Plurilock™ Critical Services

Advanced services and solutions for the world's most difficult environments and business problems.

Plurilock
CRITICAL SERVICES

Who is Plurilock?

We're a cybersecurity innovator, a world-class solutions consultancy, and a full stack technology reseller.

Unlike other organizations, Plurilock has the experience, expertise, and resources to provide end-to-end solutions, from strategy and planning through procurement, deployment and integration.

World-class research and engineering expertise. Founded as a research spinout, Plurilock holds multiple patents, boasts a team of PhD data scientists and software engineers, and offers its own comprehensive line of cybersecurity products.

World-class field expertise. Working hand-in-hand our research and engineering team, our veteran team of battle-tested technology, platform, and vendor field engineers holds some of the world's most exclusive certifications.

World-class, same-team procurement. Our Aurora division is a world-class VAR with access to every leading technology product and platform in use in business today—often at significant cost advantage due to our relationships and volume.

We offer what others can't. One team that handles every part of the solution process, from discussion and ideation through procurement and successful deployment and integration.

Selection of current and past customers that can be publicly represented

Plurilock CRITICAL SERVICES

Advanced Solutions for Critical Business Problems

Plurilock delivers the expertise and capabilities you need in a world of increasing risk—quickly.

Data and security breaches. Regional warfare. Natural disasters. Pandemics and social crises. Supply chain instability and opacity.

These are challenging times in cybersecurity. The rates of just about every cause of significant business risk are accelerating—along with the need to manage this risk carefully and to resolve complex, unpredictable crises as quickly as they emerge.

Plurilock Critical Services was founded to enable modern organizations to continue to safely operate—and adapt—as change happens.

- Unmatched, global, multi-domain expertise
- An extensive family of patented and proprietary cybersecurity technologies
- A comprehensive line of class-leading IT products and services

IP Protection

- Insider Threat Management
- Data Loss Prevention (DLP) Implementation
- Supply Chain Security Analysis
- IP Data Mapping + Risk Assessments
- Cloud Security Posture Management (CSPM)

Security Operations (SecOps)

- Threat Hunting Assessments
- SIEM/NDR/EDR/XDR Implementation
- Incident Response and Digital Forensics

Advisory

- Information Security Compliance Readiness
  - ISO27001, SOC2, CMMC, FedRAMP, FISMA, PCI-DSS, HIPAA, SEC, SOX
- Third Party Risk Analysis
- Cybersecurity Awareness + Training

Zero Trust (ZTA)

- Zero Trust Architecture Design + Implementation
  - Identity Access Management (IAM)
  - Zero Trust Network Access (ZTNA)
  - Secure Web Gateway (SWG)
  - Cloud Access Security Broker (CASB)
  - Secure Access Service Edge (SASE)
  - Micro Segmentation

Offensive Security (OffSec)

- Penetration Testing As A Service (PTaaS)
  - Including Network, Web, API, Mobile, Cloud, ICS/SCADA/IoT, AI/LLM, Social Engineering Testing and more.
- Continuous Red Teaming + Purple Teaming
- Managed Attack Surface Reduction
- White Box Security Architecture Analysis
- Cybersecurity Risk Assessments
  - Including Traditional + Cloud Systems
- Continuous Security Analysis In The SDLC
  - SCA/SAST/DAST, DevSecOps + SaC

Plurilock CRITICAL SERVICES

Core Offensive Security Service Offerings

Plurilock's offensive cybersecurity team is composed of veteran battle-tested security engineers who lead at the front with as cyber researchers and leaders, uncovering numerous zero-day CVEs in software utilized by the world's largest organizations. This deep industry underpins the "next-level" insight delivered through our services and is why Plurilock is the "go-to cyber strike team" for many Global 2000 organizations and governments.

