Whitepaper

uptycs

14 Kubernetes and Cloud Security Predictions for 2023 and How Uptycs Meets Them Head On

Introduction

The future of container and Kubernetes adoption is extremely optimistic, with innovation happening across the cloud native ecosystem. As the number of adopters and contributors continues growing, we are seeing more innovation and attention to how containers are built, supported, and secured. Over the coming year, we will see new technologies incorporated to support the container ecosystem and even address concerns that extend outside of the tech stack and into the world of policy. The next year will bring both innovation for containers and also obstacles that we, as a cloud native community, will be looking to overcome together.

ControlPlane conducts threat modeling, penetration testing, and cloud-native security training to the highest standard for its global clients. The company has a deep understanding of secure-by-design and secure-by-default for cloud, Kubernetes, and supply chain security.

Andrew Martin is the founder and CEO of the open-source cybersecurity consultancy. His recently published Kubernetes (k8s) security predictions for 2023 is spot-on. Here is how Uptycs solves the fourteen forecasts Martin highlights.

This paper goes through each prediction, highlighting how each prediction will realistically be incorporated or addressed through the Uptycs solution. Uptycs offers a highly customizable and scalable solution for protecting container and Kubernetes deployments, while staying true to the values of open telemetry, high customization, and breaking down silos across your ecosystem. Today, security teams use Uptycs to secure some of the world's largest container deployments.

Secure your container deployments holistically, from the moment they start on a developer’s laptop all the way through runtime deployment. Attackers don’t think in silos, and modern applications call for security solutions that unify and protect from laptop to container. Security teams are shifting up their security with Uptycs by removing siloed tools and taking a unified approach that looks across diverse attack surfaces from containers to laptops to cloud servers.

Prediction 1:

CVEs continue to rampage and tear through the supply chain

Year-on-year growth of CVEs is rising dramatically. What's more, supply chain attacks are showing exponential growth. Teams need to gather contextual indicators to fully understand the impact of a given CVE on specific assets.

> **Uptycs catches CVEs in the build, deploy, and runtime stages of the container pipeline and provides clear guidance for context and remediation steps.**

Packages included in software images often have vulnerabilities, or CVEs, published in NIST's National Vulnerability Database. When incorporating these packages in your software—commonly done by almost everyone today—you're at risk. Managing this ever-growing backlog of CVEs is becoming a widespread challenge.

Uptycs scans your images regardless of where they sit in the CI/CD pipeline. We inform you if a CVE is present, whether an exploit has been found, and how many images are impacted so you can prioritize mitigation. Uptycs uses the Common Vulnerability Scoring System (CVSS) to mark vulnerabilities as critical, high, medium, and low. We arm security teams with context about the CVEs to quickly remediate. These key indicators inform whether there are remediation steps available, how to perform those steps, and, crucially, if the Uptycs Threat Research team is currently observing this CVE being actively exploited in the wild.

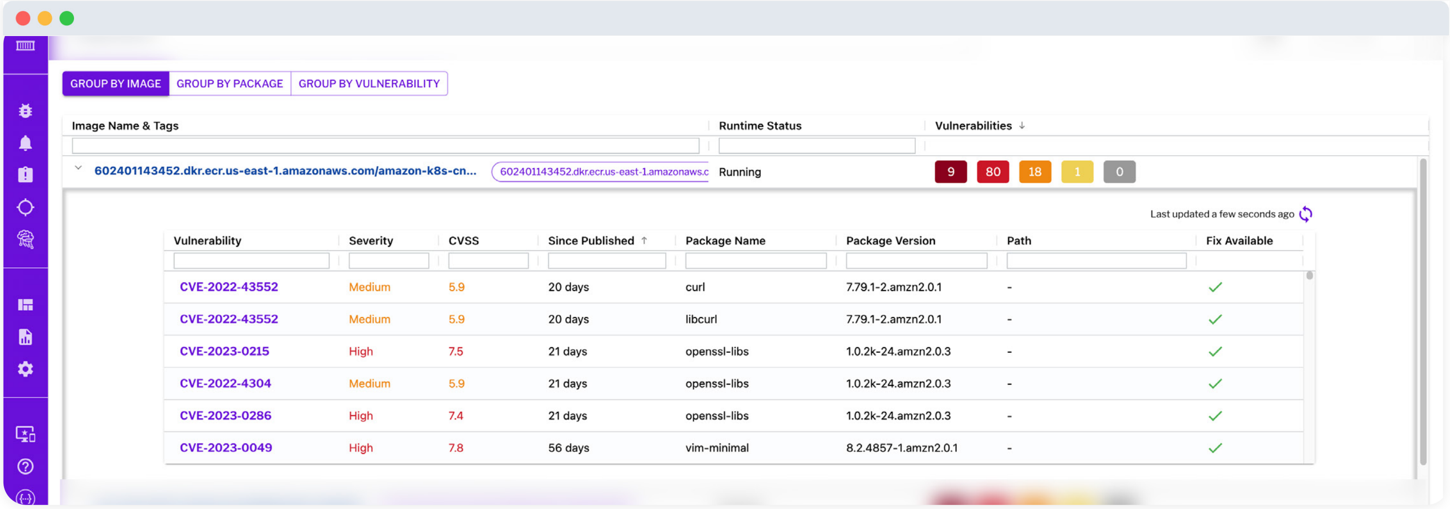


Image Name & Tags		Runtime Status	Vulnerabilities ↓
602401143452.dkr.ecr.us-east-1.amazonaws.com/amazon-k8s-cn...	602401143452.dkr.ecr.us-east-1.amazonaws.c	Running	9 80 18 1 0

Last updated a few seconds ago

Vulnerability	Severity	CVSS	Since Published ↑	Package Name	Package Version	Path	Fix Available
CVE-2022-43552	Medium	5.9	20 days	curl	7.79.1-2.amzn2.0.1	-	✓
CVE-2022-43552	Medium	5.9	20 days	libcurl	7.79.1-2.amzn2.0.1	-	✓
CVE-2023-0215	High	7.5	21 days	openssl-libs	1.0.2k-24.amzn2.0.3	-	✓
CVE-2022-4304	Medium	5.9	21 days	openssl-libs	1.0.2k-24.amzn2.0.3	-	✓
CVE-2023-0286	High	7.4	21 days	openssl-libs	1.0.2k-24.amzn2.0.3	-	✓
CVE-2023-0049	High	7.8	56 days	vim-minimal	8.2.4857-1.amzn2.0.1	-	✓

Figure 1: Uptycs tracks CVEs for all your container images, here Uptycs is providing contextual evidence around the severity of each CVE and the specific package details that can be remediated immediately.

From a volume viewpoint, you can assess important indicators such as: Is it exploitable? Is a fix available?

Addressing vulnerabilities in containerized environments is also important. Once deployed, Uptycs scans k8s nodes, Pods, and containers to reveal underlying vulnerabilities. Additionally, Uptycs can scan images as they're being built in the CI/ CD pipeline. If critical vulnerabilities exist, you're able to automatically stop the build, thereby giving DevOps time to fix or disable the vulnerability altogether.

