

Product Section

Best of 2008

A fond look back



This was a year of challenges for SC Labs. Convergence in some areas was happening faster than we could set up product groups, and the road ahead often was foggy. For all of that, external pressures changed the market materially. There is nothing like an economic meltdown to give one pause.

Our annual year-end issue takes a look back at the products we saw this year – and all had a couple of things in common. They were a monument to staying the course, and they were solid offerings. This was

not a year to take risks.

Here you will find those products that received Best Buy, Recommended or SC Magazine Lab Approved designations over the past 11 months. Picking winners was very difficult – the scores were close and the differences between a Best Buy and a Recommended were down to the judicious picking of nits.

In addition to some bruised corporate egos from these perceived slights, we also got some great ideas, and that was another new experience for us. We found senior marketing and technical management stepping into self-defined roles as our partners with great suggestions for things, such as tuning our scoring methods. We will be looking at those suggestions over the coming months.

Overall, we found that the products we saw in 2008 tell us a lot about what we will be seeing in 2009. We expect to see a resurgence of creativity as our economy improves. The problems that need solving are becoming increasingly complicated and, as always, vendors are stepping up to the plate.

Another thing we learned is that more points of view make a better review section, so we are expanding our team in the coming months. More on that as we progress.

We anticipate an exciting 2009 after a lackluster 2008. That's OK, every market needs to have points where it can stop and look at what comes next. While new challenges from the bad guys and an economy in chaos have certainly posed challenges, our vendors have stood strong, and it is clear that regrouping will have a positive effect as we move toward the next decade.

For you, our readers, our mission is providing the absolutely, most reliable analysis of the products you are looking to buy. We take seriously our role in your selection process, so we listen when vendors want to help us represent their products.

Happy holidays and best wishes for a prosperous new year from the team at SC Labs. And, my wish for you is the same one I have been wishing for 30-plus years: May your net work. – Peter Stephenson, technology editor

SECTION CONTENTS

Anti-malware management . . .	4	Multifactor authentication . . .	2
Application vulnerability	5	Network forensics	6
Biometrics	10	NAC	8
DRM	11	Password management	12
Email content management . . .	7	Policy management	9
Email security	7	Portable devices	3
Encryption	11	Unified threat management . .	4
Endpoint security	10	Vulnerability assessment . . .	9
Extrusion prevention	12	VPN	8
Identity management	2	Web content management . . .	5
Media forensics	6	Wireless security mgmt.	3



Security Gateway 320 v7.1



V-Station



ProtectDrive

How we test and score the products

Our testing team includes SC Magazine Labs staff, as well as external experts who are respected industry-wide. In our Group Tests, we look at several products around a common theme.

The general test process is a set of criteria built around the six review areas (Performance, Ease of Use, Features, Documentation, Support, and Value for Money). There are roughly 50 individual criteria in the test process. These criteria were developed by the SC Lab in cooperation with the Center for Regional and National Security at Eastern Michigan University and have been in use and refined over the past four years.

What the stars mean
Our star ratings indicate how well the product has performed against our test criteria. These are marked as follows:

- ★ Seriously deficient. An "F" on the product's report card.
- ★★ Fails to complete certain basic functions. A "D" on the product's report card.
- ★★★ Carries out all basic functions to a satisfactory level. A "C" on the product's report card.
- ★★★★ Carries out all basic functions very well. A "B" on the product's report card.
- ★★★★★ Outstanding. An "A" on the product's report card.



What the awards mean

Best Buy goes to products that the SC Lab rates as outstanding. **Recommended** means the product has shone in a specific area. **Lab Approved** is awarded to extraordinary standouts that fit into the SC Lab environment, and which will be used subsequently in our test bench for the coming year.

Multifactor authentication

Multifactor authentication today usually means two factors: something you know and something you possess. There are a few examples of true (i.e., more than two simultaneous) multifactor authentication, but these mostly are for deployment in very high security environments

and almost always include some form of biometrics. However, the “something you possess” may or may not be a token.

Start by looking for true multifactor authentication. Are the factors strongly connected through the user, for example?

Next, look for ease of deploy

ment, especially self-enrollment, and administration. Self-enrollment needs to be robust and secure.

The final consideration is cost. One thing we saw clearly in these products is that there is a wide range of cost for a wide range of products.



