Panda and Devo join forces to stem next-gen malware attacks, secure proliferating endpoints

Overview and current situation

Data security is top of mind for many corporate IT and security leaders. The volume of malware has increased exponentially, with attacks and threats becoming more sophisticated and more persistent. In addition, the number of endpoints within an organization has grown rapidly, and this growth shows no signs of slowing down. And those end-points, as we've seen recently in the news, may include data streams coming from IoT networks, which may represent one of the most serious threats the cybersecurity industry has ever faced.

IT departments are overwhelmed: The large volumes of information that they must handle and the appearance of next-generation malware, causes many details to be overlooked or not recognized, compromising the security of the system.

Panda Security and endpoint protection

Panda Security, a leader in cloud-based security solutions for businesses and consumers, offers endpoint security protection for endpoints and servers. The solution, available via Amazon AWS, is packaged as a centralized console which manages configuration and deployment of client agents.

Panda Adaptive Defense is an endpoint detection and response service that protects businesses against targeted attacks and advanced threats. The offering is the implementation of a new security model that correlates data from multiple data sources, and brings together the capabilities of machine learning and Big Data within the Panda Security platform. Adaptive Defense accurately classifies every process running in an organization, allowing only legitimate behaviors to run. Real-time security analysis is performed in the Panda Malware Intelligence Platform to detect and prevent events such as zero-days security attacks, targeted attacks, and ransomware attacks.

INDUSTRY: IT SECURITY

LOCATION: EUROPE, ASIA, PACIFIC, AFRICA, AMERICA

CHALLENGE

IT departments are overwhelmed by malware's growing sophistication and volume, and the number of endpoints that must be secured. To deliver the next generation of endpoint security, Panda needed a partner with a cloud-based platform that could rapidly collect and analyze a wide range and large volume of data, and make the information easy to understand and act on.

SOLUTION

Devo gives Panda a Data Operations Platform capable of processing hundreds of thousands of events per second per core. Devo also delivers tools to easily create/configure dashboards with key indicators, adaptive search options, and alerts for a wide range of security, usage and governance issues.

RESULTS

Panda uses Devo, running in Amazon AWS, to automatically generate security intelligence and allow organizations to pinpoint attacks and unusual behaviors, as well as internal misuse. It enables users to:

- Perform calculations and graphical visualizations
- Receive alerts on Network Security Status Indicators and IT resources usage
- Determine threat origin and perform forensic analysis
- Gain visibility into endpoint vulnerability
- Monitor and control misuse of corporate resources.

Devo: The clear choice

Even with a robust endpoint security offering, Panda recognized the need for a forward-thinking partner to help create new tools and value propositions for its customers.

Devo fit the bill. A key priority for Panda included having a partner with a cloud-based platform with the ability to both collect a wide range of data and rapidly analyze large volumes of data in human and machine real-time. With Devo, Panda is able to leverage a Data Operations Platform capable of processing hundreds of thousands of events per second, per core.

Panda also wanted to ensure its partner was able to provide new and innovative offerings and tools to make data gathered and analyzed as meaningful as possible to the end user. Devo delivers on this need, providing tools to easily create and configure dashboards with key indicators; adaptive search options; and default as well as custom alerts related to security incidents, risk situations, user access to critical information, and application/network resource usage.

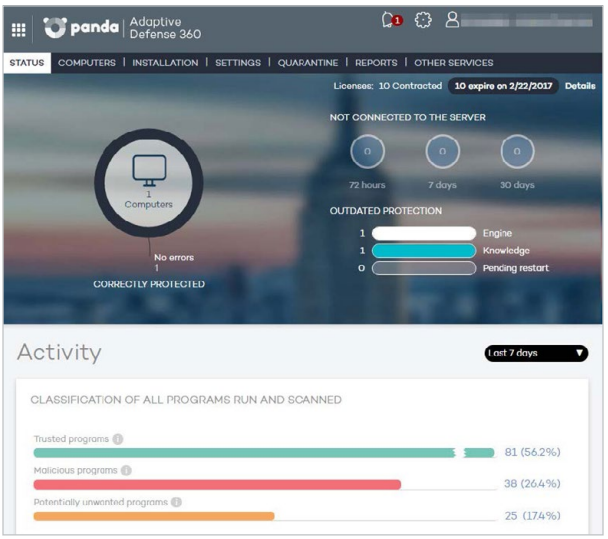

Figure 1: Panda Security dashboard

Delivering security analytics in the cloud, at scale

Working together, Panda and Devo have created a module for the Adaptive Defense offering called Advanced Reporting Tool (ART). ART automates the storage and correlation of the information related to process execution and its context extracted by Adaptive Defense from endpoints. This information enables ART, delivered through the Devo Data Operations Platform, to automatically generate security intelligence and allow organizations to pinpoint attacks and unusual behaviors, regardless of their origin, as well as detect internal misuse of corporate systems and networks. ART's unique capabilities enable calculations, graphical visualization and alerts on Network Security Status Indicators and IT resources usage.

