

## RE: HIDS solution for NT4 machines

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ids/2005-10/0009.html>

---

**From:** Jason ([securitux\\_at\\_gmail.com](mailto:securitux_at_gmail.com))

**Date:** 10/06/05

To: <[bcihak@gmail.com](mailto:bcihak@gmail.com)>, <[focus-ids@securityfocus.com](mailto:focus-ids@securityfocus.com)>

Date: Wed, 5 Oct 2005 18:25:19 -0400

If you can't find a HIDS, then you can always put in a network IPS and use it to separate your NT4 servers from the rest of the environment. If 6a breaks your software, a HIDS may as well, even if you find one that works on less than 6a. So a network IPS would be a good alternative.

-J

-----Original Message-----

From: [bcihak@gmail.com](mailto:bcihak@gmail.com) [<mailto:bcihak@gmail.com>]

Sent: Monday, October 03, 2005 12:52 PM

To: [focus-ids@securityfocus.com](mailto:focus-ids@securityfocus.com)

Subject: HIDS solution for NT4 machines

I work in a large distributed network. We have several workstations and servers that are running on NT4. I've been tasked with finding some sort of a HIDS (Host based Intrusion Detection System) software solution to protect these machines from zero day exploits, worms, and BO's. I've looked at Cisco, Blink by Eeye, Destop Protector by ISS, and Primary Response by Sana Security. None of these will support anything lower than NT4 SP6a. My biggest problem is I have several machines that are running below SP6a and because of the flaky software running on these machines, I can't install SP6a without breaking the app. Does anyone have any good experience with other products for NT4 server/workstation below SP6a.

Just a side note, most of these machines will be replaced within 2 years, but that is a long time to leave exposed machines on the network.

Thanks!

Bcihak

---

Test Your IDS

Is your IDS deployed correctly?

Find out quickly and easily by testing it with real-world attacks from CORE IMPACT.

SecurityFocus IDS: RE: HIDS solution for NT4 machines

Go to [http://www.securityfocus.com/sponsor/CoreSecurity\\_focus-ids\\_040708](http://www.securityfocus.com/sponsor/CoreSecurity_focus-ids_040708)  
to learn more.

---

Test Your IDS

Is your IDS deployed correctly?  
Find out quickly and easily by testing it  
with real-world attacks from CORE IMPACT.  
Go to [http://www.securityfocus.com/sponsor/CoreSecurity\\_focus-ids\\_040708](http://www.securityfocus.com/sponsor/CoreSecurity_focus-ids_040708)  
to learn more.

---