Defender v5.2

Product	Vendor	Our verdict	URL	Rating
Defender v5.2	PassGo	A feature-rich product, easy-to-use and an excellent value for organizations of most sizes.	www.passgo.com	
Armored Credential System (TACS)	TriCipher	A very good product with solid capability, flexibility and ease of use.	www.tricipher.com	

ID management

Figuring out what identity management really means in the context of product selection can be an administrator’s nightmare. That, it turns out, is only part of the story. We looked at products that presented themselves as identity management products and we found that many of them, good as

they were in their own context, did not fit our concept of what identity management is.

The bottom line is that the immature level of the genre has spawned many products that address a piece of what may be loosely interpreted as identity management. For a solid definition of

identity management, then, we turned to federal standards.

The real benefit in these systems is that they even out the process of assigning, managing and auditing access. They are, in effect, full user management systems. Most important, perhaps, is that they are extensible.



Enterprise Provisioning Suite

Product	Vendor	Our verdict	URL	Rating
Identity Manager 3.5	Novell	For functionality, ease of use and support, our choice for large and growing mid-sized organizations.	www.novell.com	
Enterprise Provisioning Suite	Courion	An excellent overall product with ease of use and excellent pricing.	www.courion.com	

Portable devices

This is not simple endpoint security, although some of the products we looked at also do that. In fact, we had to separate the functionality on which we evaluated these products between portable devices and other endpoint products.

This is not simple endpoint

security, although some of the products we looked at also do that. In fact, we had to separate the functionality on which we evaluated these products between portable devices and other endpoint products.

This differs from some other endpoint devices that focus on

data at rest. In short, we consider a PDA or smartphone to be a unique beast. Many of these products have portable versions of common operating systems (e.g., Microsoft Windows) and all can run applications that are equal or similar to typical MS Office applications.



DeviceWall v4.6

Product	Vendor	Our verdict	URL	Rating
DeviceWall v4.6	Centennial Software	Stops transfer of data based on security policy, and encrypts data that needs to be transmitted.	www.centennial-software.com	SC BEST BUY
SafeGuard PDA v4.25	Utimaco	Advanced security algorithms and biometrics keep confidential info secure at rest and in motion.	www.utimaco.com	SC RECOMMENDED

Wireless security

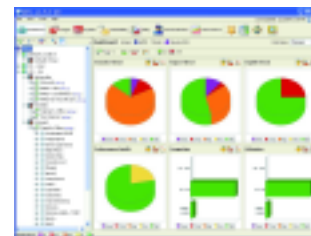
Wireless vendors are promoting wireless connectivity very heavily as a replacement – not an alternative – to wired networks. Cisco has made huge investments in development and acquisition as an example of this market growth. The new 802.11n standard, though hotly

debated, is likely to play a major part in driving the WLAN market as well.

Virtually all of the products we tested support 802.11n. What is interesting about these is that three of the five products are new to our labs. The products all are part of larger integrated systems. In one

case, endpoint security can be added. This points to a convergence of functionality that includes both wired and wireless security.

As your enterprise approaches the 80 percent wireless predicted by some mavens, what you spend on protection is trivial compared to the potential risk.



AirDefense

Product	Vendor	Our verdict	URL	Rating
Enterprise	AirDefense	Provides protection against wireless threats and offers policy compliance monitoring.	www.airdefense.net	SC BEST BUY
Enterprise	AirMagnet	Delivers active full-time protection against the entire spectrum of wireless threats with ease of use.	www.airmagnet.com	SC RECOMMENDED

UTM

The UTM is maturing. What we find most interesting is that the fundamental concepts behind UTMs have not changed much since they began to be popular as an economical way to protect the perimeter. What has changed are two important things: their functionality is increasingly

tightly coupled and the number of functions is growing significantly.

Starting with the second, we saw a lot more functionality than in the past. We define a basic UTM as a device that has an IDS/IDP, anti-virus gateway and firewall. Not all of the products that claimed to be UTMs had this basic functionality.

Beyond the basics, we saw specialized anti-malware, including anti-phishing and spam protection. We see this as a two-edged sword. The more that you expect the device to do, the more performance is required. Overall, our impression was that the UTM really is coming into its own.



