SENETAS

Security without compromise

END-TO-END ENCRYPTION SOLUTIONS

SECURING SD-WAN INFRASTRUCTURE

SOLUTION PAPER

SD-WAN

IT networks are growing larger and becoming more widely dispersed. With endpoints stretching across multiple sites, national borders and remote locations, IT professionals are turning to more advanced ways to manage them.

SD-WAN, also known as software defined networking, does just this. Evolved to simplify the deployment and management of WAN infrastructure, its benefits range from improved agility and dynamic routing to cost efficiency and network standardisation.

Its popularity is growing; The SD-WAN market is expected to surpass $4.6 billion by 2023, and is projected to continue growing at double digit CAGR for the predictable future.[1]

The role of data networks

By 2023, Gartner predicts more than 90% of WAN edge infrastructure refresh initiatives will be based on virtualised customer premises equipment (vCPE) platforms or SD-WAN software/appliances[2].

As network administrators will be able to apply this orchestration layer remotely, SD-WAN is heavily reliant on data networks to work correctly.

While core IT infrastructure – such as backup services and data centre interconnects – rely on networks of 10Gbps or higher, wide-area networks will typically operate at speeds of 1Gbps or less.

One of the roles SD-WAN fills is to optimise network performance through dynamic routing, meaning that any security and encryption software deployed alongside it must be cost-effective.

The makeup of these networks is different too; while core infrastructure will still run over private networks, many organisations will utilise public networks in an SD-WAN deployment.

Borderless infrastructure

As part of deploying SD-WAN, organisations must acknowledge the reality of borderless infrastructure.

Digital transformation, the demand for agility and mobility, and the rise of the IoT means there is no longer a line where one network ends and another begins.

While these trends deliver innumerate advantages, they also pose a security challenge: Networks that are normally closed to the outside world become open and vulnerable to attack, while each endpoint added to the WAN represents another security risk.

Threats to SD-WAN

While organisations may focus on protecting the high-speed links within their core network infrastructure, they must not forget to protect endpoints stretching out to the network edge.

The consequences of a breach can result in anything from a loss of IP and customer data to financial loss and reputational damage.

Alongside existing threats, organisations must also be aware of emerging technologies, such as the impending age of quantum computing.

SD-WAN security

While SD-WAN unquestionably brings a host of efficiencies, the technology also poses an inherent security risk if communication between endpoints is not properly protected.

By encrypting data in motion across SD-WAN, it is possible to guarantee data integrity as, even in the event that this data is stolen, it will be unreadable and thus rendered useless.

In addition, organisations must find a cost-effective method of securing WAN data in motion as deploying hardware encryption across each endpoint is not financially viable.

This Solution Paper analyses the threats that organisations deploying SD-WAN face, explains why data in motion should be encrypted and offers guidance on choosing the right encryption solution.

[1] Futuriom SD-WAN Growth Report

[2] Gartner Magic Quadrant for WAN Edge Infrastructure

WHY ENCRYPT?

By utilising both public and private networks, instead of relying on isolated MPLS networks for example, the data transmitted between endpoints via SD-WAN is vulnerable to attack.

Prevention technologies such as firewalls ensure data is protected at rest, yet data remains exposed when in motion. In order to guarantee the trust and integrity of the data being transmitted, organisations must act to secure it against a wide range of threats.

The breach landscape

According to security firm Risk Based Security, there were 3932 publicly disclosed data breaches in 2020, with the number of compromised records amounting to over 37 billion.[3]

The primary cause of data loss is still attacks by malicious outsiders, accounting for over 70% of breaches in 2020.[4] 45% of breaches involved hacking and 86% of the attacks were financially motivated.

While data breaches occur across all industries, they are most frequent in the technology, social media, retail and government sectors due to the quantity and detail of information exchanged.

It takes organisations an average of 280 days to identify a data breach and contain it[4]. The consequences of these breaches include:

- Intellectual property theft
- Business disruption
- Compliance issues
- Loss of customer data
- Privacy breaches
- Financial loss

Alongside this, firms must address the loss of trust and reputation amongst stakeholders; something that is much more difficult to attribute a value to.

Popular trends and emerging threats

Alongside existing threats, organisations must be aware of technologies that are gaining popularity, as well as those about to be introduced.

The growth in SD-WAN deployment itself is an area of particular interest, with the market expected to see a compound annual growth rate of 34.5% between 2020 and 2025[5].

