Technology And Product Review For Endpoint Protection Solution

Posted on October 31, 2018

Endpoint Protection Platforms and Enterprise Security Requirements

A set of technologies and software tools that enable the securing of endpoint devices is called an endpoint protection platform, EPP. This unified security solution combines antispyware, antivirus, personal firewall, intrusion prevention/detection and other endpoint protection solutions.

It is mainly developed for the protection of endpoint devices in an IT enterprise environment where the devices largely include standard workstations. Mobile devices today are now considered part of the supported devices as well. The core functionality of an EPP solution involves protecting devices from spyware, viruses, unauthorized access and phishing while also providing protection against data loss, along with services such as data encryption in order to secure the data stored on endpoint devices (Lord, 2017). Endpoint security software is able to develop security reports for security analysis in an instant. They lessen incident response time by 31% and reduce overall time to about 45% (Dominguez, 2016).

The first thing to consider when choosing an EPP solution is the platform coverage, such as what operating systems are supported and whether mobile devices are compatible or not. The detection rate of the security feature is to be checked on the net in order to evaluate the product's performance. The price of the EPP solution and the support available from vendors are also to be taken into consideration. In a large-scale commercial setting, the price of the EPP solution is particularly important since it usually involves an annual license renewal fee. EPP solutions suitable for today's enterprise needs are mostly cloud-managed and allow continual collection and monitoring of activity data alongside the capability to remotely take remediation actions when needed, regardless of the location of the end-point at the time. The solutions, additionally, are cloud data-assisted, where the endpoint agent does not have to maintain a record of known Indicators of Compromise (IOC), as it can easily check the cloud resource to find the latest information on objects that it is not able to classify. Security automation, orchestration, and response tools are also to be considered when making a decision (Gartner, 2018).

Bitdefender GravityZone and Comparative Product

Features

According to PC Mag, the topmost EPP software include Bitdefender GravityZone Elite, Trend Micro Worry-Free Business Security Services, F-Secure Protection Service for Business, Webroot SecureAnywhere Business Endpoint Protection and Avast Business Antivirus Pro Plus (Matthew D. Sarrel, 2017). Based on the rating, the endpoint security solution we chose is Bitdefender GravityZone Elite.

The Bitdefender Endpoint Security for Mac is a computer security solution that is fully automated and remotely managed by a network administrator. Upon installation, it protects against a variety of security threats, such as Trojans, viruses, spyware, keyloggers, adware, and worms. It can detect malware not only in a Mac system but also in Windows malware in order to protect workstations from sharing infected files on a network. It allows a complete history log of events relating to Endpoint Security activity on the Mac. It offers several features, such as the On-Access scanning module, that monitors the system continuously for any malware-like actions and blocks threats from penetrating the system. The network administrator controls the On-Access scanning through the security policies. Enabling it allows malware and threat signatures and product updates to be automatically downloaded to the system to keep it updated. It does not affect the product's operations nor leave it vulnerable during the period. It can update without authentication through proxy servers that are not required to do so (BitDefender, 2017).

The cybersecurity features offered by BitDefender's GravityZone Elite EPP solution include its capability to attack surface reduction through application control, firewall, content control and patch management. It offers full disk encryption to protect data. Further features include pre-execution eradication and detection of malware through tunable machine learning, sandbox analysis, and real-time process inspection. To prevent any intrusions and maintain system integrity, it has automated detection features that allow easy investigation and remediation, making use of its even recorder and threat analytics features in Endpoint Security XDR. Threat prevention is seamless, with a smart response to accurate incident detection in order to minimize any exposure to infection and stop potential breaches. Since the entire IT environment is covered for a consistent level of security, attackers do not find any endpoints that are poorly protected in order to use as starting points to launch malicious activity against the organization. Gravity Zone Ultra provides centralized management for both datacenter and endpoints in its integrated architecture, which requires less administration effort, thereby letting companies deploy the endpoint protection solution easily and quickly. The indicators of compromise are clearly visible, and a one-click incident response workflow or threat investigation can be launched. Its interface is user-friendly and does not require high skill levels for cybersecurity teams. The data recorder lets the security team visualize the complete chain of events in an attack covering the entire enterprise (BitDefender.com, 2017).