Security Gateway 320 v7.1

Product	Vendor	Our verdict	URL	Rating
InstaGate 604	eSoft	Comes as a firewall and VPN; can be customized with web, email or mail server ThreatPaks.	www.esoft.com	SC BEST BUY
Security Gateway 320 v7.1	The Astaro	Can be loaded up with so many feature sets that it could become the only security appliance needed.	www.astaro.com	SC RECOMMENDED

Anti-malware

We saw nowhere near the number of products this year that we saw last year. That does not mean that the anti-malware gateway product vendors are turning out lackluster products. Far from it, these products we saw were slick, well conceived and easy to set up and manage. The big

strength of these gateways is their ability to manage endpoint anti-malware products, as well as provide a solid gateway. This all led me to consider why the convergence trend has slowed.

First, the trend toward a single gateway device impacts the concept of defense-in-depth badly.

Leaving the UTM as the only device at the perimeter forces one to extend protection to the desktop to achieve defense-in-depth. Managing malware at the perimeter is a difficult problem and, frankly, I question whether it can be built into a UTM effectively. Time will tell whether I'm right.



Email Security Gateway v7.1

Product	Vendor	Our verdict	URL	Rating
InterScan Web Security Appliance v3.1	Trend Micro	A real-time, security-rich product for protecting organizations from web threats.	us.trendmicro.com	SC BEST BUY
Email Security Gateway v7.1	BorderWare	Incorporates two interwoven features to work together seamlessly to provide solid protection.	www.borderware.com	SC RECOMMENDED

Application vulnerability assessment

Application security has continued as one of the primary issues on the minds of information security professionals everywhere. Due in part to the increased exposure to stories in the media, application security has come under scrutiny for being a favorite target for malicious users. As

reliance on information assets continues to grow exponentially, the protection mechanisms at the application layer have created a void between the bad guys and the stakeholders who are tasked with protecting the infrastructure.

As focus has shifted away from network perimeter attacks, client-

side attacks and specialized application layer vulnerabilities now have some personnel scrambling. Regulatory compliance mandates, such as PCI-DSS, and even greater industry awareness have created an elevated level of interest in taking the proper steps to secure external facing applications.



Hailstorm Enterprise ARC 5.5

Product	Vendor	Our verdict	URL	Rating
Hailstorm Enterprise ARC 5.5	Cenzic	Impressive configuration and control over scanning environment. receives a Best Buy designation.	www.cenzic.com	SC BEST BUY
DbProtect 2007	Application Security	Flexible configuration options, impressive enterprise-class integration with other components.	www.appsecinc.com	SC RECOMMENDED

Web content management

For almost three years, we have been watching the web content management landscape. We have seen a steady evolution from a group of products that were largely URL filters.

The first time we tested these products all we had to do was develop a suite of black lists for

various websites and types of content and tell the device being tested to try to go to those sites. We then read the success rates. That was then and this is now.

Today, web content managers go way beyond filtering on bad sites and dirty word lists. Today they include P2P, IM, social networking

sites, and they even look at malware. Once you decide on a product – after a thorough requirements analysis, of course – plan your deployment carefully. That means plan your policies, address everything you need to, but don't set up a needlessly complicated set of policies.



Web Filter

Product	Vendor	Our verdict	URL	Rating
Professional Edition	8e6	Powerful analysis capabilities along with surprising ease of use.	www.8e6.com	SC BEST BUY
Web Filter	Barracuda	High value and affordability in most environments.	www.barracuda.com	SC RECOMMENDED

Network forensics

There are two classes of tools that seem to be lumped into the network forensics category. The first is tools that do much of what traditional computer forensics tools do – only they do it over a network. The second category is tools that analyze traffic over the network. We saw both.

The tools that analyze computers over the network usually are able to look at some things that typical computer forensics tools cannot see. It also is easy to watch file openings and closings. These additional abilities provide the analyst with more forensic data. The network forensic tools that

watch the traffic on the network are of more than one type as well.

These products take input from a variety of log sources. They may or may not have explicit forensic functionality, but they all provide the necessary features that enable forensic analysis over the network whether implicitly or explicitly.



LogRhythm

Product	Vendor	Our verdict	URL	Rating
NetDetector	Niksun	This appliance goes way beyond simple network-based forensics.	www.securewave.com	SC BEST BUY
LogRhythm	LogRhythm	A powerful network forensic tool that serves double duty as a very capable SEIM.	www.logrhythm.com	SC RECOMMENDED

Media forensics

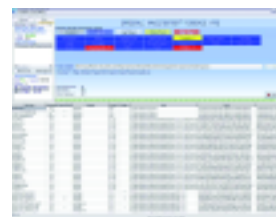
Forensics has become a much maligned discipline in the information security realm. As tools get more advanced, the need for understanding appears to become less, but, there is no substitute for knowledge and experience.

