Acronis

WHITEPAPER

Five Phases of Cyber Immunity: **Acronis** Cyber Protect

How health practices can help our digital well-being

Considering the human body contains about 40 trillion cells and roughly the same number of bacterial cells, it's astonishing that such a complex system with so many complex functions can usually operate without a problem. The complexity is mind-boggling.

Modern computer systems are significantly less complex. They typically have 40 billion processing elements and 10-times as many memory elements. Each of these elements has a comparatively simple structure with a very narrow and specific function, which is then optimized to perform its function at billions of cycles per second (as opposed to human neurons, which fire at 200 cycles per second). Despite their relatively simple structures, these elements enable computers to communicate with each other very quickly and over very long distances – creating their own challenges of complexity.

This whitepaper explores how biological and digital threats are similar, and shows how Acronis Cyber Protect takes advantage of the unique properties of computer systems to deliver the ideal anecdote to the modern risks to data, applications, and systems – enabling MSPs to help their clients become digitally immunized and #CyberFit.

Similarities of biological and digital systems

History has shown many cases where computer viruses tried to mimic their biological namesake. HIV attacks the human immune system, for example, making humans more vulnerable to other diseases. Some malware strains take a similar approach, disabling the anti-virus tools in a machine's operating system (OS) to weaken the overall security – as Conflicker does to Windows and Shlayer to macOS.

Another clever cybercriminal tool, called Double Agent, turns anti-virus solutions into malware that attacks the system, just as an autoimmune disease instructs the body's own defenses to attack healthy tissue.

And just as outbreaks in the real world like hand-foot-and-mouth disease are made worse by poor hygiene, unhealthy habits in the digital world can make cyberthreats much worse. The WannaCry ransomware attack was able to explode into a global epidemic not because it was particularly sophisticated, but because victims had not applied available security patches to their systems – a basic practice of good computer hygiene.

Looking at these similarities, it's easy to see how early detection and containment of new pathogens are essential for both physical and digital health.

When thinking about other ways to fight the threats of the outside world, there are other lessons we can learn by comparing biological to cyber systems. That's because in both cases, the steps follow five main phases: prevention, detection, response, recovery, and forensics.

1. Prevention

In preventing biological diseases, there are four approaches:

- **Healthy habits**. Eat well, sleep well, exercise, and avoid too much stress. Together these actions make our bodies healthier, stronger, and more resilient – and better able to fight off disease. Regular doctor visits also help support good health.
- **Good hygiene.** Simple acts like washing our hands, taking daily showers, and keeping our homes clean, especially kitchen and bathroom surfaces, reduces the risk of infection by eliminating unnecessary exposure to harmful bacteria and viruses.
- **Vaccination.** By exposing our bodies to weakened, controlled strains of known pathogens, we can train the immune system to effectively counter more dangerous strains in the future.
- **Isolation.** In high-risk environments, wearing personal protection equipment (PPE) such as masks or suits can stop transmittable diseases from spreading, isolating dangerous pathogens.

These same approaches can be also be applied in computer systems to prevent harm:

- **Healthy habits.** Regular analysis and testing of your system build resiliency, as does identifying and addressing potential weaknesses. Acronis Cyber Protect keeps your systems in good shape by periodically checking for vulnerabilities and installing the latest patches. It also includes a self-protection mechanism similar to the body's immune system, which ensures your protections are operating to keep you #CyberFit.
- **Good hygiene**. Just as simple actions like washing hands are critical, IT users need to learn to best practices for preventing infections – such as not downloading dubious software, avoiding questionable websites, being cautious of links, and not believing what strangers tell you, even if they pretend to be your friend.

  It's also important to keep your data organized because even if your data is safe and uncompromised, it is useless if you don't know how to access it. Also, it is critically important to run regular backups.

  And just as a doctor can advise you about health dangers, staying well-informed and alert can help you avoid new dangers. Our global network of Acronis Cyber Protection Operation Centers (CPOC) offers smart alerts to help IT stay clear of even the newest dangers, while their Smart Protection Plans can protect all of your data, even when risk levels are rising.
- **Vaccination.** While certain software can strengthen your system's defenses, Acronis Cyber Protect is your computer's immune system. Like its biological counterpart, it detects and neutralizes dangerous foreign substances in your system before they can do any harm. That's because Acronis Cyber Protect has integrated defenses based on rules provided by the Acronis Cyber Engine. Since this engine is distributed, all protected computers benefit when it learns of new malware – establishing instant immunity to these new threats, just like a vaccine.
- **Isolation.** Sandboxes, containers, network firewalls, intrusion prevention systems (IPS), and network filters are all designed to isolate malicious software and agents before they ever reach your system, keeping it safe from harm.

