- PRODUCT DEMO REVIEW

Mackenzie Olson's Malware bytes.

Malware bytes is a security software designed to provide real-time system protection against malware, ransomware, and web attacks. It is well-suitable for a plethora of users no matter the dimension. - small, medium, or large company -, and the typology of user – personal or professional -. All thanks to a vast assortment of coverage packages. On top of that, it seems gather consensus among professionals, because of its user-friendly graphic interface. I think the software might be useful as a foundation for a more sophisticated line of security. As far as I am concerned, it does not possess built-ins for intrusion detection or APT preventions.

From the looks of it, the company provides extensive support to walk a user through the complete installation. All backed-up with online resources and customer service. In addition, training is offered for business users. Marketing and Sales department states "quick and easy installation process". Also, business customer review highlights, "the software was extremely easy to deploy on mass because it creates a customized installer, this meant we could deploy via remote desktop software".

Even though the software seems cool, as a future Cybersecurity professional there are few concerns to be addressed. Does the software support top vulnerabilities management methods? In essence, how often the application gets updated or scans vulnerable web servers, applications, or databases? Does the vendor have past regulatory inquiries, citations, or standing litigations regarding privacy or data security?

Charan Singh's IBM security qradar.

Qradar is an application software released by IBM. It offers complete threat detection against any sort of cyberattack. It can detect, understand, and prioritize threats by ingesting user data and then correlating it against confidential data. As far as I am concern, Qradar specialty is its integrations with endpoint detection & response, security information & event management, network detection & response, and (security orchestration, automation, and response).

On top of that, it offers several benefits such as alerts focus prioritization, facile deployment on cloud or premise, and can catch threats. Qradar's price may vary depending on the number of events per second and flows per minute, but eventually the package starts from $1250/ months. Also, there's the chance to have a free cloud trial for 14 days.

IBM QRadar architecture supports deployments of varying sizes and topologies, from a single host deployment, where all the software components run on a single system, to multiple hosts, where appliances such as Event Collectors, and Flow Collectors, Data Nodes, an App Host, Event Processors, and Flow Processors, have specific roles. However, before to plan the deployment, a company should consider: How does the company use the Internet? Does it upload as much as it downloads? Increased usage can increase the exposure to potential security issues. How many events per second (EPS) and flows per minute (FPM) does it need to monitor? EPS and FPM license capacity requirements increase as a deployment grows. How much information does it need to store, and for how long?

Moreover, a company should reflect on the following before adopting this software. What skills must be in place prior to adoptions? Does the company need a full implementation software, or is threat detection sufficient? How much are the company willing to spend?

Duraisamy Bhagyalakshmi's Perimeter 81.

It provides a cloud-based platform that enables companies to securely access, manage all their cloud applications, and resources from any device, no matter where the user is. Also, it has received recognition for its innovative solutions.

The product offers a zero-trust security model, where it ensures authorized users and devices to have access to the company's network, cloud infrastructure, and SaaS applications. Besides, it features MFA, real-time protection, and centralized user/device management. Some of the benefits are enhances security, improves productivity, simplifies management, and reduces costs. It comes with four different price tags, depending on the company's needs. These are, Essentials with a price of $8 per user/mo., Premium at $12 user/mo., Premium Plus (most popular) at $16 user/mo., and Enterprise which requires a talk before a price is set.

As for the installation as concerns, the company states that it takes just 15 minutes to get on board by following these steps: Create your network: Set up an SDP secured network consisting of regions and private gateways. Click here to learn more about our network components and structure. Connect your infrastructure: Deploy site-to-site connections to securely connect your local and cloud resources (click here to find out if you meet all the prerequisites). You can integrate seamlessly with the SaaS applications and tools you rely on, such as Salesforce, Microsoft Azure, AWS, or Google Cloud Platform. This allows you to build and secure your networks from one place - and model them in a simple, visual way. Invite your teammates: Create user groups and attach them to a network according to the resources the group member needs access to, integrate with your Identity Provider and invite your users. Regulate access to internal resources and enhance platform security: Configure agent-less access Zero Trust Applications, Download our agents, and adjust their configuration according to your own needs, apply DNS Filtering, and MFA Authentication. Monitor users' activity: Track users' activities and devices and integrate with a SIEM platform (AWS, Azure, or Splunk).

Some questions I would like to ask here, which specific data transmissions does the software encrypts? What is Perimeter 81's role in protecting data and mitigating security incidents?

Jessica Dao's Absolute.

It a platform that enables customers and ecosystems partners to address every Secure Endpoint and Secure Access use case. Also, it leverages a cloud-based, secure multi-tenant architecture that is available across different regions. The platform has four components such as persistence, application resilience, network resilience, and intelligence. All of them with unique features.

Price tag ranges from $30 to $75 per device depending on the duration – generally 1 year to 3 years.

No implementation process – just check dell website for info.

Two questions here, how is user data transmitted and store? Does the solution support to vulnerability management methods?

Sondos Bafaqeeh's Okta.

It is an application software that offers SSO – single sign-on. In essence, it allows users to access multiple applications and services using just one set of credentials. Once the user is granted access to the system, he/she/they can access all of the other trusted systems and applications. The software aligns with four types of protocols and standards such as SAML, OAuth, OIDC, and SWA.

Having said all of that, perhaps is necessary to list some advantages and disadvantages. It helps to decrease attack surface but cyberhackers may access all applications and systems if they get the user's credentials. Also, it simplifies secure user access but some applications are not compatible with SSO tools.

No price tag or implementation plan.

Gina Perez's darktrace.

It is an advanced Artificial Intelligence threat detection. It analyzes thousands of metrics to reveal inconsistencies that may indicate an evolving threat. Distinguishing whether is malicious or benign behavior. It supports cloud, apps, email, endpoint, network, and OT. Darktrace is able to learn what is normal, and takes appropriate action to neutralize threats, with minimal disruption to business operations. Also, it delivers clear reports with intelligence for security teams to make informed decision.

This software may be installed within an hour, deployed on cloud, SaaS, or Web-based, and does not require manual configuration or tuning. Unfortunately, there's limited education materials on how to fully use it. The price tag ranges from $30000 to $100000 yearly depending on the bandwidth. There's a free month trial to test the product.

From the looks of it, an AI requires high-skilled employees. How does the company think to manage the knowledge gap to let the AI run efficiently?

Peiling Zou's Onelogin Proposal.

It is an identity management and SSO service. It brings business agility by supporting internal employees and millions of external users with the same ease. The cloud infrastructure delivers unparalleled reliability to avoid major internet and datacenter outages, giving the confidence to deploy new technologies across the organization at scale. Also, it offers multiple benefits such as it saves employees time and prevents data breaches, makes the platform reliable, increases its usability, and integrates with popular directories.

Price tag starts at $4 up to $8/user per month depending on whether choosing advanced or professional bundle.

Nothing on implementation.

Two questions here, what is affected when the service experiences an outage? How can the company minimize the single point of failure created by an SSO?