BLACK CELL
Protecting critical infrastructures

WHITEPAPER

NEXT-GENERATION FIREWALL BUYER'S GUIDE

Technical decision-maker edition 2026

Created by

Istvan Szallos | Integration

July 2026

TABLE OF CONTENTS

01

ABOUT BLACK CELL

Black Cell is a European cybersecurity company focused on protecting critical infrastructures and the organizations that support them. Our business units cover SOC, Integration, Offensive Security, Cloud Security, Compliance, and ESM (Enterprise Security Monitoring). We take a customer first approach that starts with listening, then shaping solutions to fit the way our clients operate.

Our teams are adaptable and draw on deep knowledge across industries and technologies, from IT and Cloud to ICS/OT. We engage for the long term, providing continual support, service improvement, and measurable outcomes over the lifecycle of the relationship. Clients rely on us to connect regulatory requirements with technology choices and to guide organizational transformation that sticks.

We combine architecture, implementation, and managed operations to close gaps quickly and build sustainable capability. Local presence in Central Europe matters to us, with teams in Budapest and Frankfurt am Main that understand the regional context. This proximity helps us respond faster, coordinate with partners, and keep stakeholders aligned. Above all, we aim to be a trusted partner who strengthens resilience today and prepares you for what comes next.

DISCLAIMER

The information provided in this document is for general guidance only and is used at your own risk. No contractual or advisory relationship is created between Black Cell and any person accessing or using this document or any part of it. Black Cell accepts no liability for any actions, decisions, or consequences arising from the use of this material.

References to third-party sources are included where appropriate. Black Cell is not responsible for the content, accuracy, or availability of external sources, including websites mentioned in this publication.

CONTACT

Istvan Szallos
Integration Director
istvan.szallos@blackcell.io

COPYRIGHT NOTICE

02

EXECUTIVE SUMMARY

The firewall buying decision has changed. For many organizations, the NGFW is no longer just an internet edge device; it has become a central policy enforcement point across users, applications, encrypted traffic, cloud connectivity, branch networks, and incident response.

A strong evaluation process should therefore assess the platform as part of the wider security operating model, with particular focus on:

- security efficacy and prevention quality;
- operational maturity and manageability;
- performance under realistic inspection load;
- integration with identity, endpoint, SIEM/XDR/MDR and response workflows; and
- total cost of ownership across licensing, support, logging, operations and lifecycle.

Sophos emphasize, secure-by-design hardening, proactive monitoring, automatic patching, integrated NDR, automation, and simplified management. Palo Alto Networks emphasizes the NGFW as a prevention-focused platform, with strong application/user/content controls, TLS decryption, advanced threat prevention, DNS security, cloud and mobile workforce coverage, policy optimization, automation and analytics. This guide combines those perspectives into a vendor-neutral evaluation method for technical decision makers.

2.1. RECOMMENDED DECISION PRINCIPLE

Select the platform that gives the organization the most measurable risk reduction per operational hour, not simply the highest datasheet throughput or the longest feature list. Require proof through a pilot, validated sizing, migration workshop and clear operational runbook.

03

HUNGARY AND EASTERN EUROPE NGFW MARKET CONTEXT

The Hungarian and wider Eastern European NGFW market is being shaped by three forces: regulatory pressure, increased ransomware and credential-abuse risk, and the modernization of traditional perimeter networks into hybrid, identity-aware and cloud-connected environments.

- **Regulation and audit readiness:** NIS2-driven obligations are pushing many Hungarian organizations to formalize cybersecurity controls, incident handling, logging, risk management and audit evidence. This increases demand for NGFW platforms with clear reporting, policy governance, SIEM integration, and documented operational processes.
- **Budget and skills constraints:** Mid-market and enterprise customers often need stronger controls without adding too many consoles, products or highly specialized daily tasks. Operational simplicity and automation are therefore buying criteria, not only convenience features.
- **Hybrid reality:** Most organizations still operate significant on-premises networks, but remote work, SaaS, cloud workloads and branch connectivity require consistent policy across users and locations.
- **Procurement maturity:** Technical decision makers increasingly ask for proof-of-value pilots, validated performance with security subscriptions enabled, predictable licensing and migration services rather than datasheet-only comparisons.

04

WHAT A MODERN NGFW MUST DELIVER

APPLICATION, USER AND CONTENT AWARENESS

Policies must be based on applications, users, devices, content and risk, not only IP addresses and ports. Application identification should work across ports, evasive behavior and encryption where technically possible.

ENCRYPTED TRAFFIC CONTROL

The platform must support modern TLS inspection, including TLS 1.3 where required, with exception management, privacy controls, performance transparency and reporting on decryption failures or bypasses.

