NIL Malware Protection Solutions

Customer-specific prevention of business-impacting malware

Do you still think you are not a target?

While the most serious malware attacks are targeted against a specific organization, and the hardest (but very possible) to defend against, criminals today cast an extremely wide net that attempts to infect EVERYONE, and based on this large volume, provides significant financial gain as malware indiscriminately infects consumers and businesses alike.

Therefore, without a suitable malware protection system, not relying on a single “magical” software program, it is only a matter of time before a business suffers significant financial loss – either through extortion (ransomware) or the astronomical cost of complex system repair.

Computer malware (ransomware, viruses, Trojans, logic bombs, etc.) has traditionally been a threat that attacks consumers and businesses alike, thereby primarily causing denial-of-service, such as the deletion of data or corruption of systems. Legacy technologies, such as anti-virus software, have outlived their effectiveness many years ago, and even modern extensions to anti-malware desktop and server software do not satisfactorily protect you against modern malware threats.

Today, all businesses are at a significantly higher risk from malware, as modern malware has become a tool of criminals: extortion through ransomware and theft of personal and financial data represent 90% of the motivation behind the current Internet-sourced attacks. In addition, because of the simplicity of malware creation, and consequently large-scale infection epidemics inside organizations, the costs for remediation have now soared up to 100,000 to millions of dollars per incident.

Deliverables

- Customer audit, consulting, and requirements analysis
- Malware Protection System design
- Malware Protection System implementation
- Malware Protection System support and
- operations/incident response (if needed)

Typical Use Cases

Organizations with a high risk of ransomware and targeted malware

Organizations with complex systems and processes that use legacy anti-malware solutions

People, network, or endpoint defense? It should not be an exclusive choice.

One can only prevent modern malware by using a welldesigned **system of countermeasures** that brings together several technologies and teams. Our security philosophy is that protection solutions are much more effective when tailored to the individual customer, for which we have ample evidence in the failure of generic, consumer-grade anti-malware systems in the past.

Our malware protection solutions take a holistic view of your organization, and they design countermeasures by using:

- A clear solution design based on your environment's process (user roles and needs) as well as the technology needs and limitations.
- Network countermeasures, such as content filtering, content striping, true sandbox execution, traffic signature, policy, and anomaly analysis, URL and reputation filtering, classic network segmentation and firewalling, cloud sampling, etc.
- Endpoint countermeasures, such as content analysis, cloud sampling, application whitelisting, full application sandboxing and/or containerization, etc.
- Process countermeasures, such as user training (based on role), development of proactive and reactive/ response processes, policy development, etc.
- Correlation of many information sources to improve the detection rates and data quality and, therefore, reduce the administrative load.

We help you sleep soundly at night: effective prevention of day-zero malware and targeted malware

Day-zero (previously unseen) malware used to be rare, as it had to be written anew and/or specifically for a target organization. Today, such malware can be easily purchased from online shops in the price range of some hundred dollars per package.

Day-zero defense is, therefore, acutely needed by all organizations seeking non-trivial defense, as the investment threshold for using these modern cyberweapons is currently very low. Our malware protection solutions employ a variety of complementary countermeasures designed specifically to fight day-zero malware: from process defenses, for limiting potentially dangerous content to specific user roles, to technology defenses, such as network and endpoint sandboxing, whitelisting, selective/critical software patching, etc.

We conduct an extensive audit of your environment, needs analysis, and threat modeling specific to your environment.

We do not carry out run-of-the-mill projects, because you and your IT environment are not run-of-the-mill: they are complex, interdependent systems that have evolved to support your specific processes over time. Our typical team, therefore, comprises IT architects, penetration testers, and system designers in order to build a solution that is effective, user-friendly, and manageable for YOUR individual organization.

References

In the field of malware protection, we are trusted by large and complex financial, health, industry, and government agencies. As most of our projects involve strict confidentiality agreements, abstracted examples of such projects are available upon request.

Why NIL?

- More than 20 years of experience in zero-day malware protection
- Reliable multi-technology, defense-in-depth solutions
- Consulting and help with an incident response

About NIL

NIL part of Conscia is a globally recognized provider of advanced data center, network, cloud, and cybersecurity solutions, as well as services for business and industry environments, state institutions, public organizations, and telco companies.

By enabling a more efficient, secure, and reliable way of doing business, NIL helps organizations become more successful in the digitalized world.

NIL is part of the Conscia Group.

For more details contact **consulting@nil.com** | NIL Ltd., Baragova ulica 5, 1000 Ljubljana, Slovenia | www.nil.com