A shortage of qualified investigators has arisen as college campus-

es, local police departments and even private citizens in civil lawsuits all need to have forensic analysis performed. This has led to a growth in tools that are easier to use than the tools of the past.

Another twist in the world of forensics is the multitude of changes in where data resides. You

may benefit financially from putting all of your forensic eggs in one basket and buying a generic tool with lots of capabilities. That may or may not be a good idea depending on the product. We recommend purchasing specialized tools, even if the general purpose ones cover most of your bases.



Gargoyle Investigator

Product	Vendor	Our verdict	URL	Rating
Forensic Toolkit 2.0	Access Data	A great product. It is well put together and worth several times the price.	www.accessdata.com	SC BEST BUY
Gargoyle Investigator	WetStone Technologies	A unique product that can be used to search for some of the most difficult to find malware.	www.wetstonetech.com	SC RECOMMENDED

Email security

Securing enterprise email has been a growing concern for many organizations. There are several important reasons to investigate technologies that help an organization control the use of email within the corporate environment. Confidentiality of email messages is one of the most important

issues facing enterprises that deal with personally identifiable information. Ensuring that sensitive information is properly protected and preventing data leakage are not only abest practice concerns, but also compliance issues across many regulations. A second growing concern is message integrity.

Client-side email attacks, phishing, spam and other integrity issues have information security managers taking notice in record numbers. Sophisticated methods for infiltrating organizations have steadily turned to email-based attacks using a combination of techniques.



Entelligence Messaging Server 9.1

Product	Vendor	Our verdict	URL	Rating
Universal Gateway Email 2.8	PGP	A true enterprise-class product at the forefront of email security.	www.pgp.com	SC BEST BUY
Entelligence Messaging Server 9.1	Entrust	A fantastic value given the price point and feature set. A truly competitive player in the space.	www.entrust.com	SC RECOMMENDED

Email content management

This category covers protection of the enterprise from things that can ride an email message into your enterprise. Arguably, there are only two ways into a secure enterprise from the outside: email and web services. We control web services through secure programming and good architec-

tures. We control email by forcing it through gateways that look for things that could harm us. That was an easy task in the days when the threats were limited. Today there are, essentially, no limitations on the threats that could enter the enterprise in an email message.

We saw one overriding charac-

teristic as we looked at a large number of products: more, sometimes, really is more. These products, in general, expected everything but the kitchen sink to be thrown at them and they usually have the means necessary to protect against just about any type of email-carried threat.



MailGate

Product	Vendor	Our verdict	URL	Rating
ThreatWall	eSoft	A full scale email content management appliance with several excellent features at a good price.	www.esoft.com	SC BEST BUY
MailGate	Tumbleweed	Offers solid email protection and easy management in one device, and it's quick out of the gate.	www.tumbleweed.com	SC RECOMMENDED

VPN

As this market grows to find its identity in the network access management environment, we see developers adding lots of functionality, as well as converging with other product types.

While NAC is struggling with its own identity crisis, SSL VPNs simply are seeking their best deploy-

ment options. VPNs and firewalls as combined gateways into the network are nothing new. IPsec, though, usually is the preferred venue for this type of implementation. However, there is a lot of discussion that IPsec is less desirable than SSL. That's really not entirely the case. SSL VPNs have a special

strength: low cost (or no cost) client-side implementations that use a standard protocol to communicate with web portals. In this case, the capability on the server side almost always is there by default, usually on port 443. IPsec client-side agents generally require more space, resources and effort.



SSL-VPN 2000

Product	Vendor	Our verdict	URL	Rating
SSL Explorer Enterprise Edition	3SP	Ease of use, low price and simple migration path from the free open source version.	www.3sp.com	SC BEST BUY
SSL-VPN 2000	SonicWALL	Solid performance, ease of use and good feature set.	www.sonicwall.com	SC RECOMMENDED

NAC

We looked at network access control (NAC) devices, a group of security management utilities that enforce which system should be allowed on the production network. NAC is most commonly used as software to determine if a machine is in compliance with the NAC policy.

Most, if not all, vendors also support an agentless client, which uses Java and a web browser to check for policy compliance. The typical configuration uses virtual local area networks to segregate the physical LAN into multiple parts. Usually, one VLAN is configured as part of the production

network. The other VLAN is a quarantine/purgatory network segment, which only has internet access at best.

