CYBERCRYPT.

How to Choose An Intrusion Detection System

February 22, 2021

The recent zero-day attacks on SolarWinds and more than 100 other businesses and nine government agencies spell it out as never before: every enterprise needs an intelligent, application-based intrusion detection system (IDS).

The recent zero-day **attacks on SolarWinds and more than 100 other businesses and nine government agencies** spell it out as never before: every enterprise needs an intelligent, application-based intrusion detection system (IDS).

This valuable cybersecurity tool can prevent intruders from lurking in

IDS can often identify rogue outbound traffic such as a malware-infected endpoint communicating with a command-and-control botnet server. Using an IDS can make it easier to find the compromised device and block the suspicious signals.

So – why isn't everyone already using an IDS? The answer, often, comes down to a lack of expertise.

IDS is incredibly complex, and requires a laundry list of skills and knowledge to configure and use properly. But just choosing an IDS is a challenge per se and many organizations fail to move beyond this first step.

That's because IDS comes in several different forms. To the uninitiated, selecting one can be baffling and even intimidating.

Perhaps your enterprise's IDS program has faltered or halted amid the plethora of possibilities.

Maybe you're dragging your heels waiting for the ultimate IDS solution to appear.

Either way, the outcome is the same: without IDS, it's more likely every minute that hackers are nefariously working, undetected, in your systems and networks. Is this a risk you really want to take?

Types of intrusion detection systems

Intrusion detection systems are typically **network-based** or **host-based.**

- **Network-based IDS (NIDS)** monitors communications at the network level.
  The communications flowing through a network-based IDS typically consists of units of data, or "packets," that its hosts send to one another internally or to external hosts outside the network.

make gathering and analyzing all that data very complex and difficult, thus prone to errors.

- **Host-based IDS (HIDS)** resides on a single computing device and monitors traffic flowing into, out of, and on, that device. It checks local files, environment variables, system calls, logs, and local network traffic.

  Many enterprises prefer host-based IDS because encryption protocols typically end at the host. By the time the IDS views the data, it's decrypted.

  Host-based IDS includes intrusion detection systems that work at the application level. Growing in popularity, **application-based IDS** takes a more precise and intimate approach, looking for unusual activity in and on specific host applications.

  Application-based IDS must be designed or configured for each individual application. An application-based approach might require more work up front, but offers superior access to information, performance, and detection abilities than a general host-based or a network-based IDS.

Whether to base your IDS on the network, host, or application is only one decision you must make as you start your IDS program.

What kind of detection will your IDS use? And — should you buy a ready-made IDS solution, design your own, or have IDS experts tailor one to your specific needs?

CYBERCRYPT.

WE ARE

THE CRYPTOGRAPHY AND SECURITY EXPERTS

At CYBERCRYPT, we combine decades of experience in cryptography, secure architecture, and security analysis to keep your product protected.

GET IN TOUCH →

CORPORATE HEADQUARTERS
Sankt Annæ Plads 13, st tv.
1250 Copenhagen, Denmark

info@cyber-crypt.com
+45 53737400

WHAT WE DO

OUR APPROACH

ABOUT US

CONTACT

PRIVACY POLICY