ESET MSP PROGRAM

OPTIMIZED ANTI-RANSOMWARE

Some common ransomware infection scenarios, and how ESET security solutions allow you to optimize settings to protect your clients.

Why these additional anti-ransomware settings?

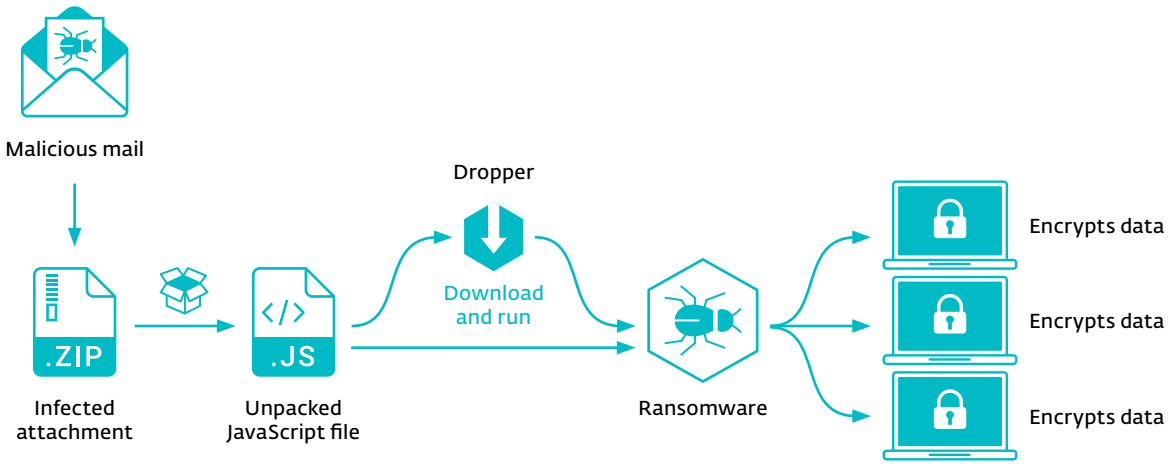
Ransomware relies on JavaScript — but as it has many legitimate uses, we do not routinely block the execution of JavaScript, as this could cause problems for regular users. However, here we share with you, our professional MSP partners, a range of extra settings that will allow you to help your customers harden the security of their networks.

“Our anti-ransomware setup has been successfully tested and implemented by hundreds of organizations. It comes as a package of policies, that you can easily import into your ESET console.

A typical email ransomware attack

Current ransomware attacks use advanced infection techniques that persuade users to execute a so-called **dropper**, which in turn downloads the malicious malware payload to start the encryption process.

In most cases, a **phishing mail** is used to deliver the dropper, with a ZIP file containing a “.js” JavaScript file. Hackers will heavily obfuscate the malicious JavaScript code in order to prevent its detection.

