups, such as employee, engineering, and management. A flexible policy tool will allow IT to create policies that provide the intersection of permissions of all three groups.

Enterprises that want granular user access control should look for a solution that supports these policy parameters:

- User – including both individuals and groups/roles
- Application – including individual applications such as Firefox, as well as groups of applications such as all Web browsers

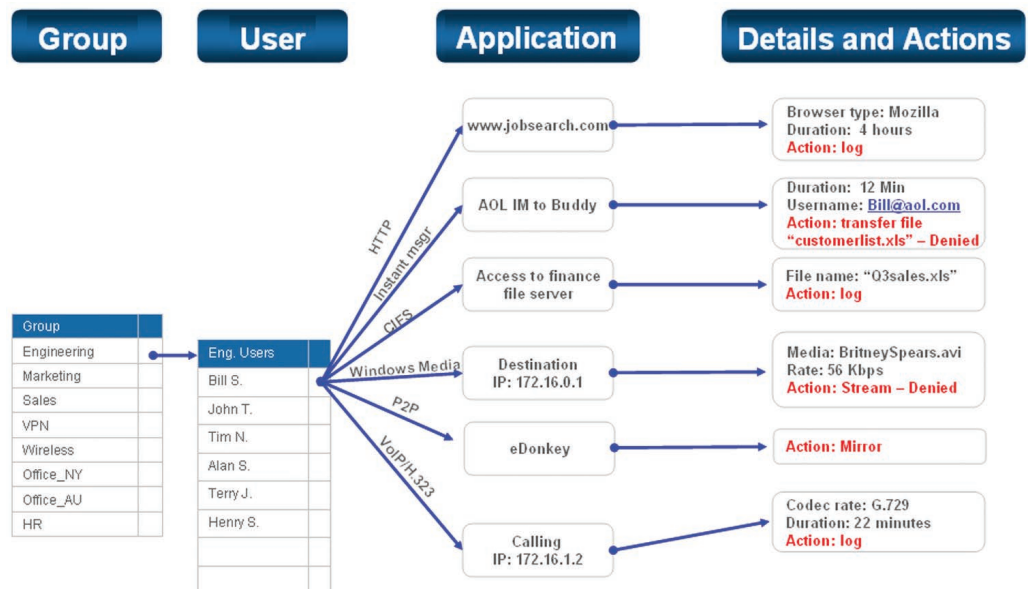


Figure 4. User and Application Visibility: Inline appliances can tie users to applications in use and even to file names

- Applications and content at layer 7 and above – including applications that use the same port, such as when Web browsing and SAP both run on Port 80; application content, such as specific FTP files; and application attributes, such as the file name in a Windows file-sharing transaction
- MAC address – including individual addresses and wildcard ranges that start with the same addressing information, such as a collection of VoIP phones
- IP address – including individual IP addresses and IP ranges associated with a cluster of devices
- TCP and UDP ports
- Network destinations or zones – including a

1

Worm propagation (malware) – inline appliance sees all traffic, detects malware – blocks only the offending app

2

"Good" applications are still able to traverse the network

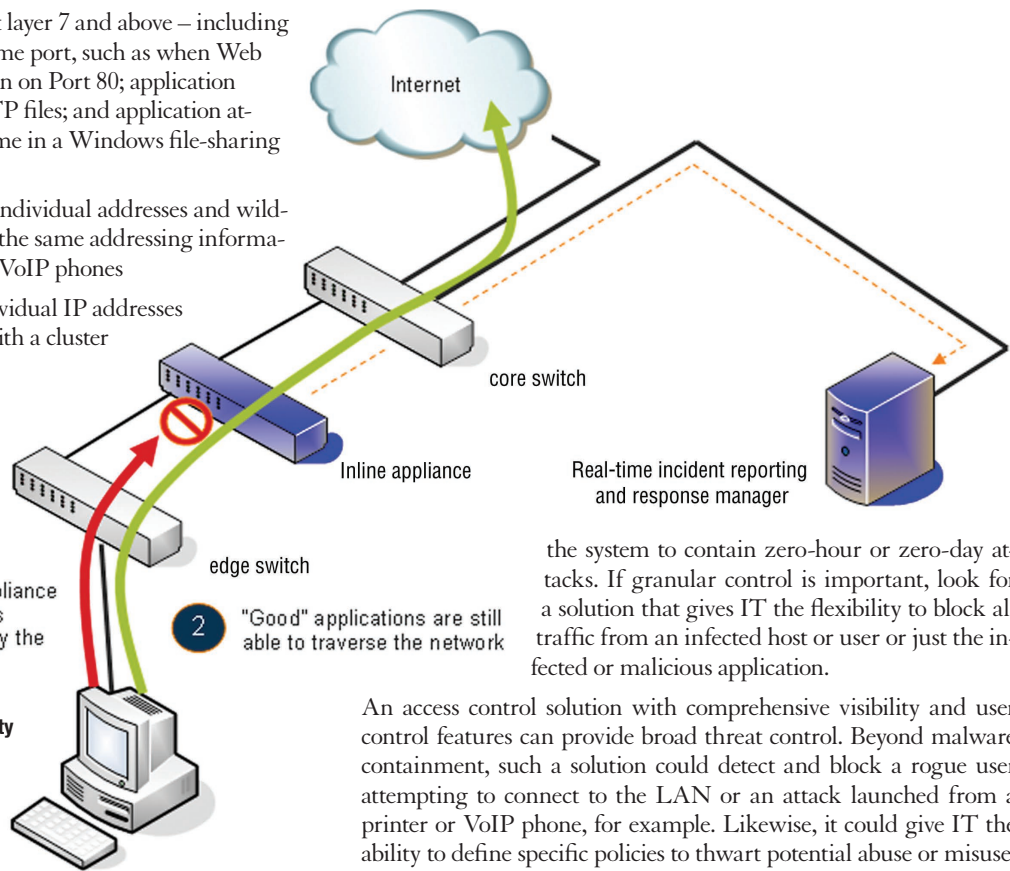


Figure 5. Worm Containment: The security appliance can block an application or all traffic from an infected user.

the system to contain zero-hour or zero-day attacks. If granular control is important, look for a solution that gives IT the flexibility to block all traffic from an infected host or user or just the infected or malicious application.

