TECHNOLOGY AUDIT

Entarian ForestSafe version 4.1

Reference Code: OI00197-010

Publication Date: April, 2012

Author: Andrew Kellett

SUMMARY

Catalyst

One of the most challenging areas within IT security concerns the requirement to control privileged account access. It involves managing users, the segregation of duties for authorized users, and the protection of vulnerable servers, databases, workstations, and network devices, all areas where it is common to find inadequate password controls.

The Entarian ForestSafe password-management solution controls access for privileged accounts with non-expiring passwords. ForestSafe provides the ability to monitor, secure, and manage privileged accounts for use across Windows, Unix, Linux, AIX, and Solaris machines. It also operates with network devices that support secure shell (SSH) and telnet protocols such as routers and firewalls and other legacy equipment.

Key findings

- ForestSafe manages and secures the passwords of privileged accounts, especially non-expiring machine passwords that under normal operational circumstances rarely change.
- The secure elements of ForestSafe are maintained using a reverse pattern matching algorithm approach, Microsoft enterprise best security practices, and Kerberos authentication protocols.

- Once user groups, access controls, and device setup is configured, ForestSafe automates the management of hardware and its availability throughout the operational lifecycle.
- ForestSafe operates using an industry-standard, three-tier architecture, which provides further control over the segregation of support roles.
- A SaaS version of ForestSafe that helps achieve faster rollout is now available.
- The solution is supported by common dashboard views and centrally managed reporting facilities.
- The product helps with Sarbanes Oxley (SOX) and Cobit compliance through the management of critical passwords, creating accountability from audited secured sessions, and segregation of roles.

Ovum recommends

- Entarian's ForestSafe privileged account management solution is relevant to medium-sized to large organizations with a significant number of corporate machines where there is a requirement to restrict access to users with the necessary credentials. This type of business-protection requirement is now commonplace across a wide range of industry sectors. The weaknesses associated with fixed passwords on servers and other network devices create a vulnerability that has been tolerated for far too long. The only surprise is that the demand to improve the levels of protection from compliance managers and auditors has remained on the backburner.
- ForestSafe brings a realistic approach to controlling administrator access to corporate devices. It provides audited, password-free, auto-login access that as well as being secure, can where necessary incorporate senior manager approval processes using email-alerting to highlight particular activities, progress, and approvals. Service delivery is built around an organization's existing Active Directory (AD) infrastructure. This simplifies administration overheads and fits the operational comfort zone of most IT departments.

Value proposition

Entarian ForestSafe is an enterprise-level password-management and identity-based access-management solution. The product competes, in what largely remains a specialist area of the security marketplace, with larger vendors such as Manage Engine (the IT management software

division of Zoho) and its Password Manager Pro product set, Cyber-Ark with its Privileged Identity Management Suite, and also e-DMZ.

The core role of ForestSafe is to manage privileged-user access and protect the integrity of non-expiring machine passwords. This involves servers and databases with device passwords that under normal operational conditions rarely change, but at the same time must be kept secure and safe from malicious activity.

ForestSafe enables IT administrators to scan for, identify, and secure vulnerable devices. At the domain level, existing passwords are scrambled so that they cannot be recognized by outsiders, and controls are put in place to restrict access to users, groups, and operational processes that have the necessary credentials.

Simplicity of approach, service delivery, and strong user management are seen as key product differentiators. These elements are driven by product integration with existing AD infrastructures and by remote terminal access facilities that provide controlled access for administrators and privileged users through a secured web interface. Speed of deployment is also seen as a further advantage of the product's AD associations. ForestSafe, with its range of enterprise and platform-focused products, has the capacity to scale its operations across most common enterprise platforms and network devices.

The solution fits the device-protection requirements of medium to large organizations, especially those that operate in highly regulated markets such as financial services, utilities, pharmaceuticals, manufacturing, and government sectors. Although Entarian has only a small customer base, its ForestSafe solution has already proved its worth in the banking and government sectors.

SOLUTION ANALYSIS

Functionality

Entarian ForestSafe controls access to privileged accounts. It manages access to accounts and devices with non-expiring passwords. It controls user access and uses password-scrambling techniques to ensure that unauthorized users cannot see existing passwords or gain access. Its privileged account protection approach integrates with existing AD directories.