Some teams prefer to push the build into a registry, where Uptycs can scan for vulnerabilities there. Again, you're provided details as to which images have known vulnerabilities. Use the remediation steps we provide to fix the CVE or send the Uptycs telemetry to a ticketing system for a team member to address.

Uptycs also scans registries for the presence of credential exposure patterns, e.g., shared secrets with AWS, a database, or a payment system such as Stripe. These can often be the end goal of a threat actor, working through a CVE to get to your organization's crown jewels.

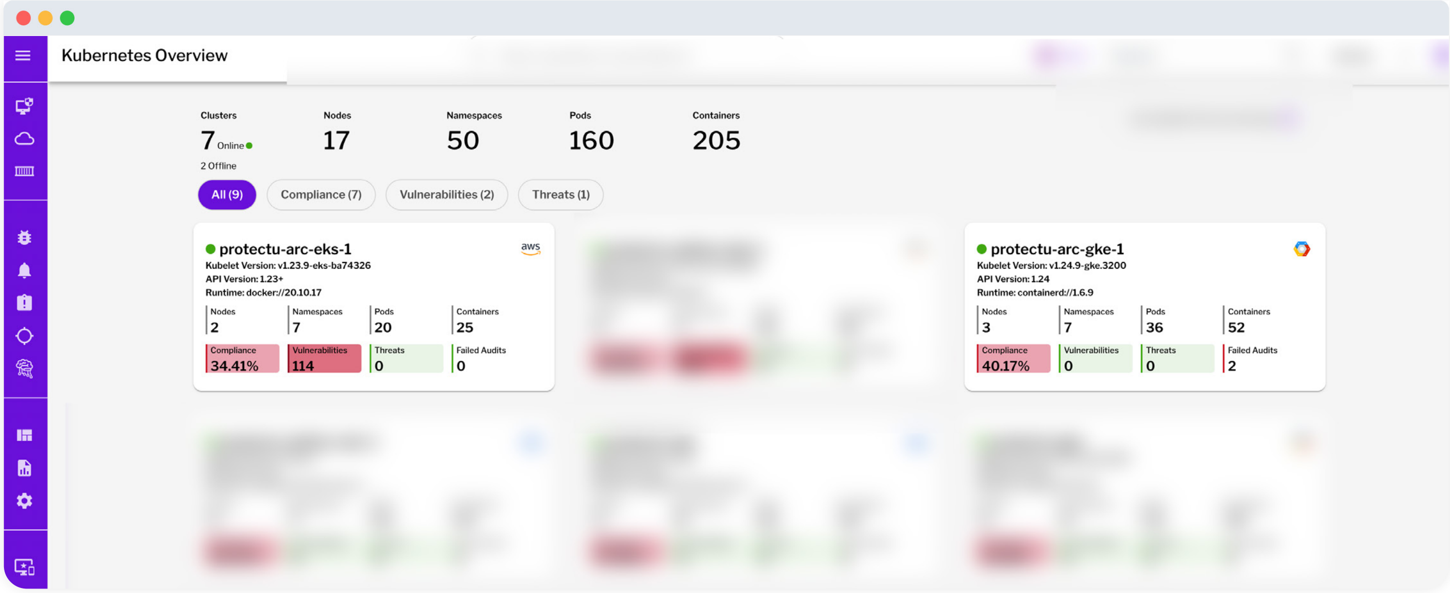
Prediction 2:

Kubernetes RBAC and security complexity continue to intensify

As the open-sourced k8s API continues to be extended, and applications build out functionality using custom resource definitions (CRDs), the operational complexity of running Kubernetes will continue to rise. Many are implementing security in role-based access control (RBAC) for k8s access as well as across the various applications, Pods, and clusters running inside their environment.

> **Uptycs provides deep information and visibility into highly-scaled k8s control planes and container deployments.**

Uptycs' sensor correlates a large volume of information at the control plane level. This includes role policy rules, binding subjects, configuration maps, cron jobs that are present, ingress rules, and web hooks, in addition to network and security policies. This depth of visibility lets you create rules (or use out-of-the-box rules) that notify you of changes to your configurations and enforce policies from your k8s to container layer.



Kubernetes Overview

Clusters	Nodes	Namespaces	Pods	Containers
7 Online ● 2 Offline	17	50	160	205

All (9) | Compliance (7) | Vulnerabilities (2) | Threats (1)

● protectu-arc-eks-1
Kubelet Version: v1.23.9-eks-ba74326
API Version: 1.23+
Runtime: docker://20.10.17

Nodes	Namespaces	Pods	Containers
2	7	20	25
Compliance	**Vulnerabilities**	**Threats**	**Failed Audits**
34.41%	114	0	0

● protectu-arc-gke-1
Kubelet Version: v1.24.9-gke.3200
API Version: 1.24
Runtime: containerd://1.6.9

Nodes	Namespaces	Pods	Containers
3	7	36	52
Compliance	**Vulnerabilities**	**Threats**	**Failed Audits**
40.17%	0	0	2

Figure 2: Uptycs correlates Kubernetes and Container runtime data, here Uptycs is giving deep visibility into running clusters, pods, and nodes for an AWS and GCP cluster.

The k8s control plane is the orchestrator for running containers; it determines how they're deployed and the roles used for doing that. There's a DevOps aspect to this as well—many organizations are very specific regarding registry access, e.g., a developer might only be allowed to see scan results pertaining to templates or code they're checking in.

DevOps teams need granularity into their security gaps to control the saliency of code going into their repository—as well as the container image registry. Unauthorized access might be inadvertently granted to the underlying cloud account if not managed correctly by enforced RBAC policies. Uptycs speeds up response times with alerts that can be forwarded to your SOC or ingested by a SOAR or SIEM tool; notifications can also be distributed via Slack or PagerDuty to speed up this time to action.

