Stormshield

Overview document

hammer cloud cybersecurity

STORMSHIELD



A market in transition

Dominic Ryles

Over the past decade, cybersecurity has been shaped by expansion. As threats evolved, organisations responded by investing in more tools, more layers, and increasingly complex architectures. While this has driven advancements in detection and response, it has also introduced a new challenge — a gradual loss of visibility and control.

Today, many organisations operate security environments that are effective, but not fully understood. Critical capabilities are often delivered through external platforms, with limited transparency over how systems are built, where data resides, and who ultimately retains control. As a result, the conversation is shifting. Businesses are no longer asking only whether they are protected, but whether they truly own and govern the technologies they depend on.

This shift is being accelerated by a convergence of factors — geopolitical uncertainty, regulatory pressure, supply chain scrutiny, and an increased focus on data sovereignty. Together, these forces are driving a more deliberate approach to cybersecurity, where trust, transparency, and accountability are becoming as important as performance.

Within this context, the firewall market has become a key point of reassessment. As the foundation of network security, firewalls have evolved into highly capable platforms, but also increasingly complex and exposed ones. Recent vulnerabilities have reinforced the need for assurance — not just in what these systems can do, but in how they are designed, controlled, and maintained. Selecting a firewall is no longer purely a technical decision; it is a strategic choice that underpins trust in the wider security architecture.
It is against this backdrop that a sovereign approach to cybersecurity is gaining momentum. Stormshield reflects this shift, offering a model built on control, resilience, and transparency. Developed in Europe and aligned with stringent certification frameworks, it represents a growing demand for security solutions that prioritise ownership and accountability alongside protection.

For partners, this evolution presents a clear opportunity. As customers seek greater clarity and control, the ability to lead conversations around trust, governance, and long-term resilience is becoming critical. Cybersecurity is no longer defined solely by defence, but by how confidently organisations can understand and control the environments they operate.



Understanding sovereignty in cybersecurity

Sovereignty in cybersecurity refers to the ability of an organisation to maintain authority over its data, infrastructure, and security technologies — including how they are developed, deployed, and governed.

It goes beyond questions of data location. True sovereignty requires control across the full lifecycle of a technology: the jurisdiction under which it is built, the standards it adheres to, the transparency of its operation, and the extent to which an organisation can operate independently of external influence.

In practical terms, this means being able to clearly understand who controls the technology, how it is secured, and how risk is managed throughout its lifecycle. These considerations are becoming increasingly important as cybersecurity becomes more closely aligned with regulatory accountability, operational resilience, and national infrastructure priorities.

At the same time, the threat landscape is continuing to evolve. Attackers are increasingly targeting foundational layers of security — particularly network and edge devices — where trust is assumed but not always validated. Industry observations indicate that a significant proportion of cyber defence activity now originates from vulnerabilities within these systems, reinforcing the importance of assurance at the core of the architecture .

This places network security, and the firewall in particular, at the centre of the sovereignty conversation.

As the primary control point between internal environments and external networks, the firewall is not only responsible for enforcing security policy, but also for underpinning trust across the wider infrastructure. Its design, governance, and operational transparency have a direct impact on an organisation’s ability to maintain control.

Sovereignty, therefore, becomes a critical lens through which network security must be evaluated — not only in terms of capability, but in terms of how confidently an organisation can understand, trust, and control the technology it depends on.



A sovereign approach to network security: Stormshield

It is within this context that Stormshield emerges as a compelling choice for organisations seeking greater control, transparency, and assurance in their network security strategy.

Stormshield is a European cybersecurity provider with a strong heritage in protecting critical infrastructure, public sector organisations, and highly regulated environments. Its approach is grounded in a simple principle: security should not only protect, but also enable organisations to retain full control over their technology and data.
This philosophy is reflected in how the platform is designed, developed, and maintained. Stormshield's network security solutions are built on hardened operating systems, engineered to reduce attack surfaces and provide resilience at the architectural level. This focus on security-by-design ensures that protection is embedded into the foundation of the platform, rather than layered on as an afterthought.

