tool, yet it carries considerable power. Netstat, AR Cache and local routing tables are all up for grabs, Burdette says. Using these, attackers can spot, contact and compromise other systems.

"The challenge is that when adversaries masquerade as legitimate users, how can network defenders identify what is legitimate activity versus adversarial activity?" he asks.

> "...attackers are really less interested in being brilliant than they are in the end effect."
>
> – Adam Firestone, president and GM, Kaspersky Government Security Solutions

Hiding in plain sight

Savvy attackers will also use legitimate tools to hide in plain sight when communicating with existing malware and stealing data from networks. One good example of an attack using legitimate tools to communicate with its controllers and extract information from its target is HAMMERTOSS, a backdoor inserted onto victim systems by a Russian threat group that FireEye calls APT29.

Phil Burdette, senior security researcher, Dell SecureWorks

APT29, which according to a FireEye report is an expert at covering its tracks, crafted a tool that communicated with team members via Twitter. The company explained that the tool would reach out to Twitter accounts with frequently changing, algorithmically-generated names. Each account contained a message with a URL and a hashtag indicating an image size. The backdoor was configured to check Twitter only during office hours making it indistinguishable from regular office traffic.

FireEye researchers found that APT29 tweeted a URL and a hashtag to the account, which directed the malware to a webpage containing an image. Command instructions for malware were hidden in the image using stenographic encryption and the hashtag told HAMMERTOSS where in the image to look. The decryption key for the data in the image was created using hard-coded information from the malware binary along with characters from the tweet making it hard for security practitioners to access the command instructions.

The image would contain PowerShell instructions, or an executable file, FireEye revealed after examining the malware. It would often tell HAMMERTOSS to upload victim data to a cloud storage service, again cloaking its activity by appearing to be a legitimate tool.

Unpredictability is also a key feature in many APTs. HAMMERTOSS varied the image file size and Twitter handle used, making it difficult to look for consistent patterns in its behavior. It also used an alternative variant, identified by FireEye, called Uploader, which communicated directly with a URL instead of Twitter.

What can companies learn from these attacks and how can they protect themselves? If, as KGSS's Firestone says, few zero-days are used at the outset of these attacks, this suggests that anti-malware solutions and web protection software to check URLs are still important. These alone won't be enough, however, says Barry Vengerik, principal threat analyst at FireEye.

It's all too easy to reach for an "anti-APT" product offering, but real protection is more complex, involving a mixture of basic network hygiene and panopticon-like vision, he says. Companies must master IT Operations 101 first, patching their vulnerabilities and setting up internal penetration testing programs. "It's having the best practices in place, which plenty of folks still don't have, as well as having visibility," he says.

That level of visibility can be difficult in larger companies or in recently-merged organizations. FireEye sees a spike in attack attempts on companies undergoing merger and acquisition activity, Vengerik says. Techniques such as log aggregation and scanning can help to improve visibility, as can internal IDS monitoring.

Baselining networks to find "normal" behavior can help to detect anomalies, but that can be difficult, admits SecureWorks' Burdette, because administrators may find themselves baselining an already-flawed system. That's why the initial anti-APT engagement begins by scanning for ongoing attacks.

Looking for specific tools is only one part of the approach, though. "We focus on how they operate, how they move laterally, keying off known behaviors and identifying those," says Burdette. Attack groups typically take the path of least resistance. Investigation teams identify these attacks with different groups, creating a modus operandi that they can use to predict what a new attack will look like.

That can also help to close all the backdoors that the attackers put on the network to regain access to a system. These can stretch into double figures in some cases. It's impossible to tell with 100 percent certainty that they're all gone.

"We see re-entry attempts within about two weeks of eviction, mostly," Burdette says. "Until we raise the bar by implementing some fundamentals of good security practices, adversaries will use the same behaviors as they have done before. And if we don't see a re-entry attempt? That's even more worrying." ■

Product Section

Bayometric
Adds biometrics to your apps
P38

PistolStar
Front-end authentication portal **P42**

Yubico
Ridiculously easy to use authentication **P46**

Authentication: Strength, cost and simplicity

This month we look at authentication. This is a constantly evolving group and, therefore, an interesting one. Historically, authentication meant username and password. We got to the point where those "in the know" understood that simple protections are simply defeated. "Strong authentication" was born, but it was unclear what that really meant.