According to Gartner, 60% of enterprises will have implemented SD-WAN by 2024, compared with about 30% in 2020, aiming to enhance agility and support for cloud applications.[6]

The rapid growth in IoT devices and the introduction of borderless infrastructure by default will also impact data security greatly. If organisations fail to protect devices at the network edge (Layers 3 and 4), they provide hackers with opportunities to gain access to networks and farm sensitive information or input rogue data.

There has also been a notable rise in the theft of metadata (data about data). Despite the common myth, this information is sensitive and can provide a wealth of exploitable information if not properly encrypted.

The coming age of quantum computing also plays a growing part in cyber security. While the immense computing power of quantum computers will have a transformative effect on computing, there is also a risk of the technology being used for harm.

Quantum computers will be able to break current AES encryption standards in a fraction of the time taken by traditional computing methods, threatening the protocols that underpin much of the world's data security.

While this seems like a distant concern, the reality is much closer. It is estimated that a quantum computer capable of breaking today's cryptography will be available within the next 10 years, meaning organisations need to introduce quantum-ready encryption now or risk the integrity of their data.

[3] Risk Based Security 2020 Year End Review

[4] 2020 Verizon Data Breach Investigations Report

[5] Futuriom SD-WAN Growth Report

[6] Gartner Critical Capabilities for WAN Edge Infrastructure

SECURING SD-WAN

By tapping into data in motion flowing across the networks utilised by an SD-WAN solution, hackers can bypass security systems in place around the data when it is at rest.

Upon accessing the network, cyber criminals can intercept and steal data as it flows between the point of origination and endpoint. By gaining unsolicited access, hackers can also inject rogue data into the network – compromising the integrity of the data and the platform as a whole.

Network administrators must take steps to secure this data in motion, whilst ensuring that the performance of the network is not adversely affected.

Protection vs prevention

There is a common misconception within many organisations that a robust firewall is enough to prevent unwanted access to their network. Another is that networks - private or Carrier - are inherently secure.

Unfortunately, this is not the case. Whilst the firewall can detect and eliminate a variety of penetration or denial of service attacks, it is no protection against a physical tap either inside or outside the firewall.

The only fail-safe solution to ensure that your data is secure as it travels across the network is encryption. Furthermore, your encryption solution should be de-coupled from any specific network architecture and accredited against recognised world-wide security standards.

By utilising both public and private networks, instead of relying on isolated MPLS networks for example, the data transmitted between endpoints via SD-WAN is vulnerable to attack.

Prevention technologies such as firewalls ensure data is protected at rest, yet data remains exposed when in motion. In order to guarantee the trust and integrity of the data being transmitted, organisations must act to secure it against a wide range of threats.

End-to-end encryption

Encryption is crucial to SD-WAN and should form part of any security solution the IT community desires. Moreover, it should be deployed as an end-to-end solution.

Importantly, this end-to-end crypto solution should also be network transport layer independent, allowing it to be deployed across all layers of the network (Layers 2, 3 and 4) – extending to the virtual edge. It should also secure metadata alongside main data packets.

In the event of a breach, encrypted data is unreadable by hackers and is therefore rendered useless. In addition, the forward secrecy provided by encryption solutions prevents rogue data being injected into systems.

Encrypting data also benefits organisations from a compliance perspective, with data protection regulations such as the GDPR treating 'secure breaches' differently to those that are not; potentially saving organisations from hefty fines as they demonstrate the importance of protecting the sensitive information they collect.

Network and application performance

It is crucial that an encryption solution does not impact network speed or performance.

Any increase in latency will impact the performance of the WAN; an area that an SD-WAN solution looks to improve via dynamic routing.

Of equal concern is that some organisations opt for 'low-grade' data encryption technologies that appear to be effective, but come at a cost:

- Compromised network performance
- Hidden costs of lost effective bandwidth
- Adverse impact on endpoints and applications
- Complex implementation and ongoing management

END-TO-END ENCRYPTION SOLUTIONS

CN Series Encryption Hardware

The CN Series of Ethernet encryptors provide certified, high-assurance data protection for core IT and communications network infrastructure.

All CN Series encryptors share a common encryption platform and are 100% compatible and interoperable.

CN Series hardware is used to secure sensitive data in motion across networks operating at anything from modest 10Mbps to ultra-fast 100Gbps bandwidths.

CN4000

Small form-factor (desktop) encryptors for 'in the field' network link security (e.g. CCTV) – offering 10Mbps, 100Mbps and 1Gbps bandwidth speeds.

CN6000

Rack-mounted high speed encryptors for business-critical applications – offering 1Gbps to 10Gbps bandwidth speeds.