> "ART is a leap forward in how companies approach security, so it naturally requires tremendous speed and power to achieve its objectives. The Devo Data Operations Platform, which processes over 150,000 events per second/per core, more than meets these performance requirements."
>
> — IRATXE VAZQUEZ, PANDA SECURITY

The Devo platform provides Panda customers with increased visibility into their endpoints, malware and other security issues. Because a massive amount of data is collected at endpoints, the Panda/Devo solution affords the ability to search for external and internal threats, diagnose critical vulnerabilities, and report and alert in real-time, so businesses can take immediate action to prevent or limit the impact of attacks. Devo capabilities enable wide visibility in forensic intelligence regarding any event registered.

Additional benefits for customers using the ART offering

Determining the Origin of Threats and Forensic Analysis. When an organization is facing a security incident, it could take a significant amount of time before that organization is able to determine the incident occured. In these instances, the organization and their security partner need to look back at data to find the threat, identify its source, and determine how deeply rooted the problem is. With Devo, Panda is able to go back in time one year to correlate data from endpoints, identify the malware, pinpoint every place the malware has touched and done damage, and highlight the vulnerable application. With this knowledge, the organization can quickly take action to remediate the issue and apply security measures to prevent future attacks.

Visibility into Vulnerabilities. Most organizations believe they know where all their endpoints are installed, and that these endpoints are secure. In reality, they may not have full visibility. Working with Devo, organizations now have clearer visibility into all machines running on the endpoint that are vulnerable. In addition, customers also receive a list of vulnerable elements and applications so they can take action to eliminate vulnerabilities quickly.

Monitoring and Policies. Using the Devo platform, customers can monitor and control misuse of corporate resources that may have an impact on business and employee performance. For example, the customer is able to monitor data usage and identify outliers, such as specific endpoints utilizing excess bandwidth. Armed with this information, customer can assess if this usage is normal and expected, or if it is a matter that needs to be addressed and corrected. The information gives the organization the power to take appropriate action, such as implementing more restrictive policies and limiting access to critical business issues.

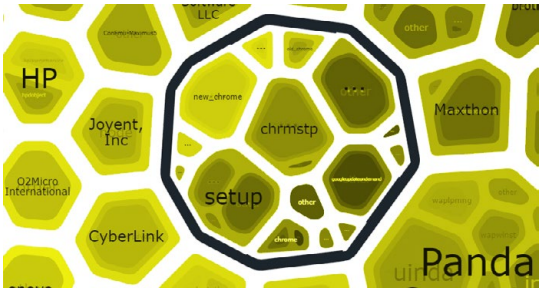

Figure 2: Panda Monitoring and Policies

Unexpected Cost Savings. Customers have found additional benefits to deploying the Panda-Devo solution. For example, organizations may be purchasing more software licenses than they need. By deploying Devo as part of a larger security offering, organizations can easily determine how many licenses are actually in use. If they're using fewer than they have purchased, they can reduce the number of licenses, often achieving immediate cost savings and faster ROI on their security investment.

Looking towards the future with Devo

Devo and Panda are planning to expand their partnership with several future initiatives. One potential upcoming offering may involve integrating Adaptive Defense (events/data, vertical applications, queries and alerts) into Devo as a third party. When this model is ready, customers will be able to correlate events from endpoints and other devices, giving greater visibility into their networks.

Conclusion

The ART offering brings a number of capabilities to customers that are critical in today's security environment, in which some companies may even need to stem attacks coming from IoT networks. These include real-time alerts and reports, access controls for confidential or sensitive business data, and the ability to diagnose network issues. Partnering with Devo, Panda Security has been able to identify new business opportunities and connect the dots between security and endpoint IT management to give its customers knowledge that enables them to gain competitive advantage.

About Devo

Devo is the leading Data Operations Platform for the digital enterprise. Devo delivers real-time business value from analytics on streaming and historical data to help Fortune 1000 enterprises drive sustained performance and growth. The Devo Data Operations Platform collects, enhances and analyzes machine, business and operational data from across the enterprise. Devo provides real-time analytics and insight for IT operations, security analytics, business analytics, customer insight and log management for the world's leading organizations.

For more information about Devo, visit **www.devo.com**

ABOUT DEVO

Devo delivers real-time operational and business insights from analytics on streaming and historical data to operations, IT, security and business teams at the world's largest organizations. The Devo Data Operations Platform collects, enhances and analyzes machine, business and operational data, at scale, from across the enterprise.