

In this issue, we announce a major new version of CyberArmor, and take a closer look at endpoint-based NAC.

Issue Highlights:

[CyberArmor 4.0 released](#)
[Protecting Endpoints](#)
[Using Dynamic NAC for LAN and WAN access](#)
[Product End of Support Schedule](#)
[Customer Corner](#)

**CyberArmor 4.0 Announcement**

InfoExpress is pleased to announce the release of the 4th generation of CyberArmor, its enterprise class personal firewall solution. CyberArmor is fully customizable and environmentally sensitive, adjusting its policies dynamically. This ensures maximum protection at all times, whether a user connects on the corporate network, over wireless, or over a dial-up.

CyberArmor 4.0 adds new features such as Windows 7 support (32-bit, and 64-bit), IPV6 blocking, and client plugins. For a complete listing of CyberArmor 4.0 features, or if you would like more information on CyberArmor 4.0, please contact InfoExpress at support@infoexpress.com.

**NAC on the Endpoints**

To protect network assets themselves as well as the network at large, organizations deploy NAC software directly on each computer that access the network. There are so many benefits to having an agent on each computer, including deeper compliance-checking in assessing the endpoint and proactive enforcement on the endpoint, providing better security and protection. An agent can also provide remediation options, which help reduce help desk costs.

We use our CyberGatekeeper Agent to communicate with our CyberGatekeeper Server for NAC posture check and enforcement. Because the organization controls the endpoints, installing our small footprint CyberGatekeeper Agent along with all the other required software is simply part of the provisioning of any new device.

We offer NAC Agents in two basic flavors.

A NAC agent that is permanently installed on the endpoint is known as a *persistent NAC agent*. A persistent NAC agent is the most practical way to use NAC to keep managed endpoints correctly configured and in alignment with security policies. When the endpoint tries to access the network, our persistent NAC agent, CyberGatekeeper Agent, connects to CyberGatekeeper Server for NAC assessment and enforcement. If the endpoint needs remediation, the software can be configured to assist with or even automate remediation, perhaps by going to a specific site to download software updates or by following a predefined script.

A NAC agent that temporarily installs itself for the purpose of NAC assessment and enforcement is known as a *dissolvable NAC agent*. CyberGatekeeper offers a dissolvable NAC agent useful for unmanaged

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](#)

InfoExpress in the News

“Dynamic NAC can be a cost-effective solution for organizations that have many sparsely populated branch offices, because it doesn’t require additional hardware ... customer satisfaction with InfoExpress remains high.”
—Gartner, 2009 NAC report

Customers Talk:

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

endpoints that want temporary access to the network. This allows your organization some control over the endpoint, despite the fact the endpoint is ultimately not under the organization's control.

CyberGatekeeper Enforcement Options

Dynamic NAC (DNAC)

Continuing our series on the various CyberGatekeeper enforcement options available to InfoExpress customers, we'll examine in this issue a unique approach in the NAC market that provides some very unique benefits—a peer-based method called Dynamic NAC (DNAC). As with all CyberGatekeeper enforcement options, the same pre- & post-connection assessment, quarantine, remediation, and reporting functionalities exist.

DNAC's approach to enforcement is based on a "neighborhood watch" model. Endpoints that have passed audit and are compliant with the security policy are considered trusted, and therefore are eligible to become enforcers. DNAC automatically elects a subset of these eligible endpoints to enforcer status. The enforcers use a combination of active and passive detection mechanisms to discover a new endpoint when it joins the network.

When an enforcer sees a new endpoint join the network, it checks to see if that endpoint has passed audit or is white-listed. If neither of these is true, the endpoint is considered a rogue, and the enforcers take action to quarantine the endpoint. Any endpoint, with or without an agent, is prevented from obtaining full network access until it has passed audit or unless it has been white-listed.

DNAC will fully enforce all endpoints with no additional configuration or network changes - including Windows XP through Windows 7, Linux, Mac, and network devices.

