



We Get **IT** Done

CYBERSECURITY PORTFOLIO OF SERVICES

Cybersecurity **Portfolio of Services**

Comprehensive Protection Across Every Layer of Your Digital Ecosystem

 24/7 Security Operations (SOC)

 Vendor-Agnostic Approach

 ISO 27001 & NIST Aligned

CONFIDENTIAL

The Cyber Threat Landscape



\$10.5T

Projected annual cost of cybercrime globally by 2025

2,200+

Cyberattacks occur every day across industries

277 Days

Average time to identify and contain a data breach
breach

Organizations need a multi-layered defense strategy that addresses every attack vector — from the core infrastructure to the network edge.



Our Approach

We deliver an integrated portfolio spanning major security pillars, combining best-of-breed technologies with managed services to protect your entire digital footprint — on-premises, in the cloud, and at the edge.

Pillars of Protection



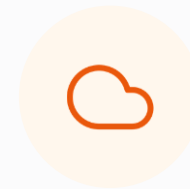
**Infrastructure
Security**



**Endpoint
Security**



**Perimeter
Security**



**Cloud
Security**



**Network
Security**

Infrastructure Security

Hardening the foundation — servers, operating systems, and data centers



Server Hardening & Patching

Automated configuration baselines, CIS benchmarks enforcement, and continuous patch management for physical and virtual servers.



Vulnerability Management

Continuous scanning, risk-based prioritization, and remediation tracking across your entire infrastructure footprint.



Identity & Access Management (IAM)

Centralized identity governance with role-based access control, privileged access management (PAM), and multi-factor authentication.



Data Center Physical Security

Biometric access controls, surveillance systems, environmental monitoring, and compliance with tier standards.



Security Information & Event Management

Real-time log aggregation, threat correlation, and automated alerting with 24/7 SOC monitoring and incident response.



Backup & Disaster Recovery

Immutable backup strategies, automated failover, and tested recovery runbooks to ensure business continuity.

Infrastructure Security — Tools & Approach



KEY TECHNOLOGIES

SIEM & Monitoring

Splunk, Microsoft Sentinel, IBM QRadar, Elastic SIEM

IAM & PAM

CyberArk, BeyondTrust, Okta, Microsoft Entra ID

Vulnerability Scanning

Tenable Nessus, Qualys, Rapid7 InsightVM

Configuration Management

Ansible, Chef, Puppet, CIS-CAT Pro

Backup & Recovery

Veeam, Commvault, Rubrik, Zerto

IMPLEMENTATION APPROACH

1

Assess & Baseline

Full infrastructure audit against CIS/NIST benchmarks

2

Harden & Configure

Apply security baselines, enforce least privilege access

3

Monitor & Detect

Deploy SIEM with custom correlation rules and 24/7 SOC

4

Patch & Remediate

Automated patch cycles with rollback capabilities

5

Test & Validate

Penetration testing and red team exercises quarterly

6

Report & Optimize

Monthly executive reporting and continuous improvement

Endpoint Security

Protecting every device — laptops, desktops, mobile, and IoT endpoints



Endpoint Detection & Response (EDR)

Advanced threat detection with behavioral analytics, automated containment, and forensic investigation capabilities across all endpoints.



Endpoint Encryption

Full-disk and file-level encryption with centralized key management, ensuring data protection even on lost or stolen devices.



Extended Detection & Response (XDR)

Cross-layer visibility correlating endpoint, network, email, and cloud telemetry for holistic threat detection and response.



Zero Trust Endpoint Access

Continuous device health verification, conditional access policies, and micro-segmentation for endpoint-to-resource connections.



Mobile Device Management (MDM)

Device enrollment, policy enforcement, remote wipe, app management, and containerization for BYOD and corporate devices.



Anti-Malware & Ransomware Protection

Next-gen AV with AI-driven detection, anti-ransomware rollback, and fileless attack prevention capabilities.

Endpoint Security — Tools & Approach



KEY TECHNOLOGIES

EDR / XDR Platforms

CrowdStrike Falcon, Microsoft Defender XDR, SentinelOne

Mobile Management

Microsoft Intune, VMware Workspace ONE, Jamf

Encryption

BitLocker, FileVault, Symantec Endpoint Encryption

Threat Intelligence

MITRE ATT&CK, VirusTotal, Recorded Future

Patch Management

WSUS, ManageEngine, Automox, Tanium

IMPLEMENTATION APPROACH

1

Inventory & Classify

Discover all endpoints; classify by risk and criticality

2

Deploy EDR/XDR

Roll out agents with behavioral detection policies

3

Enforce Policies

Apply encryption, patching, and compliance baselines

4

Monitor & Hunt

Continuous monitoring with proactive threat hunting

5

Respond & Contain

Automated isolation and guided remediation playbooks

6

Measure & Mature

KPI tracking, coverage dashboards, and maturity assessments

Perimeter Security

Defending the boundary between trusted internal networks and external threats



Next-Gen Firewall (NGFW)

Deep packet inspection, application-aware filtering, intrusion prevention, and SSL/TLS decryption
SSL/TLS decryption at the network boundary.