Most NAC offerings include an agent, which can be used on several operating systems. Some even included installation clients for Mac systems.



NAC Advanced

Product	Vendor	Our verdict	URL	Rating
Enterprise Server	BigFix	A true top-shelf product with easier administration than most; includes a massive number of features.	www.bigfix.com	SC BEST BUY
NAC Advanced	Sophos	A great balance between ease of use and security and free lifetime support.	www.sophos.com	SC RECOMMENDED

Policy management

Configuration weaknesses and missing patches for servers, workstations and network devices continue to make their way into the information security headlines on a daily basis. Like many other well-publicized events that tend to whip people into action, IT and security stakeholders are unin-

dated with reactive mandates to patch quicker without breaking applications, deploy faster with less resources, and to provide more protection without impacting productivity. As companies experience growth, acquisition or even expansion to different lines of business, the configuration of workstation,

server, network and security devices becomes more difficult to manage. Changes in the regulatory landscape and threats to information assets have put a burden on managers and administrators.

Customers may want to steer clear of solutions that have changed hands several times.



Enterprise Suite 7

Product	Vendor	Our verdict	URL	Rating
Secure Configuration Manager 5.7	NetIQ	A good risk-based approach for managing known weaknesses in configurations and patches.	www.netiq.com	SC BEST BUY
Enterprise Suite 7	BigFix	Represents a great value given the number of platforms that it supports.	www.bigfix.com	SC RECOMMENDED

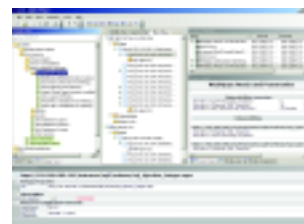
Vulnerability assessment

The environments in which we all work have become more complicated as the years have passed, and one of the outcomes is that they are far more difficult to test for vulnerabilities. The process of security testing has both improved and become more difficult. Today, we actively invite

strangers into our networks. Well, not exactly all the way in, but far enough to cause concern if the perimeter is not very secure. Never before has the notion of layered security been more important.

These tools enable testing of the infrastructure. By that I mean the network and the platforms on it.

This introduces the concept of reachability. If applications are exposed to the outside, simple vulnerabilities become potential disasters. That means that the platforms they sit on and the routes to those platforms must be protected. Sometimes that's easier to talk about than it is to do.



Core Impact

Product	Vendor	Our verdict	URL	Rating
Core Impact	Core Security Technologies	The ultimate tool for finding and exploiting possible holes in a network.	www.coresecurity.com	SC LAB APPROVED
Digital Security Retina Security Management Appliance	eEye	Solid performance, good value and a venerable pedigree.	www.eeye.com	SC BEST BUY
NeXpose	Rapid7	A feature-packed vulnerability assessment and risk analysis tool that goes above and beyond.	www.rapid7.com	SC RECOMMENDED

Endpoint security

In this group review, there were three major categories of endpoint device protection: the network protection type, which would include firewall, anti-virus, encryption and VPN technologies or some combination thereof; the device protection would protect sensitive data from being transferred to

external devices, such as drives and iPods; and the data leakage type would protect the endpoint by verifying which apps running on the endpoint are legitimate.

These solutions help to eliminate the legal liability, customer service costs and other ramifications of data breach disclosures through

the use of extensive monitoring and reporting of data, not just at rest, but in transit as well.

Endpoint security solutions should help the enterprises meet regulatory compliance requirements for data security and provides assurance that data leakage did not actually occur.



Endpoint Security and Control

Product	Vendor	Our verdict	URL	Rating
BigFix	BigFix	Protects endpoint devices from all types of security threats.	www.bigfix.com	SC BEST BUY
Endpoint Security and Control	Sophos	An elegant solution, which does not place undue burden on the administrator.	www.sophos.com	SC RECOMMENDED

Biometrics

We saw a lot less breadth this year in biometric authentication. For example, last year we had a facial recognition product. Lack of such a product this year should not be construed as counting it out of the biometrics landscape. Rather, it has been sufficiently successful that this

group review came as the new product was upgrading and was not available for review.

There is an interesting trend toward lower cost. In fact, some biometric PC access control systems are at or below the price of tokens. Last year when we looked at these products, fingerprint scan-

ners were criticized by their competition for false positives and negatives and higher cost given what they are intended to do. This year I can't agree. Most of our products this year are fingerprint scanners, and they show specifications that are quite acceptable for false positives and negatives.



