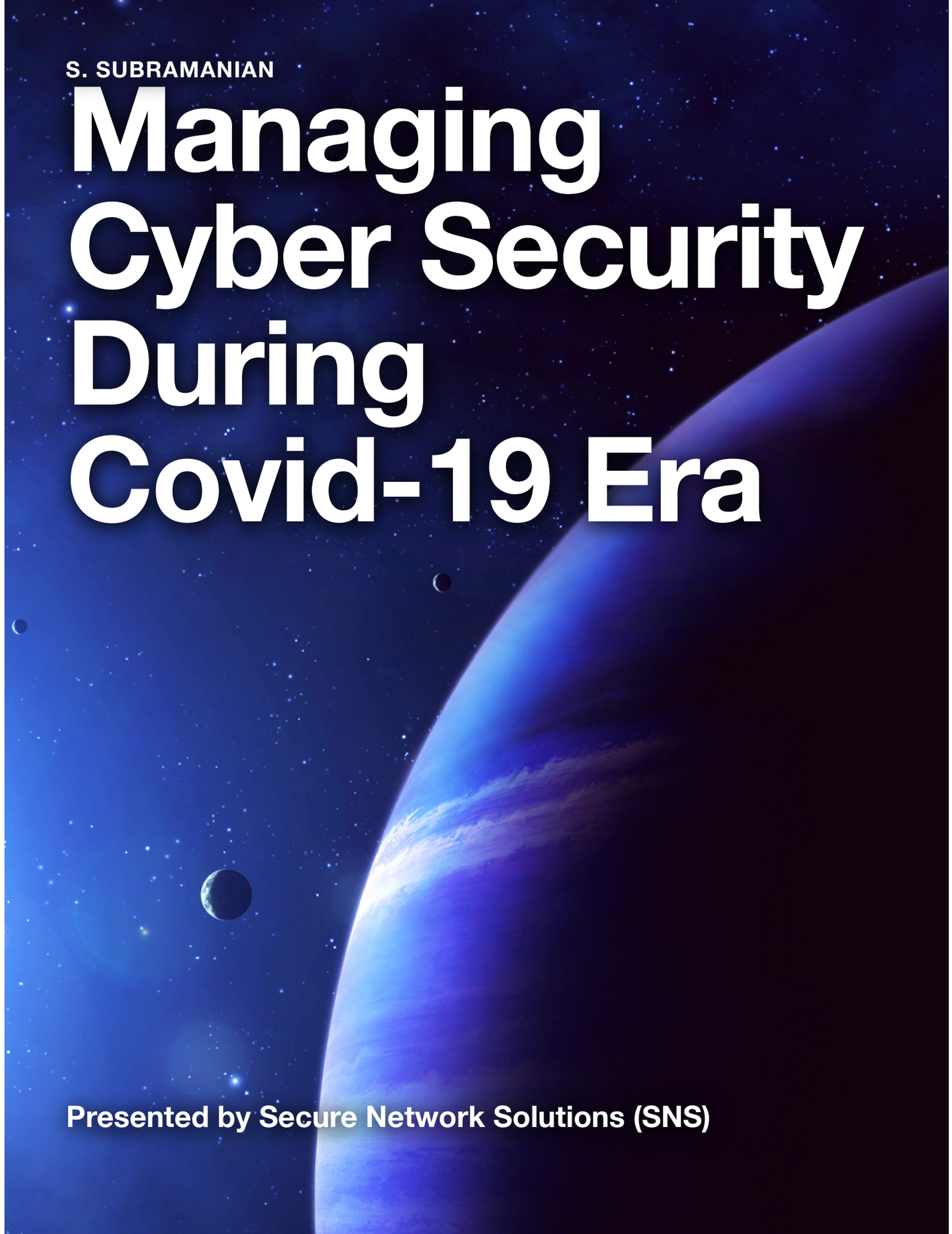

S. SUBRAMANIAN
Managing Cyber Security During Covid-19 Era
Presented by Secure Network Solutions (SNS)

S. Subramanian

Managing Cyber Security During Covid-19 Era

White Paper

Author is an experienced Network & Security Consultant, presently, Head-Technology, Secure Network Solutions India Private Limited (www.snsin.com)

Subramanian has deployed wide range of security solutions during his hands-on days, and as a leader has trained and developed hundreds of Cyber Security Specialists.

Subramanian is an expert in cross-platform Cyber Security solutions integration. He manages some of the largest and complex infrastructures in India.