Penetration Testing As A Service (PTaaS)

Emulating malicious actors with the intent to compromise company IT systems

Continuous Red Teaming + Purple Teaming

Advanced penetration testing, social engineering and ransomware exercises

Managed Attack Surface Reduction + Vulnerability Analysis

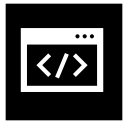
Real-time analysis + response to newly emerging vulnerabilities at the perimeter

White Box Security Architecture Analysis

Threat modeling + analysis of complex tech Stacks + platform ecosystems

Cybersecurity Risk Assessments

Risk based assessments of corporate and technology security controls



Continuous Security Analysis In The SDLC

Managed static + dynamic application security testing with continuous insights

Security Testing Domains

Traditional Network + Server Infrastructure

Cloud Systems + SaaS (M365, AWS, Azure, GCP)

Web Applications

APIs + SDKs

Mobile Applications

ICS/SCADA/IoT Systems

Generative AI + LLM Agents

Staff Social Engineering

Physical and Wireless

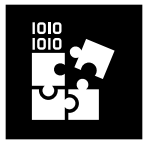
Plurilock
CRITICAL SERVICES

Advanced OffSec Research + Reverse Engineering Services

Plurilock's advanced security research services are designed emulate the sophistication of a state-level threat actor and identify zero-day vulnerabilities and exploits within complex ecosystems and products leveraged across critical infrastructure which include Web/Mobile/Thick-Client applications, REST/SOAP/GraphQL APIs, RTOS embedded devices, IoT devices and SCADA/ICS systems.

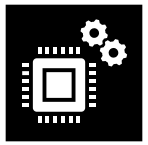
Conventional Static + Dynamic Application Security Testing

Automated SAST/DAST scanning
Dependency analysis
Input fuzzing + injection testing
Manual code review



Static Software Reverse Engineering + Binary Analysis

Embedded credential, API key, cryptographic key extraction + exploitation
Binary disassembly + decompilation
Manual control flow graph analysis
Dependency + code signing manipulation



Dynamic Software Reverse Engineering + Runtime Analysis

Network communications + protocol analysis with certificate pinning bypass
Runtime memory dumping + process analysis with anti-debugging trap circumvention
Real-Time Function Hooking + code tracing
Dynamic binary instrumentation

Hardware Reverse Engineering + Firmware Analysis

JTAG/SWG/UART/serial interface debugging, sniffing, tampering + data extraction
SPI/LPC/I2C/CAN bus sniffing + analysis
SPA/DPA side channel analysis
BGA Chip, EEPROM + NAND/NOR memory data extraction

Public CVEs Discovered by Our Network of OffSec Engineers

- Screen Connect CVE-2023-47256 Local Privilege Escalation
- Screen Connect CVE-2023-47257 Remote Code Execution
- Polycom CVE-2023-24282 Cross-Site Scripting
- Edge Nexus CVE-2022-37719 Cross-Site Request Forgery
- Edge Nexus CVE-2022-37718 Remote Code Execution
- Snapt Aria CVE-2022-24237 Remote Code Execution
- Snapt Aria CVE-2022-24236 Insecure Permissions
- Snapt Aria CVE-2022-24235 Cross-Site Request Forgery
- A10 Networks CVE-2020-24384 Remote Code Execution