V-Station

Product	Vendor	Our verdict	URL	Rating
DigitalPersona Pro	DigitalPersona	A solid performer with solid performance, self-enrollment and a range of AD schema extensions.	www.digitalpersona.com	SC BEST BUY
V-Station	Bioscrypt	A multifactor authentication tool for physical access control.	www.bioscrypt.com	SC RECOMMENDED

Encryption

Several states have enacted laws that require businesses that have reported a data breach to encrypt customer data. As these requirements take the spotlight and consumers realize the dangers, businesses are pressed to take action. For all the extra level of security that encryption affords

an organization, the mismanagement of technology can also add to the risk. Organizations are looking for simple solutions that can not only integrate with existing directories or technologies, but also do the job of encrypting endpoints without impeding performance or user productivity.

Transparency to the user is a must today, and vendors are responding. As the market matures, we are starting to see several feature sets that allow for an organization to implement a solution without having to invest significant resources in deployment and management.



ProtectDrive

Product	Vendor	Our verdict	URL	Rating
Whole Disk Encryption	PGP	A client software app that provides whole disk encryption as part of a suite.	www.pgp.com	
ProtectDrive	SafeNet	Software-based encryption that uses a client-server based architecture for full disk encryption.	www.safenet-inc.com	

DRM

Some people think of digital rights management (DRM) as copy protection. More accurately, DRM applies fundamental principles of access control to intellectual property. DRM enforces access to and use of documents, art, music and video, etc., rather than simply preventing the copying of it.

That makes DRM a bit more complicated than copy protection or watermarking. Detractors of DRM tend to oversimplify the problem in order to overemphasize the solution. This tends to make DRM appear as a solution looking for a problem. DRM is not just copy protection. Properly implemented,

it does not interfere with legitimate use of the intellectual property.

For the purposes of our Group Test review, we were not interested in how these tools could be over- or excessively used. So, we have evaluated these products in the context of what they purport to do and how well they do it.



Documentum Information Rights Management (IRM)

Product	Vendor	Our verdict	URL	Rating
Avoco Secure	secure2trust	A solid product priced right.	www.avocosecure.com	
Documentum Information Rights Management (IRM)	EMC	A fully integrated product with very good value for the cost.	www.emc.com	

Extrusion prevention

Data is typically in one of three forms: at rest, in motion or in use. For a good extrusion prevention package to be effective, it must protect data in all three forms. In addition to the state of the data, the data needs to be protected from the three most common sources of data leakage.

Number one is the internet – either through the corporate email system, web-based email solutions, or through an IM program or other solutions, such as gotomypc.com.

The internet is the most likely place for a leak to occur, but it is not the only place. The second type of breach is through the con-

nection of removable media to a device connected to the corporate LAN through a laptop or workstation. USB drives are cheap, plentiful and have massive amounts of storage capacity. Without extrusion prevention protection, a disgruntled employee can download gigabits of sensitive files.



Leak Proof

Product	Vendor	Our verdict	URL	Rating
Leak Proof	Trend Micro	An all-in-one app which comes with everything pre-loaded. It's very solid product at a great price.	us.trendmicro.com	SC BEST BUY
Enterprise DLP	Nextlabs	A unique offering that provides an elegant solution to data-hiding techniques.	www.nextlabs.com	SC RECOMMEND

Password management

Password management is a term that has come to mean a lot of things. This is a case where marketing has gotten in the way of clear, unambiguous definitions. We may think of password management as a sub-context of ID management, access management and policy management. In this set

of reviews, we are looking at ways to manage access to passwords themselves. This is another somewhat ambiguous way of looking at the problem. For example, is single sign-on (SSO) password management? Some would argue that it is. In fact, at least one of the products we looked at acted a bit like a SSO

tool. Caching a collection of passwords for different apps and platforms and accessing the cache with a single password certainly smells like single sign-on. But, without some of the enterprise management capabilities of full-on SSO systems, this probably is a bit simplistic to think of as a solid SSO system.



Enterprise Password Vault

Product	Vendor	Our verdict	URL	Rating
Enterprise Password Vault	Cyber-Ark	A high-end and complete password management appliance at a very reasonable price.	www.cyber-ark.com	SC BEST BUY
ManageEngine Password Manager Pro	AdventNet	Ease of deployment, a small software footprint and superior pricing.	www.passwordmanagerpro.com	SC RECOMMEND