Case Study

Cybersecurity

What is Cybersecurity?

Cybersecurity aims at protecting company assets including hardware, software and data from cyberattacks. It comprises of an evolving set of tools, technologies, trainings and security best practices designed to protect networks, devices, programs, and data from attacks or unauthorized

access. The general goal of cybersecurity is to protect the assets and reduce the risk of being attacked by hackers with malicious intent which intern damage the company reputation.

Why Cybersecurity is the need of the hour?

In today's age of technology, nothing seems to be more critical than data. Enterprises are compelled to adopt various cyber security norms as cybercriminals are continuing to launch increasingly dangerous & sophisticated attacks. As per the latest report from Privacy Rights Clearinghouse (PRC), a nonprofit consumer education and advocacy organization based out of California, there have been 9,693 data breach incidents since 2005 in US alone. According to the 2017 study report by IBM Security and Ponemon Institute, the average direct financial cost of a data breach is over USD 3.6 million. There may also be substantial hidden and indirect costs such as damage to corporate reputation and loss of customer confidence as a result of such data breaches. A recent DDOS attack on one of the world's biggest cloud platforms produced a situation where thousands of enterprises had been left unable to use cloud services for several hours. It could be difficult to even imagine the quantum of financial loss for these enterprises and the additional dollars and efforts they had to invest in mitigating such havoc. Back in 2017, one of the three largest consumer credit reporting agencies in US announced that its systems had been breached and the sensitive personal data of 148 million customers had been compromised. The agency had to pay up to USD 700 million towards compensation and penalties. A single data breach can have a range of devastating consequences for any business. It can unravel a company's reputation through the loss of consumer and partner trust. The loss of critical data, such as source files or intellectual property can cost a company its competitive advantage. The growth in the number of connected devices and the increasing dependency of individuals, businesses, industries and governments upon them means that there are an increasing number of systems at risk. The Internet, the wireless network standards such as Bluetooth and Wi-Fi, the "smart" devices including smartphones, televisions, and the various devices that constitute the "Internet of things" (IoT) are collectively contributing to increasing complexity thereby posing cybersecurity as one of the major challenges in the contemporary world.

How Pi Can Lead The Way

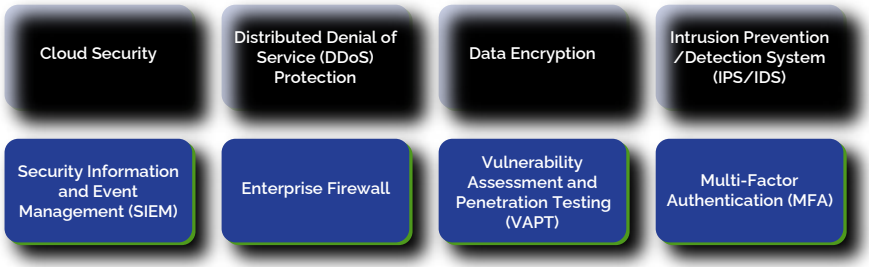
Pi, Asia's Largest Uptime Institute Tier IV Certified Data Center, offers cutting edge tools, technology and practices across the entire spectrum of cybersecurity including Application Security, Information Security, Disaster Recovery, Network Security and Cloud Security. Pi Cloud, provides uncompromised security for valuable data of enterprises with a variety of state-of-the-art features. The cloud platform is protected by a high-speed perimeter firewall with intrusion detection systems (IDS) and intrusion prevention systems (IPS). Additionally, enterprises can opt for a virtual firewall for zone-based, policy-driven security at the VM layer. Moreover, the firewalls are also present at the OS level for virtual servers. The evervigilant team at Pi Cloud periodically performs security tasks, such as OS hardening and vulnerability assessment to ensure the highest level of security. Underneath the virtual layer, security features are embedded in the hardware processors of Pi Cloud fabric, to leave no scope for even a fraction of a security breach. As the volume and sophistication of cyber-attacks grow, companies and organizations, especially those that are tasked with safeguarding information relating to national security, health, or financial records, needs to take steps to protect their sensitive business and personnel information. Pi has successfully deployed various cybersecurity measures across few of the large BFSI organisations in India. Pi's latest practices such as multi-factor authentication has enabled enterprises including the country's largest Small Finance Bank for 2FA of both Legacy (web & client-server) and SaaS applications with device health monitoring. Most of Pi's customers across different industries/verticals avail the benefits of security via intelligent access gateway & stringent authentication protocols.

How are the enterprises threatened by the Cybercriminals?

Threats can come in many forms. Some of the most common cyber threats or challenges witnessed by the modern day enterprises include:

- Backdoor: A backdoor in a computer system, a cryptosystem or an algorithm, is any secret method of bypassing normal authentication or security controls
- DDoS: Distributed Denial of Service attacks (DDoS) are designed to make a machine or network resource unavailable to its intended users
- Multi Vector Polymorphic (MVP) Attacks: A new class of cyber threat that combines several types of attacks and change forms to avoid cyber security controls as they spread. These threats have been classified as fifth generation cyber attacks
- Spoofing: An act of masquerading as a valid entity through falsification of data (such as an IP address or username), in order to gain access to information or resources that one is otherwise unauthorized to obtain. There are several types of spoofing, including Email spoofing, MAC spoofing and Biometric spoofing
- Botnets: Cybercriminals no longer need to develop complex malware solutions since they can easily purchase a ready-to-use botnet kit from the dark web instead and launch malwares and ransom wares on the click of a button

Pi's Cybersecurity Portfolio



How Pi continues to instill trust &confidence in its customers?

Pi is a modern-day organization driven by the values of customer at the core. In the quest to offer preeminent experience to our customers, Pi has enhanced its technology portfolio to offer cuttingedge cybersecurity solutions. Following are few differentiators that keep Pi ahead and makes it the preferred choice of enterprises for hosting their business-critical data:

Advanced Encryption Standards:

Strong authentication, encryption both in transit and at rest, and audit logging

Predictive Security:

Works like a counterintelligence agency that hunts the spies even before they attack is launched

Multi-Tenancy:

Isolation of a user's data from other tenants (user) on a cloud environment together with privacy controls

Big Data Stack:

The Pi cloud can leverage big data and stant analytics over a large swath of end users to instantly ddress known threats and predict threats that seek to overwhelm security of customer's data

Cyber Preparedness:

Continual audit, Periodic Data Back Up as per defined SLA and 24x7 surveillance of customer's sensitive data because ultimately it comes down to diligence and watchfulness

Security First:

With cloud web security services, traffic is redirected to the security cloud first where it gets filtered before reaching the application system

Conclusion:

Pi Cloud is a powerful and robust cloud platform that is fully equipped with multi-tier security. But it is crucial for customers to understand the shared responsibility model and take steps to secure the applications and data they host on Pi Cloud. The interconnected age is magnificent but comes with its own problems and requires every one of us to stay aware of threats and use best practices to mitigate them.