DDoS Mitigation

Volumetric, protocol, and application-layer attack mitigation with always-on or on-demand scrubbing centers.



Intrusion Detection & Prevention (IDS/IPS)

Signature and anomaly-based detection engines with automated blocking of malicious traffic patterns and known exploits.



Secure Web Gateway (SWG)

URL filtering, malware scanning, data loss prevention, and policy enforcement for all outbound web traffic.



Web Application Firewall (WAF)

Protection against OWASP Top 10 attacks, bot mitigation, rate limiting, and virtual patching for web-facing applications.



Email Security Gateway

Advanced threat protection for email including anti-phishing, sandboxing, impersonation detection, and DMARC enforcement.

Perimeter Security — Tools & Approach



KEY TECHNOLOGIES

NGFW & IPS

Palo Alto Networks, Fortinet FortiGate, Check Point

WAF

Cloudflare WAF, AWS WAF, Imperva, F5 Advanced WAF

DDoS Protection

Cloudflare, Akamai Prolexic, AWS Shield Advanced

Email Security

Proofpoint, Mimecast, Microsoft Defender for Office 365

Secure Web Gateway

Zscaler, Netskope, Cisco Umbrella

IMPLEMENTATION APPROACH

1

Architecture Review

Map traffic flows and identify perimeter exposure points

2

Layer Defenses

Deploy NGFW, WAF, IDS/IPS in defense-in-depth model

3

Tune Policies

Minimize false positives with traffic-specific rule tuning

4

Enable DDoS Shield

Activate always-on or threshold-based DDoS mitigation

5

Secure Email & Web

Deploy gateway solutions for email and web traffic

6

Continuous Testing

Penetration testing and red team perimeter assessments

Network Security

Securing internal communications, segmentation, and traffic visibility



Network Segmentation & Micro-Segmentation

Isolate critical assets with VLANs, SDN policies, and micro-segmentation to limit lateral movement of threats.



VPN & Secure Remote Access

Enterprise VPN, split tunneling policies, and always-on connectivity with certificate-based authentication for remote workers.



Network Access Control (NAC)

Enforce device authentication, compliance posture checks, and dynamic VLAN assignment before granting network access.



DNS Security

Protective DNS with real-time threat intelligence feeds to block malicious domains, tunneling, and phishing at the DNS layer.



Network Detection & Response (NDR)

AI-driven traffic analysis to detect anomalous behaviors, command-and-control communications, and data exfiltration attempts.



Network Forensics & Packet Capture

Full packet capture, metadata indexing, and forensic analysis tools for incident investigation and threat hunting.

Network Security — Tools & Approach



KEY TECHNOLOGIES

Micro-Segmentation

Illumio, Guardicore (Akamai), VMware NSX

NAC Solutions

Cisco ISE, Aruba ClearPass, Forescout

NDR Platforms

Darktrace, Vectra AI, ExtraHop Reveal(x)

VPN & ZTNA

Zscaler Private Access, Palo Alto Prisma, Cisco AnyConnect

DNS Security

Cisco Umbrella, Infoblox BloxOne, Cloudflare Gateway

IMPLEMENTATION APPROACH

1

Network Mapping

Complete asset inventory and traffic flow analysis

2

Segment & Isolate

Implement micro-segmentation based on data sensitivity

3

Deploy NAC

Enforce pre- and post-admission access controls

4

Enable NDR

Deploy AI-driven detection across network traffic

5

Secure DNS

Route all DNS through protective filtering services

6

Hunt & Respond

Ongoing threat hunting with packet-level forensics

Cloud Security

Protecting workloads, data, and identities across AWS, Azure, GCP, and multi-cloud



Cloud Security Posture Management (CSPM)

Continuous monitoring for misconfigurations, compliance violations, and drift across IaaS, PaaS, and SaaS environments.



Cloud-Native Application Protection (CNAPP)

Unified platform combining CSPM, CWPP, and pipeline security for full lifecycle cloud-native application protection.