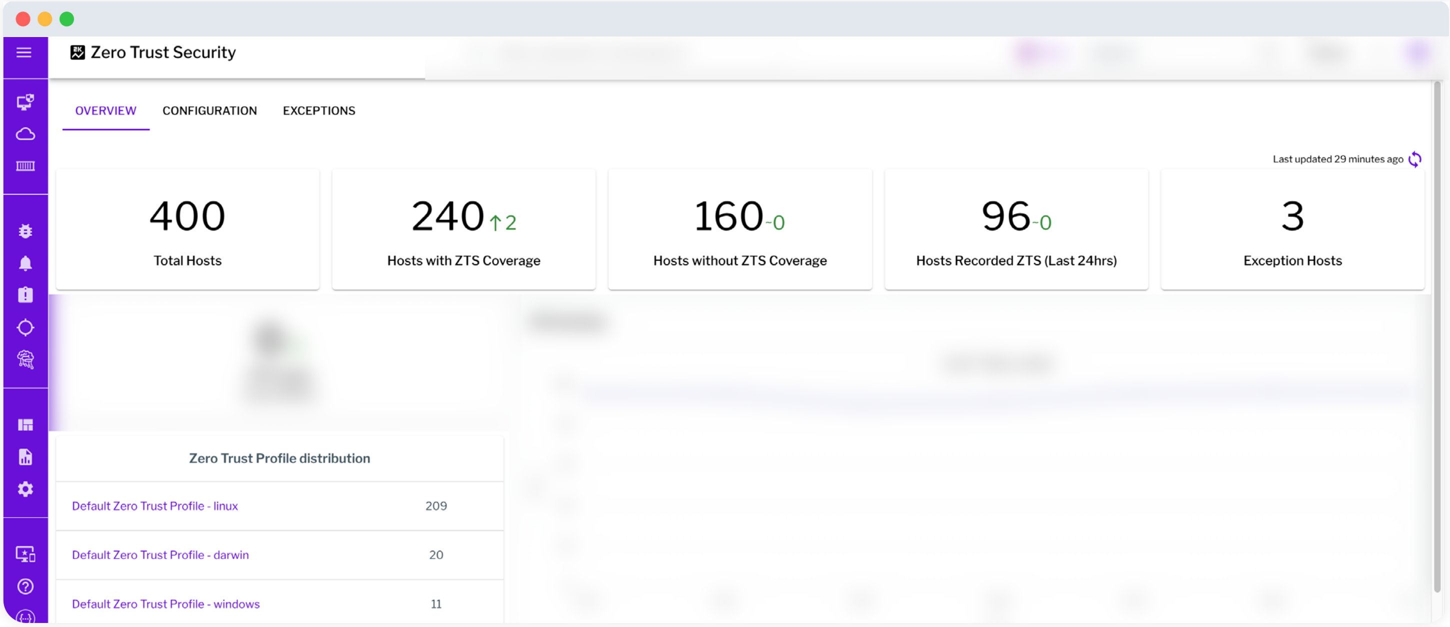
Prediction 3:

Passwords and credentials will continue to be stolen as zero trust is slow to be adopted

Attackers use compromised credentials to gain network access. They can often grant themselves elevated privileges, move laterally within systems, and subsequently exfiltrate sensitive data. Tightly scoped credentials having a short time-to-live can assist in mitigating a large range of attacks. Adoption of a zero-trust security model can help minimize the risk of key and data exfiltration.

> **Uptycs computes dynamic zero-trust scores using a series of compliance checks and user-driven security information.**

Exceptions can be added for critical host devices or servers that would otherwise have difficulty in proving their compliance checks. After calculating this zero-trust score, Uptycs sends this trust score in real time to zero trust services like Cloudflare Zero Trust to determine if a request should be allowed to reach a protected resource.



Last updated 29 minutes ago

400	240 ↑2	160 -0	96 -0	3
Total Hosts	Hosts with ZTS Coverage	Hosts without ZTS Coverage	Hosts Recorded ZTS (Last 24hrs)	Exception Hosts

Zero Trust Profile distribution

Default Zero Trust Profile - linux	209
Default Zero Trust Profile - darwin	20
Default Zero Trust Profile - windows	11

Figure 3: Uptycs Zero Trust Coverage provides dynamic trust scores to your fleet, here Uptycs is supporting 400 endpoints with ZT scoring and giving clear visibility into which assets are using specific ZT configurations.

Uptycs can detect when passwords and credentials have been stolen and if an unauthorized party has gained access to your environment. Within cloud architectures, a common practice is to provision short-term tokens to be used by applications, but there's a risk that such tokens can be exposed—even during their short-lived existence. You're able to see if you've accidentally exposed an EC2 instance or a virtual computer machine to brute force login attacks or credential exposure.

Uptycs provides detections that look for suspicious combinations of cloud trail activity related to access and authorization. This helps identify when credentials have been stolen by a malicious user. Should an entity get access to your containerized or host (on-prem or cloud) environment, Uptycs technology can see where those assets are located and the IP addresses of illicit logins.

Prediction 4:

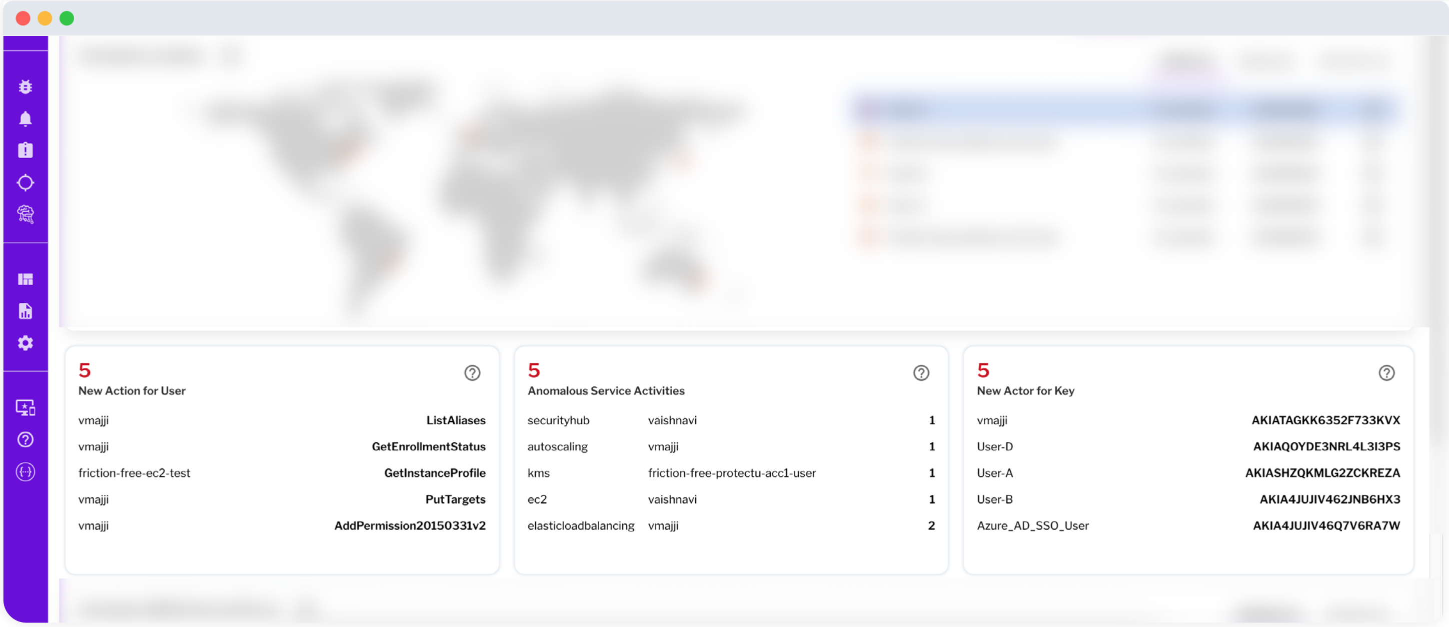
AI and ML will be harnessed by attackers more effectively than defenders

Hackers are using artificial intelligence to make attacks more effective. One way they're doing that is by using machine learning to poison AI models that rely on data sample labeling to build detection profiles. They're building malware that introduces benign files in a way that a defender's AI algorithm interprets as, 'Oh, that pattern isn't doing anything—it's safe.' Once that occurs, they can then drop in malicious activity under that same pattern and be undetected.