Plurilock
CRITICAL SERVICES

Continuous Security Insights That Drive Full Risk Lifecycle Management

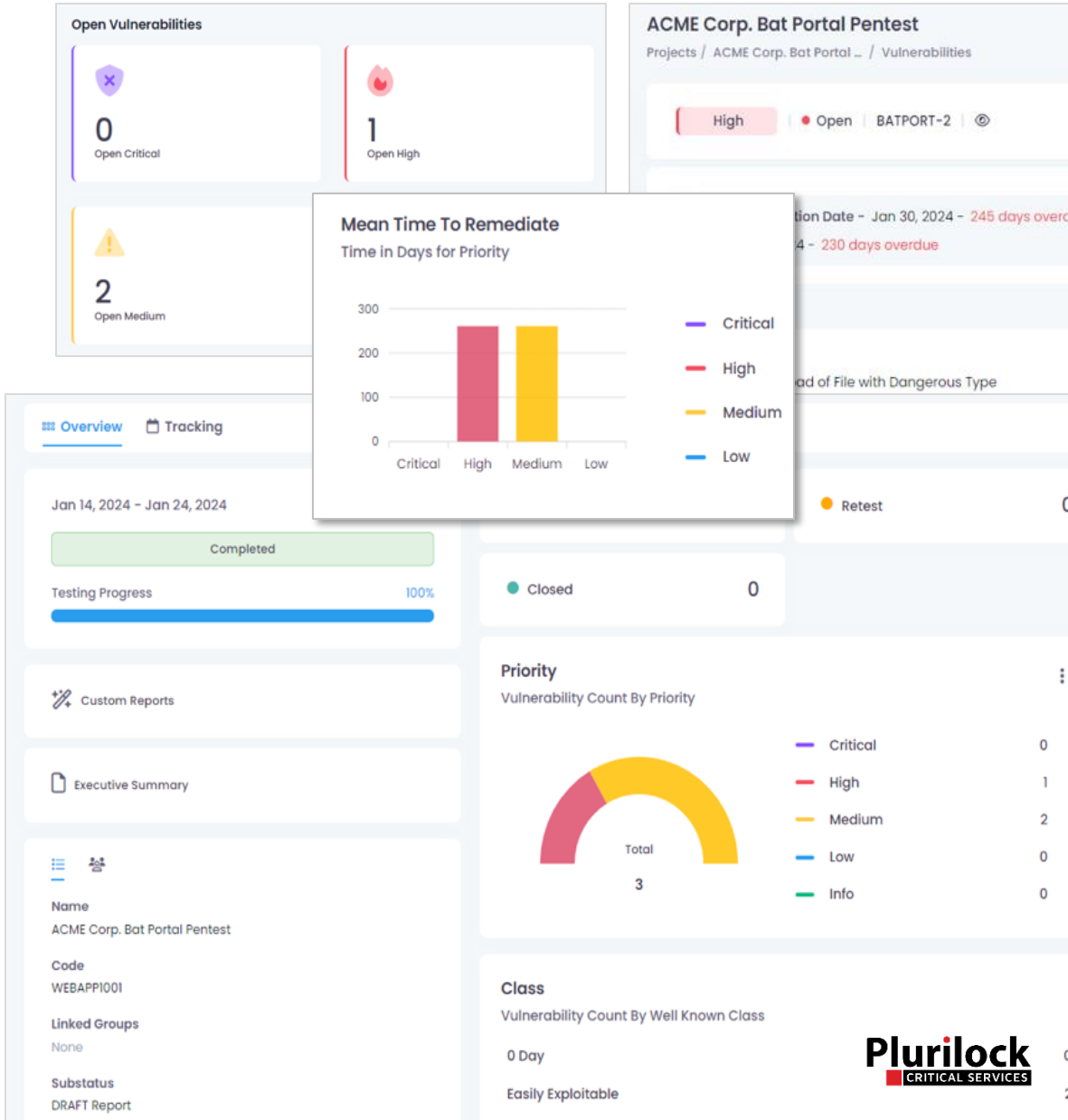
With Plurilock's continuous security testing portal and A+ cyber strike team, we go beyond the broken "one-time snapshot" security model. We drive action with prioritized security findings, curated remediation recommendations, testing KPIs, and status/remediation/retesting tracking that reduces vulnerability mean time to remediation (MTTR).

Where other cyber firms stop at just finding vulnerabilities, Plurilock's offensive cybersecurity goes beyond.

We demonstrate how the organization DiD (defense-in-depth) security model withstands against a real APTs (advanced persistent threats)

We provide specific and actionable risk remediation recommendations from veteran engineers

Our team provides a platform for prioritizing, tracking and retesting security findings that's backed by expert guidance



Elite and Trustworthy Ethical Hacking Team

At Plurilock, we prioritize quality above all else, this means our entire offensive cybersecurity team is made up of passionate and well-vetted security engineers that are respected leaders and researchers. While our team prides itself the most on the results we deliver, they maintain leading certifications in their respective domains.

