GORILLA

GORILLA SECURITY CONVERGENCE

Detect, Analyze, Respond, and
Prevent Internal and External Threats with Gorilla's AI

Endpoint Protection

gorilla-technology.com

INNOVATIVE DIGITAL & PHYSICAL ASSET PROTECTION

FOR SMARTER CITIES AND ENTERPRISES

Protect your systems from aggressive and ever-evolving digital threats with cutting-edge IT and OT security solutions from Gorilla.

Our Security Convergence technology offers everything from AI-based threat pattern learning which identifies unknown malware to taking protective actions and processing incidents. Protect your network and digital assets from malicious external networks and endpoint hosts.

This series delivers early intervention with automated and uninterrupted protection against various threats and attacks to reduce potential damage and loss.

SECURITY CONVERGENCE VALUES

AI-Based Detection

Intervene early when unknown threats are identified and easily process incidents with automated and always-on AI-based threat pattern learning.

Localized Protection

Automatically create tailor-made network security with AI-based behavior analysis of targeted attack activities while reducing the large and recurring costs of increasing staff.

Asset Safety

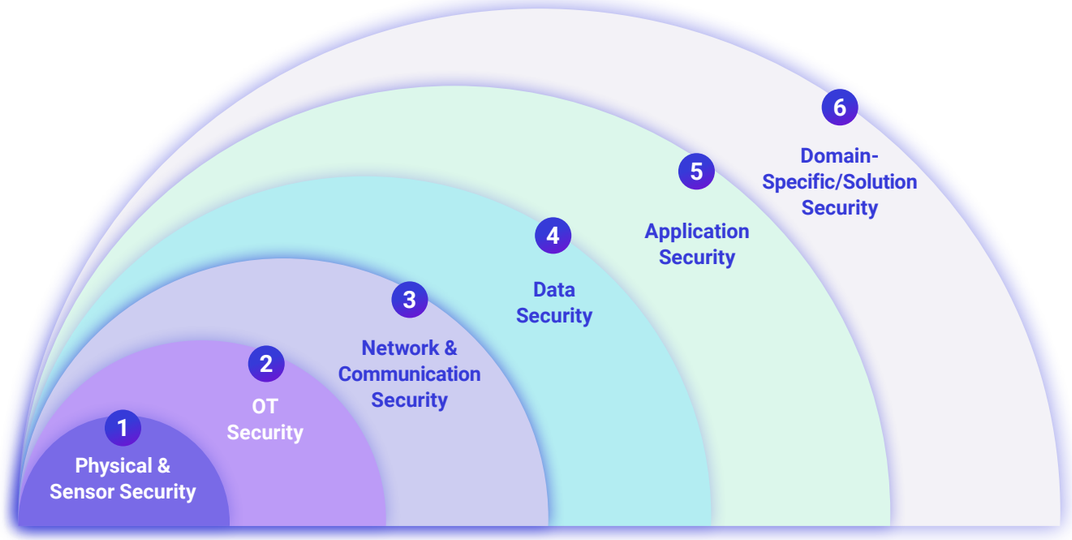
Protect intellectual property, customer loyalty, brand reputation and revenue by reducing the risk of internal confidentiality and customer information being leaked.

Quick Recovery

Shorten response times when attacks occur, uncover the root cause of security problems, and restore business operations without interruption.

GORILLA'S

CYBERSECURITY FRAMEWORK



1 Perception Layer (Physical IOT Devices)

- Device Identity & Authentication
- Data Integrity, Non-Repudiation, and Encryption

2 Edge AI / Control Layer

- Asset Inventory & Risk Assessment
- Access Control & Authentication
- Endpoint Detection & Response

3 Network Layer

- Network Segmentation and Zoning Design
- Communication Channel Protection: SD-WAN, VPN and Tunneling
- Network Access Control
- DoS/DDoS Protection, Firewall, IDS/IPS, WAF, NDR, DLP

4 AI PaaS Layer

- Data Classification
- Data Availability, Backup and Restore
- Privacy Protection and Data at Rest Encryption
- Data Lifecycle Management

5 Application Layer

- API Security
- Static Code Analyzer
- Vulnerability Scanner and Fuzzing
- Audit Log and Accountability

6 Smart Solution Layer

- Understanding Industry Threat Landscape
- Supply Chain Security
- User Education and Awareness
- Compliance with Industry Regulations & Standards
- Collaboration and Information Sharing
- SIEM: Security Monitoring
- SOAR: Incident Response and Automation

GORILLA'S MANAGED

CYBERSECURITY SERVICES

01 Define the Scope

02 Regulatory and Standard Compliance

03 Identify Assets and Critical Infrastructure

04 Threat Modeling

05 Endpoint, Network, Data, Cloud & Physical Security

06 Continuous Monitoring & Information Sharing

07 Periodic Reviews and Updates

WHO WE MAKE SMARTER

1 Smart & Safe City

Revolutionize quality of life and boost economic competitiveness with Gorilla's cutting-edge AI solutions.