Strong authentication today seems to be evolving as a sort of a back seat to convenience. It is convenient to use a username and password. You can use one password for everything, make it your dog's name and you've got an easy-to-remember – and compromise – authentication. Afterall, what could be simpler than "Fido1234"? Easy to remember, but a very bad idea compounded, of course, by using the same password for everything.

So, the big question is: How do we retain the simplicity of Fido1234 and still get something secure? Really, as much as being about the cool technologies surrounding today's authentication schemes, answering that question is at the top of what we view today as strong authentication. We want the strength of the one-time pad with the simplicity of Fido1234.

The second issue – or, if you include the strength of the authentication scheme itself, the third – is cost. I really want my bank customers to use strong authentication. It minimizes phishing impacts and a bunch of other things. But I have 100,000 or more customers (this is a smallish bank) and I don't want to send every one of them a $75 hardware token, half of which will be lost or broken and which I'll have to replace. Also, teaching my blue-haired granny to use a time-based token may be more of a challenge than my help desk is up to.

The alternative, though, is a user-selected PIN. With a four-character minimum, you can bet that 90 percent will be four characters. And the number? 1234 always is a good choice. Neither of these options is particularly appealing. So that, really, is what strong authentication – and this month's offerings – are all about: strength, cost and simplicity. Perhaps you, as did I, will find something new to consider in the evolving field of strong authentication.

—Peter Stephenson, technology editor

How we test and score the products

Our testing team includes SC 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 based on a predetermined set of SC Labs standards (Performance, Ease of use, Features, Documentation, Support, and Value for money). There are roughly 50 individual criteria in the general test process. These criteria were developed by the lab in cooperation with the Center for Regional and National Security at Eastern Michigan University.

We developed the second set of standards specifically for the group under test and use the Common Criteria (ISO 1548) as a basis for the test plan. Group Test reviews focus on operational characteristics and are considered at evaluation assurance level EAL 1 (functionally tested) or, in some cases, EAL 2 (structurally tested) in Common Criteria-speak.

Our final conclusions and ratings are subject to the judgment and interpretation of the tester and are validated by the technology editor.

All reviews are vetted for consistency, correctness and completeness by the technology editor prior to being submitted for publication. Prices quoted are in American dollars.

What the stars mean

Our star ratings, which may include fractions, indicate how well the product has performed against our test criteria.
★★★★★ Outstanding. An "A" on the product's report card.
★★★★ Carries out all basic functions very well. A "B" on the product's report card.
★★★ Carries out all basic functions to a satisfactory level. A "C" on the product's report card.
★★ Fails to complete certain basic functions. A "D" on the product's report card.
★ Seriously deficient. An "F" on the product's report card.

SC MAGAZINE BEST BUY | SC MAGAZINE RECOMMENDED | SC MAGAZINE LAB APPROVED

What the recognition means

Best Buy goes to products 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 Labs environment, and which will be used subsequently in our test bench for the coming year.

Authentication

The products in this year's authentication group go a long way toward addressing both cost and ease of use issues, says Technology Editor Peter Stephenson.

PICK OF THE LITTER

For its low cost of ownership, easy customization and rugged good looks, we make **YubiKey** our Best Buy.

For topnotch features, customer service and ease of use we select **Vasco** as our Recommended product.

SC MAGAZINE BEST BUY SC MAGAZINE RECOMMENDED SC MAGAZINE LAB APPROVED

This group has been around so long that it is getting harder and harder to come up with an opening column each year. After all, how much is there to say about a product type whose reason for existing is to make sure that you are who you claim to be. There. That's it. Nothing more to say, right? Well, not exactly. We are constantly amazed by the level of ingenuity that this product group displays year after year. Really, our best course of action is to let the products speak for themselves. But, just for the sake of formality, we'll continue to help them along.

The basic idea behind authentication is that a subject identifies itself, proves it's who or what it claims, and then becomes authorized to do certain things, usually based on a policy of some sort. That's really all there is to it. But, if this is so simple, why do we keep getting it wrong? Why are there record-breaking breaches month after month, year after year? The reason is simplicity itself: The simplicity of taking the easy way out. The username and password that are predictable and crackable. The predictable username patterns that can be guessed easily by looking at a dozen or so email addresses from a given organization, and the passwords that are simple (remember Fido1234?) and that get reused on all of that user's accounts. That's the problem, and a tough nut it is to crack – much tougher than Fido1234.

We access the US-CERT portal for some of our research. They have a really neat approach – one that took us aback somewhat. When we type our username to login, it is masked in exactly the same way that passwords are. Then we use a combination of an assigned PIN and an RSA SecurID token-generated PIN. Nice and secure.