> **Uptycs is rolling out statistically-based anomaly detections to catch threats that traditional threat modeling misses.**

Uptycs anomaly detection framework works in parallel with traditional threat modeling. Given such detection, Uptycs is able to analyze your haystack of data to find the anomalous needle of malicious activity or malicious users.

Our statistic-based detections help secure scaling cloud environments with hundreds of thousands of API and resource calls made between users and applications every day. It's impossible for a team to manually sort through such logs or write prescriptive rules for every use case. Looking across matrices of user actions, Uptycs can correlate anomalous actions to understand legitimate vs. illegitimate user patterns and alert on those threats.



5
New Action for User

vmajji	**ListAliases**
vmajji	**GetEnrollmentStatus**
friction-free-ec2-test	**GetInstanceProfile**
vmajji	**PutTargets**
vmajji	**AddPermission20150331v2**

5
Anomalous Service Activities

securityhub	vaishnavi	**1**
autoscaling	vmajji	**1**
kms	friction-free-protectu-acc1-user	**1**
ec2	vaishnavi	**1**
elasticloadbalancing	vmajji	**2**

5
New Actor for Key

vmajji	**AKIATAGKK6352F733KVX**
User-D	**AKIAQOYDE3NRL4L3I3PS**
User-A	**AKIASHZQKMLG2ZCKREZA**
User-B	**AKIA4JUJIV462JNB6HX3**
Azure_AD_SSO_User	**AKIA4JUJIV46Q7V6RA7W**

Figure 4: Uptycs monitors and alerts for statistically anomalous behavior, here Uptycs alerted on abnormal actions for users, anomalous service token activity, and abnormal user access key activity.

As AI is used to create more effective cyberattacks, the onus will be on security companies to develop more advanced defense technology, e.g., search for anomalies in behavior and activities. To detect AI-trained malware on your critical infrastructure, you'll want to use a system agent to be 100% protected.

Prediction 5:

eBPF technology powers all new connectivity, security, and observability projects

extended Berkeley Packet Filter (eBPF) has been increasingly used in recent years to enhance performance, security, and observability of Linux-based systems. It permits the creation of in-kernel programs that can be used for purposes such as packet filtering, system call tracing, and security enforcement.

> **Uptycs incorporates eBPF into Linux deployments to improve optimization and event processing efficiency at scale.**

By moving processing out of user space and into the kernel, eBPF offers a very stable, lightweight, low-cost way of providing extremely detailed security and observability to a machine. Everything happens inside the kernel using programs or hooks.

As a well-positioned leader in this space, Uptycs expects to see greater adoption of agents and sensors. Several large customers already use our eBPF sensor on their high-volume Linux systems to get clear visibility into their container and cloud workloads.

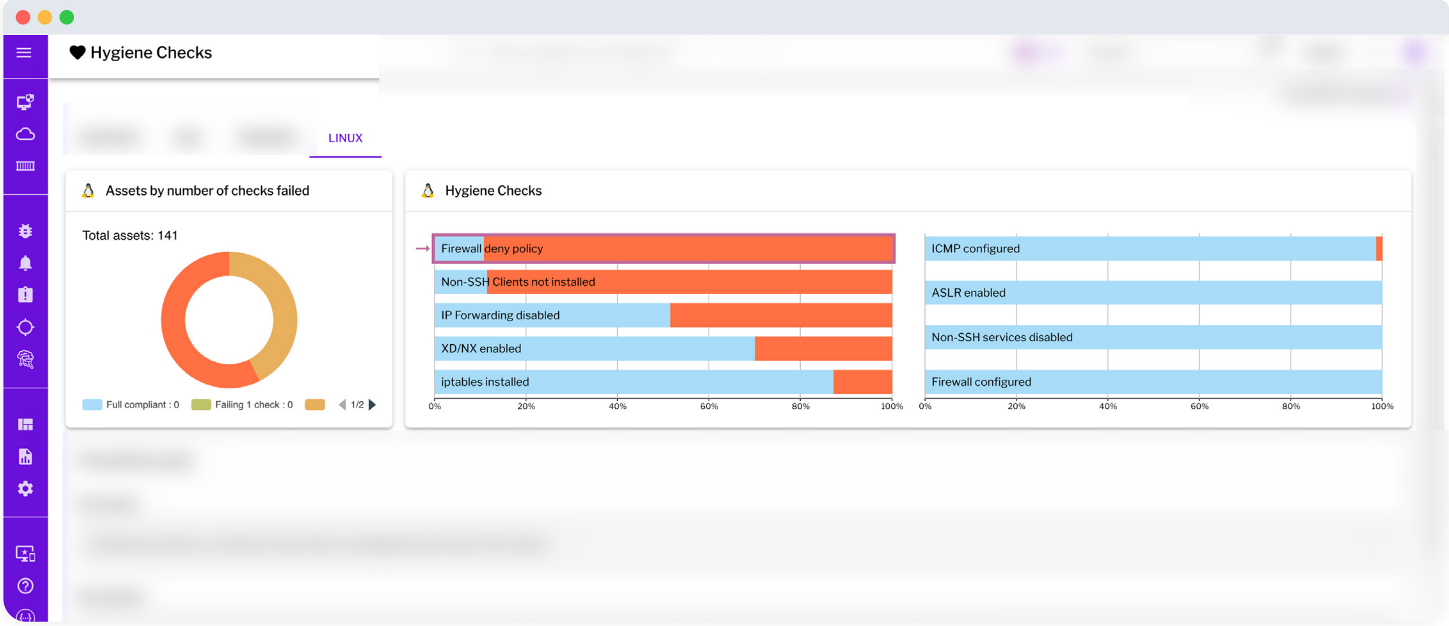


Figure 5: Uptycs uses eBPF on Linux container deployments, giving powerful security and visibility monitoring with lightweight resource utilization.

eBPF offers an ideal tradeoff between getting granular, process-level event data from your systems without burdening them with the resource requirements of a traditional agent. Uptycs keeps its resource usage extremely low to maximize system performance and eliminate any burden on host machines.

Prediction 6:

CISOs will shoulder unjust legal responsibility, thus exacerbating the talent shortage

Robust security is difficult to realize. Removing the incentive for intelligent people to lead departments by belaboring them with onerous legislation and responsibility is not commensurate with their already challenging work.

> **We can't change laws, but we can ease the burden of overworked security professionals. Uptycs provides CISOs with clear metrics and reporting dashboards that are ready for presenting to executive boards.**

With respect to the talent shortage, Uptycs amplifies your ability to control and defend your IT infrastructure. Our growing managed detection and response service assists teams that don't have in-house talent. With Uptycs, get complete coverage over your infrastructure while reducing burnout of your teams. We empower security teams with tools that reduce uncertainty and provide clear remediation steps and swift, automated responses. Teams should feel that their tools reduce their workload, not add to it.