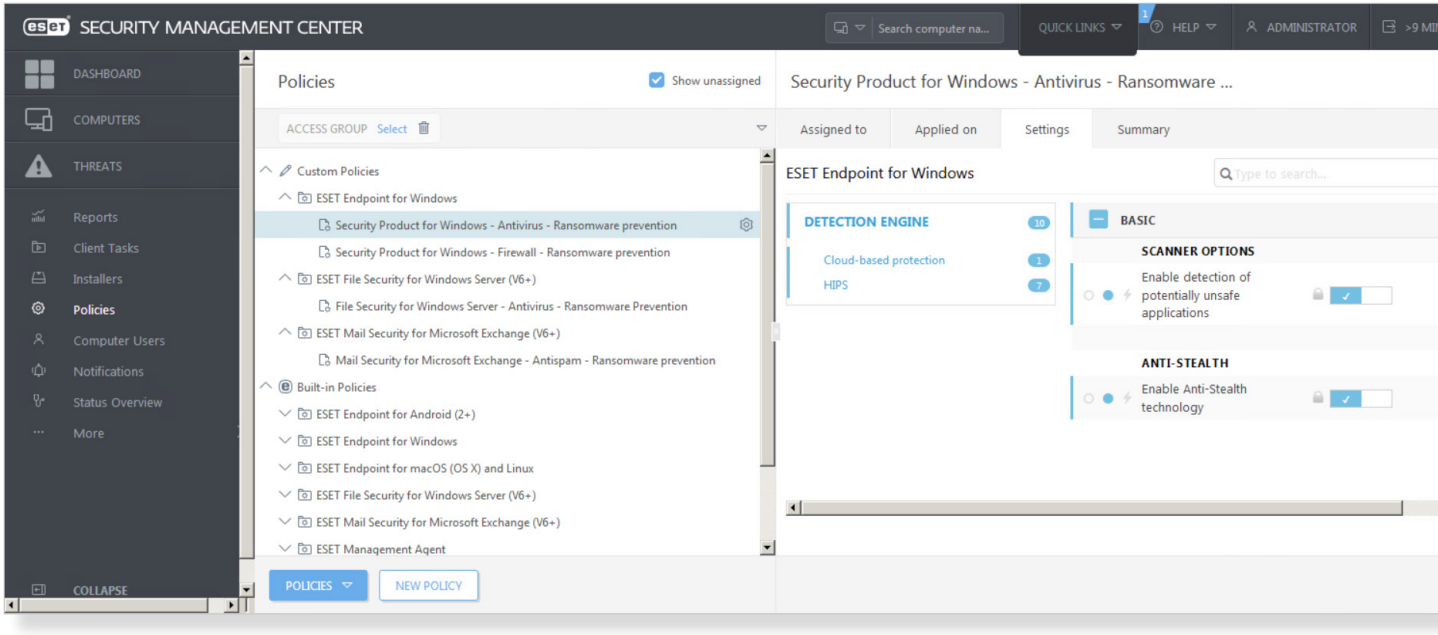


Our multilayered anti-ransomware approach

Anti-ransomware modules

The anti-ransomware setup we offer is intended to **block infection** by preventing the JavaScript dropper from doing its job. ESET security solutions comprise **multiple security modules**. The following are important for ransomware detection:

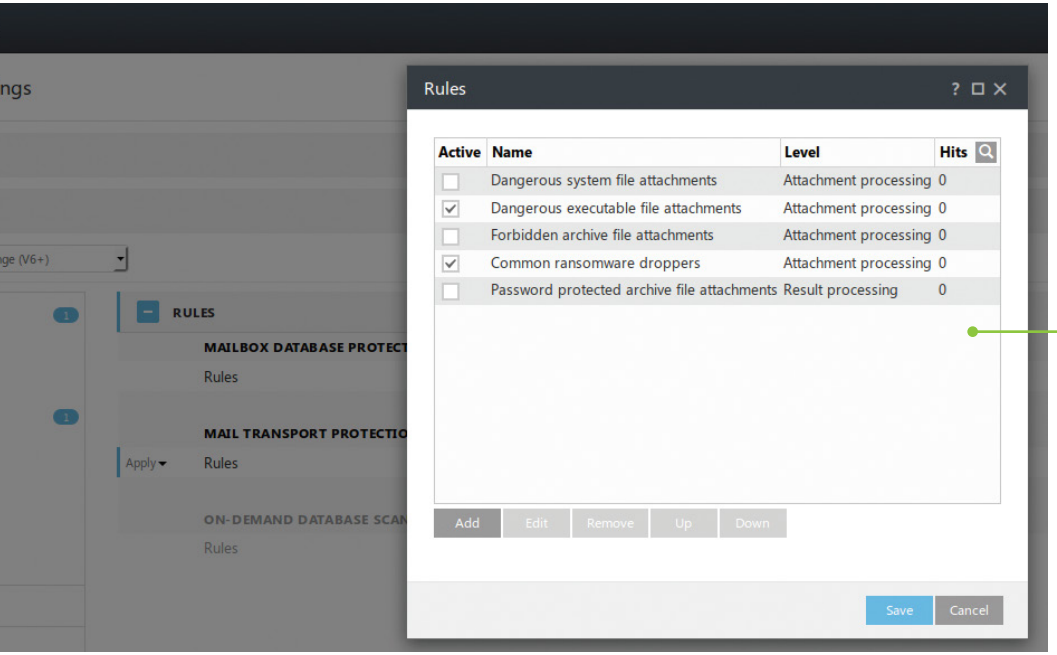
1. **Antispam** (in ESET Mail Security for Exchange only)
2. **HIPS** — Host-based Intrusion Prevention System
3. **Firewall**
4. **Additional** protection modules (LiveGrid, Botnet Protection, etc.)