2. Detection

Our bodies detect pathogens by scanning for bacterial cells or viruses that have certain attributes, determining if they are "domestic" or "foreign". Cytotoxic t-cells, for example, flag foreign entities as dangerous, activating the immune system to counter the attack.

This biochemical detection process is highly complex and sometimes it can go haywire – flagging the body's own healthy cells as threats, which turns the body against itself. While autoimmune diseases like this are rare, they are extremely dangerous.

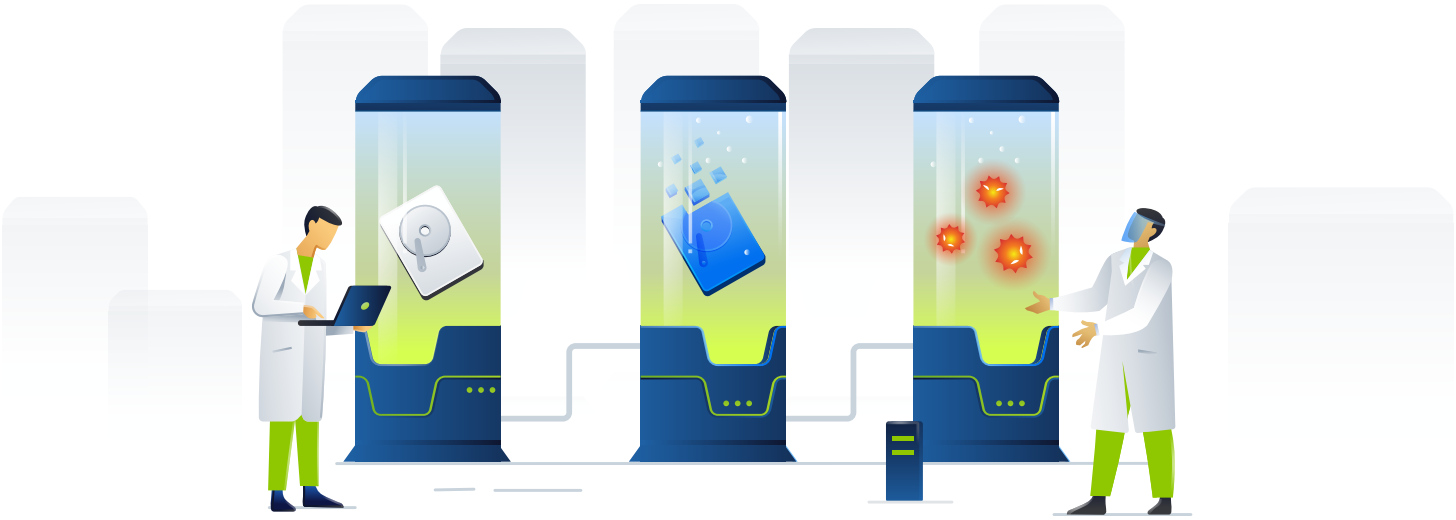
In addition to the body's own detection system, doctors can screen patients for typical symptoms such as a fever and cough. More detailed and time-consuming tests can detect antibodies, antigens, or the genetic material (DNA/RNA) of the pathogen in the bloodstream.

The good news is computer systems are much easier to observe than the human body. To do anything, a computer program has to interact with other system components, invoke system services and APIs, etc., which means it cannot completely conceal what it's doing – making malicious programs detectable.

Since Acronis Cyber Protect is powered by the Acronis Cyber Engine, it constantly monitors all applications and users for suspicious behavior. It is also capable of learning new heuristic rules for detecting bad behavior – both individually on its own and with input from cyber analysts.

Specifically, it can detect the presence of malicious code on a computer (even if this code is designed to hide, acting as a part of an approved application) or flag a cybercriminal who's using stolen-but-valid credentials. If Microsoft Word starts calling file reading/writing APIs frequently or downloads something from a website it never went to before, for example, the behavior is immediately detected and flagged.

And like a good doctor, Acronis Cyber Protect is learning all the time – on its own, from analysts and partners providing input, and from previously stored knowledge. This means Acronis Cyber Protect can detect infections more quickly and reliably than a biological system – with fewer false positives and negatives.



3. Response

Once a threat is detected, a body's immune system sends out "troops" to get rid of the threat. We can observe our body's response to infection as inflammation, fever, and other, sometimes unpleasant effects as our body fights the infection.

That said, it can take time for the body to mount the proper response to an infection – the signal first needs to travel through the blood vessels to the lymph nodes to activate the body's response. Only then can the body can start responding to the infection.

That means, even though our body detected the infection earlier, we only become aware there is a problem when we experience our body's response to it. When the symptoms become noticeable, people may go to the doctor to get medical advice and, when needed, medicine that eases symptoms or speeds up the recovery.