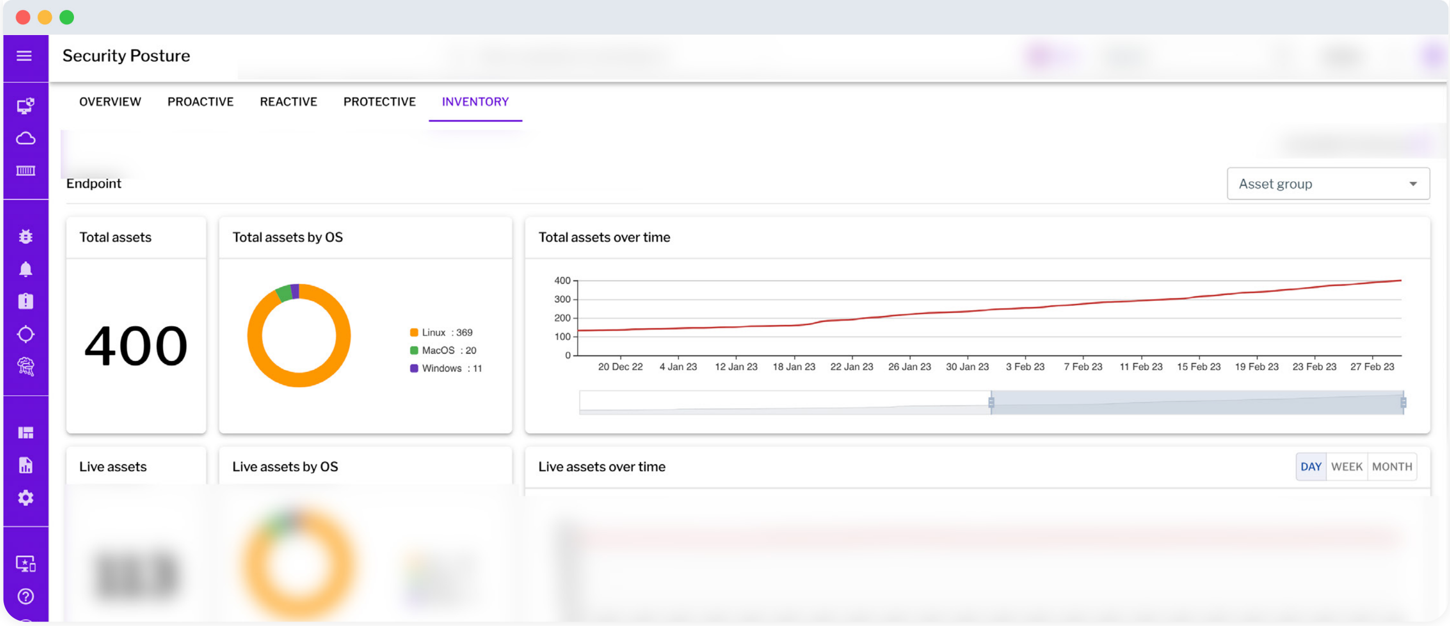


Figure 6: Uptycs provides clear reporting of your inventory and visibility in ready-to-deliver dashboards with export functionality.

Prediction 7:

Automated vulnerability remediation will continue to grow slowly

The inherent risks in these approaches are false negatives that result in production downtime, so they're not yet widely seen. But risk reduction made possible with companion AI systems could see this as a viable approach over the coming years.

> **Uptycs has widespread remediation and blocking to help teams take action out of the box or with custom rules.**

There are two camps for this issue. Some organizations want their security tools to perform automated remediation (at least in some cases), while others prefer to take action themselves. As the breadth of attacks grows, we believe more people will come to embrace automated remediations. Being flexible, Uptycs provides functions to take automated remediation steps, if desired, or can provide steps for your security teams to remediate issues.

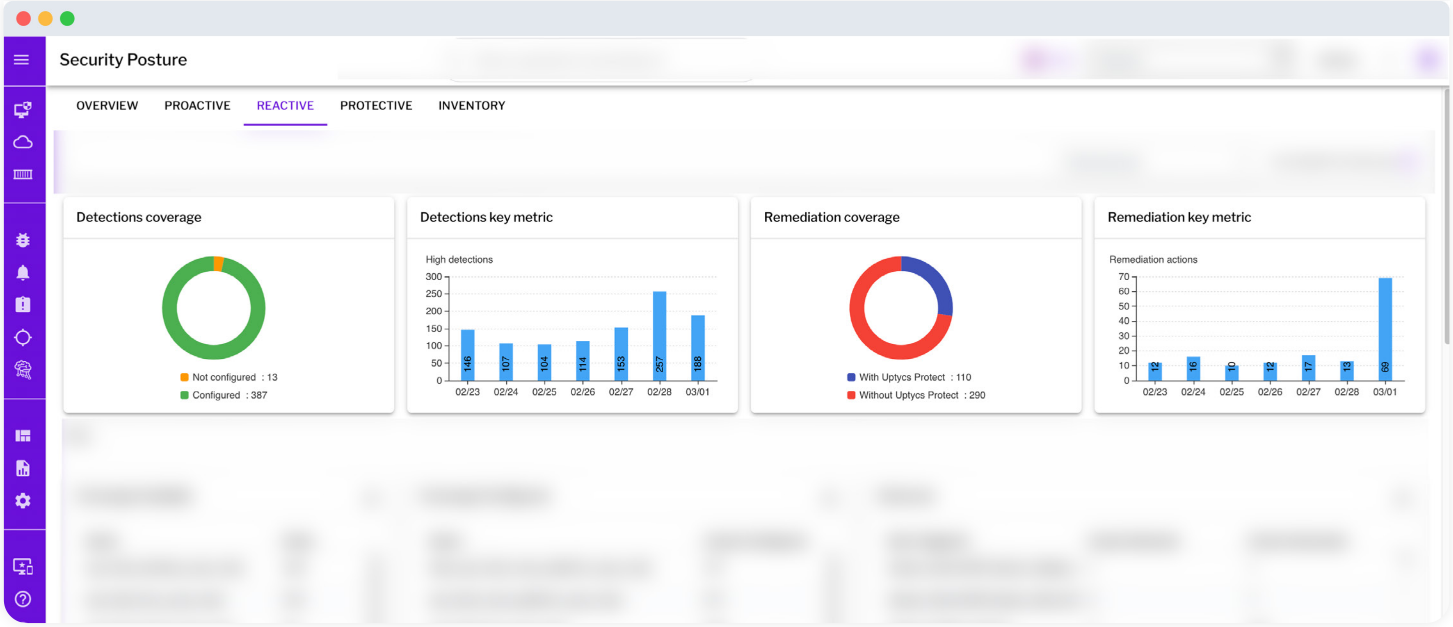


Figure 7: Uptycs detect and respond capabilities provide automated remediation coverage across your scaling infrastructure.

Uptycs provides custom YARA rules for teams to proactively hunt for specific malware signatures and binaries in their applications. With YARA scans, Uptycs monitors millions of hosts for emerging malware, increasing clarity about emerging vulnerabilities (e.g., log4J) and validate configurations after auto-remediated responses.