Custom anti-ransomware settings added to ESET Security Management Center

1 Antispam module rules

Using the antispam rules within our anti-ransomware setup, incoming emails are filtered for ransomware on the mail server, ensuring that any attachment containing a malicious dropper is not delivered to the end-user.



Blocked filetypes

- Windows Executable (*.exe, *.dll,* .sys*, *.drv; *.ocx, *.scr)
- MS-DOS Executable (*.exe)
- ELF Executable and Linkable format (for example, Linux) (*.elf)
- Adobe Flash (*.swf)
- Java Class Bytecode (*.class)
- Windows Installer Package (*.msi)
- Apple OS X Universal binary executable
- Apple OS X Mach-O binary executable
- Android executable (*.dex)

What do the additional ESET rules do?

The antispam rules block two groups of objects:

1. Dangerous executable file attachments
these are filtered out and **immediately deleted** before they even reach users' mailboxes

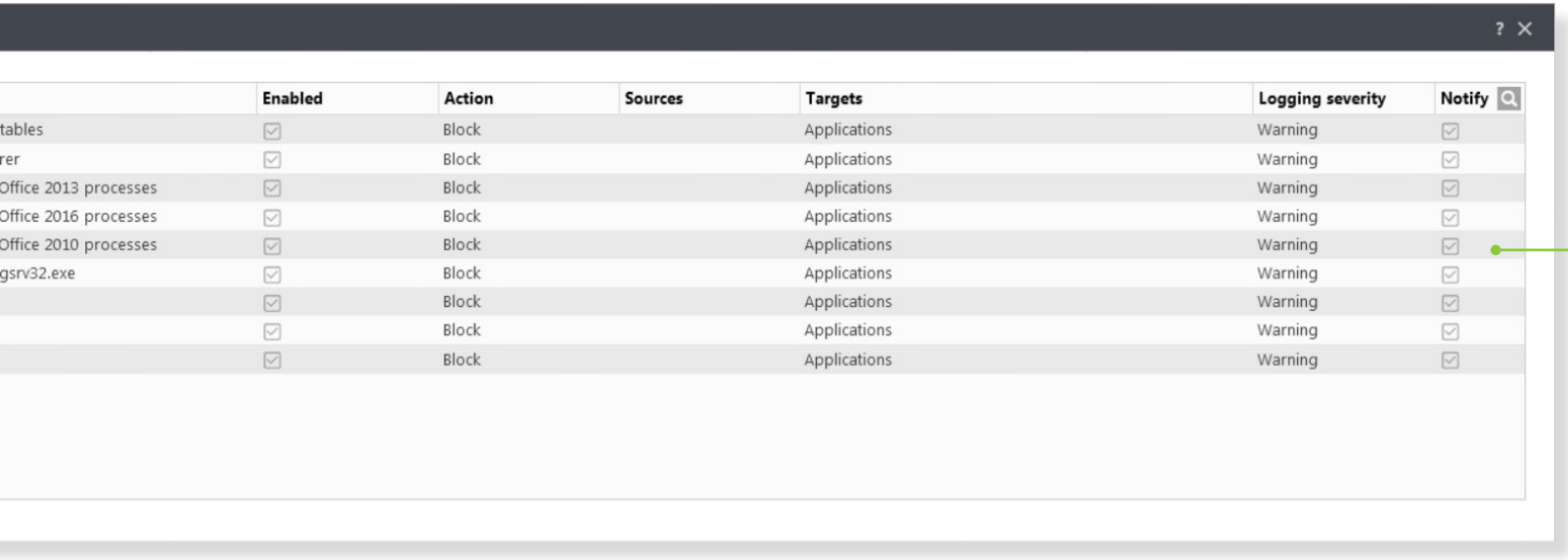
2. Common ransomware droppers
specific file extensions are **quarantined**

2 HIPS module rules

ESET's Host-based Intrusion Prevention System (HIPS) defends your client's systems from within, and is able to interrupt unauthorized actions in processes before they execute.

By prohibiting the standard execution of JavaScript and other scripts, **it prevents ransomware from being downloaded or executed**.

HIPS is also part of **ESET File Security for Windows Server**, making it applicable to servers.