CN9000

Ultra-high bandwidth, rack-mounted encryptor with "mega-data" performance – offering speeds of up to 100Gbps.

CV Series Virtualised Encryption

The CV1000 virtual encryptor provides strong and effective data encryption for large-scale and virtualised wide-area networks.

Scalable to thousands of end-points, the CV series of virtual encryptors is a software application of the trusted Senetas encryption platform. It delivers cost-effective, transport Layer agnostic data protection at up to 15Gbps (with DPDK).

As a Virtualised Network Function (VNF) that will run on any x86 hardware, the CV Series virtual encryptor is 100% interoperable with Senetas CN Series hardware encryptors and is built on FIPS compliant technology.

SureDrop Encrypted File Sharing and Collaboration

SureDrop delivers the file-sharing convenience of popular box-style applications, but with the addition of end-to-end encryption security and 100% data location control.

It also offers users a choice of the resilience of a bespoke, on-premises solution or the flexibility of a managed service provider solution.

SureDrop clients include government agencies and service providers that are concerned about the inherent risks associated with sharing documents outside of their protected LAN.

SureDrop represents a new way to enjoy secure file sharing; with the emphasis on delivering a service that meets the needs of large commercial and government organisations who are required to frequently share sensitive and confidential information across the web.

SureDrop also provides organisations with the user-authentication security benefits of active directory compatibility.

Votiro Secure File Gateway

VOTIRO

Votiro Secure File Gateway leverages patented, next generation anti-malware technology to proactively protect your files from the most advanced, persistent cyber-attacks.

It sanitises incoming, shared and stored files, enterprise-wide; eliminating the risks associated with both known and zero-day, or undisclosed, attacks. At the same time, it preserves 100% of original file content and functionality, without disrupting user workflows.

WHAT MAKES SENETAS STAND OUT?

Best Performance

High-speed

The designed-in, market-leading performance capabilities of Senetas encryption solutions are what make them stand out from the crowd.

Whether operating at 10Mbps, 100Mbps, 1Gbps, 10Gbps or 100Gbps; time after time, they consistently win competitive performance tests.

Their encryption speeds, near-zero data overhead and near-zero latency make Senetas encryption solutions ideally suited to the most demanding network environments.

Ultra-low latency

Senetas high-speed encryption solutions operate in full duplex mode at full line speed 99.99% without loss of packets.

Latency is not affected by packet size (<2 microseconds per unit at 100Gbps) meaning maximum throughput with near zero protocol overhead.

Importantly, by using Field Programmable Gate Array (FPGA) technology, this outstanding performance is predictable and dependable.

Zero impact

The zero impact of Senetas encryptors is not limited to network bandwidth and latency; it extends to network operations and management.

They simply fit in within the user network. They don't require changes to other devices or network reorganisation; making them a favourite among network engineers.

High-Assurance

Certification in-depth

Senetas CN Series encryptors include the only multi-certified products of their types, as a result they are trusted by governments and defence forces around the world.

Rigorous testing is carried out over many years and provides our government and commercial customers with maximum confidence. Senetas CN Series encryption solutions are certified by: FIPS, Common Criteria and NATO.

For over 20 years, Senetas R&D has included a commitment to 'certification in depth'. Customers value the benefits of exhaustive and ongoing testing authorities' product evaluation.

Best encryption key management

All Senetas products adopt state-of-the-art encryption key management. Your encryption keys are only ever held by and accessible to you, on your premises; securely stored and encrypted.

Solution integrity

Senetas encryptors provide maximum solution integrity; unlike 'low assurance' solutions, such as router-based network data encryption or multi-function devices with embedded encryption.

Senetas high-assurance encryption solutions feature dedicated, tamper-proof hardware and provide gapless, end-to-end, authenticated encryption with standards-based (AES256) encryption algorithms.

Versatile & Simple

Crypto-agility

All Senetas encryption solutions are agile by design; from 100% compatibility and interoperability to customisable encryption and FPGA based flexibility.

Selected Senetas encryptors also support Quantum Key Distribution (Quantum Cryptography) and Quantum Random Number Generation, for long-term data security.

Support for all topologies

Senetas CN series encryptors operate in point-to-point, point-to-multipoint and fully meshed network topologies. Senetas CN9000 encryptors are the only 100Gbps encryptors that support multipoint-to-multipoint topologies.