Prediction 8:

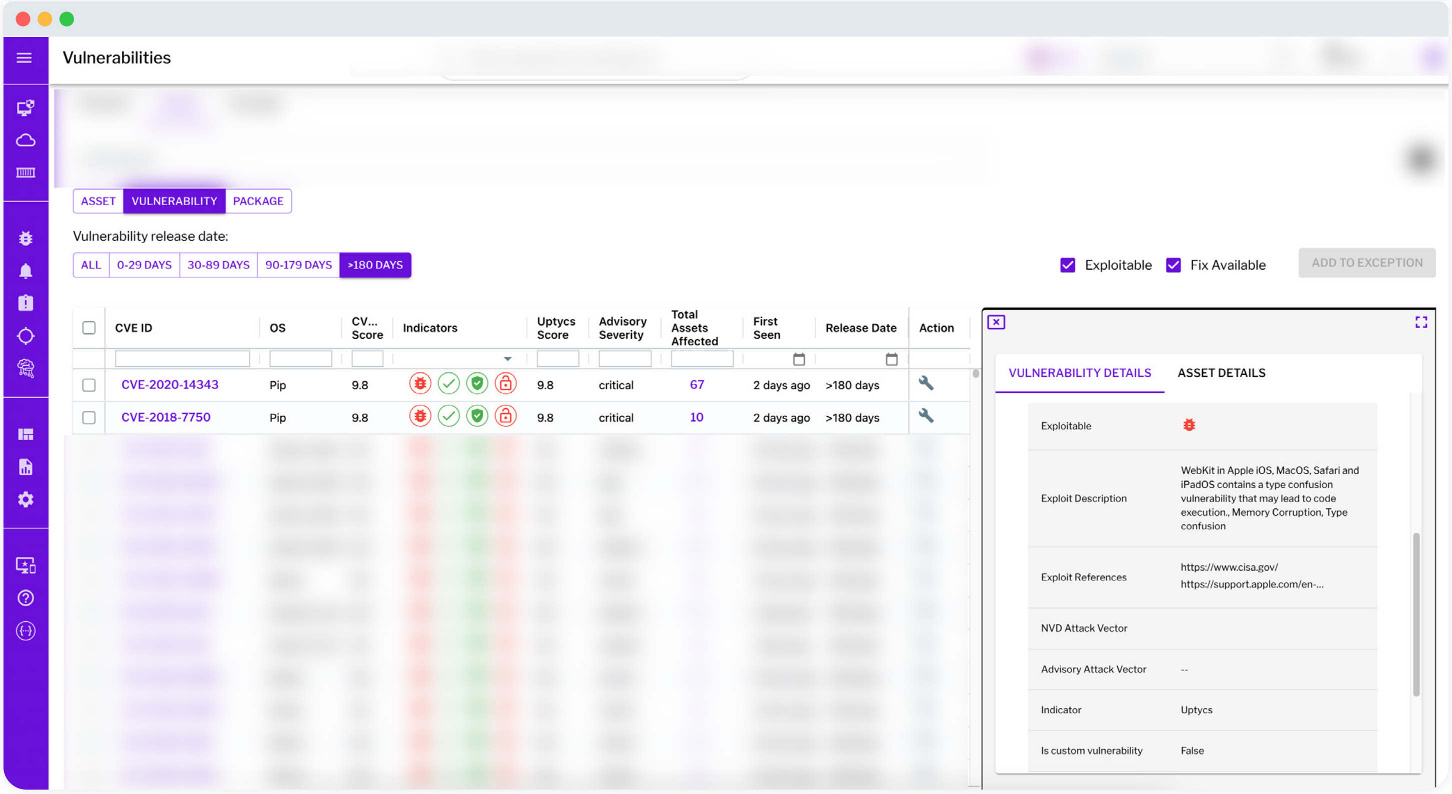
Vulnerability exploitability eXchange (VEX) sees initial adoption

CVEs muddy the vulnerability remediation waters with unexploitable false positives. Thus, one of the hardest jobs in security is analyzing those critical warnings. A potential solution is the vulnerability exploitability eXchange. VEX brings transparency to exploitability, detailing whether a software package that includes a dependency is actually affected by that vulnerability. Many CVE-scanning approaches don't take this into account, thereby duplicating the responsibility of vulnerability assessors in every organization.

> **Uptycs' Threat Research Team compiles data on exploitability and infuses it into the assessment of each CVE's true priority.**

Security analysts don't just want a list of all known vulnerabilities on their machines—they need clear context and guidance to take the right steps and prioritize actions. As mentioned, CVEs present an ever-growing backlog of vulnerabilities. Uptycs helps teams manage these findings and systematically harden your environment.

One way we help triage priority is not only in relation to those CVEs having a high score, but also by calling out those that are exploitable on a given machine. We detail information for each CVE to 1) provide context regarding how high its CVSS score is and 2) whether it's being actively exploited by threat groups.



Vulnerability release date: >180 DAYS

☑ Exploitable ☑ Fix Available

□	CVE ID	OS	CV... Score	Indicators	Uptycs Score	Advisory Severity	Total Assets Affected	First Seen	Release Date	Action
□	CVE-2020-14343	Pip	9.8		9.8	critical	67	2 days ago	>180 days	
□	CVE-2018-7750	Pip	9.8		9.8	critical	10	2 days ago	>180 days	

Exploitable	
Exploit Description	WebKit in Apple iOS, MacOS, Safari and iPadOS contains a type confusion vulnerability that may lead to code execution., Memory Corruption, Type confusion
Exploit References	https://www.cisa.gov/ https://support.apple.com/en-...
NVD Attack Vector	
Advisory Attack Vector	--
Indicator	Uptycs
Is custom vulnerability	False

Figure 8: Uptycs helps you focus on the CVEs that matter most, dig deep into CVEs, and understand which ones are being actively exploited by threat actors right now.

Prediction 9:

Linux kernel ships its first Rust module

Rust is a programming language that has gained popularity due to its focus on safety and performance. Despite scant initial support at present, inclusion of a device driver written in Rust is a significant step toward a new era for the Linux kernel. It assuages risk presented by memory-unsafe languages (e.g., C). Rust's placement as a memory-managed system language distinguishes it—as long as "unsafe" mode isn't used to bypass memory safety guarantees. Its developer community expects to see more Rust modules in the kernel going forward.

> **Uptycs is exploring an osquery add-on to report on Rust programs that exist in your Linux machines' kernel.**

Being similar to C but much safer due to its managed use of memory, Uptycs expects to start seeing Rust programs sit in the Linux kernel. Initially this will yield many useful programs, and there are efforts to rewrite many C applications in Rust, but eventually, we'll see related malware.

Prediction 10:

Closed-source vendors face calls for SBOM delivery to derive mean time to remediation (MTTR) statistics

A software bill of materials (SBOM) is a detailed inventory of all software comprising an application. It lists all dependencies, libraries, and frameworks used in an application.

> **Uptycs is adding support for SBOM capabilities in H1 of 2023.**

A SBOM helps teams understand internal dependencies that their applications have. For example, when log4j became a widespread issue, teams struggled to get a clear understanding of which applications in their supply chain relied on that specific Java logging library.

Uptycs is adding SBOM support in 2023 H1. In doing so we'll be able to further support inventorying while providing granular visibility into disparate versions and sources of software dependencies. We currently have a strong parallel function to SBOM through YARA scanning. As for log4j, YARA scans have enabled teams to quickly peer into uber JAR (aka, fat JAR) and even shaded JAR files to check configuration flags.