One of the key benefits of Choosing Bitdefender for EPP solutions is that it expands its role beyond traditional EPP functionalities. It has an Endpoint Security XDR that provides incident response teams

and cybersecurity analysts with all the tools needed to assess suspicious activities and assist in investigating and responding to advanced threats. It provides real-time endpoint visibility and provides an investigative report with a single click to expose suspicious. Cybeattack's lateral movements can be tracked live in order to deliver rapid response, enabling fast containment, resolution, and remediation. Memory protection is also offered to prevent exploits. Furthermore, it's behaviour-based detection and machine-learning features can minimize exposure and prevent unknown threats at the pre-execution and on-execution phases (BitDefender.com, 2017).

Centralized Management, Performance, and Product Limitations

The Control Center provides a centralized and integrated management console that displays all security management components in a single-pane-of-glass view, including datacenter security, endpoint security, and mobile device and exchange security. For larger enterprises, it allows multiple virtual appliances to be configured with several instances of certain roles with the built-in load balancer for high availability and scalability (Stephenson, 2015).

One of the reasons Bitdefender's GravityZone ultra is selected as a vendor is its leading position for having the fewest false positives for Linux and Mac endpoints and the highest malware detection efficiency. It can function alongside Windows Defender Advanced Threat Protection (WDATP) users to further ensure all devices, computers, and endpoints remain protected against a full range of cyber threats (BitDefender, 2017). This provides holistic visibility for security operations and protection across non-Windows and Windows endpoints and guarantees quick and accurate detection so that security can investigate and respond to cyber-attacks across the entire install base.

Some users have stated a few drawbacks to Bitdefender's EPP solution. Some find its web console's design to look a bit dated, and if, for instance, ransomware succeeds, then it doesn't have rollback capabilities. Generally, however, it has remained a top choice because it has succeeded in countering direct attacks where other solutions have not, in both real-world and simulated environments (Brame, 2017). Furthermore, its configurability and reporting capabilities are regarded as highly efficient and are therefore recommended as the EPP solution for Sifers-Grayson.

References

BitDefender. (2017, November 8). *Bitdefender to Deliver Cross-Platform Cyber Security to Enterprises.* Retrieved March 17, 2018, from Cision: https://www.prnewswire.com/news-releases/bitdefender-to-deliver-cross-platform-cyber-security-to-enterprises-656138903.html

BitDefender.com. (2017). *Bitdefender GravityZone Ultra SUite dataSHeet.* Retrieved March 17, 2018,

from BitDefender: https://download.bitdefender.com/resources/media/materials/business/en/Bitdefender_NGZ_UltraSuite_Datasheet_creat2199_A4_en_EN.pdf

Brame, D. (2017, December 26). *BitDefender GravityZone Elite.* Retrieved March 17, 2018, from PC Mag: https://www.pcmag.com/article2/0,2817,2495686,00.asp

Dominguez, J. (2016, March 21). *Endpoint Protection Platform (EPP) vs Endpoint Detection & Response (EDR)*. Retrieved March 17, 2018, from Cisco Blogs: https://blogs.cisco.com/security/endpoint-protection-platform-epp-vs-endpoint-detection-response-edr

Gartner. (2018). *Endpoint Protection Platform (EPP)*. Retrieved March 17, 2018, from Gartner: IT Glossary: https://www.gartner.com/it-glossary/endpoint-protection-platform-epp

Lord, N. (2017, July 27). *What Is Endpoint Protection? Data Protection 101*. Retrieved March 17, 2018, from Digital Guardian: https://digitalguardian.com/blog/what-endpoint-protection-data-protection-101

Matthew D. Sarrel, D. B. (2017, December 26). *he Best Hosted Endpoint Protection and Security Software of 2018*. Retrieved March 17, 2018, from PC Mag: https://www.pcmag.com/article2/0,2817,2492322,00.asp

Stephenson, P. (2015, July 1). *BitDefender Gravity Zone.* Retrieved March 17, 2018, from SC Media: https://www.scmagazine.com/bitdefender-gravity-zone/review/7009/