

maXecurity

The Next Generation of Web Access Management

How maXecurity™ Saves Millions of Dollars Each Year

A large financial institution used a competitive product for Web Access Management. By working with P2 Security, the company was able to determine its true Total Cost of Ownership (TCO). An analysis following the installation of maXecurity revealed annual cost savings of millions of dollars per year. In addition, by switching to maXecurity, the Return on Investment (ROI) was measured in months.

*This organization used WAM to protect 500,000 users. While this example does not exemplify every organization's potential cost savings, it **does** represent the savings that any large organization could gain by switching to maXecurity. Please contact us for a cost-savings analysis for your organization.*

Note: the institution did not allow us to release its name for publication, so it will be referred to as "Bank A."

Initial Purchase Price

Software Costs

"Bank A" purchased a software-based WAM solution. It paid a per-user licensing fee of \$1.50. Therefore, the total initial cost was \$750,000 covering 500K users. The competitive product was software-based -- it included both Web agents (software plug-ins that run on the Web servers) and policy servers (the program that communicates with the Web agents regarding policy information).

Hardware Costs

Since the competitive product is software-based, hardware is also needed in order to run the policy server software. The vendor-recommended server platform was Sun V490. Based on internal performance testing, Bank A concluded that they needed 65 V490s. Their discounted price from the manufacturer was \$60,000 each, for a total cost of \$3,900,000.

Initial Purchase Price Savings

The maXecurity Enterprise appliances (the top of the line), are able to handle 10,000 simultaneous connections each. maXecurity appliances are priced based on performance, not number of seats. Only six appliances were needed to net Bank A equivalent performance as previously. Since they load-balanced all of the appliances together, it was decided that eight appliances would be ideal, so that there would always be some redundancy in case of failure; plus it gave them the flexibility to handle any extra demand that may be incurred during normal and peak use, and expected growth.

Eight maXecurity Enterprise appliances have a retail price of \$250,000 each. Since the appliances include both the hardware and policy server-equivalent software, and eliminated the need for Web agents, the total initial cost for Bank A's maXecurity-based solution was



Definitions

Web Access Management

Web Access Management (WAM) is a Web security technology that protects an enterprise's sensitive Web resources, applications and data from unauthorized use. Web Access Management systems perform this security function by validating a user's credentials (authentication), determining whether the validated user is entitled to requested resources (authorization), and keeping a record of all unauthorized access attempts and policy changes (auditing). Most Web Access Management solutions also provide for single sign-on (session management).

Single Sign-On

Single Sign-On (SSO) is a technology that offers a convenience to users, enabling them to enter a single set of credentials just once to access a variety of resources and applications. This also saves companies money by dramatically reducing Help Desk calls. Stand-alone SSO products do *not* handle policy authorization, nor do they audit access to resources as does a Web Access Management product.

\$2,000,000. Again, the competing product they had in place cost \$750,000 for the software licensing fees and \$3,900,000 in hardware to run the policy server software, or \$4,650,000 -- a premium of \$2,650,000.

Annual Administrative Personnel Costs

Centralized vs. Delegated Administration

Like almost all WAM products on the market today, Bank A's competitive product had a centralized administration console. That meant that there was a single application interface, or more importantly, login for administering the product. Since there was a single login, a team was formed at Bank A to handle all administration requests, and each user shared the "master" password to make changes to policies. With over 1,000 Web applications to maintain, this team consisted of 10 people whose full time responsibilities were to:

- monitor and maintain the policy server infrastructure (monitor the software processes on all 65 servers, perform policy server software upgrades, etc.)
- translate Web application security requirements into policies that are configured in the policy servers for all 1,000+ Web applications across the enterprise

At an "actual cost" of \$200,000 per year, per employee (including salary, benefits, real estate costs, etc.), Bank A was paying \$2,000,000 per year for a centrally-administered infrastructure.

Before WAM products came into existence, each Web application developer group would code and configure their own access policies. It is logical to conclude that developers would understand their access control needs best, because they understood their Web application and user needs.

A key feature of the maXecurity product line is delegated administration. Therefore, with maXecurity, Web application developer groups administer their own access control policies. This results in not only more efficient development and maintenance cycles, but also obviates the need for any additional policy administration personnel.

A common requirement (as well as an industry-determined best practice) is to segregate roles to administrative functions. Sarbanes-Oxley requires such controls, and maXecurity includes it right out of the box. Two roles (in addition to the application developer) are Infrastructure Administrator and Security Administrator. These roles allow control over the configuration and operation of maXecurity appliances to be segregated and delegated to the appropriate groups, while preventing unauthorized users from accessing functions outside the scope of their job functions. Bank A reallocated a total of 6 employees to manage and secure the maXecurity appliances.

Software vs. Appliance-Based Maintenance

Software products offer the flexibility to run on a variety of hardware platforms which customers may already own. However, for something as critical to an enterprise as Web Access Management, software-based products are inefficient both from a performance and security point of view. As described earlier, Bank A was able to reduce the number of machines that need to be monitored by a factor of ten. In addition, since maXecurity appliances have no user access other than via the intuitive Web-based interface, there are no accounts to secure (as with traditional Unix or Windows servers), no competition for disk space, processor usage, or memory usage due to other files/programs accessing the server, and no OS upgrades that may conflict with the policy server software running on the servers. Bank A dedicated three employees to perform general system monitoring, OS upgrades, monitor disk space, etc., for

Controlling IT Costs

The most cost-effective way to implement a technology infrastructure is to consolidate hardware while distributing management tasks.

maXecurity takes advantage of both of these efficiencies -- the appliance form-factor consolidates all WAM functionality into a small number of devices, thus creating a simple, easy-to-scale and administer piece of infrastructure. The delegated administration feature allows all the policy administration tasks to be split among many users, thus eliminating the need for a dedicated, single-purpose team.

all 65 Sun V490 servers at a combined cost of \$600,000 per year.

