Article

Avecto

FORRESTER®

4 pillars of an effective endpoint security strategy

Webinar Q&A with Chris Sherman, security analyst at Forrester.

Following our webinar with Forrester's Chris Sherman we asked four burning questions on today's key security trends.

How important is prevention as part of an effective endpoint security strategy?

Threat prevention is a critical component of your overall endpoint security strategy. If you can eliminate as much of your attack surface as possible through preventative tools such as application control and patch management, this will give you the ability to control (and predict) which areas of your attack surface attackers are most likely to target.

After you have this strong prevention in place, then you can get to work protecting the remaining exposed areas through detection-focused tools. The bottom line is, if you can use prevention to eliminate 80% of the attacks against your organization, you can focus your limited resources on detecting and responding to the more advanced attackers that have the motivation and capability to do the greatest harm.

What are the common security pitfalls for organizations?

All too often, organizations are so focused on finding the latest endpoint security tool that they fail to address some of the fundamental "housekeeping" tasks that help to create a more secure environment. Examples include limiting the number of non-work applications, timely security patch deployment, secure configuration management, proper enforcement of least privilege access, and many others. We as security professionals are hyper-focused on detecting threats; it is important not to lose sight of the greater goal of providing a secure working environment with a limited attack surface.

What are the quick wins that organizations can implement from a security perspective?

Attackers are constantly evolving new tactics, but exploiting vulnerable software is used in almost half of all data breach events according to the 2016 Forrester Business Technographics Security Survey. Despite this, many organizations do not have a managed patch deployment strategy.

One of the easiest ways to quickly increase your security posture is to simply keep track of the most commonly exploited vulnerabilities, especially those exploited by the popular hacker toolkits, and patch those vulnerabilities in your own environment as quickly as possible. This will lead to a smaller attack surface and greatly increase your resistance to the "commodity" malware that many non-targeted attacks leverage.

Avecto

How can organizations avoid “expense in depth” ?

Security pros will often invest in additional point products layered on top of their existing portfolio of endpoint security tools, thinking they’re supporting a “defense in depth” strategy. More often than not, however, S&R pros fail to exercise due diligence on these investments. They rarely ask “Do any of our existing technologies offer this capability?” or “Do we have the internal expertise to leverage this product effectively?”

To avoid this trap, every new purchase your security team makes should be evaluated for it’s overall fit within your existing portfolio. As you invest money and time into new products, you must continuously evaluate your own capabilities and make sure there is no overlap or major gaps. This will help you avoid falling into the ”expense in depth” cycle by ensuring you are always getting an adequate return on your security investments.

About Avecto

Avecto is a leader in Privilege Elevation and Delegation Management. Since 2008, the company has enabled over 8 million users to successfully work without admin rights, enabling many of the world’s biggest brands to achieve the balance between overlocked and underlocked environments.

Avecto’s Defendpoint software has been deployed in the most highly regulated industries, enabling organizations to achieve compliance, gain operational efficiency and stop internal and external attacks.