With experience across every major vertical, Plurilock's security testing services support the frameworks, regulations and certifications that mean the most to your organization—including NIST CSF, CMMC, FedRamp, SOC2, PCI-DSS, HIPAA, SOX, GLBA, ISO27001, and more.

Our Core Security Testing Methodologies

- Penetration Testing Execution Standard (PTES)
- MITRE ATT&CK Framework
- NIST SP800-115 — Technical Guide For Information Security Testing and Assessment
- NIST SP800-37 — Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
- OWASP Web Security Top Ten
- OWASP Mobile Security Top Ten
- OWASP API Security Top Ten
- OWASP Serverless Top Ten
- OWASP LLM AI Top Ten

"Plurilock's offensive cybersecurity team is at the forefront of the latest malicious actor tactics, industry threats and security trends which is underpinned by a world-class advisory council, with many advisors formerly serving in high-ranking positions across the US department of defense"

OFFENSIVE SECURITY OSCP

OFFENSIVE SECURITY OSWE

OFFENSIVE SECURITY OSWP

CISSP® Certified Information Systems Security Professional

CERTIFIED RED TEAM PROFESSIONAL

Plurilock CRITICAL SERVICES

Zero Trust Architecture + IP Protection Offerings

In today's evolving threat landscape, large enterprises must secure not only their **IT and cloud systems** but **also operational technology (OT) systems** that are important to business operations.

Our zero trust architecture (ZTA) and intellectual property protection (IP) services help organizations **implement continuous + adaptive protection across users, edge endpoints, server infrastructure, cloud systems, applications, and networks** against both sophisticated external and internal threats.

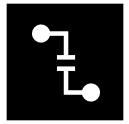
ASSESS | DESIGN | IMPLEMENT | MIGRATE | INTEGRATE | SUPPORT | MANAGE | TRAIN

Identity Access Management (IAM) + Privileged Access Management (PAM)

Secure Access Service Edge (SASE) + Secure Web Gateway (SWG)

Public Key Infrastructure (PKI) + Post-Quantum Cryptography (PQC)

Holistic Email Protection + Social Engineering Prevention



Traditional Networking, Software Defined Networking (SDN) + Micro-Segmentation

TECHNOLOGY PARTNERS

paloalto NETWORKS

FORTINET

SailPoint

Abnormal

CISCO

JUNIPER NETWORKS

Extreme networks

Plurilock CRITICAL SERVICES

Zero Trust Architecture + IP Protection Offerings (cont'd)

Our team delivers end-to-end security solutions encompassing the entire lifecycle including **evaluation, design, implementation, migration, integration, support, and training.** Our approach begins with in-depth risk assessments and solution evaluation, followed by expert deployment and migration of Zero Trust and IP protection technologies across IT and OT environments. **Where singular vendors stop at the edge of their product, our team ensures complete integration** with existing security and technology systems; for a **comprehensive security solution ecosystem**.

ASSESS | DESIGN | IMPLEMENT | MIGRATE | INTEGRATE | SUPPORT | MANAGE | TRAIN

Endpoint Detection + Response (EDR), Extended Detection + Response (XDR)

Data Loss Prevention (DLP) + Data Security Posture Management (DSPM)

User & Entity Behavior Analytics (UEBA) + Insider Risk Management (IRM)

Cloud Access Security Broker (CASB) + Cloud Security Posture Management (CSPM)

Remote Browser Isolation (RBI)