When the need for centralized policy administrators was removed from Bank A's infrastructure, the staff was eliminated and the Infrastructure Administrators described above monitor and maintain the appliances.

Annual Administrative Personnel Cost Savings

Considering the same "true cost" of \$200,000 per year, per IT employee, the maXecurity infrastructure required \$1,200,000 per year to maintain -- resulting in an annual savings to Bank A of \$800,000.

Annual Engineering Personnel Costs

Web Agent Certification

Traditional WAM products intercept and perform policy decisions on Web requests by closely integrating with Web servers via server APIs. These small software applications are known as "Web agents". Web agents offer WAM products the ability to monitor and control access to Web resources of any Web server against which Web agents are written. When WAM products were originally developed in the late 1990s, there were very few Web servers, few versions of these Web servers, and few platforms for them to run on. In more modern times, unfortunately, there is an overwhelming combination of servers, versions, etc. At Bank A, they have struggled to standardize on a single Web server platform. Unfortunately, through many mergers, acquisitions, and developer demands, it has been a rigorous and futile effort. Currently at Bank A there are six different Web server products in use, and at least three different versions of each (a "legacy" version, the enterprise's current standard, and an "advanced" newer version). Each of these run on three different hardware platforms, each in turn with three different versions of the underlying Operating System. With 162 different Web server combinations (6 x 3 x 3 x 3), Web agents were a frustrating part of the infrastructure at the Bank's Web server group. They employed a team of 12 Full Time Engineers at a true cost of \$200,000 each (annually) to certify each of the Web agents against each of the 162 combinations of Web servers. In addition, every time there was an upgrade of the Web agent software, an additional headcount from the Web server hosting group would be required in order to upgrade the software on all the Web servers. The \$2,600,000 team of engineers was also responsible for monitoring and audit functionality that is not provided by the vendor.

Audit Reporting

Because Bank A is a publicly-traded financial institution, it is subject to many types of regulatory compliance rules. Competitive WAM products contain minimal (or raw) logging capabilities out of the box. Bank A's team of engineers would develop software tools to parse these logs and generate reports for their auditors. In addition, since the tools were very customized, and usually required changes to them (or to the infrastructure configuration), an additional headcount was required at Bank A to assist the auditor during the annual audit process. This equated to \$2,800,000 for performing engineering work around Bank A's traditional WAM product.

Out of the box, maXecurity includes built-in reporting for all major regulatory requirements (Sarbanes-Oxley, HIPAA, PCI, CPNI, etc.). In addition, it includes a first-class role for auditors so that they can log into a maXecurity appliance and generate reports at any time, on-demand. This eliminates the need for any engineering personnel (no Web agents to certify, no audit reporting tools to build), as well as the additional headcount for upgrading Web agents

Web Agents - Good or Bad?

Web agents are small pieces of software that are installed on each and every Web server in an organization. They are used to bridge the communication gap between Web servers and policy servers. maXecurity takes a different approach -- the appliances act as proxies to all Web requests, eliminating potential issues of compatibility, integration, security, and performance.

NetworkWorld's Tim Greene says, with regard to agents in general, "Enterprises are fed up with agents on their endpoints - very fed up. Part of the reason is that the more agents on an endpoint, the more demanding the task of maintaining them."

and the additional headcount for hand-holding the auditor during an annual audit.

Annual Engineering Personnel Cost Savings

Because of maXecurity's proxy-based architecture and its built-in support for regulatory compliance reporting Bank A's \$2,800,000 in annual personnel costs is eliminated (or more accurately, migrated to other areas of the company).

What's your True TCO?

P2 Security, or one of our certified partners, can provide a complimentary True TCO analysis.

Summary

Bank A Realizes TCO

True TCO transcends the initial purchase price in almost all cases. Bank A could have originally saved over \$2.5MM by purchasing maXecurity instead of its current product. Instead, it will allocate two employees for six months (at a cost of \$200,000) to migrate away from their existing product and switch to maXecurity. The added cost of migration plus the initial cost of the maXecurity-based appliance will cost Bank A \$2.2MM. The current annual personnel and maintenance costs of over \$6MM (vs. \$1.6MM from the maXecurity-based solution), however, make a compelling enough case for Bank A to switch. By doing so, Bank A will see a Return on Investment in under six months.

True TCO for Bank A			
Cost	Competing Product	maXecurity	Savings
Software License	\$750,000	\$2,000,000	57%
Hardware Cost	\$3,900,000		
Total Initial Cost	\$4,650,000	\$2,000,000	57%
20% Support & Maintenance*	\$930,000	\$400,000	57%
Policy Server Administrators*	\$2,000,000	\$1,200,000	54%
System Administrators*	\$600,000		
Engineering*	\$2,800,000	\$0	100%
Total Personnel Cost*	\$5,400,000	\$1,200,000	78%
Total Year 1 Cost	\$10,980,000	\$3,600,000	67%
Total Year 2 Cost	\$6,330,000	\$1,600,000	75%

* Annual, recurring costs

For more information on this case study, or to learn more about maXecurity, please visit www.maXecurity.com or contact P2 Security at (888) 877-7272.