	Enabled	Action	Sources	Targets	Logging severity	Notify
tables	☑	Block		Applications	Warning	☑
rer	☑	Block		Applications	Warning	☑
Office 2013 processes	☑	Block		Applications	Warning	☑
Office 2016 processes	☑	Block		Applications	Warning	☑
Office 2010 processes	☑	Block		Applications	Warning	☑
gsrv32.exe	☑	Block		Applications	Warning	☑
	☑	Block		Applications	Warning	☑
	☑	Block		Applications	Warning	☑
	☑	Block		Applications	Warning	☑

Deny child processes started by explorer

- wscript.exe
- cscscript.exe

Deny child processes from dangerous executables

- wscript.exe
- cscscript.exe
- powershell.exe
- ntvdm.exe

Deny child processes from Office 201x processes

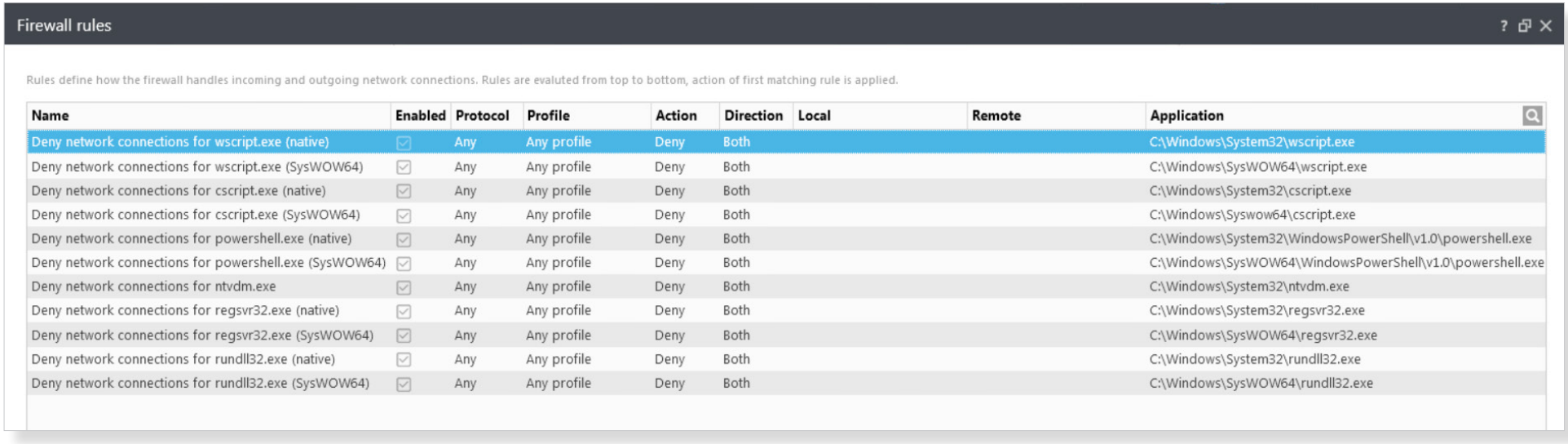
- winword.exe
- outlook.exe
- excel.exe
- powerpnt.exe

3 Firewall module rules

Should a ransomware dropper with malicious JavaScript code be executed, ESET Endpoint Security still prevents the download of malware thanks to its integrated firewall.