Here is how it works:

When a new endpoint attaches to the network, the DNAC enforcers on that segment detect it and immediately redirect its traffic, and local DNAC endpoints block the new endpoint. The quarantine and blocking continues while waiting for an audit to be performed against the new endpoint. There are three ways to perform the audit:

- i. The DNAC enforcer can redirect the endpoint's traffic to a web agent allowing guests, who do not have the desktop agent, to perform an audit;
- ii. The endpoint may already have a desktop agent running which will automatically perform the audit;
- iii. The policy server may have included the new endpoint in its white list, indicating that it is allowed access regardless of its audit status.

The enforcer is auditing with the same policy server as the new endpoint, so the enforcer can determine if the new endpoint has passed the audit. When the new endpoint passes audit, the enforcer releases the quarantine and allows traffic to communicate normally. If not, the enforcer maintains the quarantine against the new endpoint. DNAC differs from host based solutions because the enforcers control other PCs access to the local subnet and to other networks, not just traffic to itself.

Dynamic NAC is InfoExpress' most popular enforcement option for the LAN and WAN, because it offers many benefits:

1. Strong security against rogue devices
2. Eliminates network changes, network reconfigurations, and quarantine VLAN's (Low TCO)

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](#)

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](#)

3. Provides a responsive and transparent end-user experience
4. Authentication agnostic (Windows Domain, 802.1x, other)
5. Scalability (10,000 users and 200+ VLAN's per appliance)
6. Supports remote offices over WANs without requiring additional hardware or management platforms

DNAC's unique design provides many unique benefits, with its key advantage being strong security that is easy to deploy. For more information on CyberGatekeeper and copies of past newsletters, please visit <http://www.infoexpress.com/news/newsletter.php>.



Product End of Support Schedule

The [Product End of Support](#) schedule details product versions that will no longer be supported or updated, and shows supported status for all InfoExpress product versions. All customers should be aware of this schedule and plan accordingly. [View detailed schedule](#).



Customer Corner

In this issue's Customer Corner, an overseas government customer asks how to get the most out of their 'captive portal' in DNAC:

Q: I have redirection working fine in DNAC, however I would like to 'exclude' certain sites from the redirection. For example, I would like my users to be able to download patches directly from our local patch server. Is this possible?

A: Yes. The ACLs that define redirection in DNAC are actually quite flexible. First, you will want to see what redirection (if any) is already in place. You can see your ACLs by going to Default Settings → Global Defaults. At the bottom of that page is a section containing the global ACLs. (Note that each subnet scope may also have ACLs which are prepended to the global rules.)

Now down to the nuts and bolts of the problem. Let's say you want to redirect all your quarantined users to the web server at <http://remediation.example.com>, however you still want them to be able to download patches from <http://windowsupdate.com>. You may want to start these rules:

```
ALLOW DNS windowsupdate.com
ALLOW TCP REM windowsupdate.com 80
DENY DNS * REPLY remediation.example.com
ALLOW TCP REM remediation.example.com 80
ALLOW TCP REM remediation.example.com 443
```

Line by line, here is what these rules do:

```
ALLOW DNS windowsupdate.com
```

When the client does a DNS lookup for windowsupdate.com, allow it through; they will get the actual IP address for windowsupdate.com.

```
ALLOW TCP REM windowsupdate.com 80
```

Allow HTTP traffic to windowsupdate.com. This is not implied from the above rule and must be explicitly ALLOWed by a rule.

```
DENY DNS * REPLY remediation.example.com
```

For every other DNS lookup, return the IP address for

remediation.example.com. So for example if the user attempted to go to google.com, DNAC would return the IP for remediation.example.com. While the user's browser would think they went to Google, it would show the landing page from remediation.example.com instead. This is how we accomplish the 'captive portal' experience for the user. Note that instead of using the hostname remediation.example.com, you could redirect to an IP address instead.

```
ALLOW TCP REM remediation.example.com 80  
ALLOW TCP REM remediation.example.com 443
```

Allow HTTP and HTTPS to remediation.example.com, so the user has access to the landing page, hosted patches, etc. As with the previous ALLOW TCP rule, this access is not implied.

In concert, these rules allow quarantined systems to access windowsupdate.com directly, and be redirected to the landing page at remediation.example.com for all other web sites. For more information on writing ACL rules, the online help (?) icon next to the ACL edit box is a good place to start. If you still have questions, please contact InfoExpress support.



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

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 2010 InfoExpress