Cybersecurity

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users through ransomware; or interrupting normal business processes.

Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative.

A successful cybersecurity posture has multiple layers of protection spread across the computers, networks, programs, or data that one intends to keep safe. In an organization, a unified threat management gateway system can automate integrations across products and accelerate key security operations functions: detection, investigation, and remediation. People, processes, and technology must all complement one another to create an effective defense from cyberattacks.

Why is cybersecurity important?

In today's connected world, everyone benefits from advanced cybersecurity solutions. At an individual level, a cybersecurity attack can result in everything from identity theft to extortion attempts, to the loss of important data like family photos. Everyone relies on critical infrastructure like power plants, hospitals, and financial service companies. Securing these and other organizations is essential to keeping our society functioning.

Everyone also benefits from the work of cyberthreat researchers, like the team of 250 threat researchers at Talos, who investigate new and emerging threats and cyberattack strategies. They reveal new vulnerabilities, educate the public on the importance of cybersecurity, and strengthen open-source tools. Their work makes the internet safer for everyone.