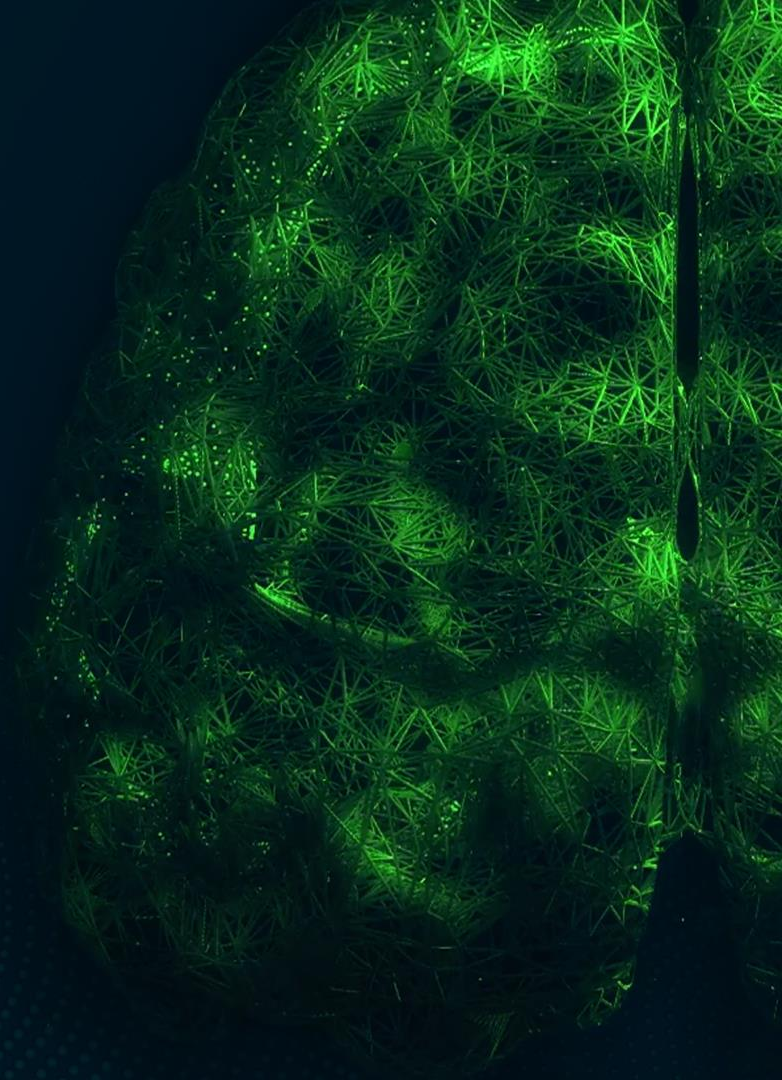
ERMES™

Intelligent Web Protection

Move to the real time human centric protection



ERMES
Intelligent Web Protection

PRICE MODULES END USER
LICENSING PER DEVICE*

SECURITY MODULES FOR A CUSTOMIZED OFFER
INVISIBLE USER
ZERO DAY PROTECTION (ANTIPHISHING)
EXTENSION VETTING (MALICIOUS BROWSER EXTENSIONS DETECTION)
BUSINESS ACCOUNT PROTECTION
CYBER SQUATTING & MALICIOUS URLS PROTECTION
CUSTOM CONTENT FILTERING

* “Device” stands for PC or Mobile per user, independently from browser used

ERMES
Intelligent Web Protection

PRICE MODULES – THREAT DESCRIPTION
INVISIBLE USER

Web tracking
The practice by which operators of websites (called Web trackers) collect, store and share information about visitors' activities on the World Wide Web. Analysis of a user's behavior may be used to provide content that enables the operator to infer their preferences and may be of interest to various parties, such as advertisers. In addition, should be considered that statistically each year more than 15% web trackers suffer a data breach due to a cyber-attack.

Session-replay script
Programming that enables a website users' keystrokes, clicks, mouse movements and scrolling behavior to be recorded along with the full contents of the webpage they are visiting. Session replay is a popular tool for helping companies determine how their websites are being used and for identifying potential problems such as broken links, page design issues or reasons users leave a site.

Malvertising
A portmanteau of "malicious software (malware) advertising", is the use of online advertising to spread malware. It typically involves injecting malicious or malware-laden advertisements into legitimate online advertising networks and webpages without directly compromising those webpages.

Crypto Jacking
Web services that force computers to use them to mine cryptocurrencies usually without users' knowledge. Cryptojacking services can lead to slowdowns and crashes due to straining of computational resources.

Insight: Link 1, Link 2, Link 3, Link 4, Link VIDEO

CONFIDENTIAL

PRICE MODULES – THREAT DESCRIPTION
ZERO-DAY PROTECTION (ANTIPHISHING)

Zero-day protection (antiphishing)

Phishers have become very nimble in their approach. About 85% of phishing sites exist for less than 24 hours, with an average life cycle of under 15 hours. There are even some cases where the site is active for as little as 15 minutes. The short lifecycle and fast-paced nature of many of these phishing campaigns does not generally provide enough time for these sites to be properly analyzed and placed on blacklists.

Insight: Link 1, Link 2, Link 3, Download Whitepaper

PRICE MODULES – THREAT DESCRIPTION
EXTENSION VETTING

Extension-Vetting

Malicious extensions are dangerous software that can inject malicious code into pages to cause malware downloads, steal credentials, redirect to fake pages and so on. Extension vetting is the ability to analyze and rate the behavior of any browser extension so that users and IT administrators can then decide whether to install or dis-install extensions.

Insight: Link 1, Link 2, Link 3, Download Whitepaper

PRICE MODULES – THREAT DESCRIPTION
BUSINESS ACCOUNT PROTECTION

Business account protection

Despite the usual existence of written policies on the legitimate use of company accounts, employees tend to reuse their business credentials on sites not related to work activity (for example e-commerce, social networks, forums), thus expanding the risk surface for credential loss. Thanks to Ermes, it is finally possible to enforce account usage policies, preventing users to signup or login to non-work related sites using their business account. Also, this feature is a further layer of protection against advanced credential phishing attacks, such as the new Browser In The Browser technique.

Insight: Link 1

ERMES
Intelligent Web Protection

PRICE MODULES – THREAT DESCRIPTION
CYBERSQUATTING & MALICIOUS URLs PROTECTION

Cybersquatting
The attack technique that uses web domain names which resemble and/or sound like famous legit ones to trick the visitor thinking he/she is visiting the legit counterpart to encourage conducting the same activity he/she would do on the legit website, e.g., buying products, logging to a service, and so on, ultimately giving to hackers very sensitive information.

Malicious URLs
A URL (Uniform Resource Locator) is categorized as malicious when the service that provides, whatever it is, is recognized for having malicious behaviors. Bad URLs can be created and used, for example, as a malware distribution point, or they can refer to a website which executes attacks such as downloading and installing an infected executable on the user machine or steeling sensitive information. Users can encounter malicious URLS while browsing and from emails.

Insight: Link 1, Link 2, Link 3

ERMES
Intelligent Web Protection

PRICE MODULES – THREAT DESCRIPTION
CONTENT FILTERING

Content filtering

Most of the websites on the Internet are categorized based on the purpose they were created for or the contents they provide. Content Filtering is the ability to block or allow websites based on their categorization. The benefit of having this kind of feature is to make sure that company devices don't have access to unnecessary websites and also decrease the risk surface avoiding all categories that typically hide threats.

CONFIDENTIAL