There are several methods of deploying ForestSafe, and there is a single version, containing all product features.

- ForestSafe is designed to meet the wide-ranging platform needs of medium-to-large enterprise organizations. It is a combined password-management and remote access identity managed system that operates across all major enterprise platforms and network devices.
- Windows ForestSafe provides password-management and access-control services for system user accounts within the Microsoft framework. It allows all administrator accounts to be managed with a single Windows usage policy.
- Unix ForestSafe provides password-management and access-control services for system user accounts within the Unix framework. The password of each host's root account can be managed within a single usage policy.
- ForestSafe Remote Terminal enables Windows systems to be accessed through a web-based remote terminal. Unix systems are accessible using a Java-based SSH terminal. The preferred option for Entarian is the AppGate MindTerm SSH Terminal.

ForestSafe offers secure, auditable, password-free access to protected systems. There are also optional approval and progress-checking facilities available. These allow senior staff to be alerted when particular activities occur or when higher levels of authentication are needed.

Device security is maintained using reverse pattern matching algorithms for matching domain computers by organizational unit (OU), AD group, IP address ranges, or SSH Keys. The ability to manage and control devices using SSH keys is important because SSH is one of the most widely used security protocols. Over a period of years, millions of SSH keys have been created by organizations and the external management of these keys represents a significant IT overhead.

Passwords are generated for each device using the ForestSafe algorithm and unique machine information. Passwords are scrambled and recovered within the control of the system and can be

regenerated on a regular timeframe that is controlled by the organization and its risk requirements. Checks are also maintained to ensure that passwords remain secure and have not been tampered with.

Once passwords have been randomized, only users and user groups with the correct privileges will be able to sign into those accounts. Further controls extend to enforcing who can connect to what systems, when access will be allowed, and, for temporary workers, how long the window of opportunity will remain open.

Controls include the ability to:

- Maintain users and accounts within groups that are used to assign rights. Usage rights are based on group membership and attributes within existing corporate directories such as AD.
- Machines and devices are collected into sets based on their address, type, and other attributes.
- Users and accounts are linked to machines and devices based on their name and group memberships.

The system's central-dashboard approach addresses monitoring, user administration, and reporting requirements. It provides the visibility required to show all users, user groups, and machines under ForestSafe control. Its shows machine status, and, where necessary, highlights vulnerabilities. Reporting using graphs and charts is delivered at different administrator and management levels and can also be provided for use via an organization's existing reporting tools.

Once the solution, its privileged user groups, and the devices under control are configured within ForestSafe, hardware management is automated across the complete device lifecycle. In operational use ForestSafe uses an industry-standard three-tier architecture consisting of application service, web application, and Microsoft SQL database. Security is based on Microsoft Enterprise best security practices. Sign-on is achieved using AD tokens passing from the user's browser session, through Kerberos service principal names (SPN), to the database and ForestSafe service. Communication between the web application and ForestSafe service uses secure .NET Remoting custom transmission control protocol (TCP) channels.

The three-tier approach supports segregation of roles within organizations. Installation, support, and security is mainly based on Microsoft technology with the ForestSafe uncoupled, multi-threaded object-oriented (OO) engine at the heart. There are no hidden or customized components, no passwords stored on the database, and no requirements for special hardware.

Go-to-market strategy

The Entarian ForestSafe Enterprise solution is mainly targeted at medium-to-large enterprise organizations, especially those that operate in the more highly regulated business sectors. There are also versions of the product available that enable less specialized customers rapid deployment, such as single-tier installations, pre-configured virtual images, and SaaS.

Entarian offers remote and on-site installations, and works with the customer to identify existing vulnerabilities and fulfill their service delivery objectives. The company's pilot-based introductory approach enables it to offer a detailed audit of an organization’s high-risk and unmanaged accounts. The results of the audit can help organizations to identify user and device-management issues and vulnerabilities that need to be prioritized. The company's key implementation, technology, and distribution partners include ORB Data in the UK, and IBC Online in Hong Kong for the Asia-Pacific region.

Future technology developments for the ForestSafe product set include the horizontal requirement for additional language support, which is positioned by the company as being straightforward to achieve using existing language maps. Other vertically focused requirements include the need for additional platform support as specified by existing customers. The company's product release strategy tracks the Microsoft .NET release framework for major version numbers, incremental minor releases, and when adding new features and fixes.