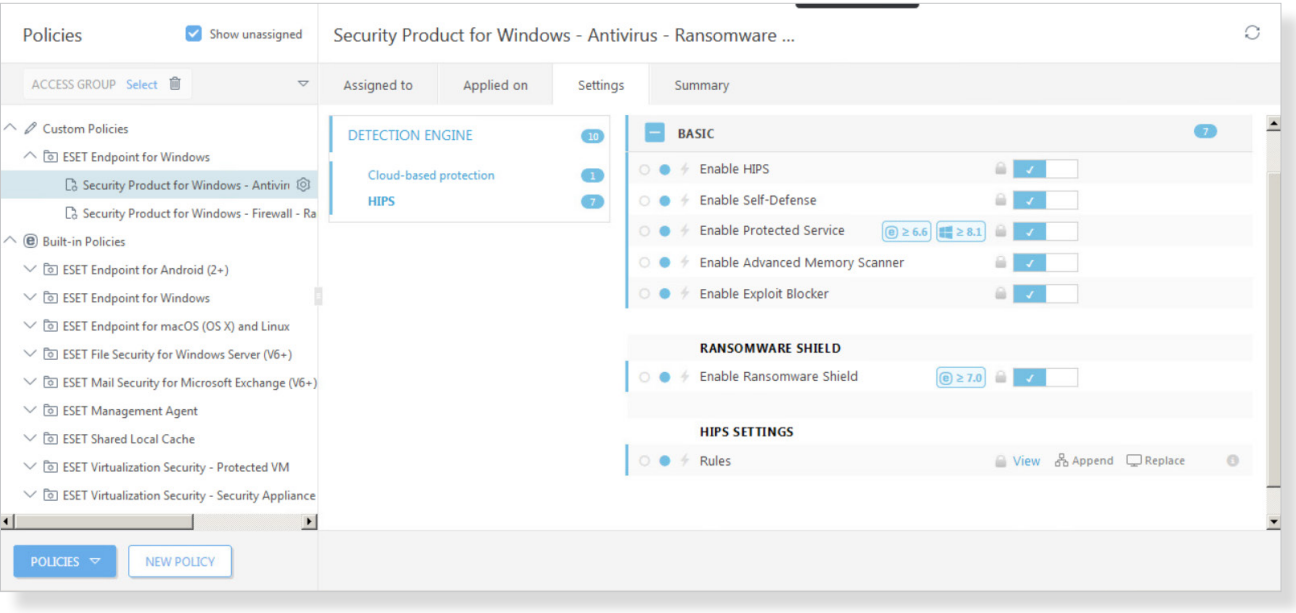
What do the additional ESET rules do?

They deny network connections to specific processes, both for incoming and outgoing communications.



4 Additional ESET protection modules

Using our setup, you can ensure that the following ESET modules are turned on. This is an additional measure against unauthorized tampering with modules that are crucial for ransomware detection.



ESET LiveGrid reputation system – Compares scanned files to a database of whitelisted and blacklisted items in the cloud.

Advanced Memory Scanner – Monitors malicious processes and scans them once they decloak in memory.

Exploit Blocker – Closely monitors typically exploitable applications (browsers, document readers, email clients, Flash, Java, and more).

Ransomware Shield – Detects and blocks processes whose behavior resembles ransomware.

Botnet Protection – Detects malicious communication used by botnets, and identifies the offending processes.

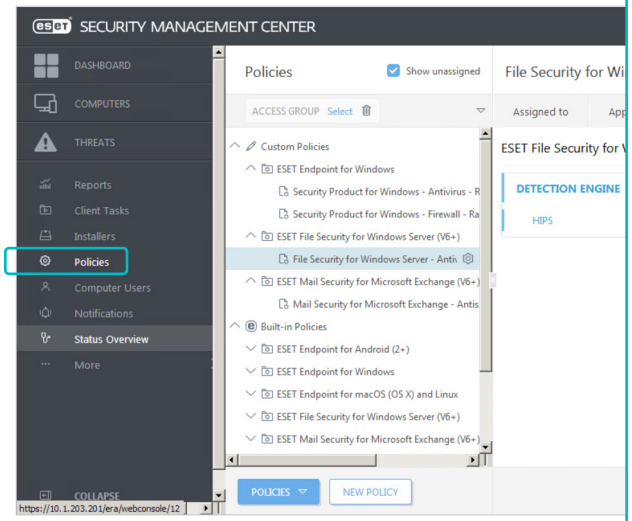
Self-Defense – Prevents malicious software from corrupting or disabling Antivirus and Antispyware protection.

Protected Service – Enables kernel protection (this option is available in Windows 8.1 and Windows 10).

Implementing our anti-ransomware setup

After downloading our anti-ransomware policies, implementing them on your clients' systems takes just 5 easy steps, within ESET Security Management Center (ESMC).

1. Download your anti-ransomware setup
2. Log in to ESMC Webconsole
3. Navigate to the Policies section
4. Then click "Policies" at the bottom and select "Import"
5. Import the policies one at a time
6. Adjust the policies to a group or client



The policies are deployable with ESET Endpoint Antivirus, ESET Endpoint Security, ESET Mail Security for Microsoft Exchange Server, and ESET File Security for Windows Server.

ESMC also lets you perform any additional changes that you identify during testing, such as removing specific extensions or modifying rules.

Be careful with executable files

Legitimate applications can use executables. Also, some organizations may be using scripts for production purposes. Please test before fully implementing the policies within your area!

Don’t forget about ransomware attacks via RDP!

