CSO
FROM IDG
January 8, 2019 www.csoonline.com

UPDATED

Best security software, 2019: Lab-tested reviews of today's top tools

We go hands-on with some of the most innovative, useful and, arguably, best security software on the market. By John Breeden II

Threats are constantly evolving and, just like everything else, tend to follow certain trends. Whenever a new type of threat is especially successful or profitable, many others of the same type will inevitably follow. The best defenses need to mirror those trends so users get the most robust protection against the newest wave of threats. Along those lines, Gartner has identified the most important categories in cybersecurity technology for the immediate future.

We wanted to dive into the newest cybersecurity products and services from those hot categories that Gartner identified, reviewing some of the most innovative and useful from each group. Our goal is to discover how cutting-edge cybersecurity software fares against the latest threats, hopefully helping you to make good technology purchasing decisions.

Each product reviewed here was tested in a local testbed or, depending on the product or service, within a production environment provided by the vendor. Where appropriate, each was pitted against the most dangerous threats out there today as we unleashed the motley crew from our ever-expanding malware zoo.

With each review, listed in alphabetical order, we will endeavor to show how these new and trending cybersecurity tools work, where they fit into a security architecture, and how they defend against the latest types of threats and attacks.

Best security software — 2018, 2019 reviews

AttackIQ - *Category: Penetration testing*

The AttackIQ platform was created to watch our watchers. It's a penetration testing tool, but one that is configured to operate from the inside, with the primary goal of identifying flaws, misconfigurations and outright shortcomings in all other cybersecurity defenses.

Balbix - *Category: Vulnerability management*

Balbix may technically be a vulnerability manager, but it does it so much better and also so much more that it breaks the bounds of its category. Balbix is able to analyze each kind of vulnerable asset sitting on a network, what kind of data it holds, how many users interact with it, whether or not it's public-facing, and other factors to determine its importance to an organization. It then compares each vulnerability with active threat feeds, and predicts the likelihood of a breach in the near future, as well as the loss or harm to the enterprise should it be successfully exploited.

Thinkstock

BluVector - *Category: Network security*

BluVector offers advanced detection and response, and even threat hunting, all performed at machine speeds. BluVector works almost right away, but also has deep machine learning capabilities, so it gets even smarter over time. It will learn the intricacies of each network that deploys it, tweaking its algorithms and detection engines in a way that makes the most sense for the environment.

Bricata - *Category: Intrusion detection*

At it's core, Bricata offers advanced IPS/IDS protection with multiple detection engines and threat feeds to defend network traffic and core assets. But it goes a step farther, adding the ability to launch threat hunts based on events, or simply anomalies.

Cloud Defender - *Category: Cloud security*

Cloud Defender is a user-friendly tool that lets local IT staff inspect their cloud deployments to look for evidence of hidden threats or breaches. But it can also be used in a SaaS model, with the cybersecurity team at Alert Logic taking over most cloud-based cybersecurity functions.

CyCognito - *Category: Network monitoring*

The CyCognito platform was designed to provide the kinds of advantages that old school penetration testing used to, but on a continuous basis and for modern, global enterprise networks comprised of mixed physical and virtual assets. It basically studies networks the same way that hackers do, from the outside with no help or internal bias inserted into the process.

Cofense Triage - *Category: phishing defense*

Deployed as an on-premises virtual appliance, Triage connects with almost any corporate e-mail program and helps to manage responses to user reports of suspected phishing. Triage is still evolving, but even now represents one of the most advanced defenses against phishing.

Contrast Security - *Category: Application security*

Contrast Security has one of the most elegant solutions out there for application security. The secret sauce is its use of bytecode instrumentation, a feature in Java used to help integrate programs and application features during development.

Corelight - *Category: Network security*

In the tradition of other great network analysis tools like Bro and Sourcefire, Corelight gives security pros deep insight into data traffic on the systems they defend.