However, this is an expensive approach – the hardware tokens are pricier than other forms of token – and it may be difficult for some people to master. We need alternatives. That is what keeps this product group interesting year after year. There are drivers that shape this market. Price is a key issue. Ease of use and, of course, security are critical. Along with the obvious customer ease of use there is, for the enterprise world, administrator ease of use. Admins may be more experienced than the people they support, but they also spend their days putting out fires.

The products in this year's authentication group go a long way toward addressing both the cost and ease of use issues. As well, they address security, but in each one's own unique way. So, with all of this choice, how do you chose? There are a few simple rules that can guide you.

First, don't buy more than you need. The US-CERT approach is very cool and quite secure, but there is a lot of really sensitive stuff behind that locked door. Stuff that affects national security. It needs a lot of protection. Start with the assumption that you need strong authentication – you do. No matter who you are, you do. Then start thinking about your users, your organization, its topological footprint and your support team. Such things as user provisioning, help desk work load and skill sets, cost, organizational growth, the things that you need to protect... all of these help define what you need for strong authentication.

Then – and perhaps we should have started here – think about what you want to protect. It is not uncommon to have multiple levels of strong authentication. In today's environment with open source standards such as OAuth, mixing and matching products is a lot easier than it used to be. So take the example of a bank. The customers need strong authentication – simple, cheap, secure. The employees need strong authentication: Perhaps not quite so simple, maybe not as cheap and probably more secure. Then there are high-risk user accounts, such as system administrators. Simple doesn't matter much. Cost, within reason, is not much of an issue. Rather, the driver here is security. That could well be three different types of devices, some hardware and some software.

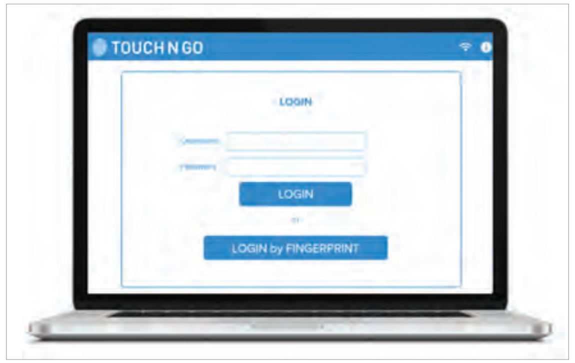
So, it's time to dive into the products. We'll just log back into the website and grab our notes... let's see: Fido1234...

Specifications for authentication security tools

●=yes ○=no

Company	Gemalto	Bayometrics	Datablink	Yubico
Supports Yubikey	●	○	○	●
Supports physical token	●	○	●	●
Supports software authentication	●	●	●	○
Offers self-service password reset	●	○	●	○
Offers API for custom products	●	●	●	●
Offers biometric support	●	●	●	○
Offers RADIUS support	●	○	●	● with supporting back-end solution
Offers VPN support	●	○	●	● with supporting back-end solution
Offers Active Directory support	●	○	●	● with supporting back-end solution
Offers SMS authentication	●	○	●	○
Offers Bluetooth authentication	○	○	○	○

At press time, we had yet to receive specification details from PortalGuard,SecureAuth and Vasco.



Bayometric

Touch N Go

Touch N Go is an unusual addition to this month's group. Although Bayometric does have many kinds of fingerprint scanners available for sale, it primarily is the developer of a fingerprint recognition API. The API can be added to any application with the addition of four lines of code in the app. From that point on, Touch N Go does all of the heavy lifting, including enrollment, administration and reporting.

The Touch N Go API has several components. The most obvious one is the user enrollment capability. Enrolling users is similar to enrolling users on most fingerprint scanner – with the exception that there are a couple of additional features. For example, if your policy requires that certain fingers be enrolled – the forefingers of each hand, for example – that can be made part of the enrollment process and no other fingers will be accepted. A second nice feature is that the administrator can accommodate a user with a missing or damaged finger. If the forefinger of the right hand is required and the user has lost that appendage, the administrator can make a substitution and note in the user's record that the required finger is missing.

The administration module, or "Admin Panel," consists of four modules: User Management, Security and Backup, Fingerprint Settings, and Status and Reports. This is part of the API and it handles the administration tasks. However, the user's application does all of the backend work. For example, the API, for security reasons, does not retain the fingerprints. That is left to the user's application backend database. User biometric IDs also are stored with the user application. In short, the API is exactly that: an API. The underlying application is left to the customer.