2 Transportation & Logistics

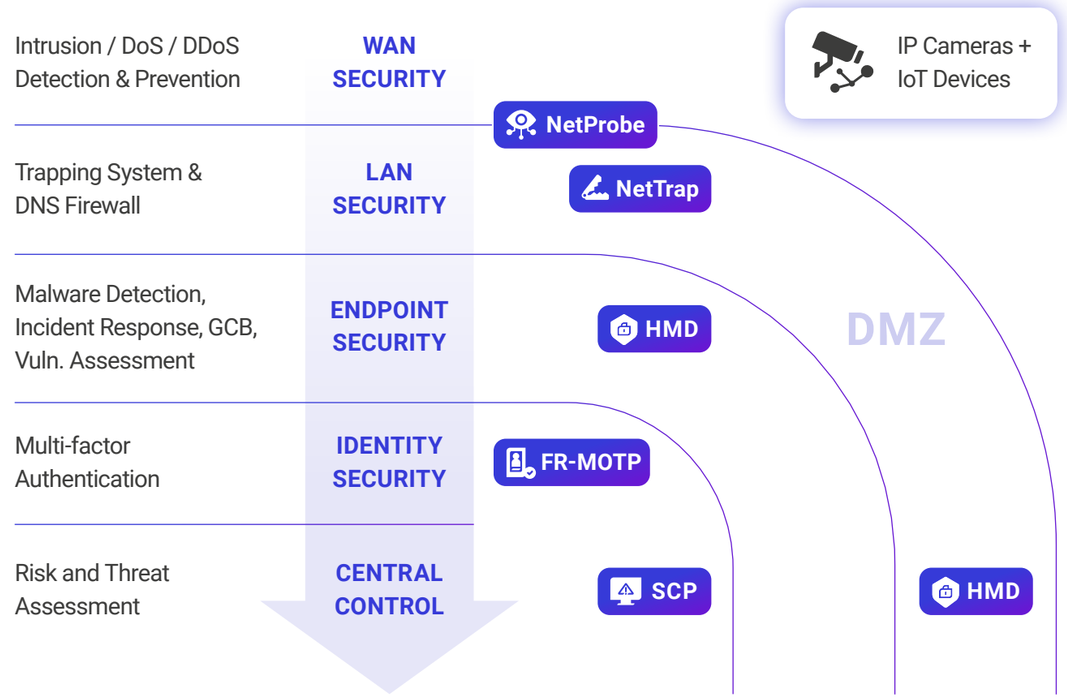
Streamline operations through advanced analytics, predictive maintenance, and intelligent route planning.

3 Buildings & Offices

Empower spaces with data-driven decision-making across all systems with innovative technology.

END-TO-END AI-BASED CYBERSECURITY

FOR OT & IT ENVIRONMENTS

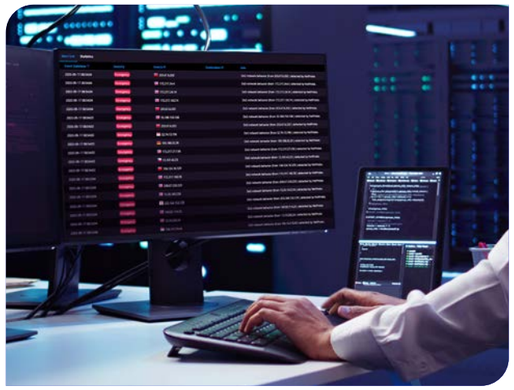


NetProbe

AI-BASED NETWORK INTRUSION PREVENTION

Detect and Block Various Types of External Attacks at The Edge of All Network Connection Points

From malicious IP connections to DDoS or other targeted attacks, the AI-based detection engine in NetProbe automatically detects and blocks without human intervention which greatly reduces manual processes & alert fatigue on staff which allows your team to focus on key security actions.



Precise & Up-to-Date

NetProbe can identify and learn localized cyber attack patterns. Moreover, it can automatically sync & update threat intelligence with the Security Convergence Intelligence Center.

DoS / DDoS Protection

Use machine learning algorithms which learn network traffic characteristics and automatically execute Layer 3 & Layer 4 DoS/DDoS detection and blocking.

