# Ransomware Protection Best Practices

www.sangfor.com

SANGFOR

Gartner analysis of clients' ransomware preparedness shows that over 90% of ransomware attacks are preventable. These attacks pose a threat to business data and productivity, but by following basic security fundamentals security and risk management leaders can mitigate risk against them.

**(Quote: Gartner, https://www.gartner.com/en/documents/3978727/defend-against-and-respond-to-ransomware-attacks)**

In early 2020, the Coronavirus (COVID-19) showed particularly sinister traits, including infected patients who showed no signs or symptoms but continued to be extremely contagious. How do we prevent infection without the ability to see it coming? We take precautions and follow the best practices recommended by professionals, such as avoiding crowded places, washing hand frequently, and self-isolating.

Similarly, most ransomware remains dormant and invisible for weeks or months until activated. While the infected hosts not only causing damage to the business operation, but they are busy infecting other systems as well. We should all take precautions and follow best practices to ensure the chances of attack are low, and the impact is minimized, should a ransomware attack be launched.

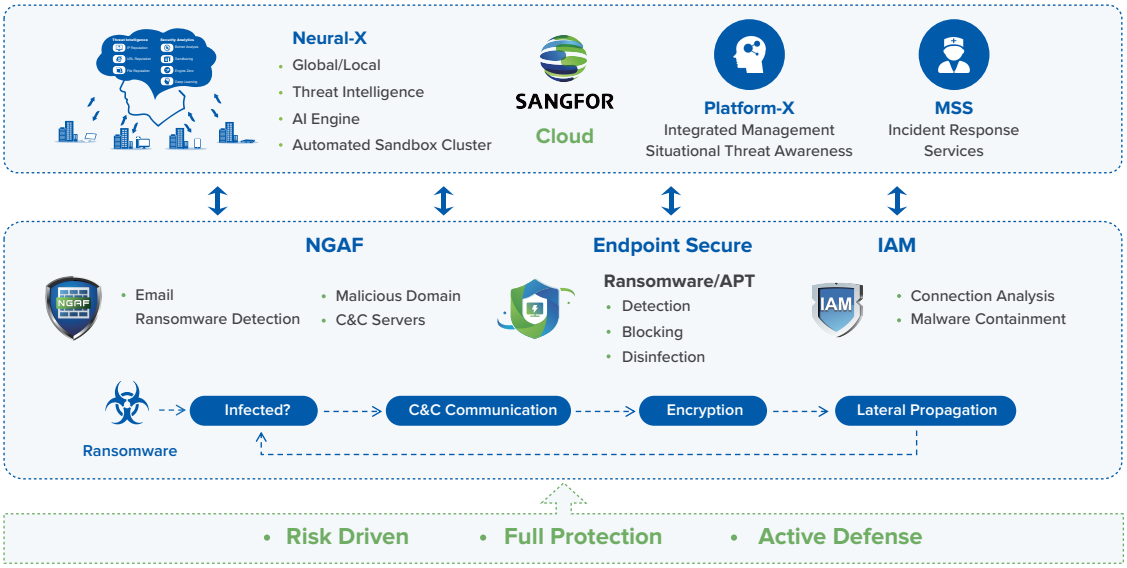
Do not make the mistake in thinking that you will be the lucky one who will never be attacked and crippled by ransomware. Just as with COVID-19, prevention will always be preferable to waiting for symptoms of infection and then searching for a cure.


This final stage is often skipped as the business moves back into normal operations but it's critical to look back and heed the lessons learned. These lessons will allow you to incorporate additional activities and knowledge back into your incident response process to produce better future outcomes and additional defenses.

**(Quote: CSO Online, https://www.csoonline.com/article/3515234/the-six-stages-of-incident-response.html)**

But of course, aside from taking preventative measures, learning a lesson from past experiences and those who have suffered an attack is important for an organization in the fight against ransomware. Some organizations look at ransomware statistics and mistakenly think, "It will never happen to me," and thus ignore vital elements of protection, like setting sufficient security controls, implementing proper security practices and improving or overhauling their security capabilities. These are the institutions at the most risk.


Sangfor offers solutions that go well beyond helping organizations defend themselves from ransomware, by providing their years of expertise to assist in incident response and creating a comprehensive roadmap of how the crisis found a foothold within the system, helping organizations learn vital lessons in prevention.




**Feel free to talk to Sangfor local sales representatives to find out more. You can also contact us by sending an email to marketing@sangfor.com.**

As a service to those seeking security information, Sangfor offers the following best practices suggestions in hopes of helping to reduce the risk of ransomware attack and protecting the most at-risk attack surfaces.

***Stay safe out there!***

| Best Practices | |
|---|---|
| 1 | Backup important data regularly and ensure the backup server is not on the same segment as the production environment. Offsite backup is recommended. |
| 2 | Regularly apply the latest security patches to hosts, software and applications. |
| 3 | Conduct security assessment periodically to ensure no vulnerabilities and misconfigurations on present. |
| 4 | Implement VLAN segmentation and enforce whitelisting policies. |
| 5 | Implement perimeter and internal firewall to block unauthorized traffic. |
| 6 | Ensure licensed antivirus is installed on each host and that the virus signature database is updated frequently. |
| 7 | Perform regular bi-yearly review of firewall rulesets to ensure all firewall rules are well in place. |
| 8 | Apply access controls to Internet browsing activity to limit authorized users to browsing on work-related websites. |
| 9 | Restrict and control downloads from the Internet. |
| 10 | Enforce a strong password policy, insisting on a complex password for every account on each host and network security equipment. |
| 11 | Perform server security hardening before migrating to the production environment. |
| 12 | Perform server and network security product configuration reviews to ensure that all settings and configurations are secure. |
| 13 | Ensure high availability and redundancy on servers that support critical business operations. |
| 14 | Ensure no unnecessary ports are exposed to the Internet. |
| 15 | Think critically before downloading, executing unknown files and click on unknown links. |
| 16 | Do not attached unknown external storage drive or connect to unknown wireless network. |

## Why Sangfor?

Just as you aren't alone in trying to navigate new global developments and keep your business profitable – you aren't alone in meeting your technology needs. With 20 years of experience producing best-in-class security and cloud computing products to enable any size business, anywhere in the world, Sangfor has everything you need to keep your data secure, employees connected and business flowing. Sangfor sees real world solutions to modern problems.

Sangfor Technologies is an APAC-based, global leading vendor of IT infrastructure solutions specializing in Network Security and Cloud Computing. Visit us at **www.sangfor.com** to learn more about Sangfor's network security options, and let Sangfor make your IT simpler, more secure and more valuable.