Cloud Workload Protection (CWPP)

Runtime protection for VMs, containers, serverless functions, and Kubernetes clusters with vulnerability management.



SaaS Security & CASB

Shadow IT discovery, data protection, access control, and compliance monitoring for SaaS applications.



Cloud Identity & Entitlement Management

Least-privilege enforcement, entitlement reviews, and cross-cloud identity governance to eliminate excessive permissions.



Multi-Cloud Governance

Centralized policy management, cost optimization guardrails, and unified security dashboards across cloud providers.

Cloud Security — Tools & Approach



KEY TECHNOLOGIES

CSPM / CNAPP

Wiz, Prisma Cloud, Microsoft Defender for Cloud, Orca

CWPP & Container Security

Aqua Security, Sysdig, Lacework, Twistlock

CIEM

Ermetic (Tenable), CrowdStrike CIEM, Zscaler CIEM

CASB & SaaS Security

Netskope, Microsoft Defender for Cloud Apps, Skyhigh

IaC Security

Checkov, Snyk IaC, Terraform Sentinel, KICS

IMPLEMENTATION APPROACH

1

Cloud Assessment

Audit configurations against CIS Cloud Benchmarks

2

Enable CSPM

Deploy continuous posture monitoring with auto-remediation

3

Protect Workloads

Implement CWPP across VMs, containers, and serverless

4

Govern Identities

Right-size permissions with CIEM and JIT access

5

Shift Left

Integrate IaC scanning into CI/CD pipelines

6

Unified Visibility

Centralized dashboards across all cloud environments

Governance, Risk & Compliance



Aligning security strategy with business objectives, regulatory mandates, and enterprise risk appetite



Regulatory Compliance Management

End-to-end compliance program design for NIST, ISO 27001, SOC 2, HIPAA, PCI DSS, GDPR, and GDPR, and CMMC with automated evidence collection.



Internal Audit & Assessment

Independent security audits, gap analyses, and maturity assessments against CIS, NIST CSF, and ISO 27001 benchmarks with remediation roadmaps.



Enterprise Risk Management

Quantitative risk assessments, risk register maintenance, third-party risk scoring, and board-level risk reporting.



Third-Party Risk Management

Vendor security assessments, continuous monitoring of supplier risk posture, and contractual security requirement enforcement.



Policy & Standards Development

Creation and lifecycle management of security policies, standards, and procedures mapped to regulatory requirements.



Security Awareness & Training

Role-based training programs, phishing simulations, executive briefings, and culture-building initiatives to reduce human-factor risk.

GRC Services — Tools & Approach



KEY TECHNOLOGIES

GRC Platforms

ServiceNow GRC, Archer (RSA), MetricStream, OneTrust

Compliance Automation

Vanta, Drata, Tugboat Logic, AuditBoard

Risk Management

RiskLens, ProcessUnity, Prevalent, BitSight

Policy Management

NAVEX Global, PowerDMS, LogicGate, ZenGRC

Audit & Assessment

Workiva, TeamMate+, Galvanize (Diligent), HighBond

IMPLEMENTATION APPROACH

1

Assess & Baseline

Comprehensive compliance gap analysis against target frameworks

2

Define Governance

Establish GRC committee, risk appetite, and policy hierarchy

3

Implement Controls

Deploy GRC platform with automated control mapping and testing

4

Train & Certify

Role-based awareness programs and compliance certification tracks

5

Monitor & Report

Continuous compliance monitoring with executive dashboards

6

Audit & Improve

Regular internal audits and maturity model progression

GRC — Frameworks & Market Impact



The GRC platform market reached \$44.2B in 2025 and is projected to exceed \$64B by 2029, growing at 13.4% CAGR



NIST Cybersecurity Framework

Comprehensive five-function model — Identify, Protect, Detect, Respond, Recover — adopted by — adopted by 83% of U.S. organizations.



PCI DSS v4.0

Payment card industry standard with 64 new requirements effective March 2025, mandating enhanced authentication and encryption.



ISO 27001 & 27002

International gold standard for information security management systems with 93 controls across 4 domains.



HIPAA & HITRUST

Healthcare data protection framework with the HITRUST CSF integrating 50+ authoritative authoritative sources.



SOC 2 Type II

Trust services criteria audit demonstrating operational effectiveness of controls over 6–12 months.



CMMC 2.0 & GDPR

Defense contractor maturity certification and EU data privacy regulation requiring demonstrable security controls.

Security Operations Center



24/7 threat monitoring, detection, and response — the nerve center of your cybersecurity defense



24/7 Threat Monitoring

Round-the-clock surveillance of network, endpoint, cloud, and application telemetry with real-time alert triage by certified analysts.



