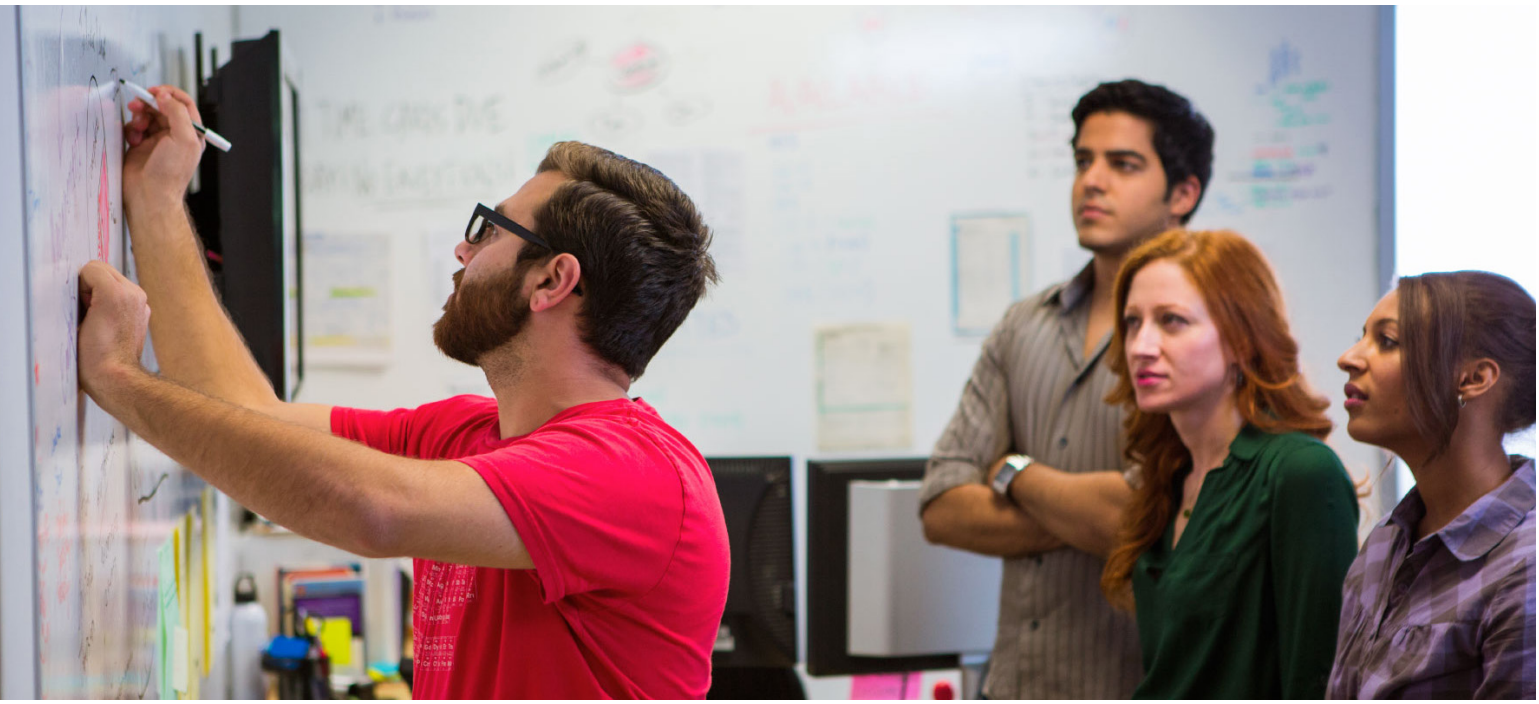
SonicWALL

Five Best Practices for Advanced Threat Protection

Discover must-have capabilities for an effective sandbox environment.



Introduction

Advanced threats such as zero-day exploits and custom malware are on the rise. Today, organizations of every size are targeted by cyber criminals who continually seek, find and exploit holes in vulnerable software. They do this to gain access to networks, systems and data, often perpetuating serious harm within minutes. To better detect these unknown threats, security professionals are deploying advanced threat detection technologies such as virtual sandboxes, which analyze the behavior of suspicious files and uncover hidden malware.

