

The executive team and all the staff at InfoExpress wish you a successful year ahead. We are pleased with the continued growth of the company, and know that it comes directly from satisfying our customers, bringing new innovations to the market, and backing them up with solid deployment services. Read on for more useful insights for you in this issue.

Below, be sure to check out our new Georgia Legal Services case study, download our new whitepaper on Aruba-NAC integration, see our new FAQ on Dynamic NAC, and, last but not least, read the fifth installment in our CyberGatekeeper Enforcement Options series, focusing on Alcatel-Lucent's Omniswitch.

#### Issue Highlights:

[Case study: Securing a non-profit's network](#)  
[Integrating NAC with an Aruba WLAN](#)  
[Get all the FAQs on Dynamic NAC](#)  
[Enforcement with Alcatel-Lucent Omniswitch](#)

For copies of past newsletters, please visit: <http://www.infoexpress.com/news/newsletter.php>

#### **CyberGatekeeper Customer Case Study— Georgia Legal Services Program**

Georgia Legal Services Program has deployed CyberGatekeeper with Dynamic Network Access Control (DNAC) and CyberGatekeeper Remote to help secure the non-profit's network. CyberGatekeeper was chosen for its ease of deployment and manageability, proven security, flexibility and price. A single, centralized, out-of-band DNAC server manages users on the LAN and WAN, while a single in-line CyberGatekeeper Remote appliance is able to control remote users.

To read this new Customer Case Study in full, please visit [http://infoexpress.com/media/case\\_study/case\\_study\\_georgia\\_legal.pdf](http://infoexpress.com/media/case_study/case_study_georgia_legal.pdf).

#### **NAC Integration with Aruba Wireless LANs** *A new InfoExpress whitepaper*

InfoExpress has just released a new whitepaper describing integration of NAC with an Aruba wireless LAN.

NAC provides many benefits including compliance control, threat mitigation, and visibility into endpoints. However, it has limitations on uses with guests and dynamic policy assignments. By using NAC integrated with the native Aruba API, CyberGatekeeper offers NAC without these compromises while leveraging the full capabilities offered by Aruba controllers. To learn more, please download the PDF from: <http://infoexpress.com/media/products/aruba-110208.pdf>

#### **New Dynamic NAC FAQ**

InfoExpress has just released an updated Frequently Asked Questions on

#### Quick Links

##### Solutions

[LAN Security](#)  
[Remote Access](#)  
[Diverse Users](#)  
[Endpoint Security](#)  
[AV/Software Updates](#)  
[Demo](#)  
[Support](#)  
[Contact InfoExpress](#)

[Subscribe to this newsletter](#)

#### Watch a demo:

Seeing is believing. Watch a demonstration of how the Dynamic NAC solution works, and see first-hand the DNAC end-user experience.

[Watch Demo](#)

Or request a personal webcast to learn more about Dynamic NAC.

[Request Webcast](#)

#### Upcoming Events

[RSA Conference](#)  
February 14-18, San Francisco  
Moscone Center, Booth #2417

[Interop Las Vegas 2011](#)  
May 10-12, Las Vegas  
Mandalay Bay Convention Center, Booth #1220

#### Customer Corner

In this edition of Customer Corner we answer a question from one of our technology customers:

**Q:** We have started to replace our older 32 bit systems (x86) with newer ones running 64 bit operating systems (x64). I know the Agent works on x64 systems already, but should we expect any problems during the transitional period, when we have both x86 and x64 systems present?

**A:** No, as you pointed out we have Agent installers for both x86 and x64 Windows operating systems so you will not encounter any problems.

Dynamic Network Access Control (DNAC). This is a great resource to help you understand which organizations can and should use DNAC, where DNAC fits in the NAC market, how it works, specific elements, the relationship between DNAC and other network access control techniques and software, and more.

If you're using DNAC, might use DNAC, or just want to understand a bit more about network access control, we've made it easy. Please visit [http://www.infoexpress.com/security\\_products/dnac\\_security\\_faq.php](http://www.infoexpress.com/security_products/dnac_security_faq.php)

## CyberGatekeeper Enforcement Options

### *Alcatel-Lucent OmniSwitch Integration*

In this issue, the first of the new year, we'll be highlighting CyberGatekeeper integration with Alcatel-Lucent's OmniSwitch AOS. This is one of several integration points in ALU's Safe NAC offering. Integration with ALU's IP Address Management (IPAM) solution, VitalQIP, was covered in the September/October 2010 newsletter, and in the May/June 2010 issue, we reviewed CGK integration with ALU's OmniAccess (Aruba wireless).

For more information on Safe NAC, please visit: <http://enterprise.alcatel-lucent.com/?solution=Security&page=SafeNetworkAccess>

As with all ALU integration, the same CyberGatekeeper functionalities exist (pre & post connection assessment, quarantine, remediation, and reporting). With AOS/OmniSwitch Host Integrity Checking (HIC) enforcement, endpoints are quarantined by leveraging built-in features of the switch. When an endpoint is placed in a profile where HIC is required, it will remain quarantined until the HIC server (CyberGatekeeper) has confirmed the endpoint meets compliance requirements. Once the endpoint has met compliance requirements, it is monitored continually and may be returned to quarantine if it later fails a check. OmniSwitch maintains HIC status on a MAC-address basis which allows it to manage workstations separately from other endpoints such as VoIP phones which may be on the same port.