Documentation is what you'd expect for an API, and a little less since there really is a limited amount of effort required for the developer. The website is mostly marketing, but does include a demo. There is no customer portal. However, help desk support is first-rate with phone and email assistance included in the price of the product. Bayometric engineers will do a shared computer screen if more assistance is needed beyond that.

Pricing is very straightforward – one price buys all – and it is quite reasonable for what you get, especially if you plan a fairly large user group. You can buy fingerprint scanners from any scanner vendor – Touch N Go supports just about every make and model – or you can buy directly from Bayometric.

We liked the simplicity and were surprised at the way it takes care of all of the development issues programmers are likely to encounter if they want to add biometrics to an app or web portal. Although Bayometric does not have its own application at the moment, we were told that demand has been significant enough that they are introducing one shortly. It will be interesting to see what they do.

DETAILS

Vendor Bayometric

Price $399.

Contact bayometric.com

Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★
Support	★★★★½
Value for money	★★★★★

OVERALL RATING ★★★★★

Strengths Simplicity, universality in the backend, and support.

Weaknesses Website needs something besides sales and demo info. A customer portal would be nice, for example, as would product documentation for programmers.

Verdict There is nothing like this that we've seen. It's a neat idea, well conceived and executed and, if you are thinking about adding biometrics to your app, this might just be the thing to make your decision for you.

Datablink

Device 200 and Mobile 200

These two authentication products are identical in function. However, the Mobile 200 works with an Android, iPhone or Windows phone while the Device 200 is a small tool with a screen. It's a bit smaller than a pack of cigarettes and about a quarter inch thick. It contains a physical monitoring pad, such that the only person who can authenticate with it is the person holding it..

The idea behind Datablink is that you pair up your device or mobile phone with a screen that is presented from a server online. The online web page has a blinking icon of sorts and you read the icon with your phone or device. This generates a challenge/response pair on your device or phone. You enter the response on the web page and you're authenticated. The challenge stays present for a predetermined period and if you do not respond it generates a new challenge.

We tested the Mobile 200 – the two products work identically – and it took us about 10 minutes to download the app from the app store, install, register with the website for the first time and run our tests. We don't think it could have been much simpler. Given that just about everyone has a smartphone these days we're betting that the Mobile 200 is the more popular of the two.

Through a backend connection to the organization, Datablink generates a secure channel. This allows secure authentication for banking transactions. This process can be used for secure banking or transaction signing. The Device 200 is especially good for mandating authorized user presence. It requires the authorized user to be physically present and holding the device when using it.

The Mobile 200 has the added advantage that many of today's smartphones come with fingerprint readers. While they are not always perfect, they raise the bar substantially for physically identifying the user. Using the Mobile 200 on a phone to which the user had authenticated biometrically adds an additional secure dimension to the transaction.

The management server is the backend software that controls the authentication process. It synchronizes with Active Directory or LDAP and generates everything the Device 200 or Mobile 200 need to complete the authentication process. It logs extensively and generates several different reports that can be used for audits and compliance.

The website contains an efficient demo and mostly sales information. There is a data sheet for each of the available products, but we would like to see a bit more support information on the site. The support help desk is available eight-hours-a-day/five-days-a-week and, with a separate contract, 24/7. Datablink partners also provide localized support. Documentation is good and the pricing for both products is very attractive. We liked its ease of use and the company's unique approach to authentication.

DETAILS

Vendor Datablink

Price Device 200: Starts at $28 perpetual or $1 per month; Mobile 200: $9.10 perpetual or $.61 per month.

Contact datablink.com

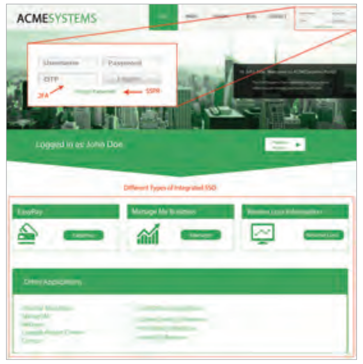
Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★
Value for money	★★★★★

OVERALL RATING ★★★★★

Strengths Ease of setup and a strong approach to simple but secure authentication.

Weaknesses We would like to see more support on the website.

Verdict A unique and user-friendly approach to strong authentication. This fits well in a banking environment and with other Datablink products can provide more universal authentication to such things as networks.