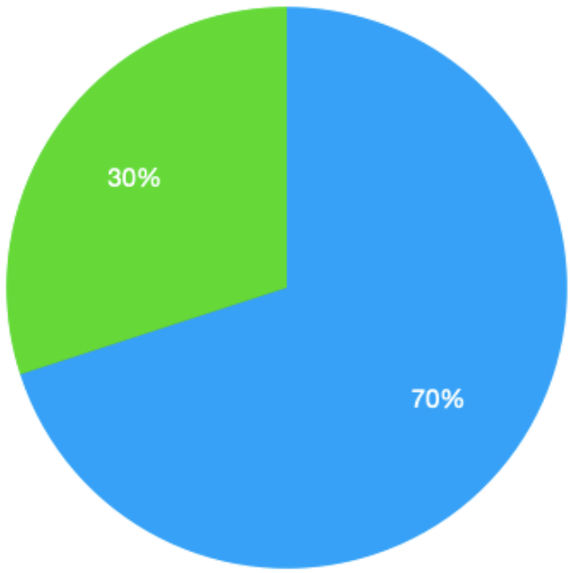
Background

Before Covid-19

ABSTRACT

1. How Organisations used to protect confidential, sensitive data before COVID-19?
2. What are the challenges faced by Organisations since COVID-19 to protect data?
3. Solutions to address these Challenges

Percentage of Employees by Location of Work



70-80% of the employees used to work from office (also known as “On-premise Users”)

- Employees commute to their Head Office, Regional Office, Branch Office, Plants, and/or Warehouses
- All these locations are interconnected using MPLS and/or P2P Wide Area Network Connectivity
- In recent times, IPSec VPN over Internet is also actively deployed instead of MPLS or P2P

20-30% employees used to work from home or field. These users are considered to be either Senior Management or Mobile Workers (also known as “Remote Users”)

Organisation of any size, may have invested in some sort of security controls by placing Firewall, Intrusion Prevention System, Anti-Malware and several other solutions. Table 1 and Table 2 explain in details, about such possible security measures for both on-prem and remote users, organisations have invested to protect against different types of threats.

Table 1: On-Prem Users, Type, Application Access and Access Mode

Type of Users	Department	Application Access	Access Mode
Head Office Users	HR	HRMS File Share Internet Access Email	Office Provided Desktop or Laptop via Office LAN
Head Office & Other Location Users	Operations	Applications of Operations Team File share Internet Access Email	Office Provided Desktop or Laptop via Office LAN
Head Office & Other Location Users	Finance	Financial Applications File share Internet Access Email	Office Provided Desktop or Laptop via Office LAN
Head Office & Other Location Users	Information Tech / EDP	Servers Desktops Applications Internet Access Email Infrastructure Management	Office Provided Desktop or Laptop via Office LAN
Head Office & Other Location Users	Production	Product Applications File share Internet Access Email	Office Provided Desktop or Laptop via Office LAN

Security Controls for On-Prem Users

Security Objectives:

- All Users have access to Confidential or Sensitive Information
- Defense in Depth Deployment

The minimum Security controls for On-Prem Users were (Table 1A):

Network Security	Endpoint Security	Infrastructure Monitoring	Application	Users & Data
Perimeter Firewall & Second Layer Firewall	Vulnerability Management	Highly Available Connectivity to Data	Application Filtering	Privileged Identity Management
Intrusion Prevention	Patch Management	Network Bandwidth / Traffic Monitoring	Mail Filtering	Data Loss Prevention
Network Access Control	Hardened Desktops	Security Incident & Event Management for Monitoring	Web Filtering	Digital Rights Management
Secure Wireless Connectivity	Endpoint Encryption	Subject Matter Experts (SME) for Proactive Monitoring	Application Security Testing	Single Sign-On & Multi-factor Authentication

Table 2: Remote Users, Type, Application Access and Access Mode

Type of Users	Department	Application Access	Access Mode
Remote Users	Sales	HRMS Sales Applications Internet Access Email File share	Office Provided Laptop over the Internet
Remote Users	Senior Management of various Departments	Business Applications Internet Access Email	Office Provided Laptop over the Internet

Security Controls for Remote Users

Security Objectives:

- All authenticated and authorised remote users have access to corporate information
- Clearly defined monitoring for remote access

Table 2A: The minimum Security controls for Remote Users were:

Endpoint Security	Endpoint DLP
Mobile Device Management	Secure VPN Access to Head Office
Access to specific Applications	Access to specific Servers

Security Challenges

Employees working from office, has reduced considerable to less than 10%. Employees working from Home has increased drastically since COVID19. Table 3 highlights this based on the information gathered from our clients:

Table 3: Representation Based on Information Gathered

Before Covid-19	Since COVID19
70-80% Users were Working from Office 20-30% Users were Remote Users	0 -10% Users Working from Office 70-80% Users are Working from Home 20-30% Users Continue to Work from Home

Considering the above scenario, the kind of security controls that were available when they were “On-Prem” is no longer available when Users are working from home.

Table 4 explains this lack of security for Work from Home Users.