The same approach can be applied to computing. The moment a digital threat is detected, Acronis Cyber Protect can quickly decide on appropriate recovery actions. Acronis MSPs and MSSPs partners, meanwhile, can constantly monitor the systems using Acronis Cyber Protect and even provide valuable insights that can enhance the Acronis Cyber Engine. These IT pros are like a family doctor who can constantly monitor your health in real-time and act immediately when an infection occurs – reacting faster than if you waited three days to see if your fever and coughing stopped.

Whether it's in the real or digital world, early action always results in less damage and a faster recovery.

4. Recovery

Typically, getting rid of an infection and rebuilding damaged cells and tissue can be slow and unpleasant: even the common cold needs several days to run its course. Many infections are much more severe and our bodies need help to fight them off.

Medications such as antibiotics, anti-virals, anti-inflammatories – and, in extreme cases hospitalizations, medical monitoring – can be expensive and time-consuming.

When it comes to recovering from cyberthreats, Acronis Cyber Protect offers a unique capability, one that's based on its tight integration with backup. It can restore a system to a previously known "good state" **without any data loss.** It also automatically applies missing patches and removes any embedded threats from the backup, avoiding the same threat from causing problems moving forward.

Acronis Cyber Protect immediately takes action, even before alerting the MSP or MSSP managing the system. Acronis Cyber Protect first tries to remove any bad code from the system; if removal is not possible or practical, it then tries to mitigate its impact. In the most complex cases, e.g. when it's hard to decide on an automated action, Acronis Cyber Protect alerts the system administrator, who can safely access the system via a built-in remote management feature.

5. Forensics

When we get sick, we rarely think about the forensics involved in fighting a disease. The work done by researchers to better understand a disease and how to treat or eradicate it goes largely unnoticed. Yet these forensic investigations help protect us from threatening pathogens in the future.

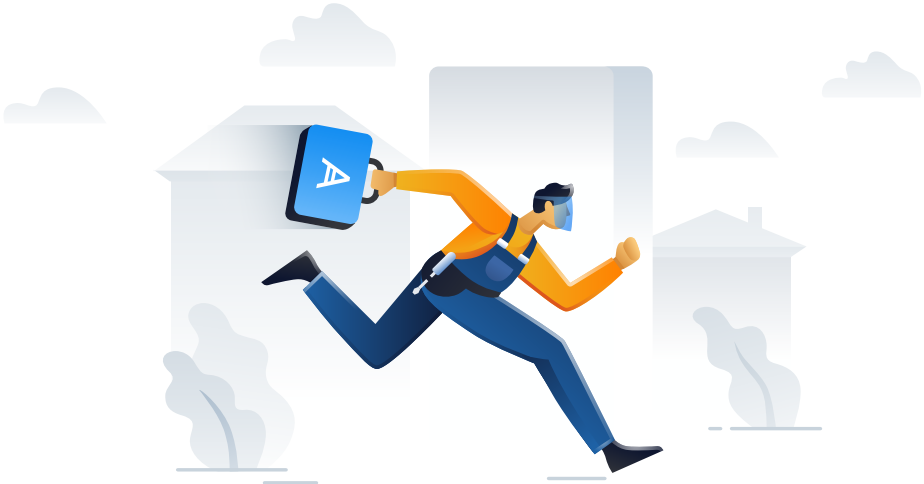
Consider this: We would still be fighting the plague, smallpox and other deadly deceases if these scientists had not traced diseases back to their roots, eliminated the "bioreactors" that produce deadly bacteria, or used genetic sequencing to examine a disease so a working vaccine could be created.

During epidemics and pandemics, it's common to trace who an infected person has been in contact with in order to quarantine, diagnose, and treat them to keep the disease from spreading.

Similar forensic work is critical in the digital world, too. Acronis gathers signals from all endpoints protected by our software around the world, which the CPOC team monitors for new threats. Once identified, the team analyzes the source code to develop a remedy. With forensic-data-enriched backups available, our analysts can easily backtrack and perform a fast and precise investigation into the root cause of the attack. This capability gives Acronis Cyber Protect the intel needed to quickly "cure" the system without losing data.

Partnering with MSPs and MSSPs

Just as we rely on medical experts to stay healthy, Acronis relies on its MSP and MSSP partners to help clients keep their systems #CyberFit and healthy. Working with an MSP or MSSP that leverages Acronis Cyber Protect is the best way to give your IT infrastructure the same level of care you get from the family doctor. Your systems are constantly monitored and tended to by highly skilled personnel. They keep your IT environment clean and maintain good hygiene to reduce the risk of infection. And if disaster strikes, they are there with expert help readily available.



Acronis

Learn more at
www.acronis.com