TECHNOLOGY PARTNERS

CROWDSTRIKE

Forcepoint

EVERFOX

BINARY DEFENSE™

Microsoft 365

ivanti

CLOUDFLARE

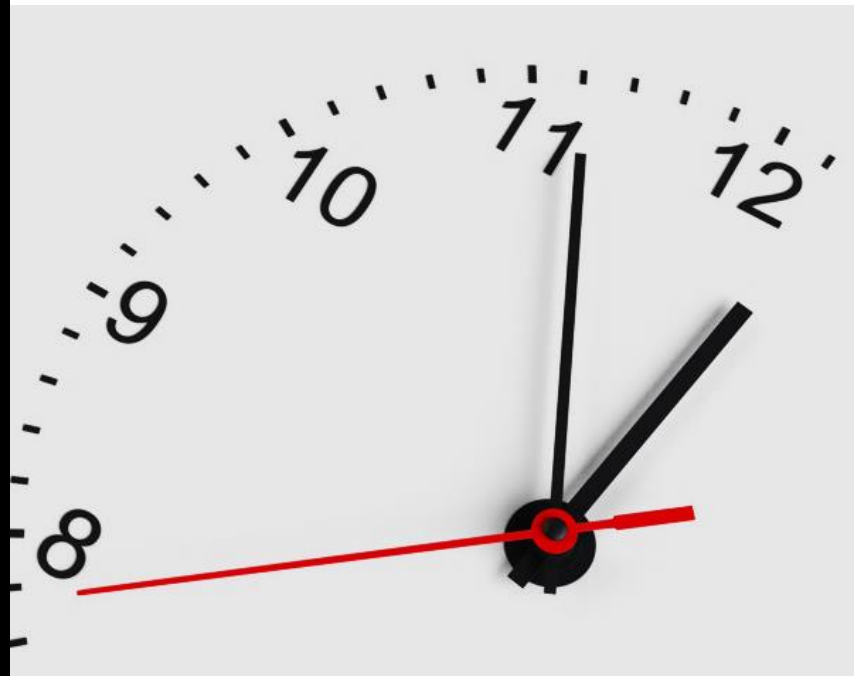
Symantec™

Plurilock
CRITICAL SERVICES

What We've Done Recently

With many decades of combined experience, Plurilock's teams have completed thousands of successful engagements.

Here's a selection of recent work to illustrate the kinds of work Plurilock is routinely engaged to do—as the diversity of environments, contexts, and problem sets that Plurilock is asked to confront.



Complex physical network refresh in dense urban environment

Enabled a major urban library system in the United States to relaunch their complex WiFi system, across many dozens of locations, in unforgiving architectural environments, without downtime.

Extensive custom integration between disparate systems

Deployed an extensive integration framework between the high-security IAM stack at a large healthcare provider and their remote access solution, enabling seamless remote work without compromising compliance.

Downtime-free network redesign and redeploy

Designed and deployed a new, redundant VPN and IPsec network for a major manufacturer, enabling transformation through advance staged configuration to achieve zero downtime.

WAN bandwidth optimization in the midst of a major rollout

Helped a major supplier with offices worldwide to rearchitect their WAN without downtime when previous plans proved insufficient during a major new infrastructure rollout.

Rapid incident response and remediation for malware attack

Ensured the rapid recovery of a public organization after multiple servers were infected by ransomware, including network-wide impact assessment, audits, and remediation to prevent future recurrence.

Urgent legacy environment lift-and-shift in a conflict zone

Transitioned a combined IT/OT network with legacy pre-gateway TCP/IP and onsite AS/400 metal into a modern, fully virtualized cloud-based environment—all while working around the uncertainties and contingencies of IT work in a conflict zone.

Plurilock Critical Services thrives where business, technology, and challenging conditions meet. We help governments and Fortune 1,000 clients to solve their hardest problems—rapidly.

Plurilock
CRITICAL SERVICES

Contact us today.

+1 (888) 282-0696 (USA West)
+1 (908) 231-7777 (USA East)
+1 (866) 657-7620 (Canada)

info@plurilock.com

Advanced cybersecurity and Zero Trust
Security assessments and consulting
IT products and solutions
Professional services
Managed services

Plurilock
CRITICAL SERVICES