DATA SHEET

SecureWorks

Advanced Managed Palo Alto Next-Generation Firewall Service

Integrated Intelligence for Proactive Protection

The Challenge

Today's networks face unprecedented security and availability challenges. Attacks such as web-based exploit kits, malware, application-layer attacks and targeted threats — coupled with the evolution of cloud technology and web-based applications — have introduced additional layers of complexity. As a result, traditional detection technologies and methods are proving to be insufficient to effectively combat today's threats. To successfully protect their networks, organizations need a combination of technology, expertise and trusted intelligence.

The Solution

The SecureWorks Advanced Managed Palo Alto Next-Generation Firewall (NGFW) service enhances existing Palo Alto NGFW capabilities through the inclusion of our Attacker Database into the platform, using its dynamic blocklist functionality. By combining this threat intelligence into the FW device, SecureWorks delivers an additional level of protection to our clients by proactively blocking traffic to known malicious domain names and IP addresses. This defense-in-depth approach provides:

- Peace of mind through proactive protection from known threat actors
- Ease of use via automatic updates of the Attacker Database blocklists on a scheduled basis (every hour)
- Granular control and in-depth protection from breaches
- Powered by the SecureWorks Counter Threat Platform

How it Works

The SecureWorks Advanced Managed Palo Alto NGFW service helps organizations protect their business continuity and critical assets by combining granular control and in-depth, application-layer protections with proactive blocking of traffic to known malicious domains and IP addresses. Working with Palo Alto Networks, SecureWorks automatically applies and updates our Attacker Database blocklists on Palo Alto's next-generation firewall devices through the NGFW's dynamic blocklist functionality. Using this integration, managed Palo Alto Networks NGFW devices can be configured to proactively block traffic to known malicious domain names and IP addresses, with blocklists being automatically updated using the Attacker Database threat intelligence data feed. The solution is part of the NGFW fully managed service, which also offers flexible monitoring and co-management options, policy and rule-set management, device upgrades and patch management, backup and recovery, as well as extensive security and compliance reporting capabilities. Organizations that use SecureWorks to monitor and manage their security appliances benefit from the visibility and correlation of data

By the Numbers:

- 4,300+ Clients
- 59 Countries
- 5 Counter Threat Operation Centers (CTOCs)
- As Many as 180 Billion Network Events Analyzed Daily

24x7

across security technologies and thousands of customer networks to detect and prevent threats prior to impact.

Attacker Database

The SecureWorks Attacker Database service provides organizations with access to a data feed of IP addresses and domain names associated with web-based exploits, malware, command and control servers (computers used by threat actors to deliver commands and/or malware to its compromised computers and mobile devices), and other known malicious infrastructure. By applying this threat intelligence to managed Palo Alto Networks Next-Generation Firewalls, SecureWorks is providing organizations an additional level of protection against malicious threats and attacks.

Solution At-a-Glance

- Available at no-cost to our managed Palo Alto Next-Generation Firewall clients
- The service includes the high fidelity portion of our proprietary Attacker Database
- Threat Intelligence Add-on: AttackerDB: Palo Alto: Managed Firewall Only (TI-ADDON-ADB-PA-MMFW)

Why SecureWorks

- **Our Expertise**
  SecureWorks hires only the best and brightest. From our in-depth technical hiring process to our continued investment in our team members through generous training programs, we seek to find and cultivate technical excellence. Our team members can be found speaking at industry conferences and releasing cutting-edge security research.
- **SecureWorks Global Threat Intelligence**
  Threat intelligence is the fuel that powers the engine of the security solutions we provide. With more than 65 of the world's most highly regarded security researchers, SecureWorks' distinguished Counter Threat Unit™ (CTU) research team is what sets us apart. Our researchers analyze threat data across our global client base and actively monitor the cyber threat landscape to provide a globalized view of emerging threats that is integrated into every security solution we provide.
- **Proven Methodology**
  SecureWorks has performed thousands of assessments and tests for a wide array of companies from small business to Fortune 500. Our methodology is a combination of proven, public industry methodology (NIST and PTES), in conjunction with our experts' advice and years of experience. Our methodology is updated on a regular basis to match current industry and attack trends.

For more information, call **(877) 838-7947** to speak to a SecureWorks security specialist.

www.secureworks.com