2020

Protegent Endpoint Security Software

Contents

Protegent Endpoint Security Software Solution

Overview: Unistal

Founded in 1994, Unistal has managed to obtain long-standing experience of delivering the top-notch solutions to IT world. From data recovery to security software's, our solutions ranges from small organizations to larger ones. Our efficiencies linked to the profound comprehension of cyber security market and varied position when it's about coming up with the finest and exceptional products and services so that it can fit it into the purpose. Protegent Endpoint security software solution is ready to be launched and hit the market with its extra advanced features to protect the enterprises from huge security threats interlinked with endpoint devices or networks. Since, the organization has successfully developed the proficient products like Protegent security software, Protegent complete security and Protegent total security solution so now with endpoint security software there is an anticipation of eradicating the massive security threats for enterprises they have to experience.

Executive Summary

The world is growing at rapid rate and so is technology. The advancements nowadays have led to make the human life easier but complex as well due to the massive upsurge in malware attacks and other security threats. Usually, when it comes to securing the endpoint people think of the available standard antiviruses but it is important that they are not efficient enough. Since, malware attacks and security threats have become very common so the probability of becoming prone to such risks are high if there is no updated and comprehensive endpoint protection.

Hence, in this Protegent endpoint security software solution is outlined inculcating the security elements and its requirement for any sort of enterprises.

Introduction: Protegent Endpoint Security Software

Protegent endpoint security software solution is linked to protecting the endpoints or devices of end-users like laptops, and computers. The security software offers an access point network to the enterprises and assists in creating an entry point which is linked to the exploitation of malicious users. This security software benefits the businesses in securing these entry points from unauthorized user and any sort of malicious activity. With this security feature, it would be easy for the businesses to maintain compliance of endpoint with the standards of data security. Also, maintaining greater control over the increasing numbers will be effortless. It is relevant for a user to understand the significance of endpoint protection especially for the organizational cyber security as there are a lot of reasons to this.

Challenges: Endpoint protection

It has been identified that endpoints are infirm links impacting the entire posture of an organization’s security. The noteworthy thing is that it not include the endpoints but also involves the users posing a relevant complexities to ensure protection. These days’ hackers increasingly make use of the campaigns related to phishing for circumventing the perimeter defensive solutions and tricking the users to click on links that are malicious.

As per the research conducted by Verizon in 2018, it has been evaluated that around 92% of the malware attacks are still taking place via emails. It is seen that in an organization employees click on the link believing that the source is trusted. And, it gives an opportunity to hacker for installing malware, spreading it and gaining the access for applications, servers and databases. Basically, perimeter security solutions are not enough to battle against the threats of malware taking benefit of security vulnerabilities.

Challenges that require endpoint protection are:

Operating system exposures

It has been analyzed that susceptibilities occur in an organization due to the operating systems. Fact is that even in the world of advancement, enterprises are running the endpoint on OS like Windows XP and Microsoft doesn't support it now. Upgrading the new operating system requires massive capital and operational outflow and this is why businesses try settling for the antivirus protection that is standard and traditional.

Management of software patch

Another challenge for endpoint protection is software patch management. Enterprises most of the times don't try discovering susceptibilities on time. In case, they are initiating patch creation, deployment and testing, it takes around months and maybe even years. It is very important for an enterprise to know that it is just not practical waiting for patches as the attacks these days are increasing in frequency. And, if there is lacking of comprehensive data governance and nonappearance of compliance necessities that are strict then it is most likely an enterprise may have to experience huge malware issue. Hence, it is relevant to comprehend the significance of endpoint security solution.

Reactive security

For endpoint security, the best protection your computer requires is anti-malware/antivirus. Although, an organization should be aware of the fact that signature-based software's are dependent upon the behaviors and is inefficient in reducing the threats that are unknown or zero-day attacks. Businesses must shift their attention towards reactive security solutions and begin approach that is proactive for protecting the endpoint devices and networks.

In a nutshell, challenges in the sphere of endpoint security are huge and solutions are less. This is one of the main reasons that Protegent endpoint software security solution has been built with the aim of reducing the security threats and delivering the utmost security to endpoints.

Choosing an endpoint security solution

In this era of fastest growing and technological world, any information or data undoubtedly is the asset for any business. And, in case, if the data or information is lost, stolen, or is accessed by unauthorized user then it is something which may lead to putting the complete business at risk. The noteworthy aspect is that the organization doesn't have to only struggle with the rising endpoints number but also with the increase in endpoints types. These aspects lead to making the enterprise security more complex. Hence, in this kind of situation Protegent endpoint security software comes to the rescue. The use of this software helps in restricting the hacker's access to come with the new methods of gaining access, stealing data or information, and manipulating the employees to reveal the information that is sensitive. The Protegent endpoint security software is developed with cloud-based innovation to closely monitor and to ensure threat detection, fortification and stoppage.

