FORTRA™

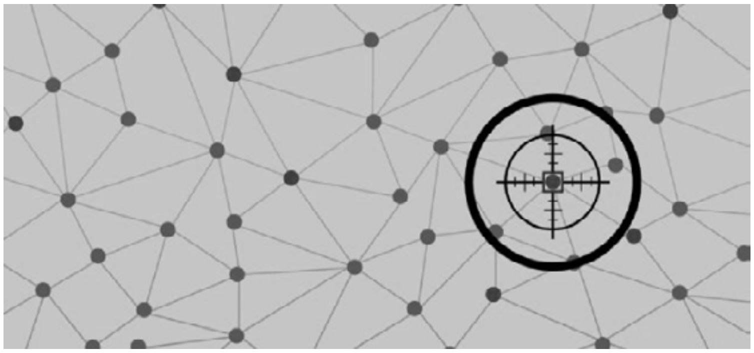
DATASHEET (INFRASTRUCTURE PROTECTION)

Active Threat Sweep

The Case for Active Threat Sweep

Today's malware is more sophisticated than ever, and traditional signature-based antivirus is notoriously bad at stopping newer threats, but it's a corner-stone in most enterprise multi-layer endpoint security strategies.

According to a 2017 survey of Black Hat attendees, 73% believe that traditional antivirus is irrelevant or obsolete. Plenty of recent research supports this point of view. Depending on which study you review, traditional antivirus can miss 20 to upwards of 40% of malware attacks.



CISOs and security operations teams are increasingly tasked with taking a more proactive approach to stay on top of the evolving threat landscape and traditional AV just can't keep up.

Next-gen anti-virus, threat hunting, endpoint detection and response, end-point protection, behavioral analysis, sandboxing, machine learning, artificial intelligence…there are numerous new solutions to aid in the battle against malware, but which one is the best fit for your organization? New technology takes time to evaluate, configure, deploy and maintain. All the while, you've got unprotected, unmanaged assets on your network. How do you fill the gap?

Many of the new technologies and more advanced capabilities require more processing power, which in turn slow down the assets you're trying to protect; can be too limiting, impacting productivity; or require more work to deploy and tune for your environment. Some vendors recommending a "rip and replace" of your existing solutions are considered too extreme (and costly) a measure. Your organization has spent numerous man-hours refining and budgeting to make your current deployment, "good enough". It's time to make it better.

Fortra's Active Threat Sweep (ATS) complements your existing endpoint protection technologies providing an agentless, easy to deploy method to quickly and reliably analyze assets for active threat activity and indications of compromise. Enhance your existing defense-in-depth coverage by uncovering gaps in your existing protection. Pinpoint which assets have no endpoint protection installed or that are out-of-sync and out-of-date leaving one or more assets at risk.

ATS enables organizations interested in threat hunting to deploy a threat detection capability on top of Digital Defense's proprietary technology architecture that is light-weight and effective to gain instant visibility into assets that demonstrate indicators of compromise.

Know What You Need to Fix Before You Go Home

ATS can aid IT Operations team members in quickly determining which assets have been infected and prioritize network hygiene mitigation and remediation efforts. With ATS you can eliminate wasted effort in rebuilding infected machines that might continue to propagate the infection. ATS can also collaborate with other network security platforms through a robust REST API to export threat details to enhance security orchestration automation and response.

Know What Has Evaded Your Defenses

ATS enables agentless analysis of enterprise networks for threat activity and indications of compromise. Determine the extent to which an infection has spread in order to better triage and prevent the infection from further infiltrating your network. Additionally, acquire insight into "shields down" conditions on assets with out-of-date or no endpoint protection in place making these assets more vulnerable to infection.

Know The Risk Before Allowing Access

In an age of overnight mergers and acquisitions, ATS can provide immediate visibility to organizations acquiring "foreign networks" to determine the presence of malware or other threats. Limit the introduction of new unmitigated risks to your network and quantify the time and expense required to inoculate the infected assets before assimilating so you can factor them into the acquisition costs and determine the true value of the deal.

Learn More:

Contact us: sales@digitaldefense.com
For more information visit: www.DigitalDefense.com

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.