Table 4: Lack of security control for 70-80% Users working from home

Security Controls for 70-80% On-Prem Users	Security Controls for the same 70-80% Users when they are not in Office
Before COVID19	Since COVID19
Same as Table 1A	Endpoint Security Secure VPN to Head Office Email Security

With this analysis, we can see that Organisations fear the risks involved while Users “Work Out of Office ”. Post COVID, the number of users coming back to office, would also see a change.

- ***From 20 security controls earlier it is now down to 3 controls for the same users***

Table 5: Risks the Users face without the required security controls

Without the following controls	Users & Organisation face the following Risk [when users Work from Home]
Perimeter Firewall	Unauthorised Access to the User Computer, serves as a first level of defense
Web Filtering	Access to Malicious Websites, there by compromising the User Computer
Application Filtering	BOT, Malware can communicate to its handler, there by gaining complete control of the User Computer. BOT, Malware can traverse across the Network and infect other computers
Intrusion Prevention System	Attackers can try every possible method to intrude, compromise & gain complete controls of the User Computer
Anti-Malware Scanning	Users can download malicious files thereby allowing complete control / compromise of data in the User Computer
Second Layer Firewall I Micro-Segmentation Firewall	Access to Critical Internal resources are not protected adequately from unauthorised access from Internal Users
Network Access Control	Any unknown user can connect and access critical, sensitive corporate data

Table 5: Risks the Users face without the required security controls (continued)

Without the following controls	Users & Organisation face the following Risk [when users Work from Home]
Secure Wireless Connectivity	An attacker can compromise Wireless Connectivity to gain unauthorised access to Critical Network & can eavesdrop to gain access & manipulate sensitive information
Vulnerability Management	Without this, User Computer remain vulnerable to attacks from the Internet. This may lead to compromise
Patch Management	Without this, User Computer remain vulnerable to attacks from the Internet. This may lead to compromise
Data Leak Prevention	Confidential & Sensitive Information Leak is possible, either intentional or unintentional
Privilege Identity Management	Any unauthorised software/service can use higher privilege to gain access to confidential data or take complete control
Physical Access Controls & Endpoint Encryption	Attackers can steal hardware & eventually gain access to confidential data especially without Full Disk Encryption on End User Computer
Physical Access Controls & Endpoint Encryption	Attackers can steal hardware & eventually gain access to confidential data especially without Full Disk Encryption on End User Computer
Hardened Desktops	Without Hardening, User Computer remains vulnerable to intrusions
SIEM	With all users outside the Network, traffic monitoring on the endpoints is not possible. Which results in lack of visibility in terms of traffic generated from end computers

Solutions

The following solutions will address the risk faced by the Users and Organisations while implementing large scale Work From Home scenario:

Table 6: Solutions to address COVID19 Challenges

Solutions to Implement	
Perimeter Firewall	Secure Internet Connectivity Solution Secure Remote Access Solution Cloud Managed Next Generation Endpoint Security
Web Filtering	
Application Filtering	
Intrusion Prevention System	
Anti-Malware Scanning	
Second Layer Firewall I Micro-Segmentation Firewall	
Network Access Control	
Vulnerability Management	
Endpoint Encryption	
Data Leak Prevention	
Privilege Identity Management	Privilege Identity Management Tool - For Secure Access to Software, Network Devices, Security Devices by Privilege Users
Hardened Desktops	Configuration & Software Management Tool - Ensure Compliance across Desktops as per Corporate Security Policy
User Security Awareness	Periodical Computer Based Awareness Sessions and Evaluation

Summary

It is evident that, Covid-19 situation has made organisations relook at existing work culture, including how and from where people work.

This new challenge has further brought out new strategies, and solutions especially related to securing the data and users .

The key takeaways are the following:

- Work from home is here to stay
- Organisation start integrating cloud solutions sooner
- The security strategy needs a relook
- New Solutions that can help organisations to handle this change to be adopted quickly

White Paper Presented by

SNSin

Secure Network Solutions India Private Limited

www.snsin.com

enquiry@snsin.com

Head Quarters:

Deva Dropa, No. 7 Krishna Street

Nungambakkam, Chennai - 600034

Phone: +91 44 28221642, +91 9789092637

SNS Locations		
Chennai	Mumbai	Delhi
Bengaluru	Hyderabad	Coimbatore
Pune	Kochi	Kolkata

Partner Ecosystem		
A10	Aerohive	Algosec
AWS	Arcserve	Array
Barracuda	Broadcom	Check Point
Cisco	Cloud Flare	Commscope
Crowd Strike	Dell	F5
Fire Eye	Forcepoint	Fortinet
Gigamon	HPE	IBM
Imperva	Ipswitch	Juniper
Logrythm	McAfee	Micro Focus
Nutanix	One Login	Palo Alto
Peplink	Pulse Secure	Radware
Redhat	Riverbed	Sonicwall
Sophos	Soti	Tenable
Trend Micro	Tripwire	Tufin
Veritas	VMWare	Watchguard
Winmagic	Zscaler	And more...