PistolStar

PortalGuard

PortalGuard is a dedicated web-based portal that provides all strong authentication for the assets it supports. As has become popular, PortalGuard allows full branding and integrates cleanly and smoothly into the organization's digital fabric. Technically, it may be deployed as an on-premises, cloud or hybrid implementation. It uses a REST API and can integrate into a variety of architectures that support such things as load balancing and fail-over, as well as allowing a distributed – multi-portal – deployment for large geographically distributed enterprises.

The portal supports most types of tokens – both software and hardware – and there is a free app for use with smartphones. It supports both SAML and non-SAML applications and just about every multifactor authentication scheme you can think of. RADIUS is built in. In short, PortalGuard is a very complete, well-conceived and executed package.

We started by examining the components of a PortalGuard implementation. In addition to the expected portal and strong authentication characteristics, there is a self-service component that allows users to perform such tasks as self-provisioning and password resets without recourse to the help desk. The administrative features are clean and comprehensive and the configuration was straightforward.

The configuration editor really is a policy editor and it is easy to use and very complete. Navigation is intuitive and we had no trouble following the setup approach necessary to deploy the portal and make it accessible to users. In terms of available one-time password tokens we did not note any important ones missing. In addition, there is a proprietary "PassiveKey" approach that uses the computer itself as the token.

User self-service includes account unlock, password reset and recovery. Retrieving forgotten usernames and self-registration. This trend has become popular enough to be a must-have, and PortalGuard implements it nicely saving a lot of help desk overhead.

The PortalGuard pricing model is simple. It is server-based so the number of actual users doesn't impact price. We found the price very reasonable and, of course, being a server-based approach, it is predictable. eight-hours-a-day/five-days-a-week. Silver level support is included and 24/7 or 12/5 support packages (Platinum and Gold) are available at an extra cost. The website is rich with information, including such things as FAQs, white papers and documentation in the form of guides.

Documentation was complete and well-presented and, perhaps more important, there was a lot of collateral that was useful in assessing the approach that needed to be taken for various types of deployments, including addressing aspects of compliance. Overall, we found PortalGuard to be a first-rate example of the application of a web portal as a front-end for strong authentication.

DETAILS

Vendor PistolStar

Price $15,000 first year, plus $5,000 annual subscription, support and maintenance.

Contact pistolstar.com

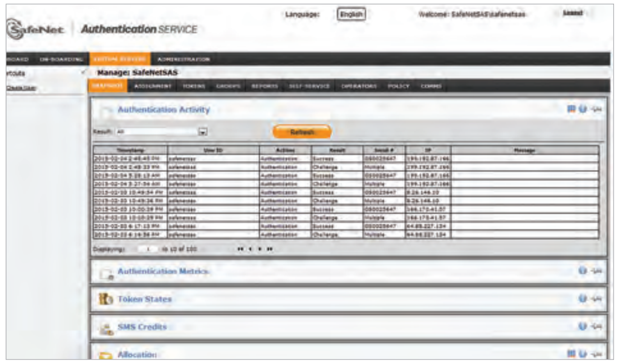
Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★★

OVERALL RATING ★★★★★

Strengths Clean deployment and superior options for integration into the organization's digital fabric.

Weaknesses None that we found.

Verdict If you are looking for a front-end authentication portal that works well in a distributed environment, this one demands your consideration.



SafeNet

Authentication Service

SafeNet is one of those products that has been around a long time and its maturity shows. We have been watching the company for a long time. The Authentication Service is a good example of that experience and maturity. It is easy to set up, designed for large deployments and easy to use. SafeNet Authentication Service is a SaaS offering, but it can be set up on-premises if desired. However, it typically is deployed as a cloud service.

Authentication Service is built around a significant collection of automation workflows that allow administrators to manage thousands of users, even with limited administrator overhead. The company prides itself on its over 200 integrations leading it to claim – rightly so, we believe – that if it takes a username and password on a login screen they can add strong authentication to it.

We looked at the SaaS version and the first thing that we noticed was the clean approach to menus. Since the first task is on-boarding new users we got a chance to see first-hand how the low support overhead works out. The workflows make a lot of difference and they are nicely integrated into the menu system. Because it is not uncommon for a user to access different levels of security – system administrators, for example – Authentication Service allows users to have multiple tokens.

Once the new user has started into the self-enrollment process, he or she creates a new token using MobilePASS. This allows him or her to create a token, give it a PIN and receive a first-time passcode. The first person to do this, obviously, must be the administrator or operator. Once the operator for the particular account is signed in for the first time, their next task is to add users. They can be added manually, automatically using a synch agent with, for example, Active Directory, or bulk loaded. If you bulk load you'll need to map fields so that whatever you are loading from matches the schema of the tool.