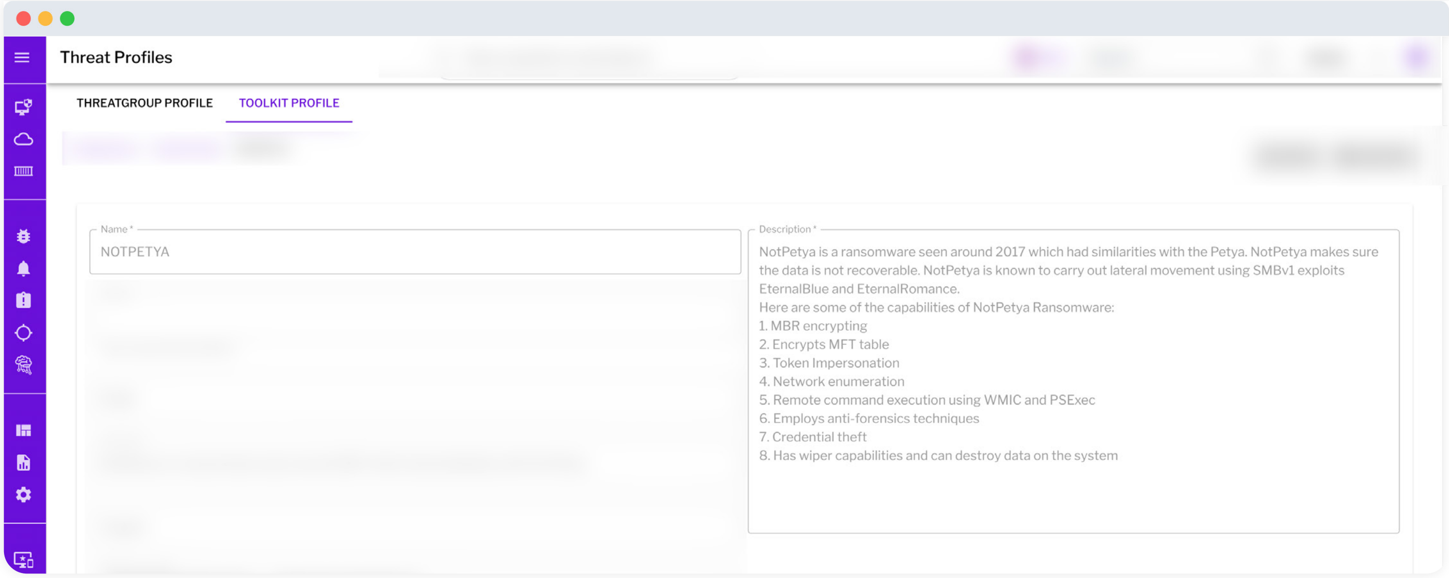
Prediction 11:

Cybersecurity insurance policies will increasingly descope ransomware and negligence

As governments increase fines for data breaches and cybersecurity incidents, insurance companies could start to descope ransomware and negligence from their coverage. This is because paying ransomware demands could be seen as encouraging criminal activity; negligence cases could be considered a failure to meet basic security standards. Therefore, insurance providers might shift their focus to incentivize organizations to invest in strong cybersecurity measures rather than relying solely on insurance coverage.

> **The Uptycs Threat Research Team compiles rootkits and specific malware used by advanced persistent threat (APT) groups to create rules mapped to the MITRE ATT&CK matrix.**

Uptycs can actively kill ransomware as an attack occurs through its use of active, automated remediation and blocking techniques. It detects ransomware two ways. First, backend rules are mapped to the MITRE ATT&CK matrix, examining granular event data coming from each asset and alerting when ransomware tactics, techniques, and procedures (TTPs) are observed. Second, Uptycs' dedicated Threat Research Team compiles signatures and toolkits of known APT groups. We update this daily, creating a diverse database of signatures that are monitored across your infrastructure.



Name *
NOTPETYA

Description *
NotPetya is a ransomware seen around 2017 which had similarities with the Petya. NotPetya makes sure the data is not recoverable. NotPetya is known to carry out lateral movement using SMBv1 exploits EternalBlue and EternalRomance.
Here are some of the capabilities of NotPetya Ransomware:
1. MBR encrypting
2. Encrypts MFT table
3. Token Impersonation
4. Network enumeration
5. Remote command execution using WMIC and PSExec
6. Employs anti-forensics techniques
7. Credential theft
8. Has wiper capabilities and can destroy data on the system

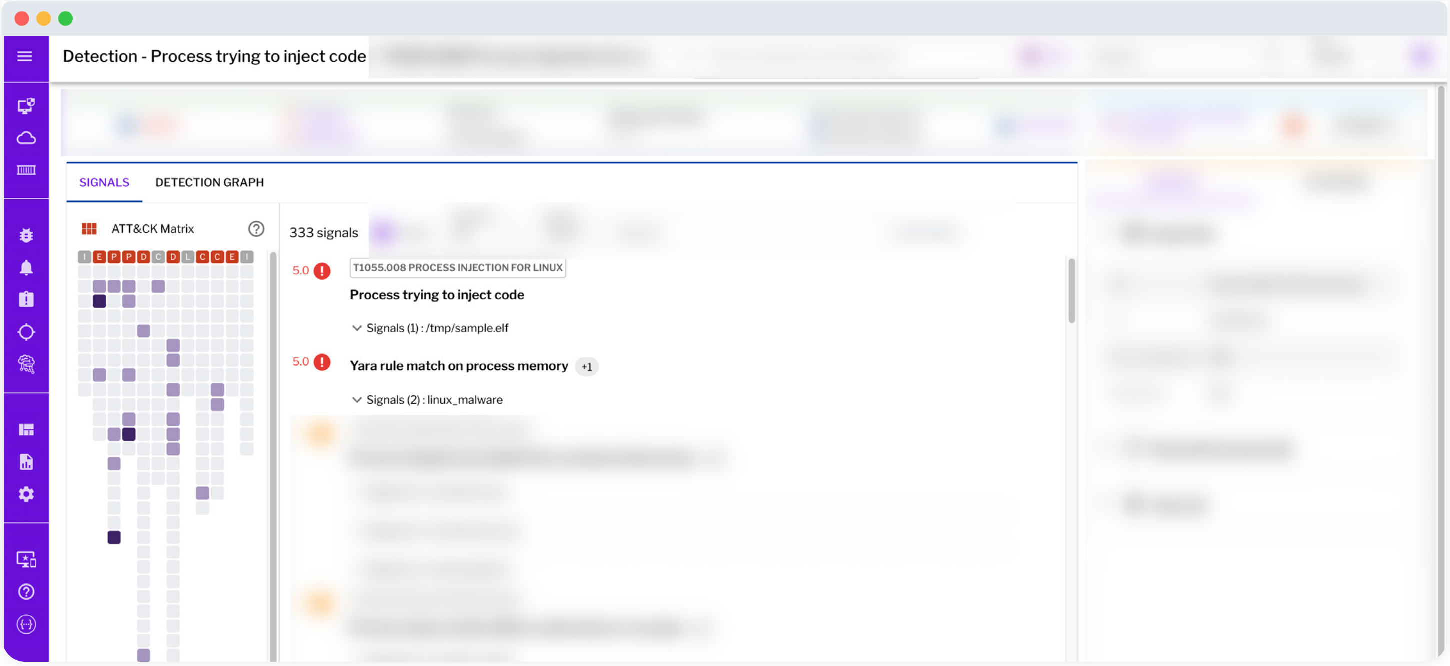
Figure 9: Uptycs Threat Research Team tracks known ransomware and threat groups, here we have identified the infamous NotPetya ransomware and scan for associated malware signatures and binaries.