Digital Guardian - *Category: Endpoint security*

The Digital Guardian Threat Aware Data Protection Platform is at the forefront of the effort to counter advanced threats, offering ready-to-deploy endpoint security locally on-premises or as a service, and with whatever automation level a host organization feels comfortable supporting.

enSilo - *Category: Endpoint security*

The enSilo platform offers traditional endpoint protection alongside the ability to offer post-infection protection. It can also trap threats, holding them in place and rendering them harmless until a threat hunter can arrive to investigate.

ForeScout - *Category: Network asset management*

ForeScout is one of a very few programs that can help to track and manage operational technology and IoT devices alongside of information technology. Everything from lighting controllers to HVAC units can be discovered and managed.

Forum Sentry - *Category: Access control*

The Forum Sentry API Security Gateway's access control abilities are impressive, but it goes beyond access control and deep into security, monitoring all those connections that it forms and enforcing very granular security policies.

InSpec 2.0 - *Category: Compliance*

The InSpec 2.0 platform from Chef tackles compliance head-on, tailored to the specific rules and guidelines that a company wants or needs. It is designed to both make sense of regulatory and technical guidelines and ensure that a network is protected according to those rules.

Intellicta Platform - *Category: Compliance*

The Intellicta Platform from TechDemocracy acts like an SIEM console, but for compliancy issues. It pulls information from a series of network collectors and correlates that data into a continuously-monitored compliancy dashboard.

Insight Engines - *Categories: Network security, threat hunting*

Think of the Insight Engines tool as Google for network security, allowing natural language searches and returning honed information to answer each query. This comparison doesn't do the program justice, but is a good starting point for understanding how it works.

Mantix4 - *Category: Threat hunting*

Mantix4 takes threat hunting into the software as a service (SaaS) realm. While the program provides robust threat hunting tools for use by clients, the company also employs a team of experts to hunt on their behalf.

Ping Identity - *Category: vulnerability management*

Enterprise networks have grown too complex to easily manage all user credentials through something like Active Directory, and letting apps handle logins creates silos that can become a security nightmare. Ping Identity offers a good alternative to these two scenarios.

RiskIQ Digital Footprint - *Category: identity management*

One thing that sets the RiskIQ Digital Footprint apart from just about every other security program reviewed for CSO magazine is the setup and installation phase. There is none. Digital Footprint scans for vulnerability information from outside the firewall, just like a potential attacker would.

Seceon Open Threat Management Platform - *Category: Network security*

The Open Threat Management Platform essentially acts as both an SIEM and a frontline security appliance. Thrifty firms may want to consider eliminating some of their other cybersecurity programs if they duplicate what the OTM is doing, especially if the OTM is consistently catching what they miss.

SentinelOne - *Category: endpoint security*

Having powerful, protected, and independent agents sitting on endpoints gives SentinelOne a huge advantage against the increasingly sophisticated attacks of today. And because those agents are capable of acting independently, they can respond instantly as attacks happen, later sharing that information with human security teams for analysis.

Senzing - *Category: Data examination*

Used to combat fraud or uncover accidental data duplication, Senzing is a powerful yet lightweight tool with an artificial intelligence that is actually extremely smart.

Solebit - *Category: endpoint security/sandboxing*

By shifting malware detection away from signatures and behavior to whether any kind of code exists where it's not supposed to be, the SoleGATE Security Platform from Solebit has the potential to disrupt both endpoint security and sandboxing.

StackRox - *Category: Cloud security*

StackRox fully integrates with Kubernetes so that it touches all three phases of containerization deployment: the building of the containers, the deployment of them into the cloud infrastructure, and finally the running of those containers as they perform their intended functions.

Threat Stack - *Category: Cloud security*

With a large number of organizations moving their data and applications to the cloud, there is an acute need for a platform designed to natively detect malicious activity occurring there without hindering the underlying network or the business functions that rely on it. The Threat Stack Cloud Security Platform was made to fill that need. Read the full review.

Vectra Cognito - *Category: Traffic monitoring*

The Vectra Cognito platform incorporates artificial intelligence (AI), deep machine learning and traffic monitoring into a tool that is able to detect threats that other programs miss, even if they are already entrenched inside a protected network.