However, threats are getting smarter. Malware is now being designed to detect the presence of virtual sandboxes and then evade them. That limits the effectiveness of threat detection technologies. Organizations need a new approach to protect their business from these advanced threats. In particular, this requires threat analysis technology that can't be detected or evaded by malicious code. To accomplish this, a best-in-class advanced threat protection (ATP) solution must be able to do the following:

- Dynamically layer sandbox analyses
- Examine encrypted traffic
- Analyze all files
- Block files until they are verified
- Expedite the remediation of identified threats

> Today's sandbox environments must be as comprehensive and dynamic as the threats they seek to prevent.

Dynamically layer sandbox analyses

Providing additional layers of threat analysis with a multi-engine sandbox is intrinsically more effective at discovering zero-day threats than a single-engine approach. A single-engine sandbox is easier for malware to detect and evade. Optimally, an effective threat analysis platform combines multiple layers of malware analysis engines, including not only virtual sandbox environments but also operating system and hardware emulation sandboxing combined with memory analysis.

Using this approach, suspicious code can be executed in the multi-engine sandbox platform, which includes virtualized sandboxing, full system emulation and hypervisor-level analysis technology. The behavior of any suspicious file can be analyzed, providing comprehensive visibility into malicious activity while resisting evasion tactics and maximizing zero-day threat detection.

It is also important to be able to add layers of threat analyses dynamically. Because threats are constantly hiding in new ways, what's needed is a threat analysis platform that changes and adopts new detection and threat engines as needed. The only thing that isn't going to change is that attack techniques will continue to change. For zero-day threat protection, solutions that can dynamically add new malware analysis engines as the threat landscape evolves are the most effective at detecting today's and tomorrow's advanced threats and malware.

Examine encrypted traffic

Today's advanced threats apply complex and sophisticated methods to remain undetected. They use completely new methodologies or adopt existing defense mechanisms, such as hiding in encrypted SSL traffic. To be effective, an advanced threat detection solution should inspect all traffic — whether it's unencrypted or encrypted — for suspicious files. Often not possible with vendors of stand-alone products, sandboxes working with a next-generation firewall can leverage the use of SSL-terminating technology to examine encrypted files.

Analyze all files

Beyond hiding encrypted traffic, malware authors hide malicious code in files and applications. To combat this, sandboxes should be able to analyze hidden malware in a broad range of file types, file sizes and operating environments to best provide comprehensive zero-day threat detection. This setup should include analysis of numerous file types, including executable programs, PDFs, MS Office documents, archives, JAR and APK files, as well as multiple operating system environments such as Windows, Android, Mac OS X and multi-browser environments. For greatest flexibility, the solution should enable custom analyses by file type, file size, sender, recipient and protocol, and it should allow the manual submission of files for analysis.

Block files until they are verified

Detecting zero-day threats is critical. But detection alone is not enough. A viable solution should not only inspect traffic for suspicious code but also provide the capability to block suspicious code from entering the network until after it's analyzed and a verdict is reached. Some siloed sandboxes reach a verdict only after a file has been allowed into the network, and in these cases, function as a fire alarm instead of a preventative measure.

Expedite the remediation of identified threats

Once a threat is identified, fast, automatic signature updates are critical. The effectiveness of threat protection depends on alleviating the time-consuming task of manually maintaining a proactive security stance. To prevent follow-on attacks, signatures for newly discovered malware should be quickly generated and automatically distributed across network security devices, thereby preventing further infiltration of the identified malware threat. In this scenario, when a file is identified as malicious, a new signature is immediately deployed to firewalls for inclusion in gateway anti-virus and IPS signature databases, as well as the URL IP and domain reputation databases. Optimally, you would want an at-a-glance dashboard to monitor advanced threat detection and provide detailed analysis reports.

Conclusion

Today's sandbox environments must be as comprehensive and dynamic as the threats they seek to prevent. By following these recommended best practices when selecting an advanced threat sandbox solution, organizations will benefit from detection and protection, high-security effectiveness and rapid response times.

Find out how Dell SonicWALL can help you deliver on the promise of advanced threat protection. Contact us to see how Capture ATP can protect your business.

For More Information

About Dell Security

Dell Security solutions help you create and maintain a strong security foundation with interconnected solutions that span the enterprise. From endpoints and users to networks, data and identity, Dell Security solutions mitigate risk and reduce complexity so you can drive your business forward.
www.dell.com/security

If you have any questions regarding your potential use of this material, contact:

Dell
5455 Great America Parkway,
Santa Clara, CA 95054
www.dell.com/security

Refer to our Web site for regional and international office information.