Components: Protegent Endpoint security software

The main agenda of developing the Protegent endpoint security software is protecting the small, medium and large enterprises from malware or security threats. Unistal is aiming to obtain the success in this sphere and rise like a star when people are worried about their protection by offering them extravagant solution. So, for better comprehensiveness, let's have a look at some of its essential components:

- Classification of machine learning to distinguish zero day hazard.
- Integration of antivirus protection with advanced antimalware to secure, identify and appropriate malware all over the endpoint devices.

- Ensures secured web browsing through proactive web security.
- Classification of data and prevention of data loss.
- Firewall integration for blocking the attacks linked to hostile networks.
- Restricts phishing and attempts of social reengineering by email gateway.
- Allow the administrators to instantly isolate any sort of infections when found.
- Enhances visibility and operations simplifications with centralized endpoint management platform.
- Software is built with the efficiency of generating audit report that is centralized.
- Accumulating anti-ransom backup centralized is another noteworthy component of this software.

Features: Protegent Endpoint security software

Let’s have a look at the main features of Protegent endpoint security software below:

- **Sandbox threat capture:** One of the best features of this software is that it helps an enterprise or business to identify the threats that are unknown. Since, it is a proprietary cutting-edge technology so sandbox threat capture has the ability to capture not known files and sending them to the endpoint antivirus threat labs so that real time analysis can be initiated to keep you protected and safe.
- **Vulnerability scanner:** It is not an intricate task for malicious registry and cookie traces to exploit any system, damaging it or stealing the personal and sensitive data. So, for this sort of cases, Protegent endpoint security software is developed with the feature of vulnerability scanner which is efficient in cleaning up the system registry from virus, spyware and malware traces includes changes which are unwanted.
- **Speed-lighting speed:** This features of Protegent is known to be new speedo scanner and providing threat updates from endpoint virus is the most lightweight software till now. It involves running the prominent portion of threat analysis in sandbox and without making the system slow.
- **USB Vaccine:** This feature of Protegent endpoint security ensure immunizing the USB drives all over your network to make sure that no malware infection is disrupting your

running business. Endpoint antivirus speedo scanner repairs the infected USB's within minutes and recovers the files that were hidden due to virus attack.

- **Bandwidth Management** - A simple way to track your Internet quota usage and quota limitation.
- **Anti-Ransomware Backup -** Data Protection will centrally backs up your configured data in a lock down mode and protects them from ransom attacks and modifications.
- **Parental Control** - Safe guard your network from access to inappropriate Internet websites content & cyber bullying based on content categories, such as Porn/Adult & time restriction.
- **Behavior Detection** - It uses the combined power of neural networks and a handpicked group of four classification algorithms. Unknown, potentially malicious applications and other possible threats are monitored and stops the offending program or process from carrying out potentially harmful activity.
- **Advance DNS Scan -** Detection types range from very specific hashes to Advanced DNA Detections, which are complex definitions of malicious behavior and malware characteristics. We perform deep analysis of the code and extract "genes" that are responsible for its behavior and construct Advanced DNA Scan
- **Junk cleaner:** This feature identifies and delete the files which are not required. This includes files created by windows and your applications such as log files, temporary files and error reporting files.
- **Data loss prevention:** Protegent endpoint security has also got the feature of device protection i.e. data loss prevention-mass storage towards the data theft and restricting the unauthorized access of devices and users.
- **Registry Repair:** This feature of Protegent endpoint helps in reducing problems with registry file which can impact your computers performance and slows down your system. It also clean up unwanted hidden traces in categories that are file extensions, font locations, help locations, menu order, shared Dll's, shared folders, startup locations, uninstall locations.

- **Updates & Upgrades:** This feature involves running very small hourly updates database without your notice.
- **Light weight antivirus:** This feature runs without slowing down your system & uses very less system resources. That's why we call it Speedo with light foot prints.

Protection against known and unknown threats: Protegent endpoint security

When it comes to offering the protection, then Unistal's developed Protegent endpoint security software ensures identifying the known and unknown threats. These threats may accommodate:

- Phishing
- Advanced Persistent threats
- Cyber attacks
- Zero day attacks
- Malware
- Trojan
- Ransomware

Conclusion

Every year, enterprises are experiencing the huge increase in malware threats in terms of complexity and frequency. It doesn't only lead to influencing the trust of a customer adversely including brand image but also lead to imply some major serious monetary aspects. Hence, in this situation it becomes very important to take a proactive approach of security with entire visibility and control at the right place following the level flow. To protect the enterprise from the attacks or threats like malware, Trojan, Ransomware, phishing, zero day attacks etc. Unistal developed Protegent endpoint security software solution delivering all the required aspects of security to SMEs.

The whitepaper concludes all the necessary details linked to software and efficiently comprehending the aspects so that the use can be adapted by enterprise of any size to mitigate the security threats effortlessly.