Now that you have email-based ransomware covered, don’t forget about Remote Desktop Protocol! RDP is increasingly being used by hackers to disable protection and then drop ransomware onto target machines.

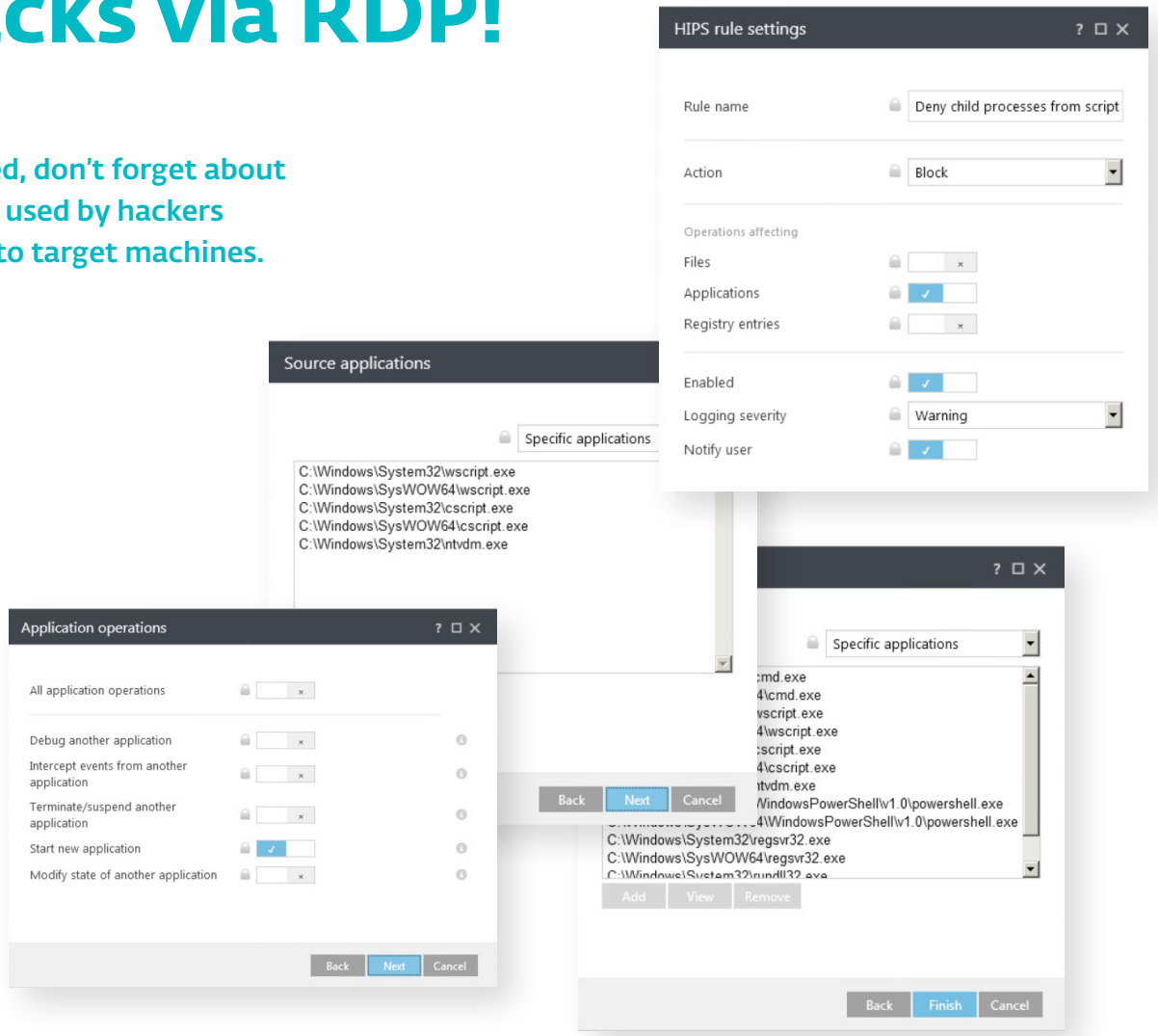
You can protect your customers in two ways:

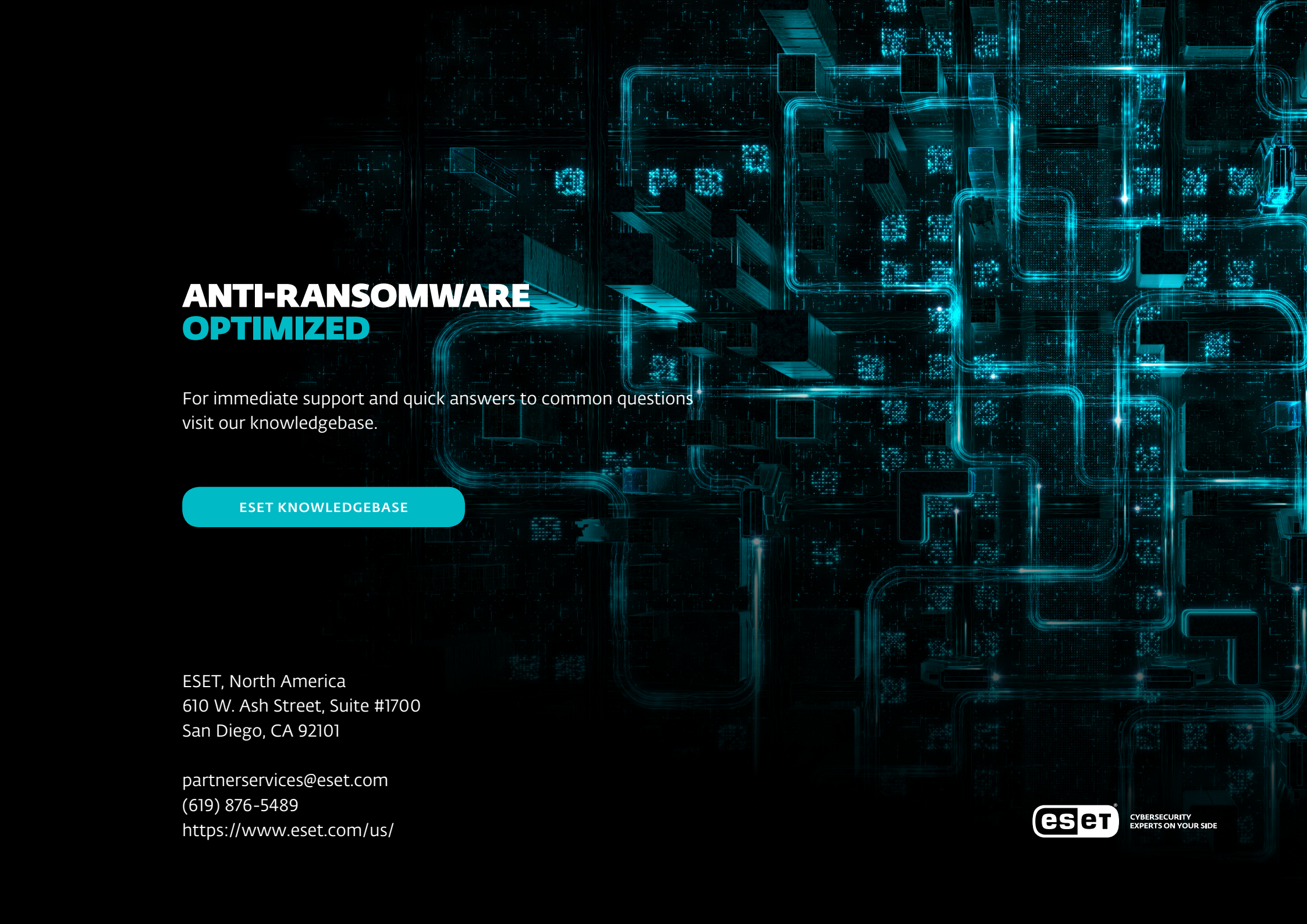
1. Disable or change RDP

If your clients do not require RDP, you can change the default port or disable RDP in order to protect machines from exploits.

2. Password-protect your ESET product settings

If your clients need to keep RDP running and cannot disable or change the RDP settings, you can use a password to protect the ESET product from unauthenticated modification of settings, disablement of protection, or even uninstallation.





ANTI-RANSOMWARE OPTIMIZED

For immediate support and quick answers to common questions visit our knowledgebase.

ESET KNOWLEDGEBASE

ESET, North America
610 W. Ash Street, Suite #1700
San Diego, CA 92101

partnerservices@eset.com
(619) 876-5489
https://www.eset.com/us/

CYBERSECURITY EXPERTS ON YOUR SIDE