SOAR & Automated Playbooks

Security orchestration with automated response playbooks for common scenarios, reducing mean time to respond by 80%.



Incident Detection & Response

Advanced threat detection using SIEM correlation, behavioral analytics, and AI-driven alert prioritization with sub-15-minute SLAs.



Forensic Investigation

Deep-dive incident analysis with full packet capture, memory forensics, and timeline reconstruction for root cause determination.



Threat Intelligence Integration

Curated threat feeds, dark web monitoring, and IOC enrichment providing proactive defense against emerging attack campaigns.



Executive Reporting & Metrics

Monthly SOC performance reports with KPIs including MTTD, MTTR, alert volumes, and risk trend analysis for leadership.

SOC Services — Tools & Approach



KEY TECHNOLOGIES

SIEM Platforms

Splunk Enterprise Security, Microsoft Sentinel, IBM QRadar

SOAR Solutions

Palo Alto XSOAR, Splunk SOAR, Swimlane, Tines, Torq

EDR / XDR

CrowdStrike Falcon, Microsoft Defender XDR, SentinelOne

Threat Intelligence

Recorded Future, Mandiant, ThreatConnect, MISP

NDR & Traffic Analysis

Darktrace, Vectra AI, ExtraHop Reveal(x), Zeek

IMPLEMENTATION APPROACH

1

Assess & Design

Define SOC scope, use cases, and technology stack requirements

2

Deploy SIEM

Implement log collection, parsing, and correlation rule development

3

Enable Detection

Tune detection rules with MITRE ATT&CK mapping and threat models

4

Automate Response

Configure SOAR playbooks for automated containment and notification

5

Operationalize

Staff SOC tiers, establish escalation procedures and SLA frameworks

6

Continuous Tuning

Ongoing rule optimization, threat hunting, and purple team exercises

SOC — Models & Tier Structure



The global SOC market is projected to reach \$18.8B by 2035, driven by 4.8 million unfilled cybersecurity positions worldwide



Tier 1 — Alert Triage

First-line analysts monitoring dashboards 24/7, triaging alerts, and escalating confirmed incidents within SLA windows.



Dedicated SOC Model

Fully staffed on-premises or virtual SOC with dedicated analysts, custom runbooks, and direct integration.



Tier 2 — Incident Analysis

Senior analysts conducting deep-dive investigations, correlating events, and determining scope and root cause.



Hybrid SOC Model

Combination of in-house security team and outsourced SOC capabilities, providing 24/7 coverage.



Tier 3 — Threat Hunting

Expert-level proactive threat hunters using hypothesis-driven analysis to uncover hidden adversary activity.



SOC-as-a-Service

Fully managed cloud-based SOC delivering enterprise-grade monitoring without capital investment.

Network Operations Center



Proactive network monitoring, performance optimization, and uptime assurance across your entire IT infrastructure



24/7 Network Monitoring

Continuous surveillance of routers, switches, firewalls, servers, and cloud infrastructure with real-time alerting and escalation.



Configuration Management

Automated configuration backup, drift detection, compliance validation, and standardized change deployment.



Performance Management

Bandwidth utilization tracking, latency monitoring, jitter analysis, and capacity planning for optimal performance.



Availability & Uptime Assurance

SLA-backed availability targets of 99.99%, proactive fault detection, redundancy monitoring, and rapid failover orchestration.



Incident & Change Management

ITIL-aligned incident response, problem management, and change control processes with full audit trails.



Capacity Planning & Optimization

Trend analysis, traffic forecasting, and infrastructure right-sizing recommendations to prevent bottlenecks.

NOC Services — Tools & Approach



KEY TECHNOLOGIES

Network Monitoring

SolarWinds, PRTG Network Monitor, Datadog, Nagios XI

AIOps & Analytics

Moogsoft, BigPanda, Dynatrace, ServiceNow ITOM

Configuration Mgmt

Ansible, Puppet, Chef, NetBox, Infoblox

ITSM & Ticketing

ServiceNow, Jira Service Management, BMC Helix

Cloud Monitoring

AWS CloudWatch, Azure Monitor, GCP Operations Suite

IMPLEMENTATION APPROACH

1

Discovery & Baseline

Complete network inventory and performance baseline assessment

2

Deploy Monitoring

Implement multi-layer monitoring with custom thresholds and alerts

3

Integrate ITSM

Connect NOC workflows to ticketing, CMDB, and change management

4

Automate Response

Build automated remediation runbooks for common network issues

5

Optimize Performance

Continuous tuning of alerts, dashboards, and escalation paths

6

Report & Plan

Monthly capacity reports, trend analysis, and infrastructure roadmaps

NOC — Tiers & Market Drivers



The NOC-as-a-Service market is growing at 10.2% CAGR, driven by hybrid cloud complexity and AI-powered network automation



L1 — Monitoring & Alerting

First-level operators managing monitoring consoles, acknowledging alerts, and escalating per defined runbooks.