Once your users are loaded into the system they need tokens and that can be done automatically. You can set policies right from the dashboard and once the users are in the system and your policies are set your token goes out to the users by email. Additionally, there is a self-service portal that users can access to update their profiles, request tokens, reset PINs, resynch tokens and other tasks. This lightens the load on the help-desk materially.

As part of its integrations, the product offers SAML and RADIUS out of the box. This eases the integration with other products where you want to add strong authentication. We found the system easy to use and set up, very complete and well thought-out and organized. Reporting is excellent and when we asked about creating custom reports the answer was that with the 46 provided there is no need to. But if you want to alter reports you can on a one-time basis and you can only remove items. We found that a bit strange.

DETAILS

Vendor SafeNet

Price Typical cost is $1/user/month for enterprise volumes. Price discounts are available for larger volume of users as well as long-term contracts.

Contact safenet-inc.com

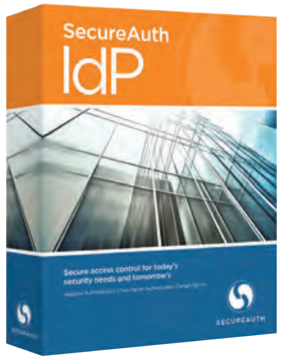
Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★★

OVERALL RATING ★★★★★

Strengths Straightforward, SaaS implementation that shows thought and maturity. Easy to deploy and use.

Weaknesses None.

Verdict This is a good choice for any size organization, but its benefits will really shine in larger ones.



SecureAuth

IdP

DETAILS

Vendor SecureAuth

Price Starts at $12 per user per year.

Contact secureauth.com

Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★½
Support	★★★★★
Value for money	★★★★★

OVERALL RATING ★★★★★

Strengths Simplifies management of strong authentication in just about any environment necessary – from applications to cloud-based resources.

Weaknesses None that we found.

Verdict Easy to set up and well-conceived front-end for all of your assets and locations that require security authentication.

SecureAuth IdP is a specialized web server that can act as a portal with strong authentication tied to the applications or web/cloud locations to which it allows connections. Using what the vendor calls “adaptive authentication,” it centralizes strong authentication for a number of resources into a single gateway. It does this by creating realms which really are specific use cases. These realms are specific to a particular asset and they provide customized strong authentication to those assets. Users cannot enter the asset except via IdP. The system can be on-premises or cloud-based, but most often is on-premises.

Each realm has associated policies and those can manage such things as user onboarding, access to cloud resources and access to applications. Because IdP uses CSS to create the portal, it can be branded easily in any manner the user wishes. Most important, because it simply is a very smart front-end, it does not take over many of the backend tasks of the customer’s organization. For example, no PII is passed to the portal itself. It remains within the organization’s control, as it would if IdP was not present.

That said, IdP does everything necessary to manage single sign-on and two-factor authentication across the assets and locations that it serves. The integration between the web presence and the managed assets is tight enough that there is no awkward feeling of a layered architecture. Everything fits nicely together. All of the strong authentication functions are managed by IdP using both its own and connected resources. We liked the clean, smooth functioning workflows that resulted.

Configuration is straightforward. Everything is laid out as workflows and the system accepts third-party tokens. It also uses existing directory stores. By design it does not have any of its own. However, it can tie to and span multiple stores so it could, for example, use AD and another similar directory services, such as SQL, LDAP or REST.

IdP supports more than 20 methods of authentication, all major federation protocols and APIs. It is supplied as a virtual appliance. Although it typically is supplied as a VMware appliance, other hypervisors are supported.

Pricing is reasonable, considering all it does, and since it can be installed as a virtual appliance there is little additional hardware. Support is provided as part of the licensing. And the website is very good. It contains a knowledge base and documentation as well as access to the support team. You can even download virtual appliance images.

There is a lot to like about SecureAuth’s approach. Even though it is built on a web platform, it is anything but a standard web portal. It has the mission of centralizing and controlling authentication or, as SecureAuth puts it, providing identity security. It does that very well, indeed.

Vasco

DigiPass 780, DigiPass for Mobile, and Identikey Authentication Server

This is another rather specialized product but, as with many such niche products, it fills a very important need. Vasco has been around quite a while and the company has a strong portfolio of security products. This particular suite – it consists of a mobile device application or a hardware token (your choice) and a backend server – addresses malicious code injection through the judicious application of strong authentication and some additional neat techniques.

