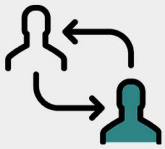
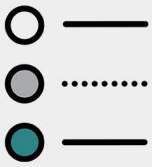
BestSafe

simarks cybersecurity

Application-level security



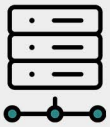
Eliminate administrators, get a highly secure network



White list for corporate applications, gray list for dangerous applications, blacklist for malware

At last, an effective solution against ransomware

Avoid having the same local password on all computers



Deny access of an application to local or remote folders

Centralized management and fully integrated with Active Directory

Visibility and analysis allow you to make sound decisions

Simarks BestSafe eliminates the need to use accounts with elevated permissions thanks to its privilege management and process control never seen before, achieving unparalleled security in all endpoints.

PRINCIPLE OF LEAST PRIVILEGE

Privilege escalation is present in most cyber-attacks and system vulnerabilities. All the security breaches caused by the incorrect allocation of privileges can be avoided by implementing the Principle of Least Privilege.

Although many organizations are aware of the risk involved in granting administrator privileges, the impact on user productivity and management effort on the part of IT personnel prevents them from carrying out projects to reduce the number of privileged accounts since, in many cases, they're necessary to run applications with elevated privileges (software installation, driver installation, changes in system configuration, etc.).

Simarks BestSafe offers an innovative, application-level security solution that allows organizations to completely eliminate administrator accounts, significantly reducing security breaches, without affecting productivity and complying with regulatory guidelines.

BESTSAFE vs PAM

Even today, the concept that accounts with administrator privileges are inevitable prevails. The current PAM (Privileged Access Management) solutions are focused exclusively on controlling the use of this type of accounts, so they require different approval flows and important infrastructure elements (most of them monitor the equipment where they are used) and are, generally, reactive.

BestSafe starts from a completely opposite approach and allows these types of accounts to be eliminated, by focusing the management of privileges on the applications instead of on the users or accounts. BestSafe offers a mainly proactive approach instead of reactive.

HOW DOES BESTSAFE WORK?

BestSafe uses Simarks' exclusive patented technology that allows assigning the necessary security context to each process or application, regardless of the credentials with which it is executed. With BestSafe, privileges are granted to applications instead of users, unlike traditional tools on the market.

Real possibility of having zero administrators

Right after the deployment of BestSafe, the organization can begin to get rid of privileged accounts. If a certain process, application, or administrative task needs special privileges, BestSafe will only grant them to the corresponding process (whitelist) in a completely transparent manner for the end user, who will continue to work with minimum permissions. However, if there's any reason to keep certain accounts as administrator, BestSafe can reduce the privileges (gray list) to applications with Internet access (email clients, browsers, etc.) that are potentially dangerous and could compromise the system, denying them access to their resources (registry, system folders, etc.), but without blocking their execution.

The possibilities of BestSafe do not end there. The ability to control the security context offers a series of functionalities to protect applications that go far beyond the traditional concepts existing until now.

Effective anti-ransomware solution

BestSafe is able to detect in real time when a certain process intends to perform an encryption operation before it is carried out. When detecting an operation of these characteristics, BestSafe stops the process and executes the actions established in the corresponding rule. The actions established in the rules can be generic or based on thresholds decided by the administrator. In addition, BestSafe offers the possibility of storing every key used to encrypt to be able to decrypt later.

The results obtained with this technology have a percentage of effectiveness close to 100%, much higher than the mechanisms of other technologies such as probes, baits, etc.

Administrators will no longer have the same password

In organizations with a high number of computers it is very common and advisable to enable different local administrator accounts to perform administrative or support tasks. Being a large number of machines the password for these accounts is, in many cases, the same for all of them, thus generating a huge security breach usually exploited by insiders.

BestSafe solves this problem in a very simple way and guarantees that the password of these accounts is unique per computer, account, and day, based on a seed that the administrator establishes. If the password is compromised, it will be valid only on that computer and only during that day, and any attempt to change the password will be registered. In addition, you can predict the password that you will have in future days and without the need to connect to the network.

Control access to resources by application

Simarks BestSafe allows blocking all outgoing connections of a certain application regardless of the user's credentials. In addition, BestSafe allows blocking access to protected local folders or generating specific firewall rules for each application to block potentially dangerous applications access to shared documents.

Centralized management at no additional cost

The Enterprise Edition of BestSafe is fully integrated into Microsoft Active Directory and takes advantage of all its features to offer a high level of centralized management, high availability and fault tolerance. In addition, the use of Active Directory means BestSafe does not require additional infrastructure (DB servers, web servers, etc.).

The administration tool is based on MMC (Microsoft Management Console) so the learning curve is extremely fast. The configuration can be applied, either directly to a specific computer or a set of computers through Active Directory elements that can contain them (such as organizational units, groups, containers, etc.), applying all the characteristics of inheritance and hierarchy that Active Directory has to offer.

Once the configuration is established, the computers at the endpoints, through a light agent, will download the corresponding configuration. This configuration is stored in cache and is applied even without connectivity to the network. The update interval is defined by the BestSafe administrator.

