Gorilla Security Convergence

Detect | Analyze | Respond | Prevent

Gorilla Technology Group
www.gorilla-technology.com

Gorilla Security Convergence

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 Value

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.

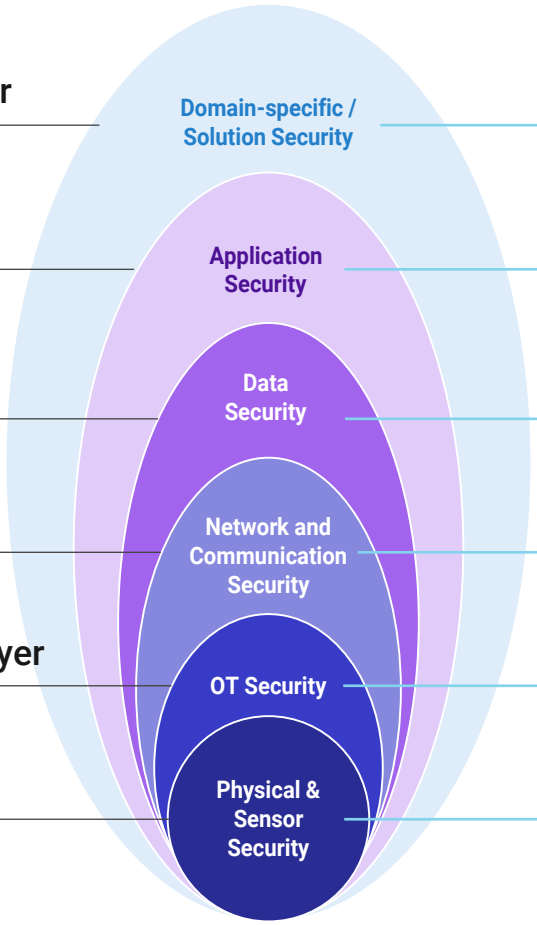
Asset Safety

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 for Smart and Safe Cities



- Understanding industry threat landscape
- Supply chain security
- User education and awareness
- Compliance with industry regulations and standards
- Collaboration and information sharing
- SIEM: Security monitoring
- SOAR: Incident response and automation

- API security
- Static code analyzer
- Vulnerability scanner
- Fuzzing
- Audit log and accountability

- Data classification
- Data availability, backup and restore
- Privacy protection and data at rest encryption
- Data lifecycle management

- 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

- Asset inventory
- Risk assessment
- Access control and authentication
- Endpoint detection and response

- Device identity and authentication
- Data integrity, non-repudiation, and encryption

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, and Physical Security

06 Continuous Monitoring and Information Sharing

07 Periodic Reviews and Updates

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.

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.

DoS/DDoS Protection

Use machine learning algorithms which learn network traffic characteristics and automatically execute Layer3 & Layer4 DoS/DDoS detection and blocking.

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 range of network services and devices like general hosts, server hosts, databases, NAS, IoT Devices, printers, IP surveillance cameras, etc. to lure hackers in and expose their whereabouts.

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 protect employees and internal systems from connecting to malicious websites and stop them from becoming springboard hosts or getting ransomware — all with a block list of over one million.
- DoH/DoT (DNS over HTTPS/TLS) can be used to avoid DNS resolution requests from being eavesdropped or modified in order to improve the level of network security and privacy.

Up-to-the-Minute Alerting

From regular reports to emergency alerts, network administrators can get emails with up-to-the-minute statistics, including the total numbers of blocklisted IPs, received packets, and malicious IPs triggered. Furthermore, alerts can be exported using sysloginterface for comprehensive investigation and analysis.

NetTrap

Our customized technology is the perfect trapping system: set up a comprised set of isolated data to entice hackers and catch potential threats.

- Catch Internal Threats (Detect Lateral Movement of Malware in LAN)
- Block Connections to Known Malicious Sites
- DoH/DoT Proxy
- Email Alert Notifications
- Detailed Reporting Analysis
- Latest Attacks / Alerts

HMD

Endpoint Protection via an AI Engine

Deploy HMD (Host-based Malware Detection) on each endpoint host to leverage our patternless AI-based malware detection engine which continuously monitors overall endpoint health, detects anomalies, and alerts about software vulnerabilities.