SC MAGAZINE RECOMMENDED

The problem this suite addresses is that malicious actors can intercept and decode online banking transactions. By providing strong authentication coupled with some additional tools to prevent malicious repackaging/tampering, keystroke monitoring and screen scraping, DigiPass and Identikey interdict and prevent these attacks from succeeding. While in many cases strong authentication by itself has become a staple of online banking, the unique addition of Vasco’s tools adds a significant measure of protection to strong authentication by itself.

The DigiPass 780 and the DigiPass for Mobile behave identically. The 780 is a small token about the size of a pack of cigarettes and about a third of an inch thick. It is mostly screen. The Identikey server can be on-premise as a physical or virtual appliance or may be provided as a cloud-based SaaS. The process of using the DigiPass is deployed as a self-provisioning portal. The user first registers an account, then activates the DigiPass for Mobile or enables the DigiPass 780. From that point forward, the user can manage their account simply by authenticating to the portal.

There is a lot going on under the hood. For example, there is Vasco’s risk management that helps detect fraud. The Vacant Controller supports just about any operating environment you can imagine and has wrappers for all popular languages, such as C#, etc.

Pricing is a bit complicated because there are lots of possible combinations of products and services. The website is exactly what one would expect from a mature company such as Vasco. Everything is there: product literature, knowledge base, consulting, support, etc.

Something else we rarely see is an incident response mechanism for security flaws in Vasco products. We think that speaks volumes about professional responsibility and concern for customers. From a purely practical perspective, it also makes Vasco one of the “good guys” who are open about flaws and work hard to prevent or, if necessary, correct them.

We like this suite of products for its completeness and its focus on using well-supported strong authentication to address – in a creative manner – a serious problem. The experience of Vasco shows.

DETAILS

Vendor Vasco

Price Depends on product and quantity.

Contact vasco.com

Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★★

OVERALL RATING ★★★★★

Strengths Excellent targeting of a serious problem, ease of use and superior customer service.

Weaknesses None.

Verdict This one is, beyond doubt, a keeper. It is especially well-suited to larger environments and the company’s pricing model supports that. For topnotch features, customer service and ease of use, we make Vasco’s tool set our Recommended product.

Yubico

YubiKey 4

We love these folks. Some years ago, when the crew of Yubico were introducing their first product, we met them at RSA and they were handing out some of their first YubiKeys. We still have some of those museum pieces and, in fact, they still work for some things. The YubiKey 4 is slick and, while it has not changed materially over the years, it has added some new features and has become more reliable, if that was possible.

The YubiKey is an odd, little touch-sensitive second-authentication factor. It can be used as the entire authentication but, because it is not biometric, we don't advise that. It is best used with a PIN or password.

There are several modes for the YubiKey. In one mode, for example, you can generate a pass-code that the tool will store statically. When you place the YubiKey into the USB port and touch it, the key generates the static code as if you were filling in the password from your keyboard.

Another way you can use YubiKey is to generate a one-time passcode. Setting that up can be very simple, depending on the application with which you want to use it. For example, we keep about 100 or more passwords in a neat little app called Password Safe. It's free, works on Androids and Windows, and you can copy/paste passwords from it to whatever you want to log into.

But the problem is not the passwords stored in the Password Safe. It is the password for the safe itself. Enter YubiKey. Password Safe is set up for YubiKey, so when we got our samples this year, the first thing we did was register a YubiKey to the Safe. Now when we go to log into the Safe, there is a little YubiKey button. We enter our Safe's password, click the button, touch the YubiKey and we're in. Without the YubiKey, it's no go. Also, each passcode the YubiKey generates is different, and the codes are quite long and not predictable.

YubiKey U2F (Universal 2 Factor) provides authentication so you can do some pretty neat stuff with it. There is no limit to the number of U2F applications that you can access from a single YubiKey. So Dropbox, Google, etc., all are serviced from your single key.

There are several form factors, but we looked at the Nano and the standard YubiKey4 device. The standard device is about the size of a very small USB stick. There is a touch-sensitive area in the middle of it and the keys are very rugged. We actually took the standard one and drove over it with a car...no damage. The down side to the Nano, if there is one, is that it could be pretty easy to lose.

Yubico's website is first-rate. Pricing is attractive. Support is email or online trouble ticket, but there is so much support material on the website that contacting the help desk should be rare.