Prediction 12:
Server-side WebAssembly tooling starts to proliferate after Docker’s alpha driver

A primary goal of using server-side WebAssembly tools is to reduce the attack surface of a running container in addition to remote code execution (RCE) attack vectors..

> **Uptycs works in parallel with threat detection that monitors attackers’ TTPs and subsequently maps these signals to the MITRE ATT&CK matrix.**

Uptycs can detect and respond to threats in containers no matter how the processes inside them are compiled, thereby quarantining hosts, killing processes, and identifying files requiring further investigation. Our eBPF-based sensor captures detailed event telemetry irrespective of the application language or runtime, providing observability into attack patterns that might lead to RCE or other advanced threat tactics. Uptycs detects such patterns early by using signals from the sensor. Responses to potential intrusions can either be automated or alerts can be triggered for further digital forensics or investigation by analysts.



333 signals

5.0 T1055.008 PROCESS INJECTION FOR LINUX
Process trying to inject code
Signals (1) : /tmp/sample.elf

5.0 Yara rule match on process memory +1
Signals (2) : linux_malware

Figure 10: Uptycs maps detections and signals to the MITRE ATT&CK Matrix, here we see how specific signals are used to inform the tactics and techniques observed in a malicious attempt to inject code.

Prediction 13:

New legislation will continue to force standards that risk lack of real-world adoption or testing

The rate of innovation will always outpace that of legislation. Strong legislation that is prescriptive in its security standards is not likely to exist or come soon; instead, legislation might only yield half-baked standards that haven't yet been battle-tested to address the larger cybersecurity gaps.

> **Uptycs makes it easy to enforce out-of-the-box compliance rules and go beyond legislation to create custom rulesets to protect your assets.**

Uptycs' predefined rules align with industry standards and regulatory requirements, such as PCI-DSS, SOC 2, and CIS Benchmarks. By leveraging these, you can be ensured your systems are compliant with relevant regulations without the need for extensive customization.

Uptycs also empowers your enterprise to create custom rulesets that go beyond legislation in protecting your assets. They can be tailored to your specific needs and can address unique risks and threats not covered by the default rules. The platform provides a flexible and extensible framework for creating them with support for a wide range of data sources and analytics techniques. With Uptycs you can achieve a higher level of security and industry compliance while also addressing your unique security challenges.

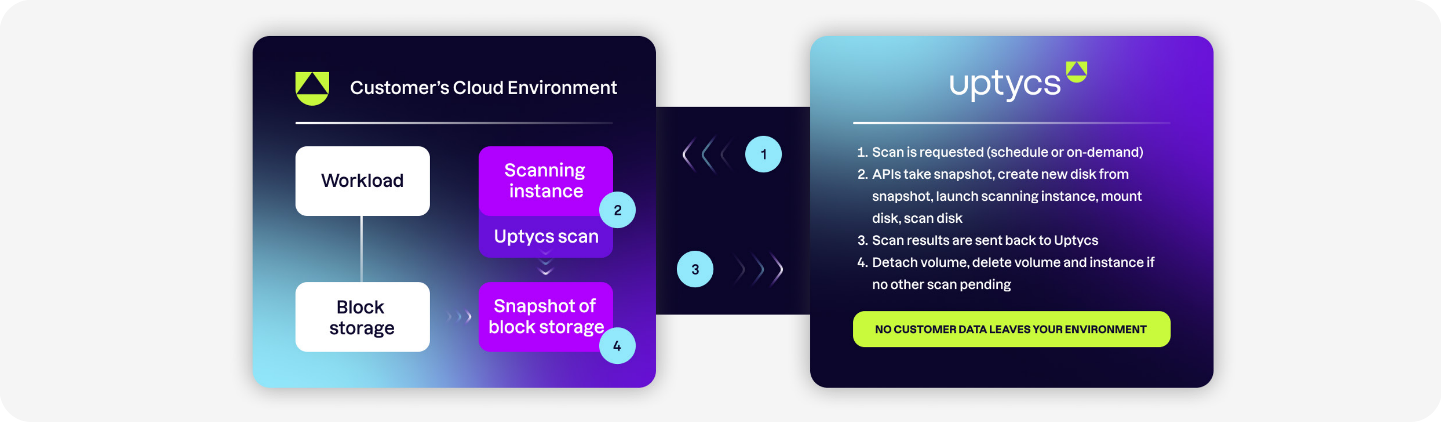
.

Prediction 14:

Confidential computing starts to be put through high-throughput test cases

Confidential computing aims to reduce data exposure from services and protect against hostile root users. This is to protect sensitive data, even in insecure environments. Traditionally, data is secured through encryption and access control means, but such measures might not be sufficient to protect data when it's being processed. Confidential computing provides a more comprehensive solution to protect data during processing by creating secure enclaves (isolated regions in memory).

> **Uptycs agentless scanning can optionally ensure no customer data leaves your environment.**



1. Scan is requested (schedule or on-demand)
2. APIs take snapshot, create new disk from snapshot, launch scanning instance, mount disk, scan disk
3. Scan results are sent back to Uptycs
4. Detach volume, delete volume and instance if no other scan pending

NO CUSTOMER DATA LEAVES YOUR ENVIRONMENT

Figure 11: Uptycs agentless scanning ensures that no customer data leaves the host environment, providing extra security and data protection for sensitive telemetry.

Agentless scanning is a powerful feature that enables you to monitor your assets without requiring agent installation. This eliminates additional software installation and configuration while also reducing your IT team burden. Uptycs agentless architecture reinforces the values of providing further modularity and confidentiality to how your security data is handled and processed. As shown in figure 11, the agentless scanning method ensures all of your customer data safely remains in your organization's environment.

Agentless scanning provides a comprehensive view of your organization's assets without compromising data security or privacy. Its parallel deployment with a traditional sensor-based approach across your environment provides deeper detection insights and real-time responses for higher-priority assets. Meanwhile, the agentless solution covers your less critical assets. Overall, Uptycs agentless scanning provides a powerful and flexible tool to enhance your security and compliance capabilities.

About Uptycs

Uptycs, the first unified CNAPP and XDR platform, reduces risk by prioritizing your responses to threats, vulnerabilities, misconfigurations, sensitive data exposure, and compliance mandates across your modern attack surface—all from a single UI. This includes the ability to tie together threat activity as it traverses on-prem and cloud boundaries, thus delivering a more cohesive enterprise-wide security posture.

Start with your Detection Cloud, Google-like search, and the attack surface coverage you need today. Be ready for what's next.

Shift your cybersecurity up with Uptycs.

uptycs