Empower staff to quickly detect Advanced Persistent Threat (APT) infections, determine the source, and take appropriate response measures. HMD integrates EDR (endpoint detection and response), GCB (Government Configuration Baseline), and software vulnerability alerts to deliver a comprehensive endpoint security solution.

Endpoint Protection

HMD goes beyond regular AVS to detect Advanced Persistent Threat (APT) infections by assessing threat level of endpoints in your systems, from networks to files and programs to memory. HMD continuously assesses risk and immediately alerts staff when abnormalities are found.

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.

HMD

HMD (Host-based Malware Detection) adds critical endpoint security protection to your network. Get summaries on the risk levels for each endpoint and take immediate action.

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

SCP

Assess, Alert, Report

System Threat Monitoring & Analysis Platform

SCP (Security Convergence Platform) integrates and unifies various network security data onto a single platform.

This advanced analysis tool leverages heterogeneous system logs to global threat data and endpoint monitoring feeds to easily perform tasks like cross-correlation of security events, finding hidden threats and compromised devices & networks — automatically alerting staff according to the security threat level.

SCP gives management and administrators the power to track, analyze, and proactively handle issues across IT and OT assets.

Comprehensive Threat Management

- Auto-sync and update threat intelligence lists with the Gorilla Security Convergence central database.
- Unify NetProbe, NetTrap, and HMD solutions under a single platform to deliver complete intelligence information covering all types of threats. This Defense-in-Depth strategy strengthens organizational security protection.

Log Integration & Analysis

Associate abnormal events by cross-correlating log content from servers, services and hosts. Search and customize alarms by integrating with existing SIEM systems and centralizing log management into a single interface.

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.

Visualized Network Management

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

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.

Incident Management

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

EdgeGuard

AI-Based OT Security Appliance

Detect and block threats with localized threat intelligence

EdgeGuard learns threat patterns and blocks attacks from external networks. Designed for rugged or industrial environments, EdgeGuard goes beyond typical IDS/IPS protection by using edge AI to determine threats and by offering a comprehensive trapping system — allowing early discovery of potential threats.

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.

Trap Threats with Simulation Techniques

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 in inline mode with bypass capabilities in case of equipment failure. It can automatically let network packets pass through without affecting network connectivity.

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

Visualized dashboard for device management and statistical data display allows administrators to easily understand the front-line network status and how to deal with problems immediately.

Deployed in OT and industrial environments, EdgeGuard can defend against cyber threats for IT & OT devices as well as safeguard industrial facilities.

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

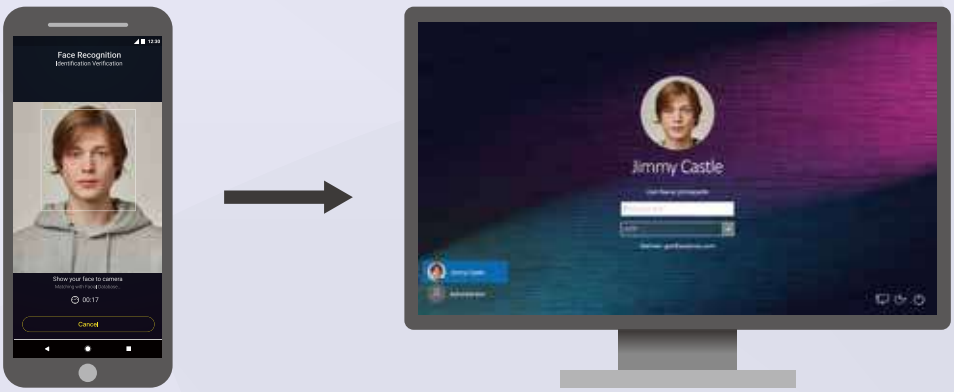
User identities are verified in real-time with the edge AI biometric technology developed by Gorilla and a one-time password is sent to their personal device - ensuring the right person's login while protecting privacy.

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.



Powered by Gorilla Technology

Specifications are subject to change. Gorilla products are sold with a limited warranty. Gorilla Technology Group.