



Novell® Sentinel™ Advisor

The number of attacks most companies face on a daily basis is staggering—about 12 every second. Some of those attacks are benign, some warrant a closer look and some are downright dangerous. Knowing the difference is key to eliminating false-positives and drastically reducing the need for manual review. Nothing makes that distinction quicker or more accurately than Novell® Sentinel™ Advisor.

Volumes of Security Data

Security products such as intrusion detection systems (IDS), intrusion prevention systems (IPS) and firewalls play a vital role in protecting corporate assets. They not only establish a perimeter defense, but they also alert IT staff to potential network attacks. Similarly, vulnerability scans review IT systems to identify weaknesses that could increase the likelihood of a successful malicious attack.

Making sense of the volumes of data generated by these systems is challenging, not only because of the sheer number of security events, but also because the various security products do not use standard naming for the signatures, or digital descriptions, of those events. This complex and confusing disparity can lead to false positives and make it difficult to prioritize appropriate responses to real threats.

Real Time Vulnerabilities

Novell Sentinel Advisor, an add-on service to the award-winning security management solution from Novell, eliminates this challenge. Sentinel Advisor acts as a translator, interpreting the naming conventions of each security product to determine the relationship between the attacks or potential exploits each product is reporting. By translating and cross-referencing the events reported by disconnected security products, Sentinel Advisor determines whether two or more of those events are actually referencing the same attack. Novell Sentinel Advisor also stays up to date on new attacks and exploits known to the industry without any manual intervention. The product captures vendor updates published to firewalls, IDS/IPS and vulnerability scanners on an hourly basis, allowing it to detect virtually every known attack and effectively prioritize any related threats.

■ Solutions:

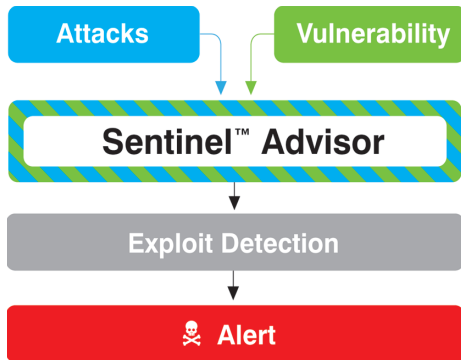
Identity and Security Management

■ Products:

Novell Sentinel

Novell Sentinel Advisor works with security products you already have to identify and prioritize events, virtually eliminating false positives and reducing the need for manual review.

www.novell.com



Novell Sentinel Advisor aggressively correlates IDS/IPS events with vulnerability scans and alerts your IT staff if an attack is targeting a known and exploitable vulnerability within an application. Once Sentinel Advisor identifies and correlates security events, it organizes and prioritizes them according to the risk they pose to the network. A red alert might require immediate action from the IT staff, even at 2 a.m., while a less-threatening attack—such as a Windows-based attack on a Linux* server—might simply be logged for later review or filtered out altogether. In each case, Advisor works with Novell Sentinel to notify the appropriate security staff member in the face of a legitimate threat, as well as define, automate and document a workflow process to counter the attack. This logical approach unifies the security infrastructure so you can use

your existing technology investments more effectively.

Take Advantage of a Complete Security System

A broad range of industry-leading security products are supported by Novell Sentinel Advisor, including Cisco* Secure IDS, Symantec* Intruder Alert, McAfee* IntruShield, ISS Database Scanner and many others. Regardless of the product or its unique format for event signatures, Sentinel Advisor can translate the data and help you determine if events exploit specific vulnerabilities and how those attacks impact your assets.

Detecting network attacks is only half the battle. Novell Sentinel Advisor can also help you determine the relationship between reported events and the relative priority of each threat. By making sense of the volumes of inconsistent data generated by IDS/IPS, firewalls and vulnerability scanners, Sentinel Advisor plays an invaluable role in identifying and mitigating real threats, alerting security staff in real time, virtually eliminating false positives and reducing the need for manual review.

Learn more about Novell Sentinel Advisor and what it can do for you today at: www.novell.com/products/sentinel



Contact your local Novell Solutions Provider, or call Novell at:

1 800 714 3400 U.S./Canada
1 801 861 1349 Worldwide
1 801 861 8473 Facsimile

Novell, Inc.

404 Wyman Street
Waltham, MA 02451 USA