A new generation of work dynamic requires the next generation of cybersecurity

Next Generation Managed Malware Services

Rethinking risk in a post-pandemic world

For most companies, the COVID-19 pandemic era has accelerated a shift to not only a changing work dynamic involving "work from anywhere" policies for companies, it also has increased the sophistication and frequency of malicious cyberactivity. Malware and the sophistication of attacks have evolved rapidly in only a few years, and the growing remote and hybrid work environment has raised the risk factor by significantly increasing the potential attack surface of businesses

What are the most common threats facing small businesses?

The number one threat faced by small businesses is a ransomware. Ransomware is a type of malicious software that encrypts your data so that you cannot view or utilize it unless you make a ransom payment to the threat actor who may or may not unencrypt it. Other commonly faced threats include malware, phishing via malicious links, and zero days.

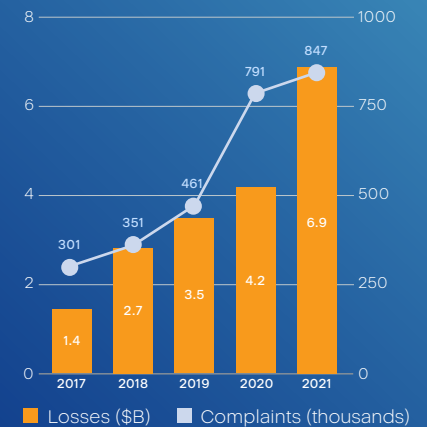### A holistic security approach is needed to mitigate risks and recover

Traditional security models have focused on layered perimeter defenses and building "better walls," but businesses need to have an always-on and holistic security approach that constantly protects all endpoints, blocking threats but also ensuring fast recovery in case of breaches. The reality is, with the increasing scale and sophistication of cyberthreats, no matter how strong your defenses are, businesses need to adopt an "assume breach" approach. Detection technologies need to be complemented by remediation capabilities. No matter what the situation, a solution is needed that allows your business to bounce back and recover.
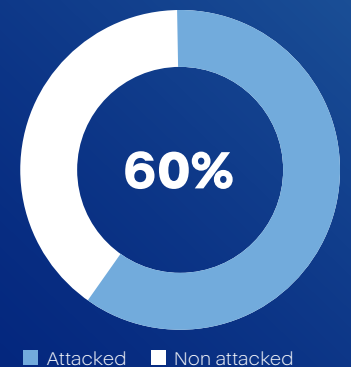
Small businesses are turning to trusted IT providers for their security needs

When a cybercrime makes the news, it is typically because a large organization has fallen victim to an attack. However, small organizations are just as enticing to criminals as large ones, and in many cases even more so. This is because large companies have access to considerable resources, which means they can afford an internal team of information security professionals and cutting-edge technology to defend themselves. Small businesses, on the other hand, have limited resources and cannot rely on internal security teams. That is why more businesses are outsourcing their security needs to managed IT service providers — to strengthen their security posture and protect their assets while also maintaining compliance requirements.

Growth in incidents and losses

Year	Losses ($B)	Complaints (thousands)
2017	1.4	301
2018	2.7	351
2019	3.5	461
2020	4.2	791
2021	6.9	847

■ Losses ($B) ■ Complaints (thousands)

60% of SMBs experienced an attack over the past year

60%

■ Attacked   ■ Non attacked

Source:
"The State of IT Security for SMBs in 2022 –2023", Devotions

FBI, 2021 Internet Crime Report

How Next Generation Managed Malware Protection secures your business

Know your risks and vulnerabilities

Knowing and being able to measure where cybersecurity risks are at any time.

Stay ahead of threats

Staying ahead of the increasingly sophisticated threat landscape is a "make or break" for your business.

Extended security through a trusted IT advisor

We stop cyberattacks as you work remotely, move to the cloud and adopt new technologies. Let us help you detect threats earlier, react faster and stay secure.

To learn more about our Next Generation Cybersecurity Managed Services, contact us:

Let our professional team deliver to your business a high level of protection and increased resilience:

What is Next Generation Managed Malware Protection?

An evolving threat landscape and changing work environment needs essential cyber protection. With Next Generation Managed Malware Protection, your business's security posture is continuously being risk assessed and automatically provided with proportional enforcement that can be dialed up or down by our team. We offer adaptive security services that use a holistic approach by detecting and blocking cyberthreats before they turn into breaches, while also ensuring fast recovery of malware–free data in case of incidents. Leveraging the experience of past threats, our security solution capabilities are constantly evolving — gathering contextual information both within your systems and the environment. This gives you access to an expert team that ensures you are provided with the best security service possible, so that you can do what you know best — growing your business.

Continuous improvement and adaptive security

Blending artificial intelligence and cybersecurity accelerates security effectiveness in real time, but also can evolve with your current or future business landscape.

Rapid recovery whenever your business needs it

Your records and data are kept secure via our unique approach of combining cloud backup with cyber protection; ensuring that a reliable copy of data is always available, anywhere, at any time.

Live threat intelligence alerts from a worldwide network of expert security analysts

Be prepared to face any emerging threats with Acronis Cyber Protection Operation Centers (CPOCs) that monitor the threat landscape and release actionable alerts.

Ongoing cybersecurity reporting so you are always in the know

Communication with transparency and clear reporting helps you understand the current potential threats and also see the value this managed endpoint security service creates.

Powered by award-winning endpoint protection from Acronis

AV comparatives	vb 100 VIRUS virusbtn.com virus BULLETIN	AV TEST The Independent IT-Security Institute Magdeburg Germany	ICSA labs	PCMAG.COM EDITORS' CHOICE	Software Reviews GOLD MEDAL 2021
AV-Comparatives participant and test winner	VB100 certified	AV-TEST participant and test winner	ICSA Labs Certified Anti-malware certified	PCMag: Editors' Choice	Software Reviews gold medal for endpoint protection