An access control solution with comprehensive visibility and user control features can provide broad threat control. Beyond malware containment, such a solution could detect and block a rogue user attempting to connect to the LAN or an attack launched from a printer or VoIP phone, for example. Likewise, it could give IT the ability to define specific policies to thwart potential abuse or misuse; for example, IT could define a policy that prevents non-VoIP protocols from reaching the call manager. Look for admission control solutions that offer multifaceted threat control.

collection of resources such as the finance servers

- Location – including region, building, device, and port

With these types of policy attributes, IT can create general as well as highly granular policies. For example, IT could create a policy that ensures service representatives run customer-facing applications only between the hours of 7 a.m. and 4 p.m. from desktop computers within the customer service department.

Beyond policy creation, a post-admission control solution must also provide policy enforcement. To enforce user- and role-based policies, an enforcement device must be able to link all traffic on the LAN to the individual users generating it and match that traffic against decision filters. Inline access control appliances perform both policy decisions and policy enforcement, whereas out-of-band appliances provide policy decision functions only, and rely on switches to provide enforcement. Because of this architecture, out-of-band devices are typically limited in their control capabilities – they can verify authentication, perform host posture check, and usually place a user into a specific virtual LAN, but they cannot provide ongoing visibility, apply context-based controls, or contain malware or other threats.

Multifaceted threat control

A third key feature to look for in a post-admission control solution is threat control. Enterprises need effective protection against external as well as internal threats, both known and unknown. Look for threat-control implementations that search for anomalous behavior and use application-specific algorithms to distinguish normal from abnormal application behavior.

This level of visibility is necessary to identify both known and unknown worms, viruses, bots, spyware, and other malware, enabling

Getting started

Moving from basic Network Access Control to a more sophisticated security tool like post-admission control can sound daunting, but it need not be difficult. The right access control solution will allow IT to start simple and modify controls over time to be as granular as the enterprise requires. Since every organization has a unique set of security concerns, no single roadmap can direct everyone. However, some basic guidelines can help IT deploy user-based access controls.

Focus on the greatest vulnerability first

Which users, resources, or locations pose the greatest security risk? For some organizations, guests will be their greatest security concern; for others it will be contractors or non-local employees. The need to secure customer data such as credit card information may be the issue for one IT group, while another group is focused on controlling who can access critical intellectual property.

In some cases, particular locations within the enterprise, such as conference rooms, wireless links, or VPN connections, will be what are keeping IT up at night. It is a good idea to identify the enterprise's most vulnerable areas and tackle the topmost one first.

Start simple

Begin with a simple policy, such as restricting guests to Internet access only. Starting simple has several advantages. It gives IT a chance to become familiar with the policy provisioning tools that an access control vendor has provided. More importantly, it makes it easy for

IT to see whether the policy is having the desired effect and to easily modify or reverse a policy if it is not performing as expected.

Expand security in stages

Taking a staged approach gives IT the opportunity to ensure one set of policies is operating as planned before introducing another control. A flexible access control solution will give IT the option to grant broad connectivity and resource access initially and then narrow access over time.

For example, IT may begin with a policy that allows all human resources personnel to access a particular server. Over time, to protect sensitive data, IT could define more granular policies that further restrict access – say, limiting salary data to HR employees who are managers.

In some cases, an enterprise may want to roll out location-based policies in stages. For example, IT might at first allow anyone in the role of bank teller to run a key customer-facing banking application, and then over time add policies that allow that application to run only if the teller is in the bank's customer area rather than in the back office.

For those persons and situations in which the tightest security controls are warranted, a robust policy-based provisioning tool will give IT the option to define access based on least privileges.

Ensuring comprehensive LAN security

Securing the LAN is more than a matter of gate-keeping. As organizations begin the process of evaluating and deploying LAN security, be sure to look for solutions that go beyond simple Network Access Control. Even if the plan is to deploy NAC first, look for a solution that can also deliver post-admission control – ideally, a solution that addresses both immediate and long-term security issues.

LANs are subject to an ever-evolving set of risks, both internal and external. Enterprises need the ability to control not only which users and machines gain access to the network, but what resources those users can reach, from where, and when. User-based access controls give IT the tools it needs to protect critical assets such as customer data and intellectual property, maintain uptime, counter malware, and comply with state and government regulations.

Given the scope and volatility of the threats enterprises face, a LAN security solution must go beyond NAC. It must encompass the granular, flexible post-admission controls needed to combat the full range of threats, both today and tomorrow.

About the Author

Jeff Prince has more than 16 years of experience developing networking and ASIC technologies. Prior to becoming chairman and CTO of ConSentry Networks, Jeff was a founder of Foundry Networks, where he lead Foundry's hardware engineering group. Prior to Foundry, Jeff was a founder of Centillion Networks, which was acquired by Bay Networks in 1995. Prior to Centillion, Jeff was a hardware engineering manager at Network Equipment Technologies. Jeff holds eight patents related to networking technologies, and he has a BS in Computer Engineering from California State University, Chico. Jeff is also a managing partner at Prince Ventures, LP.