DETAILS

Vendor Yubico

Price Starts at $40.00.

Contact yubico.com

Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★★

OVERALL RATING ★★★★★

Strengths Size, ruggedness, open source compatibility and ridiculously easy to use.

Weaknesses None.

Verdict When it comes to universal, low cost, small second-factor authentication, there really is nothing to complain about. Every organization considering two-factor authentication should have a very close look at YubiKey. For its low cost of ownership, easy customization and rugged good looks we make Yubico YubiKey 4 our Best Buy.

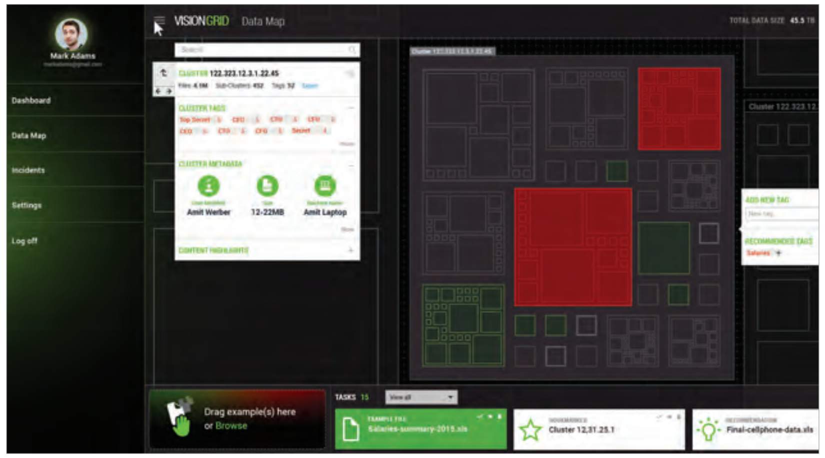
MinerEye

VisionGrid

We never have seen an organization that really wanted to do data classification – except, perhaps, the government. It is a tedious job that requires discovering and classifying hundreds of thousands of documents, determining their individual ownership and then assigning a classification. In a large, older company, the legacy documents easily can run to the millions.

Once the legacy documents are under control, there needs to be a plan for classifying documents as they are created. Finally, data leakage prevention (DLP) needs to be in place to take advantage of the classifications. It's no wonder that many, if not most, organizations skip the classification and tell the DLP device to block anything that has a credit card or Social Security number in it. It is equally understandable that many organizations never go through the exercise at all. Of course, if there are regulatory requirements to address, you must do something. Unfortunately, that often means taking the easy way out.

VisionGrid changes all that in a very unique way. We begin with the old school approach for context. The typical way to manage data leakage is to figure out what you don't want to leak. Historically, that has meant doing a couple of things. First, you decide what shouldn't leak – based on common sense and regulatory requirements – and then you figure out who owns those data and documents and tell them to start classifying. Typical DLP cares more about user behavior – did the user put a list of SSNs on a thumb drive? – than it does about the data. Of course, it's the data that determine how



we classify, but that is a static thing. If there is an SSN, we call the document sensitive or confidential. That part is easy.

Because VisionGrid doesn't care what the data are, it can classify pictures, words, multi-media files – in short, anything that is made of bytes. Once it has learned what a particular byte pattern looks like, it can pick out all documents or files that contain that same pattern. It doesn't matter how the file is oriented – for example, a vertical picture of a worker's face taken for an ID card can be identified from a group picture that includes the worker.

And the tool does not care about how the bytes got where they ended up. It could be a piece of code (pretty much any language will do), or a jpeg of a web page. It's the bytes that count – nothing more.

The first step is to group similar data – data that has something in common. Then, decide how to classify your exemplar data. Finally, scan it with VisionGrid. Once that is done, the solution can scan every file in the enterprise and those that contain the byte pattern go in the group.

Along with the necessary accoutrements for learning, classifying and identifying data, VisionGrid has a host of displays and built-in dashboards and logs. Overall, this really does set the bar for the next generation of data classification tools, all the better because it plays nice with other products, such as DLP tools.

– Peter Stephenson, technology editor

AT A GLANCE

Product VisionGrid

Company MinerEye

Price Starts at $65/user/year for 500 users.

What it does Sensitive data discovery based on data behavioral profiling rather than user behavioral profiling.

What we liked This is a completely new aproach to sensitive data discovery in the enterprise.

The bottom line VisionGrid views data simply as data – bits and bytes – and profiles those data based on comparison with a known model of similar data.