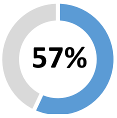
ESG
Enterprise Strategy Group | **Getting to the bigger truth.™**

First Look

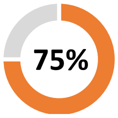
Deterministic Protection with Virsec

Date: January 2022 **Author:** Tony Palmer, Senior Validation Analyst

Cybersecurity Challenges:[1][2]



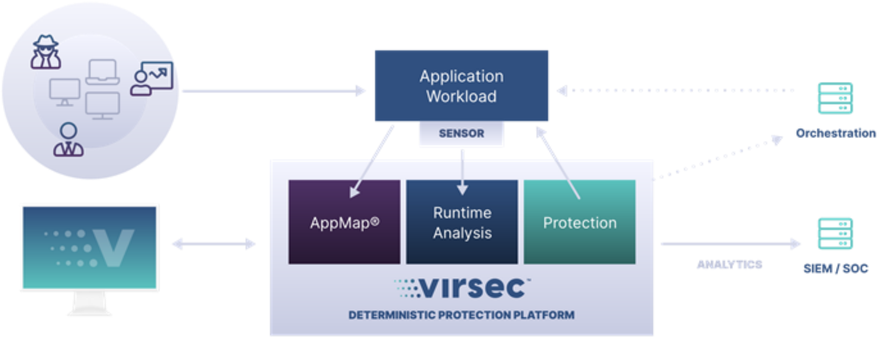
The percentage of organizations that report they've been impacted by the ***global cybersecurity skills shortage*** in 2021.



The percentage of organizations that describe *preventative protection* to be **a core capability** in terms of endpoint security.

The ongoing cybersecurity skills shortage has two major implications. The most obvious is a shortage of talented cybersecurity professionals, with simply more cybersecurity job openings than qualified candidates to fill them. The second is at least as important: Many members of the current cybersecurity workforce lack the advanced skills necessary to safeguard critical business assets or counteract sophisticated cyber-adversaries. This helps to explin why preventative protection was the most cited core capability of endpoint security solutions in an ESG survey of cybersecurity professionals.

Deterministic Protection Platform (DPP) by Virsec

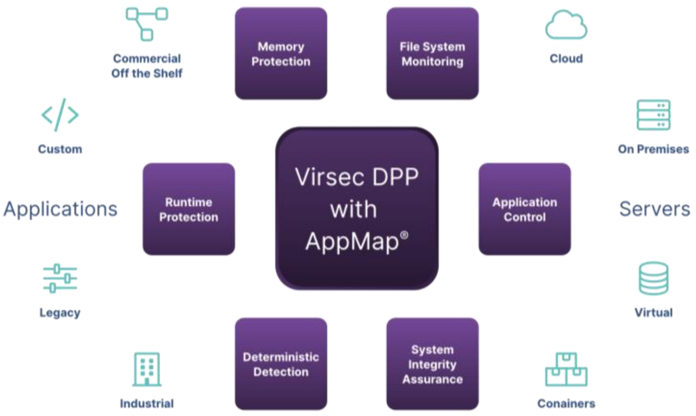


DPP by Virsec maps exactly what software is supposed to do and stops it from doing what it is not—while it is running. The platform is designed to ensure protection against all known and unknown threats to software workloads deployed in production and reduce threat actor dwell time from minutes to milliseconds, with runtime protection and observability. DPP is engineered to protect the entire attackable surface of the application covering host, memory, and web layers which can enable businesses to consolidate their security infrastructure while reducing analysis time and labor. Virsec AppMAP™ technology automatically extracts detailed knowledge and context across the entire application workload, providing defense in-depth against advanced attacks and complex kill chains. This in-depth mapping decomposes application packages to extract checksums and detect compromise at the earliest stage; decomposes executables to find library dependencies to and prevent memory injection attacks; enumerates interpreter and script combinations to prevent fileless malware attacks; enumerates files and directories that processes will access during runtime to capture malicious access to critical code early; captures directory paths and web roots for web apps to prevent attacks from corrupting the environment of the app; captures permitted remote redirects to prevent malicious code from being downloaded by end users; captures allowed syntax from a range of interpreters to prevent backdoors and remote code execution exploits using the Open Web Application Security Project (OWASP) Top 10 web application security risks; and extracts valid branches from binary code and enforces only developer-provided branch transitions at runtime to prevent remote code execution attacks using return-oriented programming (ROP) gadgets. Most of the current EDR, IPS, XDR, EPP, etc. security solutions operate outside the application which can result in alert fatigue false positives that leave the application infrastructure exposed to a significant risk. Virsec's deep application awareness and runtime visibility enables users to instantly detect and stop deviations that can be invisible to conventional security tools.

[1] Source: ESG Research Report, *The Life and Times of Cybersecurity Professionals 2021 Volume V*, July 2021.
[2] Source: ESG Research Report, *Security Megatrends and Their Impact on Endpoint Security*, December, 2021.

ESG Demo Highlights

ESG walked through hands-on testing of Virsec in multiple scenarios. Detailed here is a memory attack against a web server. We ran this test twice: once in detect mode to explore the depth of visibility Virsec offers, and again with protection enabled to show how Virsec can instantly block attacks in real-time.



Visibility and Protection

- We started with a memory attack that compromises the system without crashing the target process, so there's no indication to the ops team that anything is wrong. We executed an attack that uses native operating system components against a server running the nginx web service. The attack we used connected to the server, provided a reverse shell, and enabled us to upload the MiMiPenguin executable, which displayed system credentials and enabled us to enter the system as root, with full control. Virsec instantly built a detailed kill chain that clearly showed every step of the attack from the first buffer error to the final clean-up where the attacker removed traces of their activity. To manually build a kill chain like this would typically take days to weeks.
- Next, we enabled protection using Virsec protection profiles. Organizations define protection profiles for applications or groups of applications containing vulnerabilities and response actions. Response actions can be out-of-box micro—immediate protection of the host, and macro—integration with other systems, like perimeter protection devices, to block an attacker's IP address, for example. It's important to note that nothing was changed on the server, it contained the same vulnerability as in the first test.
- We ran the same script as in the first test, and we were simply unable to establish the connection to the server even though we had all the same information that we had before. This is what Virsec means when they say it can eliminate dwell time, which prevents destructive actions from being executed.

First Impressions

Modern attacks exploit gaps in probabilistic security tools that require prior knowledge like signatures, and the ongoing cybersecurity skills shortage is making it harder to expose and remediate attacks after they occur. What is needed is a solution that extends and automates protection across the entire workload and stack, to ensure that applications execute as intended and aren't disrupted or redirected by malicious code.

ESG observed how Virsec technology protects critical application workloads from the inside against advanced attacks that often bypass conventional security. Virsec combines deep application awareness with automated true runtime protection to derail advanced attacks instantly, without prior knowledge, across the entire attack surface. Runtime protection instantly spotted deviations down to the memory level, and precisely stopped attacks.

In ESG's opinion, Virsec delivers security that is effective, easy to manage, and simplifies compliance. Virsec's technology automatically maps acceptable execution across workloads, without the need for signatures, tuning, or learning. If your organization is looking for a solution that can provide effective deterministic protection without performance impact, Virsec is worth serious consideration.