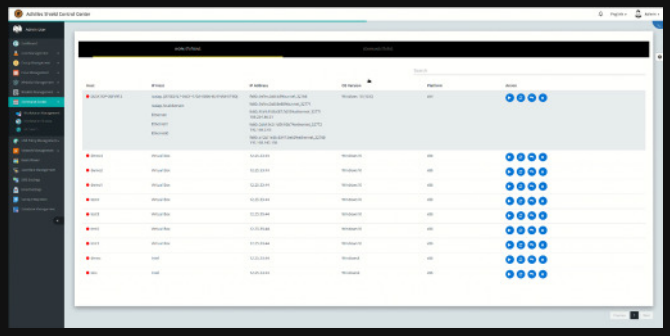
Achilles Shield
Be Impenetrable

Intuitive, high-performance security software that blocks the most advanced security threats.

Virtually every organization employs some kind of anti-virus (AV) protection. Yet, despite its nearly ubiquitous presence, security breaches are still on the rise. As it turns out, AV software can no longer adequately protect its users from today's threats - and AV

To defend a system from the latest threats, security software must be tuned to notice and block certain behavioral characteristics that are known to cause harm to systems. Most importantly, this security software must be able to respond quickly and not cause

Just like an achilles heel can be one of the most vulnerable points of the human body, an endpoint workstation can be one of the weakest points in your network or enterprise system. That's why we created Achilles Shield - an innovative software package that



FEATURES

POWERED BY ARTIFICIAL INTELLIGENCE

Achilles Shield automatically detects, classifies and eliminates all types of malware, ransomware and spyware.

REAL-TIME PROTECTION

After neutralizing threats, Achilles organizes and transmits information about malicious software to Achilles Central Server to be forensically analyzed. As the software "learns" your threat environment, your protection will increase.

INNOVATIVE AND TRANSPARENT SANDBOXING

Achilles isolates processes and runs them in a virtualized environment to learn more about them. If malicious activity is detected, there is no permanent damage to your system.

POWERFUL WHITELISTING AND BLACKLISTING

Allow or block any activity on the system, to include software, web sites, or even USB devices. It's all fully customizable.

A CENTRAL SERVER TO ORCHESTRATE EVERYTHING

Achilles Shield Central Server is fully loaded with tools to defend your network.

BENEFITS

- Protects against all types of endpoint threats in any kind of network environment
- Proven to defend against ransomware by detecting and blocking malicious activity before it runs on your base system
- Easily comply with standards, contracts, legal concerns and other requirements with Achilles Shield's advanced reporting capabilities
- Use the forensics timeline to deep-dive into the issues and assess future optimization of processes and procedures

SOFTWARE REQUIREMENTS

Windows 7
(32-bit and 64-bit versions)

Linux and Mac
OS support coming soon

Cloud and on premise
deployment options

ACHILLES PHOENIX EXTRA PROTECTION FOR YOUR WEAKEST POINTS

The most effective malware targets the same vulnerable applications and processes over and over again. Achilles Phoenix combats this with an exploit detection and prevention engine layered on top of vulnerable applications such as web browsers, desktop publishing software (such as Microsoft Office or Adobe Reader) and others. By “wrapping” these applications with Phoenix, Achilles can detect and prevent virtually all system exploits, including those that are not yet publicly known (also known as 0-day attacks).

STOP MALWARE AND ATTACKER IMMEDIATELY WITH NETWORK CONFINEMENT AND FIREWALL RULES

At RevBits, we stay one step ahead of attackers because we know how to think like hackers. One of the most common ways to gain access to a large network is to get access to an endpoint and then move laterally to other, more interesting systems.

Achilles Shield’s state-of-the-art detection and response capabilities allows you to define per-workstation firewall and network confinement rules when an infection occurs, thereby stopping attackers in their tracks and preventing them from pivoting to other systems in your network. Use the Achilles Shield control panel to set policies for network access that will automatically be enabled when an infection occurs. For example, you can configure your endpoints to only be allowed to connect to custom, whitelisted IP addresses

ONE CENTRALIZED, INTERACTIVE DASHBOARD

All security information and forensic evidence is tracked and managed from the Achilles Central Server, giving you instant insight into your whole network. The interactive dashboard provides a high-level view of security event counts, recent activity, and threat analysis, but also allows its users to conduct deep analysis with an extremely robust search and indexing feature. Run our dashboard right out of the box, or configure it to include custom indicators of compromise. The interactive dashboard equips system administrators and technicians to conduct expert analysis and quickly respond to incidents. All data is encrypted and remains on your secure, on-site host.

GRAPHIC FORENSICS TIMELINE

The clock is ticking and the pressure is mounting anytime there is a breach in your networked system. Achilles provides an easy to understand, real-time view of quarantined malware through its forensic timeline feature. The forensic timeline helps your administrators and technicians understand risks and quickly come resolve security issues. Best of all, if you combine an Achilles license with one of our Incident Response or Forensic Analysis service packages, you’ll rest easy knowing that RevBits is on call and ready to remediate any security concern, should the need arise.