Solution Brief

Uptycs for IBM Power, Linux on Z, LinuxONE, and AIX

Uptycs provides security visibility, attack surface management, security posture management, and detection and response for Linux on IBM Power, Linux on IBM Z mainframe (including LinuxONE), and the IBM AIX operating system.

High-performance security for hybrid multicloud environments

Long gone are the days of building siloed infrastructures. Enterprises are striving toward a model of interconnectedness so that the collective strength of their platforms and cloud providers can be leveraged to create the next wave of innovation. As the only unified CNAPP and XDR platform, Uptycs is uniquely positioned to work with IBM and its customers to protect their hybrid multicloud environments.

Uptycs protects some of the most demanding, high-scale environments in the world, including high-performance computing (HPC) environments. Adeptly handle the massive volume, variety, and velocity of security and IT data emanating from your IBM fleet—and beyond.

Get centralized control of IBM fleet-wide security data, instantly access the correlated insights you care about most, and take decisive action. Uptycs delivers security consistency across environments along with the comfort of knowing you have a future-proof security solution that can evolve with your needs.

Uptycs Benefits

A more unified, shift up approach enables secure digital transformation to drive better business results.

- Centralized control, and security and compliance consistency across environments
- Attack path visibility to help security teams better understand their threat exposure
- A more complete picture of software supply chain visibility
- Operational excellence and faster threat detection and remediation

IBM Power Servers deployed in data centers, private clouds, and IBM Cloud

IBM Power servers are built to economically scale mission-critical data-intensive applications, either virtual machine-based or containerized, and with the flexibility and choice to deploy in IBM Cloud and other clouds. For security teams responsible for protecting their IBM Power estate, Uptycs provides them with the ability to detect, respond, and remediate any potential security exposure.

Linux on IBM Z mainframe, including LinuxONE

Many of the world's largest enterprises rely on Linux on IBM Z for workloads that require high levels of resilience, flexibility, and security. As enterprises modernize these ecosystems, they unlock the ability to both migrate legacy workloads as well as develop hybrid cloud and container-based applications. Uptycs helps ensure these high-performance computing environments are secure options for enterprise app modernization efforts.

> "Uptycs has helped us secure critical asset categories such as IBM Power, Linux on Z mainframe, and the AIX operating system, and we look forward to deploying Uptycs across many more business units."
>
> **– Vice President of Cyber Defense and Technology**
> Fortune 500 Information Technology Services Company

Comprehensive Security and Compliance for IBM Power, Linux on Z, LinuxONE, and AIX

Modern, secure and scalable architecture

The Uptycs sensor normalizes security data at its collection point, then streams it up into your Uptycs Detection Cloud—your security data lake that's part of your Uptycs subscription. The Uptycs agent uses eBPF to noninvasively collect system-level telemetry, minimizing memory, CPU, and disk I/O footprint.

Uptycs provides FIPS compliant (Federal Information Processing Standards) versions of its sensor when installed on a FIPS compliant host. Uptycs will validate that a FIPS capable OpenSSL is installed and that your endpoint is correctly configured to FIPS before initializing and connecting to the Uptycs Cloud.

Multiple tools in one

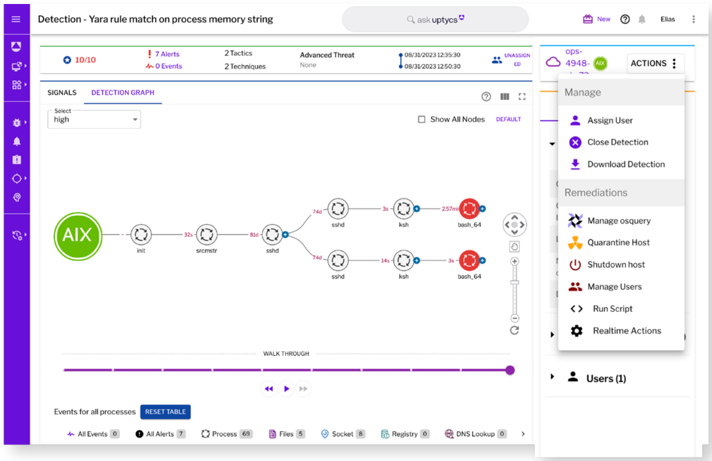
Get threat detection and response, forensics, vulnerability management, security hygiene, compliance, asset management, threat hunting, and more in a single solution. From one console you can manage the security posture of your fleet of IBM workloads located in data centers, private clouds, and IBM Cloud.

Uptycs' rich, purposeful security data supports a broader set of use cases. Get visbility into processes, sockets, files, DNS, HTTP connections, service creation, logins, and other event types including:

- YARA scanning of files and memory
- Scanning for secrets
- Forensics support
- Configuration files discovery (Augeas lens)
- Performance monitoring
- Discovery of hosts/devices in the neighborhood and port scanning

Vulnerability management

With Uptycs, you can match vulnerability feeds against system telemetry from your IBM fleet to detect software vulnerabilities—without burdening host systems. In addition, you can use prebuilt queries to identify non-compliant or vulnerable software in your environment. Uptycs prioritizes the vulnerabilities using environmental factors (Uptycs Smart Indicators). For example, if a vulnerable



shared library is currently open and in use by a process, if a process is listening on a vulnerable port, or if a binary from a vulnerable package is currently running.

