



External Attack Surface Monitoring

Use Case

Detailing Digital discovery and Inventory

When we look at the threat landscape over the past year, we have been inundated with attacks on our critical infrastructure, healthcare organizations, pharma organizations, BFSI organizations and many more. It's hard as these threats are serious and escalating.

But there is also a new threat surface emerging, one that has proven to have a critical cybersecurity gap. Rapid digital change has transformed nearly every organization, which is being adopted to remain agile, flexible, and adaptive. As we realize the many benefits of digitization, we also open ourselves to new risk levels.

For each collaboration software, social media platform, or mobile chat tool that the organization adopts, they are expanding their attack surface. That effect has magnified over the past year due to our rapid shift to remote working, wherein the employees have turned to these digital channels to stay effective. Various departmental groups within organization are also managing some of its digital assets.

Gathering an accurate, complete inventory of digital assets is a formidable task, given the number of unknown digital assets created in a decentralized manner and the security teams lack of visibility. It is also difficult for organizations security team to monitor these digital assets for future breach risks like open ports, misconfigurations, Vulnerabilities, reputation of assets on continuous basis

Attackers are actively targeting these digital assets, websites, IPs, domains, services, certificates, apps, and data and more. These threats are no longer hypothetical — they are here right now, and companies everywhere must begin to address this entirely new digital threat landscape.

Customer Case (BFSI)

The organization is one of the leading Financial Service stock exchange listed company in India. Besides being a major Housing Finance provider, the company also provides Life and General Insurance, Asset Management, Realty, Deposit and Loan services.

Customer Business Challenge:

- 1. Digital Asset Inventory Assessment:** As a very large geographically spread-out organization, customer struggled to maintain an accurate inventory of their digital assets. The decentralized structure meant that multiple teams created digital assets and on occasions without keeping IT Security team in loop. Consequently, the IT Security team struggled to maintain complete inventory of total digital assets.

2. **Digital Attack Surface Preparedness:** As customer struggled to maintain accurate inventory of digital assets, they also lacked knowledge of attack surface that could be exploited by threat actors. Various departmental groups that managed some of its digital assets were not equipped to handle attack surface. The customer struggled to analyze their current risk posture and monitor for future breach risks like Open Ports, Misconfigurations, Vulnerabilities, Reputation of Assets on continuous basis.

Solution: Volon External Attack Surface monitoring

Volon External Attack Surface monitoring will help the organization detect and monitor the vulnerable digital, allowing a business to focus on what matters. Volon's attack surface monitoring solution provides a realistic picture of exposed digital assets, that include:

- Domains/Subdomains
- IP Addresses / Subnets
- Open Ports
- SSL Certificate Scans
- Services
- Possible Misconfigurations
- Reputation Checks

Volon will provide comprehensive weekly reporting for observed changes in the digital asset.

Outcomes

40% Decrease In External Attack Surface:

With the help of External Attack Surface Monitoring (EASM), the customer got a complete overview of their digital assets and ability to monitor new or old digital assets continuously and identify if any of those are vulnerable and could be exploited by the threat actors.

Continuously Updated Asset Inventory:

Volon External Attack Surface monitoring helped the customer to have an up-to-date inventory of their digital internet facing assets.

VOLON

Volon Cyber Security

www.volon.io