AI-Driven NOC Operations

Machine learning models for anomaly detection, predictive failure analysis, reducing MTTR by up to 60%.



L2 — Advanced Troubleshooting

Experienced network engineers performing root cause analysis and resolution of multi-system incidents.



Hybrid & Multi-Cloud NOC

Unified monitoring across on-premises, public cloud, and edge environments with correlated visibility.



L3 — Architecture & Design

Senior architects handling capacity planning, network design optimization, and strategic decision-making.



Compliance & Reporting

Automated SLA reporting, uptime dashboards, compliance documentation for ITIL, SOC 2, and more.

Security Managed Services



End-to-end managed security operations delivering enterprise-grade protection without the overhead of building in-house capabilities



Managed Detection & Response

24/7 threat monitoring, investigation, and guided remediation delivered by expert analysts with guaranteed SLAs.



Managed Firewall & Network Security

Configuration, monitoring, and management of next-gen firewalls, IDS/IPS, and network security infrastructure.



Managed SIEM & Log Analytics

Fully managed log collection, correlation, and analysis with custom detection rules and compliance reporting.



Managed Cloud Security

CSPM, workload protection, identity governance, and compliance monitoring across AWS, Azure, and GCP.



Managed Vulnerability Services

Continuous vulnerability scanning, risk-based prioritization, and remediation tracking across your attack surface.



Managed Endpoint Protection

Deployment, tuning, and 24/7 monitoring of EDR/XDR platforms with proactive threat hunting.

Why Partner With Us

The trusted cybersecurity and managed services partner for enterprise organizations



24/7 Security Operations Center



Round-the-clock monitoring, detection, and response by certified analysts with average 15-minute response time.

Vendor-Agnostic Approach



We integrate best-of-breed solutions regardless of vendor, ensuring the optimal technology stack for your needs.

Compliance Expertise



Deep experience across NIST, ISO 27001, SOC 2, HIPAA, PCI DSS, GDPR, and CMMC with audit-ready documentation.

Certified Security Professionals



Team of CISSP, CISM, CEH, OSCP, and cloud-certified engineers with expertise across all security pillars.

Measurable Outcomes



SLA-backed service delivery with executive dashboards, risk reduction metrics, and quarterly business reviews.

Scalable Engagement Models



Flexible options from project-based assessments to fully managed services, scaling with your business.

Cloud Security — Expanded Services



Next-generation offerings for data, workloads, identities, and zero-trust access across every cloud



Data Security Posture Management (DSPM)

Discovery, classification, and risk monitoring of sensitive data across cloud data stores with automated remediation.



Secrets Management & Cloud KMS

Centralized vaulting, rotation, and lifecycle management of API keys, tokens, and certificates.



Container & Kubernetes Security

Image scanning, runtime threat detection, admission control, and policy enforcement for containerized workloads.



Cloud DLP & Tokenization

Tokenization, field-level encryption, and content-aware data loss prevention across cloud storage.



Cloud Detection & Response (CDR)

24/7 monitoring of cloud control planes with behavioral analytics to detect account compromise and exfiltration.



SASE / SSE with ZTNA

Converged secure access combining ZTNA, SWG, CASB, and FWaaS to enforce zero-trust connectivity.

Engagement Models

Flexible service delivery options tailored to your IT infrastructure maturity and business needs



01 ASSESS

Security Assessments

-  Vulnerability assessments
-  Penetration testing
-  Risk analysis
-  Compliance gap review
-  Architecture review

02 BUILD

Implementation & Integration

-  Solution design & deployment
-  Technology integration
-  Policy & playbook creation
-  Staff training & enablement
-  Migration & hardening

03 MANAGE

Managed Security Services

-  24/7 SOC monitoring
-  Managed detection & response
-  Continuous compliance
-  Incident response retainer
-  Executive reporting & QBRs

We Get **IT** Done



Ready to Strengthen Your Security Posture?

Partner with ExaBIT Systems for Consulting, Professional Services, or 24/7 Managed Security.



ExaBIT Systems Australia



contact@exabitsystems.com



Cybersecurity & MSSP Practice

CONFIDENTIAL