Felix
enterprise security for everyone

Felix Next Generation Anti-Virus

IDENTIFY. ISOLATE. ERADICATE THREATS

Key Advantages

Integrated Automated Application Whitelisting and Anti-Malware

Active and Passive Whitelisting allows flexible protection for SOE and non SOE Environments

Security as a Service means you are always up to date and protected

High Security for your assets

Sophisticated machine learning to identify and adapt to threats

Designed from the ground up to have very low overheads to keep the total cost down

Felix Cyber Analytics leverages the Felix threat intelligence

Go beyond anti-virus with sophisticated High Security

Light Weight and Tiny Footprint, supporting 1 to 1000's of computers

Supported platforms

Windows 7, 8.x, 10 and Windows Server Environments

Automated Whitelisting and Anti-Malware

Suitable for small and large environments, the Felix NGAV uses a sophisticated combination of machine learning, threat intelligence and endpoint monitoring for indicators of compromise (IOC's) to build the list of approved and banned applications. It is designed to be used with zero requirement for your IT staff to keep the lists maintained, or to define policies around the applications that are allowed to be run. This keeps the costs of the managing the security of your Endpoints down and means that you don't need to invest in additional expensive security personnel to maintain and manage the lists on Felix NGAV.

Felix NGAV is a downloadable piece of software that can work with your antivirus to provide you an additional layer of IT security or as complete standalone protection. Its purpose is to prevent malicious software (Malware) from running on your computer. It does this by inspecting every application you open against sophisticated algorithms to ensure that what you are opening is not Malware. If it is, it will stop it before it does any damage to your system and you will get a little pop up window advising you that you have just been protected by Felix!

As with all our Felix products, we have designed Felix NGAV to be "Zero Touch". What does that mean? It means that unlike other security products, you don't have to do a single thing besides download the application from our website, fill out the registration details and click install. Once it's installed, you won't even know it's running, it requires no input from you whatsoever! We even automatically update the software whenever there is a new version, so you don't have to worry about remembering to update.

Felix NGAV has two running modes, Standard mode and Secure mode. Standard mode is our intelligent Anti-Malware solution that leverages our built in IOC's and Machine learning AI. In this mode, not only does it inspect all applications that execute to ensure they are not malicious, it also remembers the applications that have been opened, adding them to a list of "approved applications". In Secure mode, Felix NGAV locks the endpoint down and will prevent Malware and also not allow anything to execute that's not in the "approved applications" list (created while Felix NGAV was in Passive mode). Secure mode delivers our Zero-Touch Application Whitelisting solution.

Taking Your Security Seriously

Felix NGAV provides the much-needed additional layer of security and protection against the sophisticated variants of Malware such as Cryptolocker, APT's, including Zero-day Java Script and Java attacks, banking Trojans such as Dyre and Zeus Attacks and many other Malware threats.

The proliferation of malicious software using sophisticated techniques such as polymorphic code makes it particularly challenging for anti-virus vendors to keep up with the flood of new malware (up to 20,000 per day) that is seen on the internet. The Felix NGAV will provide an extra layer of assurance and security so that if malicious software enters your environment it will trap the software and stop it from causing further damage to your business.

Built-In

By combining machine learning, threat intelligence, and endpoint monitoring to build a list of approved and banned applications, Felix NGAV makes security an automated task, taking away the need for IT personnel to constantly update these lists and see to it that the end users know about it. This, in turn, reduces the cost of operations to a great extent. Its quick installation and lightweight nature are also laudable.

Zero Touch

Felix NGAV is constantly kept up to date from the latest Cybersecurity Protection from Felix's Hyperbolic Analytics Cyber Research. Because of the Automated Whitelisting and Anti-Malware, it is the first Zero-Touch product in the cybersecurity industry.

Intuitive

The use of Automated Learning Intelligence based on mathematical algorithms and statistical relevance means that the software does what is required on its own and constantly evolves. The pre-configured layers of security based on years of research provide it a solid base to begin its learning process and helps it keep you protected from the onset. Felix NGAV will provide full protection against all known threats and malicious malware and zero-day attacks when in Secure Mode.

Deployment

Due to Felix NGAV high degree of assurance when it comes to stopping malicious software and the seamless integration, Felix Security recommends that Felix NGAV is used to generate the approved applications list for your environment. As such, Felix NGAV is your recommended list master as all other installations of Felix NGAV or Enforcer can communicate to the Felix List Master (FLM) and pull the list of approved applications from the FLM. This provides you the confidence of knowing that all the endpoints in your environment (when run in Secure mode) will only run applications that Felix NGAV has first checked. It also reduces the cost of deployment to your environment, allowing you to deploy the Felix NGAV or Enforcer (Depending on your company's needs) to the majority of your Endpoints and only needing one instance of Felix Endpoint Protection (Felix NGAV) to generate the approved applications list for each Standard Operating Environment(SOE). Our goal is to provide "Enterprise Security for Everyone" and using the above deployment model not only provides a high level of cyber security, but it is also highly affordable.