Host compliance and file integrity monitoring (FIM)

Uptycs provides auditing and compliance support for CIS Benchmarks, DISA STIG, FedRAMP, HIPAA, ISO 27001, NIST 800-53, PCI, SOC 2, and more. This greatly simplifies the task of monitoring and reporting so you can confidently answer auditor questions, provide evidence, and streamline remediation workflows.

Uptycs supports file integrity monitoring with extreme flexibility such as the ability to include/exclude folders, files, and file extensions. You can even configure Uptycs to run YARA scans against changed files.

YARA rule-based scanning

Uptycs maintains YARA rules to detect APT toolkits across your IBM environments. Uptycs also lets you create and deploy custom YARA rules used to scan process binaries and process memory. In addition, any file or process can be scanned ad hoc in real time.

Uptycs lets your team intelligently take advantage of industry-standard YARA rules to identify malware in your environment, with considerably higher degrees of effectiveness than the signature-based approach used by antivirus tools.

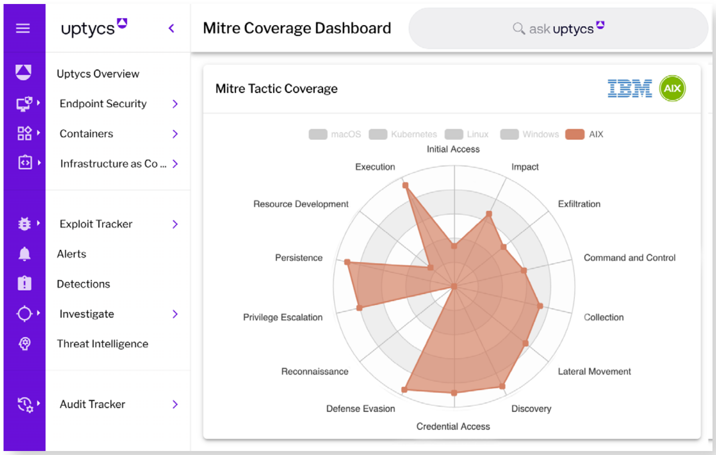
Uptycs Threat Research Team and threat books

Uptycs Threat Research Team conducts real-time research across multiple threat intel feeds and platforms and uses this information to fortify your defenses. This includes direct delivery of threat books into your Uptycs instance to scan for current and prior vulnerabilities, infections, and IoC's and IoB's associated with newly reported malware.

Sophisticated custom detections

Out of the box, Uptycs includes over 2,300 behavioral detections covering the MITRE ATT&CK Framework. You can augment these rules by customizing or writing your own rules. Uptycs works transparently, enabling you to:

- See how built-in behavioral detections work
- Create exceptions to rules
- Copy event rule logic as a basis for new detections to fill gaps in coverage
- Create custom detections as code using Sigma



Superior investigation and threat hunting

With Uptycs you can ask and get answers to your questions to understand the scope, severity, and root cause of an incident. Uptycs provides incident responders and threat hunters with a complete record of system activity through the Uptycs Flight Recorder, even for systems where an attacker's activity didn't trigger a detection and was considered benign.

When a new threat emerges, you can quickly report to management your organization's exposure to newly disclosed threats. Query your environment's historical telemetry to determine if that exploit or behavior was operating in the past. Lookback up to 90 days, and send telemetry to your AWS S3 or cold storage system for archival purposes. Uptycs is the only vendor that can give you the ability to conduct ad hoc, real-time, and historical investigations for all systems sets.

Preemptive blocking

Uptycs permits process blocking to be instrumented on specific hosts—or across your fleet— through blocking policies based on file hash, executable path, certificate, or YARA rule match. This gives you the ability to stop malicious processes before they cause further damage, thus reducing risk across your assets.

Advanced remediation

Following a detection, alert, threat hunt, or investigation, Uptycs enables faster remediation by giving you the ability to quarantine the host, kill processes, block the offending IP address and port, delete files, disable users, delete registries, run scripts (localized diagnosis), and carve files (including process binaries). These actions can be manually instrumented or automated via alerts based on triggers. Bulk remediations allow you to run a script against thousands of assets.

Faster threat eradication and containment, both for external and internal/insider threats can help you limit the legal, reputational, and operational damage of a breach.

Supported operating systems and platforms

IBM Linux on Z and LinuxONE

Red Hat Enterprise Linux 8.6

Red Hat Enterprise Linux 8.8

Red Hat Enterprise Linux 9.0

Red Hat Enterprise Linux 9.2

Ubuntu Server 20.04

Ubuntu Server 22.04

SUSE Linux Enterprise Server 15 SP3

SUSE Linux Enterprise Server 15 SP4

CentOS 8

IBM Power 7, 8, 9
AIX 7.2 TL5 and above

IBM Power 8, 9, 10
AIX 7.3 TL0 and above

Linux on IBM Power
Red Hat Enterprise Linux 8
CentOS 8

About Uptycs

Attackers don't think in silos and neither should your security. Uptycs, the first unified CNAPP and XDR platform, protects the developer laptops that build your applications to the cloud workloads that run them—all from a single console and data lake. Uptycs helps drive DevSecOps excellence, bringing teams together to master threat operations, meet compliance mandates, and reduce risk across clouds, containers, and endpoints. Take back control of your security data, get the correlated insights you care about most, and take decisive action.

Shift up your cybersecurity with Uptycs. Learn how at: Uptycs.com