A defining characteristic of Stormshield is its alignment with rigorous European certification frameworks. Its products are certified and qualified by leading national and European authorities, including ANSSI (the French National Cybersecurity Agency), reflecting their suitability for use in sensitive and mission-critical environments. These certifications provide independent validation of the platform's security posture, governance, and resilience, offering a level of assurance that extends beyond standard commercial benchmarks.

In addition, Stormshield's commitment to European sovereignty ensures that its technologies are developed and governed within trusted regulatory frameworks. This provides organisations with clarity over how their security infrastructure operates, how data is handled, and how risks are managed — critical considerations in today's regulatory and geopolitical landscape.

From a capability perspective, Stormshield delivers a comprehensive network security platform, combining next-generation firewall functionality with advanced threat prevention, secure connectivity, and unified threat management. However, its differentiation lies not simply in what it does, but in how it does it — prioritising transparency, control, and long-term trust.

For partners, this creates a strong foundation for engaging customers in a different type of conversation. One that moves beyond feature comparison, and instead focuses on aligning security architecture with the principles of sovereignty, resilience, and accountability.

Stormshield platform overview: essential capabilities

Stormshield's platform has been engineered to deliver a comprehensive and integrated approach to network security, combining core firewall functionality with advanced threat prevention, secure connectivity, and intelligent traffic management. Rather than relying on fragmented tools or bolt-on features, its architecture brings these capabilities together within a unified framework, designed to operate consistently across environments.

The following matrix outlines the essential features that underpin this approach. It is intended to provide a clear view of how Stormshield enables organisations to secure their networks, manage risk, and maintain operational control — from real-time threat protection and segmentation, through to application visibility, secure access, and performance optimisation.

Functionality	Description	Inclusive (as standard)
REAL-TIME PROTECTION		
Network and Micro-Segmentation	Divides the network into secure zones to limit lateral movement and contain breaches	✓
Anti-Virus Update	Ensures the latest threat signatures are applied to detect and block known malware	✓
Intrusion Prevention Systems (IPS)	Actively blocks malicious traffic and exploits before they reach critical systems	✓
Intrusion Detection System (IDS)	Identifies and alerts on suspicious activity without interrupting traffic flow	✓
High-Availability	Provides failover resilience to ensure uninterrupted network and security operations	✓
Cloud-Based Sandboxing	Executes unknown files in a secure cloud environment to detect zero-day threats	✓
Rugged Firmware	Hardened operating system designed to resist tampering and advanced attacks	✓
CONTROL & MONITORING		
Zero-Trust Network Access	Enforces strict identity-based access, esuring no user or device is trusted by default	✓
URL Filtering	Blocks access to malicious or inappropriate websites based on reputation and policy	✓
Content Filtering	Controls and restricts access to specific types of content across the network	✓
Geolocation of Ips	Applies security policies based on the geographic origin of network traffic	✓
Detection of Vulnerabilities	Identifies weaknesses in systems and configurations that could be exploited	✓
Application Control	Manages and restricts application usage to reduce risk and improve compliance	✓
SD-WAN CONNECTIVITY		
Management of Multiple WAN Links	Enables efficient use and failover of multiple internet connections	✓
Ease of Deployment on Remote Sites	Simplifies rollout and configuration across distributed and brand environments	✓
VPN Tunnel Management	Centralises control and monitoring of secure VPN connections	✓
Recognition of SaaS Applications	Identifies and prioritises cloud applications for better performance and control	✓
Flow Routing by Applications and Protocol	Directs traffic intelligently based on application type or control	✓
Bandwidth Management (QoS)	Prioritises critical traffic to ensure consistent performance	✓
Monitoring of Link Quality	Tracks latency, jitter, and packet loss to maintain optimal connectivity	✓
Centralised Management	Provides a single-pane-of-glass management of all policies, devices, and visibility	✓
SECURE COMMUNICATIONS		
Site-to-Site and Mobile VPNs	Connects offices and remote users securely over encrypted tunnels	✓
Mobile SSL-VPN	Enables security remote access via SSL without complex client setups	✓
Enhanced Restricted Mode	Applies strict controls to limit system exposure and reduce attack surface	✓
Post-Quantum Encryption (PQC)	Future-proofs encryption against next-generation quantum computing threats	✓

Deployment flexibility: UTM model overview

Stormshield's Unified Threat Management (UTM) model has been designed with this in mind, offering a broad range of hardware and virtual appliances to support different operational requirements, performance needs, and architectural preferences. This flexibility enables partners to align security deployments with customer environments, without compromising on capability or governance.