Intelligent Defense

AI-based technology automatically detects and blocks malicious connections without the need for IT staff intervention. Supports inline deployment methods and provides a bypass network interface so when equipment fails, packet transmission is unaffected and overall network operations go uninterrupted.

Specific Alerts & Notifications

The network administrator will receive attack detection notifications which include time, source/destination IP, triggering rules, and other key data. These notifications will be added to and sent with an automated daily email report.

NetTrap

CATCH THREATS WITH DECEPTION TECHNOLOGY

Detect Internal Infection Spread and Block Malicious External Connections

Hackers who gain network access will be caught by NetTrap when they probe the internal network or report to the C2 server. NetTrap can detect and catch potential threats within the network, suppress the spread of malicious programs and activity within the network, and at the same time intercept malicious external connection attempts.

Mimic Devices & Catch Threats

Simulate a variety of network services and devices, including hosts, servers, databases, NAS, IoT, and cameras, to trap and reveal hacker activity.

Automatic Threat Updates

The malicious domain name list is auto-updated regularly which greatly reduces the need to maintain a complex connection list on-site.

DNS Protection

- Automatically protects employees and systems from over a million malicious websites, ransomware, and springboard hosts.
- DoH/DoT (DNS over HTTPS/TLS) improves network security and privacy by protecting DNS resolution from eavesdropping or modification.

Up-to-the-Minute Alerting

Network administrators gain insights from real-time email reports (regular to emergency alerts) featuring up-to-the-minute statistics on blocklisted IPs, received packets, and malicious IP triggers. Alerts are exportable via syslog for comprehensive investigation.

HMD

ENDPOINT PROTECTION VIA AN AI ENGINE

Deploying Host-based Malware Detection (HMD) with our patternless AI engine continuously monitors endpoint health, detects anomalies, and identifies vulnerabilities. This empowers staff to quickly detect, source, and respond to APT (Advanced Persistent Threat). HMD integrates EDR (Endpoint Detection and Response), GCB (Government Configuration Baseline), and vulnerability alerts for comprehensive endpoint security.

Endpoint Protection

HMD surpasses traditional AVS by detecting Advanced Persistent Threats (APT) through comprehensive endpoint threat assessment, from network and files to programs and memory. It continuously assesses risk, alerting staff to abnormalities immediately.

Protection via Compliance

- Verify GCB and other government and industry configuration compliance at the OS level to reduce information security risks.
- Detect software vulnerabilities and understand the system's protection status at-a-glance.

Incident Response

When an incident is detected, the host is reported for further analysis while all other endpoints in the system are scanned under the same detection rules to track spread.

Multi-Faceted Threat Detection

Our cybersecurity professionals created a patternless AI-based malware detection engine which automatically detects malicious programs and effectively assists management in cleaning system infections.

Enhance Network Security with Critical Endpoint Protection, Providing Risk Level Summaries for Each Endpoint to Facilitate Immediate Action

- Anomaly Detection
- Detect Suspicious Files
- Multiple Host Deployment
- AI Algorithms & Digital Forensics
- Monitor Programs & Settings
- Endpoint Risk Alerts

SCP

SYSTEM THREAT MONITORING & ANALYSIS PLATFORM

Integrates & Unifies Various Network Security Data onto A Single Platform

SCP automates threat detection and IT/OT asset protection by cross-correlating heterogeneous logs, global threat data, and endpoint monitoring. Management and administrators gain proactive insight to track, analyze, and resolve infrastructure issues.

Comprehensive Threat Management

- Auto-sync & update threat intelligence lists with the Gorilla Security Convergence central database.
- Unifying NetProbe, NetTrap, and HMD on a single platform delivers complete threat intelligence and strengthens organizational security through a Defense-in-Depth strategy.

Log Integration & Analysis

Cross-correlate server, service, and host logs to associate abnormal events. Integrate with existing SIEMs and centralize log management for customizable alarms through a single interface.

Visualized Network Management

Easily manage network assets by visualizing their physical locations & schedule regular endpoint health checks.

Incident Management

Centrally manage the tracking, reviewing, reporting, and notification mechanisms for network security incidents to increase productivity and simplify day-to-day operations.

SIEM Integration

Can be integrated with existing SIEM systems via syslog support, it is easy to deploy and convenient to centrally query, analyze and identify key data.

Analyze Network Usage

Run real-time threat assessments, determine behavior abnormalities, and get instant alerts as well as in-depth reporting to help allocate resources.