BENEFITS FOR THE ORGANIZATION

The fastest return on investment

The implementation of traditional privilege management solutions usually take months to achieve the proper configuration. However, the implementation of BestSafe is so extremely simple and its management environment so familiar, that a full implementation can be done in a few hours thanks to its brilliant integration with Active Directory. But not only that. Simarks' high level of experience allows us to offer a series of templates permanently available and among which you can choose to adapt them to most organizations, making it even easier to deploy.

Security from the first day

Security experts and the leading consultants in the sector agree that the first step to comply with the best security practices is the suppression of as many administrator privileges as possible, along with the supervision of corporate applications, preventing the execution of all the rest. With BestSafe, this goal is extremely easy to achieve since, in addition to security at the application level and to facilitate a phased implementation, BestSafe also offers the possibility of maintaining privilege management at the user level.

Thanks to the minimal impact that the deployment of BestSafe has on the infrastructure of the organization, you can delete administrative permissions at the same time that a white list of applications is created, or you can plan on the fly a strategy of reduction of privileges and apply it stepwise. And all with the flexibility that characterizes Simarks' tools.

100% scalable solution at zero cost

The unparalleled integration with Active Directory together with a client-server approach (instead of the most common server-client) allows BestSafe to be as scalable as the organization itself. If a team has access to the corporate network, it will also have access to the BestSafe configuration.

Simply powerful, transparent for end users

The effectiveness on which BestSafe is based is to make the operating system itself the guarantor of security against intrusions, through the prior reduction of privileges at the application level. BestSafe is not an antivirus that needs to inspect each and every one of the files to determine, as far as possible, the risk associated with each file. It only acts at the process level and when there is a corresponding rule established by the administrator. This means that the impact on computer performance is so insignificant that it is completely unnoticeable in normal use.

In addition to being virtually imperceptible to the end user, BestSafe's features are as powerful and as flexible as the most demanding IT department can demand. What they will appreciate, both users and administrators, is a drastic increase in productivity since their work tools will no longer be an impediment in their daily tasks. There will be no more slowdowns, more unpleasant viruses, or queries related to such incidents, which in turn results in greater productivity in the IT department.

BUSINESS BENEFITS

The vast majority of anti-malware solutions currently on the market, known mainly as antivirus, use signature-based heuristic analysis to identify possible malware. When a certain virus ends up in the hands of a manufacturer, it is analyzed by professional researchers and/or by dynamic analysis systems. If it is classified as malware, it generates a signature that is added to its database and that is later used by the corresponding antivirus software to constantly analyze the files of the system in search of matches. The problem, apart from the great consumption of resources, is that there is a period of time until a malware is identified as malicious in which the end user and its data are completely unprotected and exposed.

Prevention of attacks, known or unknown

The new approach that Simarks proposes with BestSafe is to take advantage of the power of the security mechanisms of the operating system itself so that it is the one who denies access to intrusions. The great advantage of this strategy is that, with a correct reduction of privileges, it does not matter if the malware is known or is about to be known, because none of them will make modifications in the system, since they do not have the necessary privileges to carry out the infection.

With BestSafe, it is very easy to delete administrator privileges in the vast majority of accounts, including IT personnel, and from there assign them only to the applications, tasks, or scripts that are necessary, so that each user can carry out their tasks without affecting productivity. The application of the Principle of Least Privilege (POLP) provides a highly secure environment mitigating deliberate or accidental threats, both from within and from outside the organization, since the first objective of the vast majority of existing malware is the escalation of privileges to be able to make the infection in the system and spread throughout the network.

An efficient work environment

Simarks BestSafe was born from the analysis of a problem common to all IT departments of most organizations. Most of this problem comes down to the decision between compromising safety or gaining productivity in which finding the balance between the two is often too expensive and difficult to implement. With BestSafe, however, the right tools are provided to reinforce both the productivity and safety of the end user, reducing the intervention of technical and/or support personnel.

Get regulatory compliance

Leading regulatory compliance consultancies and agencies, such as Forrester and Gartner, agree that eliminating excessive privileges and white-listing applications is the best strategy for the security of corporate networks. Simarks BestSafe complies with the guidelines defined by these large companies through the management of minimum privileges at the application level and through the elimination of administrators in all endpoints, including the IT department. In addition, reports and trend analysis demonstrate compliance with GDPR and derivatives.

EDITIONS FOR ALL TYPES OF CUSTOMERS

BestSafe is a comprehensive security and privilege management solution available for all Windows platforms, desktop or Windows Server. It is supplied in three editions: the Enterprise edition for companies with Active Directory, the Elite edition for SMEs that do not have Active Directory, and the Home edition for the domestic environment.

BestSafe Enterprise

The Enterprise Edition of BestSafe stands out for its complete integration with Active Directory, providing companies with centralized management without additional infrastructure costs and fully exploiting its full potential such as fault tolerance, high availability and replication mechanisms. In addition, it offers complete integration with any SIEM solution, which facilitates the collection of information for further analysis.

BestSafe Élite

The Elite Edition of BestSafe contains all the productivity and security features offered by the Enterprise Edition but does not use Active Directory to store the configuration. Instead, this configuration can be established stand-alone or obtained remotely through web services and managed centrally.