Deployment

Deployment timescales are typically short. Using an initial pilot-based approach takes on average five working days to deliver an on-site Windows and Unix solution. Once the pilot is complete, a further day is required to role out a departmental or enterprise deployment. The ForestSafe SaaS option will significantly improve on on-site installation times because it requires no hardware or software installation.

Product licensing is based on either a year-one payment and then annual 20% support and maintenance charges, or a rental option of 30% of the list price payable annually. Prices are calculated based on the number of managed computers.

Entarian offers a range of professional services to support its products, including remote and on-site installations involving the client and its staff. Technical support is provided by Entarian. A 24-hour first-response system is available charged at 20% of the original contract price.

The company also provides training services, usually in the form of an on-site one -day training course for administrators and a half-day course for end users. ForestSafe is a Microsoft-based

offering that operates on the Microsoft SQL server platform and has optional requirements to work with the Oracle .NET module on the ForestSafe application server.

Customer deployment examples

- One of the world's largest banks uses ForestSafe to match domain computer candidates based on their AD organization unit. The product is deployed to protect and manage built-in administrator passwords and accounts, and to remove unauthorized visibility from 67,000 domain Windows workstations and servers. In addition, the ForestSafe “grant access” facility is used to create and remove privileged local Windows accounts across multiple computers at branch locations. This facility allows remote working engineers with short timeframe availability to log on locally with no network overheads, and control is maintained centrally because the organization is able to configure requirements in advance. Help-desk support is provided to deal with day-to-day requests using a simple text box and web page approach.
- A pharmaceutical organization uses ForestSafe to match domain computer candidates based on their AD group membership. Complete audit-level visibility of all system changes and requests is part of the requirement. The supported estate consists of Windows domain and Windows workgroup computers. The solution manages the root accounts of AIX servers, and also offers password-free access for support staff through built-in Unix Terminals via X Windows forwarding, with recorded machine fingerprint facilities used to prevent man-in-the-middle attacks. IIS pool ID domain account passwords along with Windows Service passwords are synchronized and managed. An approval layer gives management the option of accepting or rejecting both remote and password retrieval requests, and the email system is configured to forward requests and responses to staff without them having to access the system.

DATA SHEET

Key facts about the solution

Table 1: Data sheet

Product name	ForestSafe	Product classification	Credential management, enterprise password management, binary large object management, SSH key management
Version number	4	Release date	September 2011
Industries covered	All	Geographies covered	Europe and Asia-Pacific
Relevant company sizes	Mainly medium-to-large enterprise	Platforms supported	Microsoft Windows, Linux, Solaris, AIX, HP/UX, z/OS, Mac OS, Lotus Notes, DB2, IBM TADDM, SAP, Oracle, MS SQL
Languages supported	English, Chinese in development	Licensing options	License or rental options: License: First year payment then annual 20% support and maintenance Rental: 30% of list price annually
Deployment options	On premise, on premise managed and SaaS	Route(s) to market	Direct and channel
URL	www.eesm.com	Company headquarters	30 City Road London EC1Y 2AB tel: 0203 514 0910
Asia-Pacific headquarters	Suite 811 Tsimshatsui Center East Wing 66 Mody Road Tsimshatsui East Kowloon Hong Kong		

Source: Ovum

APPENDIX

Further reading

- Cyber-Ark, Privileged Identity Management Suite, Technology Audit (OI00070-005)
- 2012 Trends to watch: security (OI00127-046)

Methodology

Ovum Technology Audits are independent product reviews carried out using Ovum's evaluation model for the relevant technology area, supported by conversations with vendors, users, and service providers of the solution concerned, and in-depth secondary research.

Author

Andrew Kellett, Senior Analyst, Infrastructure Solutions, Security

Andrew.kellett@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Disclaimer

The facts of this report are believed to be correct at the time of publication but cannot be guaranteed. Please note that the findings, conclusions, and recommendations that Ovum delivers will be based on information gathered in good faith from both primary and secondary sources, whose accuracy we are not always in a position to guarantee. As such Ovum can accept no liability whatever for actions taken based on any information that may subsequently prove to be incorrect.