THREAT PREVENTION

The platform should block known and unknown malware, exploits, command-and-control traffic, credential phishing and DNS-based attacks using inline prevention, cloud intelligence, sandboxing and machine learning where applicable.

SECURE-BY-DESIGN OPERATIONS

The firewall itself is a critical infrastructure. Evaluate hardening, management-plane protection, MFA for administrators, role-based access, configuration audit trails, update process, vulnerability response and ability to patch without unacceptable downtime.

DETECTION AND RESPONSE INTEGRATION

The NGFW should feed SIEM/XDR/MDR workflows, enrich events with user/application context, support automated or semi-automated containment, and integrate with endpoint, identity, wireless and ticketing systems.

CONSISTENT COVERAGE

Assess whether the same security posture can extend to branches, remote users, cloud/virtual environments, and segmented internal networks.

OPERATIONAL MANAGEABILITY

Central management, logging, reporting, API support, templates, policy optimization and rollback capabilities directly influence security quality and time-to-resolution.

05

TECHNICAL EVALUATION FRAMEWORK

Domain	What to evaluate	Evidence to request
Security efficacy	Application control, IPS, anti-malware, DNS security, URL filtering, credential protection, sandboxing, threat intelligence, evasion resistance.	Pilot results, third-party test references, threat logs, sample reports, demo of unknown-file and malicious-domain handling.
Identity and access	User-ID, group mapping, MFA integration, device posture, remote access, ZTNA/SASE options, and admin MFA/RBAC.	Live integration with AD/Entra ID, VPN/ZTNA policy demo, admin audit log.
Encrypted traffic	TLS 1.3/HTTP2 support, inbound/outbound decryption, exceptions, certificate handling, performance impact.	Decryption policy workshop, test with representative SaaS/finance/health sites, throughput with inspection enabled.

Domain	What to evaluate	Evidence to request
Policy quality	Migration from port-based rules to application-based rules, rule cleanup, unused/disabled rule handling, recertification workflow.	Rulebase assessment output, policy optimizer demo, rollback/change review demo.
Operations	Central management, reporting, SIEM export, log retention, backup/restore, config audit, APIs, multi-admin workflow.	Operational demo, sample runbook, API documentation, SIEM parsing example.
Architecture and resilience	HA modes, link redundancy, SD-WAN, branch models, virtual/cloud support, power, interface modules, RMA.	Low-level design, failure test, licensing and support SLA.
Performance	Threat prevention, IPS, app control and TLS inspection throughput; concurrent sessions; VPN users; log rate.	Sizing calculations based on real traffic, not firewall-only throughput.
Commercial model	Subscriptions, support, logging/reporting add-ons, remote access licensing, centralized management, NDR/XDR/MDR costs.	Three- to five-year TCO model and renewal assumptions.

06

SIZING, ARCHITECTURE AND DEPLOYMENT CONSIDERATIONS

6.1. SIZING INPUTS TO COLLECT BEFORE VENDOR SELECTION

- Internet bandwidth today and expected in 3-5 years.
- Peak and average throughput by direction, including east-west/internal segmentation traffic.
- Percentage of traffic to be inspected with IPS, URL filtering, application control, and TLS decryption.
- Number of users, endpoints, servers, branches, VPN users, and concurrent sessions.
- Critical applications, SaaS dependencies, latency-sensitive traffic, and bypass requirements.
- Logging volume, retention requirements, and SIEM ingestion capacity.
- High-availability, dual ISP, SD-WAN, routing, and dynamic failover requirements.

6.2. ARCHITECTURE CHOICES

For most Hungarian mid-market and enterprise projects, the recommended design is a high-availability pair at the internet edge, with separate security zones for users, servers, management, OT/production, guest/IoT and DMZ. Internal segmentation may use the same NGFW pair or dedicated internal firewalls depending on east-west traffic volume, latency and resilience requirements. Remote access should be integrated with Entra ID or another enterprise IdP, enforce MFA, and apply least-privilege application access rather than broad network access.

07

RFP / VENDOR WORKSHOP QUESTION SET

SECURITY AND THREAT PREVENTION

- How does the platform identify applications on any port and handle evasive applications?
- Which protections are inline, and which depends on cloud detonation or delayed verdicts?
- How are DNS tunneling, DGA domains, C2 traffic and newly registered malicious domains detected and blocked?
- Can the firewall use endpoint, identity, or XDR signals to improve prevention and response?

TLS INSPECTION

- Does the platform support TLS 1.3 and HTTP/2 inspection?
- What is the tested throughput with TLS inspection, IPS, and URL filtering enabled together?
- How are decryption exclusions maintained, audited, and reported?
- How are certificate errors, pinned certificates, and unsupported protocols handled?