EdgeGuard

AI-BASED OT SECURITY APPLIANCE

Detect and Block Threats with Localized Threat Intelligence

Designed for rugged environments, EdgeGuard leverages edge AI and a comprehensive trapping system to learn threat patterns, block external attacks, and enable early discovery of potential threats, surpassing typical IDS/IPS protection.

Detect & Block Malicious IPs

Detect malicious IP connections using a 1 million IP blocklist by directly comparing the blocklisted IP, which is faster and much more efficient in detecting attacks.

Simulated Threat Trapping

Lure and trap malicious hosts by simulating network services, such as: general hosts, server hosts, databases, NAS, IoT devices, printers, and IP surveillance cameras.

Inline Bypass for Equipment Failure

Operate inline with bypass capabilities, ensuring uninterrupted network connectivity even during equipment failure.

OT Environment Deployment

Detect targeted attacks on IoT and industrial control system environments, including network protocols, communication, or topology anomalies.

Alert Notifications

When a malicious attack is detected, an alarm message will be sent to the management interface to notify network administrators.

Visual Management Interface

- Simplify device management & data display.
- Provide clear front-line network status.
- Enable immediate problem resolution.

FR-MOTP

ELEVATED IDENTITY SECURITY WITH FACIAL RECOGNITION

Multi-Layered Protection from Identity Theft and Brute Force Attacks

The increase in working from home and off-site due to the pandemic together with the increase in cross-regional operations have also increased system exposure and the risk of more network attacks. Basic VPN, account, and password login procedures adopted by most companies provide insufficient levels of protection.

Gorilla's advanced face recognition (FR) technology verifies staff biometrics on their mobile phone and a time sensitive Mobile One Time Password (MOTP) is issued. This one-use dynamic password greatly reduces the risk of corporate network intrusions.

Multi-Factor Authentication

Make it next to impossible for hackers to infiltrate your network by adding FR-MOTP to traditional account logins for multi-factor and real-time authentication.

Advanced Face Recognition

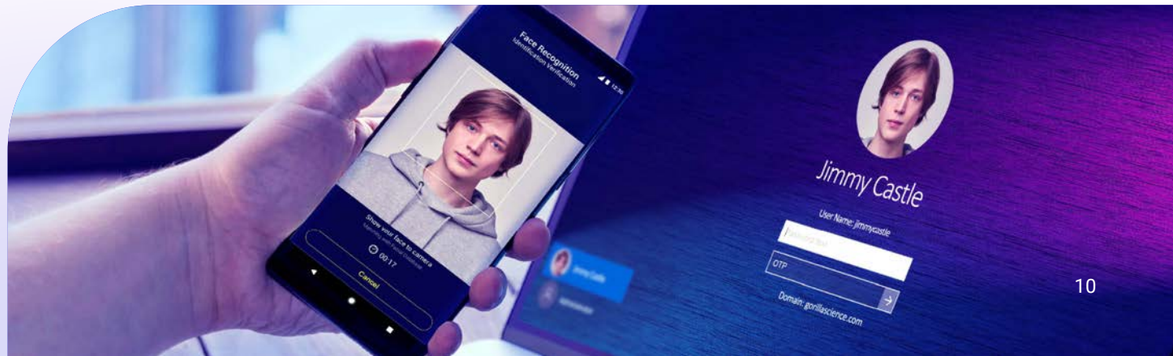
User identities are verified in real-time with the edge AI biometric technology developed by Gorilla and a one-time password is sent to their personal device-ensuring the right person's login while protecting privacy.

Log Abnormalities

Record staff logins along with face recognition results in real-time. Logs of failed verifications can allow managers to perceive intrusions in advance.

Rapid Integration and Deployment

Easily strengthen your login verification system without changing OS accounts and passwords.



LONDON OFFICE (HEADQUARTERS)
North Row, 64 North Row,
London, W1K 7DA

TAIPEI OFFICE
7F, No.302, Ruey Kuang Road,
Neihu, Taipei 114720, R.O.C

CHENNAI OFFICE
Josmans Complex, No. 8/5, 3rd Floor,
MC Nichols Road, Tamil Nadu,
Chennai-600031, India

CAIRO OFFICE
Cairo Festival City – Plot 12b03/B,
First Floor, New Cairo, Cairo Egypt

BANGKOK OFFICE
One Bangkok Tower 4, Unit 1214, 12F,
Witthayu Road, Lumphini, Pathum Wan,
Bangkok 10330

SEATTLE OFFICE
701 Fifth Ave, Suite 4200 Seattle,
Washington 98104

SINGAPORE OFFICE
1 Fullerton Road, #02-01 One Fullerton,
Singapore 049213

REQUEST A DEMO