Custom encryption

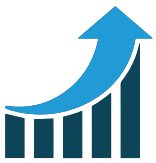
In addition to the standards-based AES256 and 128-bit algorithms, Senetas CN series encryptors support the use of customer-requested algorithms, custom curves (BYOC) and entropy (BYOE).

Ease of use

Set and forget simplicity and network transparency are underlying Senetas design themes. They ensure ease of implementation, operation and management. All Senetas encryption solutions feature automatic zero-touch key management. They also feature automatic network discovery and connection.

Local or centralised management

Configuration may be performed locally or remotely through the intuitive Senetas CM7 management software; which acts as the Certificate Authority in a network of encryptors by signing and distributing X.509 certificates.



Low Cost, High Efficiency

Suitability

All Senetas CN Series solutions operate at full line speed; enable maximum network performance and deliver 'set and forget' management simplicity.

The business investment case out-performs even 'cheap and cheerful' low-assurance solutions that prove very costly over time.

It is not necessary, nor beneficial, to opt for low-cost, low-assurance solutions to meet the toughest business case and TCO requirements.

Cost-efficiency

Senetas encryption solutions provide excellent TCO through a mix of network bandwidth savings, ease of management and reliability.

Longevity, interoperability, backward compatibility, minimal installation and management costs and solution flexibility all contribute to a rapid ROI.

Other cost benefits include, low power consumption minimal rack space use and combined rack space/ power utilisation efficiency.

Reliability

All Senetas hardware encryption solutions boast 99.999% uptime. Carrier-grade, rack mounted devices are hot-swappable and provide further network operations uptime benefits thanks to dual redundancy of consumables, such as fans and power supplies.

Flexibility

The use of FPGA technology enables maximum operational flexibility. This enables on-going operational simplicity, such as infield upgradability, as customers' requirements change; helping to protect their investment in technology.

GLOBAL SUPPORT

Senetas encryption solutions are distributed and supported internationally (outside Australia and New Zealand) by Thales

Thales is the world leader in digital security and defence, servicing over 30,000 customers across 180 countries. Senetas CN and CV Series encryption solutions are sold by Thales as part of its Cloud Protection and Licensing portfolio.

ANZ PARTNER COMMUNITY

Senetas works directly with customers and their service providers across Australia and New Zealand. We provide technical consultancy and support to data networks providers, systems integrators and cloud service providers. Visit our **ANZ Partner Page** for full details.

www.senetas.com

Senetas is a leading developer of end-to-end encryption security solutions; trusted to protect enterprise, government, defence, Cloud and service provider network data in over 40 countries.

From certified high-assurance hardware and virtualised encryption, to secure file-sharing and collaboration with data sovereignty control, all are based on the same crypto-agile platform and deliver security without compromise.

Regional Contacts:

Asia	**T:** +65 8307 3540	**E:** infoasia@senetas.com
Australia & New Zealand	**T:** +61(03) 9868 4555	**E:** info@senetas.com
Europe, Middle East & Africa	**T:** +44 (0)1256 345 599	**E:** info@senetas-europe.com
The Americas	**T:** +1 949 436 0509	**E:** infousa@senetas.com

GET IN TOUCH

Are you looking for a service provider to help you select and implement a network data encryption solution? Contact Senetas and we'll help you find the right one.

Senetas works with IT infrastructure service providers and systems integrators across the globe, to help specify the optimal encryption solution for their customers' needs.

Customers may contact Senetas directly to discuss their requirements; or ask their service provider to speak to us on their behalf.

ENCRYPTION SECURITY WITHOUT COMPROMISE

Whatever your network security needs, Senetas has an encryption solution to suit. Our certified high-assurance encryptors protect data across networks operating at speeds from 10Mbps to 100Gbps and support all network topologies.

Our virtualised encryption solution, for virtual CPE and virtualised WAN, supports bandwidths of up to 5Gbps. It provides policy-based, end-to-end encryption across multi-Layer networks.

Senetas encryptors are recognised globally for delivering maximum data security and crypto-agility, without compromising network or application performance.

SECURE FILE SHARING

SureDrop offers all the flexibility of a drop-box style solution, with the added benefit of best-in-class encryption security and 100% control over data sovereignty.

For customers seeking additional layers of content security, SureDrop is also available with the Votiro Disarmer extension.

DISARM MALICIOUS CONTENT

Votiro Disarmer leverages patented Content Disarm & Reconstruction (CDR) technology to protect your files from the most advanced, persistent cyber-attacks. It sanitises incoming files, eliminating the risks associated with zero-day or undisclosed attacks, whilst preserving 100% file functionality.

SDW-SP0621

SENETAS