POLICY AND OPERATIONS

- Can the platform help convert legacy port-based rules into application-based rules?
- How are unused, shadowed, broad, disabled and risky rules identified?
- Can changes be reviewed, approved, rolled back and linked to a ticket?
- What reports are included without additional licensing?

REMOTE USERS AND BRANCHES

- How many concurrent VPN/ZTNA users are supported on the proposed model?
- Is MFA and device posture supported, and with which identity providers?
- Can policy follow users across HQ, branch, home and mobile networks?
- What is the branch option for zero-touch deployment and LTE/5G backup?

PLATFORM SECURITY AND LIFECYCLE

- How is administrator access protected and audited?
- What is the vendor process for firewall vulnerabilities and emergency patches?
- Can security patches be applied without service interruption?
- What is the hardware warranty, RMA process, and software lifecycle?

INTEGRATION

- Which SIEM formats and APIs are supported?
- Can alerts create tickets or trigger quarantine/containment actions?
- Can the solution be integrated with existing EDR/XDR/MDR, wireless, NAC, and identity systems?
- Is central management cloud, on-premises or both?

08

SCORING MODEL FOR SHORTLIST DECISIONS

Use a weighted score to keep the decision transparent. Adjust weights by project type but avoid allowing price or raw throughput to dominate security and operability.

Area	Suggested weight	Scoring notes
Security efficacy	25%	Prevention of quality, identity-aware policy, DNS security, advanced threats, and TLS controls.
Operations and manageability	20%	Central management, reports, policy optimizer, audit trail, rollback, SIEM/API.
Performance and architecture fit	20%	Real inspection throughput, HA, branch/remote/cloud support, interface flexibility.
Integration and response	15%	EDR/XDR/MDR/SIEM/ticketing/identity integration and containment workflows.

Area	Suggested weight	Scoring notes
Commercial and lifecycle	15%	Three- to five-year TCO, renewal clarity, support, warranty, lifecycle.
Vendor/project risk	5%	Local support capability, implementation complexity, migration risk.

09

COMMON PITFALLS AND RED FLAGS

- Sizing firewall throughput only, without IPS, URL filtering and TLS inspection enabled.
- Assuming all NGFWs have equal application identification, DNS security, cloud-delivered prevention and policy optimization.
- Ignoring migration efforts from legacy port-based rules and NAT structures.
- Underestimating log storage, SIEM ingestion, reporting, and audit evidence requirements.
- Buying remote access as a VPN tunnel only, without identity, MFA, device posture and least-privilege application access.
- Treating TLS inspection as a checkbox instead of a certificate, privacy, exception, and performance design.
- Not validating high availability, link failover, and rollback during the pilot.
- Selecting a platform that needs too many separate consoles or add-on products for daily operation.

10

RECOMMENDED NEXT STEPS

- Run a discovery workshop covering traffic, applications, users, compliance, remote access, branches, HA and SIEM requirements.
- Collect 14-30 days of firewall logs and build a rule-base and traffic assessment.
- Create a target architecture and migration plan, including zones, NAT, VPN, remote access, and logging.
- Shortlist two or three vendors and require a proof-of-value with representative traffic and integrations.
- Score vendors using the weighted model in this guide and validate the three- to five-year TCO.
- Prepare operational runbooks before production cutover: backup, change, update, incident, certificate, VPN onboarding and rollback procedures.

08

APPENDIX A: DETAILED EVALUATION CHECKLIST

Use a weighted score to keep the decision transparent. Adjust weights by project type but avoid allowing price or raw throughput to dominate security and operability.

Category	Requirement
Core NGFW	Stateful firewalling, NAT, routing, zones, App-ID/application control, user-based rules, URL filtering, IPS, anti-malware, DNS security, file control.
Encrypted traffic	TLS 1.3 supports, inbound and outbound decryption, exceptions, certificate deployment, unsupported-site visibility, performance model.
Threat prevention	Known and unknown malware prevention, sandboxing, ML-assisted analysis, exploit protection, C2 detection, threat intelligence updates.
Identity	AD/LDAP/Entra ID integration, SAML/OIDC, MFA, group-based policies, admin RBAC, audit logs.

Category	Requirement
Remote access/ZTNA	VPN capacity, always-on options, MFA, device posture, split/full tunnel, app-level access, user portal.
Segmentation	Internal zones, dynamic address groups, tags, NAC/wireless integration, OT/production constraints.
Management	Central manager, templates, audit trail, approval workflow, rollback, APIs, reporting, scheduled reports.
Logging/SIEM	Syslog/CEF/LEEF/API, log volume, retention, dashboarding, alert tuning.
Resilience	HA, dual power, dual ISP, link monitoring, SD-WAN, backups, RMA, lifecycle.
Commercial	Subscriptions, support levels, reporting/logging add-ons, VPN/ZTNA licensing, cloud management, and renewal terms.