The following matrix provides an overview of the available hardware and virtual models, outlining how Stormshield can be deployed across a variety of use cases — from edge and branch protection, through to data centre and virtualised infrastructure.



	SN-XS170	SN-S220	SN-S320	SN-M520	SN-M720	SN-M920	SN1100	SN-L2200	SN-L3200	SN-XL5200	SN-XL5200
Standard Interfaces	4x 2.5GbE	8x 2.5GbE 1x 1Gb SFP+	8x 2.5GbE 1x 1Gb SFP+	8x 2.5GbE 2x 1Gb SFP+	8x 2.5GbE 2x 10Gb SFP+	8x 2.5GbE 2x 10Gb SFP+	8x 1GbE 2x 10Gb SFP+	2x 1GbE	2x 1GbE	2x 1GbE	2x 1GbE
Extended Interfaces	N/A	N/A	N/A	1x Optional	1x Optional	1x Optional	2x Modules	3x Optional	3x Optional	8x Optional	8x Optional
Form Factor	Desktop	Desktop	Desktop	1U Long	1U Long	1U Long	1U Long	1U Long	1U Long	2U	2U
Power Supply	Single	Dual	Dual	Dual	Dual	Dual	2 HS 720w	2 HS 720w	2 HS 720w	2 HS 2400w	2 HS 2400w
Maximum VLAN Interfaces	137	256	393	1,336	1,336	1,336	1,336	1,336	1,336	1,336	1,336
Threat Inspection Throughput (DPI-SSL)	400Mbps	740Mbps	1.1Gbps	1.5Gbps	2.3Gbps	3.4Gbps	6.7Gbps	6.6Gbps	10.8Gbps	10.8Gbps	12.4Gbps
Storage Included	Optional (Micro SD)	Optional (Micro SD)	Optional (Micro SD)	256Gb	256Gb	256Gb	512Gb	240Gb OP 1Tb	240Gb OP 1Tb	480Gb OP 1Tb	480Gb OP 1Tb
Maximum SPI Throughput	8.50Gbps	10.0Gbps	11.9Gbps	18.9Gbps	38.6Gbps	46.2Gbps	59.4Gbps	115.0Gbps	116.0Gbps	239.8Gbps	319.3Gbps
Maximum Connection SPI	150,000	300,000	400,000	600,000	1,000,000	1,500,000	1,800,000	5,000,000	7,000,000	15,000,000	25,000,000
New Connection p/s	25,000	39,000	60,000	90,000	120,000	190,000	250,000	300,000	330,000	420,000	500,000
VPN Throughput	1.8Gbps	3.3Gbps	4.8Gbps	7.5Gbps	7.5Gbps	13.2Gbps	13.4Gbps	23.7Gbps	27.0Gbps	43.5Gbps	59.1Gbps
Site-to-Site VPN Maximum	200	300	400	1,500	2,000	2,200	4,700	6,900	10,000	20,000	23,000
Bundled IPSec Clients	200	300	400	1,500	2,000	2,200	4,700	6,900	10,000	20,000	23,000
Maximum IPSec Clients	200	300	400	1,500	2,000	2,200	4,700	6,900	10,000	20,000	23,000
Bundled SSL-VPN Clients	200	300	400	500	700	1,200	1,600	2,400	4,000	5,000	7,500
Maximum SSL-VPN Clients	200	300	400	500	700	1,000	1,600	2,400	4,000	5,000	7,500
High-Availability	Active/Passive	Active/Passive	Active/Passive	Active/Passive	Active/Passive	Active/Passive	Active/Passive	Active/Passive	Active/Passive	Active/Passive	Active/Passive

