Rebasoft

Fighting ransomware

Use case

Datasheet

The world has entered a new era of ransomware

Unstable political conditions, increased sophistication of attacks and a reliance on new, rapidly evolving technology have created conditions ripe for ransomware. You can see this in the recent series of highly publicised attacks.

And there's no slowing down. According to Unit 42 Ransomware Threat Reports, the average pay-out of a Ransomware attack has increased from £500,000 to £800,000 in 2022.

There are now ransomware gangs posting job positions for negotiators online. Hackers are selling access to breached companies and offering hacking as-a-service. These aren't teenagers in mum's basement anymore. These are professionals. This is an industry. It has it's own ecosystem and supply chains.

> *"Ransomware is the monetisation of poor cyber hygiene"*

Are you at risk?

You are a prime target for an attack if:

- Your **hardware is outdated**
- Your **software is outdated**
- Your **browsers and operating systems are unpatched**
- You have **no backup plan**
- You have **not paid enough attention to cyber security**

What can you do?

Experts recommend taking proactive measures to prevent ransomware:

- **Create an incident response plan**—this should be reviewed and updated regularly
- **Back up your data often**—if you have an up-to-date backup that attackers have no access to, then they have no hold over you
- **Create and maintain an accurate up-to-date asset inventory**—you can only protect what you can see
- **Identify and remediate misconfigurations**—65% of cyber attacks exploit simple misconfigurations in devices
- **Ensure antivirus & firewall coverage** across all devices
- **Regularly patch and update your software**—most ransomware attacks exploit known vulnerabilities which should be patched
- **Implement a robust access control system**—it's important to ensure users only have appropriate access
- **Get cyber insurance coverage—**it can make the initial hit much more manageable
- **Conducting regular security audits and penetration testing**—to identify and address vulnerabilities within your network
- **Continuously monitor network behaviour** to identify threats

> *"64% of reported breaches are detected by people and not technology"*

Practice and educate employees on safe browsing practices

- **Never click on unsafe links**—avoid spam links and unknown websites
- **Avoid disclosing personal information**—always check who is asking for your information, attackers might be collecting it in preparation for an attack
- **Don't open suspicious email attachments**—pay close attention to the sender and that the email address is correct
- **Never use unknown USB sticks**—cybercriminals leave infected storage devices in public places in hopes someone will use it
- **Only use known download sources**—make sure there is a shield or a lock icon next to the address bar in browsers and only use the Google Play Store or the App Store for mobile downloads
- **Use a VPN on public Wi-Fi networks**—you are more vulnerable on a public Wi-Fi

How Rebasoft can help

While Rebasoft alone is by no means a "silver bullet" for ransomware, it does provide the functions of multiple cyber security programs. We help you prevent ransomware in these areas:

- **Create and maintain an accurate, up-to-date asset inventory**
- **Identify and remediate misconfigurations** in your devices
- **Identify and manage vulnerabilities**
- **Ensure antivirus, anti-malware and firewall coverage**
- **Identify threats faster** through behaviour monitoring
- **Implement a robust network access control** solution

How we provide value

Rebasoft discovers, assesses and tracks security compliance all from one platform.

- **A single deployment** collecting and consolidating information means you don't need to manually collate and report on data
- **Integration into asset management** means you do not need to waste hours tracking down systems that need security remediation
- **Lightweight**—collecting information effectively and automatically reduces the load on managed IT systems
- **Fewer systems and automation** helps reduce complexity and workload on busy IT teams
- **Automation** reduces manual tasks and human error

> *"... if you have a number of alerts being triggered in ten different systems it is quite hard to track them through to conclusion. One system allows us to easily drill through to the issue and rapidly resolve it"*
>
> *CIO, Hi-tech*

How you can help prevent ransomware with Rebasoft in 5 steps

1. Discover

- Discover all IT assets on your network in real-time
- Find all home workers though MDM's like Intune

2. Classify

- Automatically classify devices to create a detailed asset inventory
- Set criticality to prioritise important assets

5. Defend

- Implement an automated network access control policy to quarantine suspicious devices
- Identify threats by continuously monitoring for unusual network traffic
- Report on effectiveness

3. Assess

- Continuously asses misconfigurations and non-compliant devices
- Remediate misconfigurations

4. Monitor

- Continuously monitor for vulnerabilities
- Send emails to users with easy one-click-fixes for automatic patching
- Manually patch vulnerabilities that aren't handled automatically

But that's just the start

Using the asset discovery system as a base, Rebasoft provides the functionalities of multiple cyber security programs like:

- **Asset management**
- **Secure configuration**
- **Vulnerability management**

So with Rebasoft. you can cover the same ground with less solutions. So, you can save money and reduce complexity, because it's all seamlessly integrated.

So why not find out more by booking a live demo with an expert?

Try it now

There's nothing like seeing it in action. After all, you wouldn't buy a car without test driving it.

BOOK A DEMO

Contact us

You can also get in touch via phone or email. We'll happily answer any questions.

Phone: +44 (0) 800 779 7322

Email: sales@rebasoft.net

21 London Road
Twyford
RG10 9EH
United Kingdom

About us

We at Rebasoft are committed to delivering a robust cyber security solution that addresses genuine business needs. We are not interested in a "silver bullet" approach. We believe that multiple functionalities from one platform and real-time data are essential for keeping up with today's cyber threat landscape. We believe this approach is the future of cyber security and we aim to be the pioneers. We are proudly a UK based company. Visit us at www.rebasoft.net

Rebasoft is still owned and managed by the original founders:

Philip Harragan
CEO & Founder
LinkedIn - Facebook

Steve Wilkinson
CTO & Founder
LinkedIn - Facebook - Twitter