Here is how it works:

When a user/device connects to an enterprise network, the endpoint device is required to undergo a verification process. The OmniSwitch dynamically restricts network access using ACLs, which only allow the endpoint access to the CyberGatekeeper Policy Server and the remediation server(s). If the endpoint device has a permanent CyberGatekeeper agent installed, the agent communicates with the CyberGatekeeper Policy Server to assess the endpoint's integrity.

If the endpoint device does not have a permanent agent installed on it, the user is required to launch a browser that is redirected to a customer-defined web server. From here the CyberGatekeeper web agent is automatically downloaded onto the end-user's device. This web agent communicates with the CyberGatekeeper Policy Server and performs an integrity assessment. When complete, the agent reports the endpoint's status to the Policy Server. If the endpoint complies with security policies, it is allowed access to the network. Otherwise it is directed to the remediation server so it can be patched to meet security requirements.

The tests performed on the endpoint device by the agent are defined on the CyberGatekeeper Policy Server using the CyberGatekeeper Policy Manager. The policy server determines whether the endpoint device has passed or failed the HIC test and directly notifies the edge OmniSwitch to which the device is connected. Traffic restrictions and redirections are processed by the Alcatel-Lucent Access Guardian AOS feature, which

Even better, you can use a new feature in the CyberGatekeeper Policy Manager to combine the two Agent installers into a single executable that will work on both system types. To do this, simply go to Tools --> "Add new 32+64 Combination" in the Policy Manager. From here you can browse to the x86 and x64 installers, and provide the path for the new combined installer. Once you click the Build button, you will have a 'one size fits all' installer that you can deploy across your organization.

### Customers Talk:

**Georgia Legal** IT director says "CyberGatekeeper is one of those products that once it's implemented, you really don't have to do anything. You create the policies, make sure they're enforced, and forget about it." [Read case study](#)

**International manufacturer** security chief says "We now have secure remote access, and the security of our internal network is enforced continually." [Read case study](#)

**Financial institution** chief security officer says "With InfoExpress' CyberGatekeeper integrated into our network, we have created a superior level of network security and visibility. CyberGatekeeper used in conjunction with 802.1x gives us the ability to verify that every machine talking to our network is compliant and allows us to avoid dangerous rogue machines that can get in and damage corporate assets." [Read case study](#)

**Rainy River School Board** head of IT says "With Dynamic NAC from InfoExpress, we can protect our network and data from the risks associated with rogues and badly configured computers while providing students, teachers, and administrators access to services that enrich the educational process." [Read press release](#)

integrates authentication, device compliance, and NAC functions directly into the network infrastructure at the switch level.

If the OmniSwitch receives a HIC pass status for the specified endpoint device, the switch dynamically applies a new set of ACLs that allow the endpoint device access to the production network. If it receives a HIC fail status, the switch dynamically applies a restrictive set of ACLs that allow the endpoint to access the remediation servers only.

CyberGatekeeper's integration with Alcatel-Lucent's AOS provides customers with three compelling advantages. First, security is strong, as compliance is continuously enforced at the entry point to the network. Second, deployment is simplified. Quarantine ACL's are easier to deploy than 802.1x or SNMP enforcement, which involves re-architecting a network to support quarantine VLANs. Third, the end-user experience is superior when using ACL's. Compliant end-users will have faster access to the production network, and will be restricted immediately when necessary, as the use of ACL's eliminates the delays inherent in a VLAN switching approach. With these key advantages, the CyberGatekeeper and Alcatel-Lucent integration provides a compelling NAC solution. If you would like to learn more, please watch this demo: <http://enterprise.alcatel-lucent.com/docs/?id=16631>



#### About InfoExpress

[InfoExpress](#) network security solutions protect enterprise networks and the endpoints connecting to them. The company has provided network access control solutions since 2000. At the core of InfoExpress' solution is the award-winning CyberGatekeeper NAC Suite, which ensures endpoints are safe and compliant with security policies by performing real-time audits and quarantining of all network-attached endpoints. InfoExpress products have received numerous awards for innovation. The privately-held company in its 12th year of profitability is headquartered in Mountain View, California.

Visit InfoExpress at [www.infoexpress.com](http://www.infoexpress.com)

**Iona College** IT executive says "The CyberGatekeeper made the first day of school a pleasure. We cut nearly four hours out of our typical first day as the CyberGatekeeper simplified access and allowed the students to do the majority of the install and registration for network access themselves, while we provided support staff." [Read press release](#)

**Kelly College** network manager says "While we must ensure the protection of our students and the network, Kelly College cannot commit IS resources to complex system changes, and the InfoExpress solution solves the dilemma for us." [Read press release](#)

This e-newsletter is published bimonthly by InfoExpress. If you are not yet a subscriber, we invite you to [opt-in](#). [InfoExpress Privacy Policy](#)

© Copyright 2011 InfoExpress