	EVA1	EVA2	EVA3	EVA4	EVAU
Memory (min - max, GB)	2	2 - 3	3 - 6	6 - 8	8 - 64
Max Number of Virtual CPUs	1	2	4	4	16
Max Number of Filtering Rules	1,024	2,048	4,096	8,192	8,192
Max Number of Objects	5,000	5,000	5,000	20,000	20,000
Max Size of User Database	2,048	2,048	5,120	5,120	10,240
Threat Inspection Throughput (DPI-SSL)	0.9Gbps	1.7Gbps	3.1Gbps	3.1Gbps	7.1Gbps
Firewall Throughput (1,518 byte UDP)	16.4Gbps	27.0Gbps	45.0Gbps	45.0Gbps	63.0Gbps
IPS Throughput (1,518 byte UDP)	8.6Gbps	12.7Gbps	20.0Gbps	20.0Gbps	33.0Gbps
IPS Throughput (1Mb HTTP)	5.0Gbps	8.5Gbps	12.7Gbps	12.7Gbps	14.5Gbps
IPSec Throughput - AESGCM/SHA2	2.5Gbps	3.7Gbps	6.7Gbps	6.7Gbps	10.6Gbps
Max Number of Concurrent Sessions	200,000	400,000	1,000,000	1,500,000	5,000,000
Max Number of Static Routes	512	2,048	5,120	5,210	10,240
Max Number of Dynamic Routes	10,000	350,000	350,000	350,000	700,000
802.1Q VLAN	128	256	512	512	1,024
Maximum Number of IPSec Tunnels	200	500	750	5,000	10,000
Max Number of SSL-VPN Clients	50	512	512	1,024	4,096
Max Number of Simultaneous SSL-VPN	100	150	200	250	500
High-Availability	Active/Passive	Active/Passive	Active/Passive	Active/Passive	Active/Passive



Enabling partner success in a sovereign security market

The shift towards sovereignty is already changing how organisations evaluate network security. Decisions are no longer based solely on performance or price, but on trust, control, and long-term resilience. For partners, this creates a clear opportunity to lead more strategic conversations with customers.

Stormshield provides a strong foundation for this approach, combining proven network security capability with a design philosophy aligned to sovereignty, transparency, and assurance. It enables partners to position a solution that meets both immediate security requirements and evolving expectations around governance and control.
However, successful adoption requires more than technology alone.

At Hammer Distribution, we bring deep expertise in the firewall and network security market, built over decades of supporting partners through technology shifts and vendor transitions. Our role is to enable partners to confidently adopt, position, and deliver Stormshield — from initial onboarding and migration, through to pre-sales support and ongoing technical guidance.

To support this, we provide a clear pathway for partners to engage, including streamlined onboarding into the Stormshield partner ecosystem and access to structured enablement from day one. This is complemented by our 21-day Proof of Value service, designed to help partners and their customers validate the platform in real-world environments, reduce risk in the decision-making process, and accelerate time to adoption.

Our focus is not just on deployment, but on helping partners build a sustainable and differentiated offering. By combining the right technology with the right support, we enable partners to engage customers with confidence and capitalise on a market that is actively evolving.

This is not about adding another solution. It is about equipping partners with a credible, strategic alternative — and the backing to succeed with it.

Looking ahead

Cybersecurity is entering a new phase — one defined not only by the need to defend against increasingly sophisticated threats, but by the need to understand, control, and trust the technologies that underpin that defence.

The shift towards sovereignty reflects a broader change in how organisations approach risk. It signals a move away from purely reactive security models, towards environments that are designed with resilience, transparency, and accountability at their core.

For partners, this represents a clear inflection point.

The opportunity is no longer just to provide security solutions, but to guide customers through a more complex and more considered decision-making process. Those who can lead conversations around control, governance, and long-term resilience will be best positioned to differentiate and grow.

Together, Stormshield and Hammer Distribution provide the foundation to do exactly that — combining sovereign, security-first technology with the expertise, enablement, and support required to deliver it successfully.

The market is evolving.

Customer expectations are changing.

And the definition of security is being rewritten.

The question is no longer whether this shift will happen — but how quickly organisations and their partners choose to act.

Start your Stormshield journey with Hammer Distribution

Stoke
Innovation House, Bellringer Road
Trentham Lakes South
Trentham, ST4 8GH
Main Switchboard: 01782 648200