THE CYBER TOOLCHAIN

NO. 012

Head

THE WEEK'S TOP PICKS

PUBLISHED SEPTEMBER 18, 2026 · FRIDAYS

// SHARE THIS WEEK ▽ Top 5 ▽ Top Pick

The best tooling updates that shipped this week.

▸ // HOW THESE PICKS ARE MADE SHOW

▾ // THE BRIEF HIDE

What stands out in this week's picks, grouped by what it lets you do. Every tool named links to its pick below.

Three unrelated things stand out. Qualys will now quarantine a host itself when a CISA KEV bug goes past due, so an unpatchable box stops being an open door while the patch is argued over. Splunk Security Content adds 12 detections, including browser-spawned shells and Socat tunneling. Zeek 9 ingests VXLAN / GENEVE traffic directly, no sniffing workarounds.

> PROTECT
>
> **Isolate a host you cannot patch in time, without waiting on a human**
>
> Cloud Agent-native isolation triggers on overdue CISA KEV findings, so the exposure window closes at the endpoint instead of staying open through the change-approval cycle. The AI patch reliability scoring is the other half of that trade: it tells you which patches historically break things before you push them.
>
> Qualys

> DETECT

Catch Socat tunnels, LOLBAS abuse and browser-spawned shells out of the box

12 new detections plus fidelity fixes across 18 existing analytics — the tuning work a team would otherwise do itself after the first month of false positives. Browser-spawned shells and SCCM component abuse are both post-compromise footholds that generic process-creation rules tend to bury.

Splunk Security Content

DETECT

Monitor overlay-encapsulated traffic without a tap workaround

A native UDP packet source reads VXLAN / GENEVE -encapsulated flows directly, which is how most east-west traffic actually moves in a modern fabric; previously that meant a decapsulation hop or a lossy sniffing rig. `zeek.conf` plus systemd also makes cluster layout a declarative file rather than per-node scripting.

Zeek

RESPOND

Pull a timeline out of Gmail, Defender Safe Links and signed-token URLs

New parsers mean an analyst can paste a rewritten Safe Links URL or a Fernet/itsdangerous token and get the embedded original and timestamps back, instead of hand-decoding layers during a phishing investigation. Defanged IOC refanging removes the other tedious step in that loop.

Unfurl

VIEW

ISSUE VIEW

scroll



SCROLL | EXPAND IN PLACE | PREVIEW PANE

INFORMATION DENSITY

everything



BRIEFED | EVERYTHING

Every change in this week's picks, in full.

all 102 changes

Do you prefer **scroll**? 👍 👎

// THE PICKS

01	**Zeek**	Network Analysis & Monitoring
02	**Qualys**	Vulnerability Management
03	**Aviatrix**	Firewalls & Network Defense
04	**Splunk Security Content**	Detection Engineering
05	**Dreadnode**	AI-Powered Offensive Security

01 Zeek

1 RELEASE · 2026-08-21 → 2026-09-17

Network Analysis & Monitoring

// WHY IT MADE THE LIST

DEPTH 5/5 IMPACT 5/5

Zeek 9 adds a native UDP packet source that ingests encapsulated (VXLAN/GENEVE) mirror traffic directly, letting clusters monitor cloud environments without packet-sniffing workarounds; it also switches cluster comms to ZeroMQ by default, adds Encrypted Client Hello detection, and forwards LDAP SASL payloads into ntlm/kerberos logs.

> Zeek 9 switches cluster communication to ZeroMQ by default, adds a native UDP packet source for ingesting VXLAN / GENEVE -encapsulated traffic without packet-sniffing workarounds, and introduces a declarative `zeek.conf` `/systemd` cluster-orchestration workflow, alongside a wave of new TLS ECH , NTP, multicast, Kerberos, SSH, DNS and HTTP logging fields, a ZIP file analyzer, and a new `?as` type-casting operator.

└──▷ **WHAT SHIPPED · 29 FEATURES** most completely described first ? what's the number?

01 UDP packet source for encapsulated traffic (VXLAN/GENEVE) NEW

95

Ships a new packet source enabling Zeek clusters to act as a UDP server that ingests encapsulated packet streams directly for cloud environments, without packet-sniffing workarounds. Invoked via `zeek -i udp::0.0.0.0:4789:vxlan` (bundled `zeek-packet-source-udp` plugin), it uses `SO_REUSEPORT` for multi-worker kernel load-balancing, and the `policy/frameworks/conn_key/packet_source/udp/vxlan_vni` policy script adds VNI-aware connection tracking so each VXLAN tenant network is tracked separately.

Receive VXLAN mirror traffic over UDP on a busy sensor where multiple Zeek workers share the load via kernel `SO_REUSEPORT` balancing — no raw packet capture interface needed.

```
$ zeek -i udp::0.0.0.0:4789:vxlan
```

Enable VNI-aware connection tracking so each VXLAN tenant network is tracked separately — load alongside the UDP packet source.

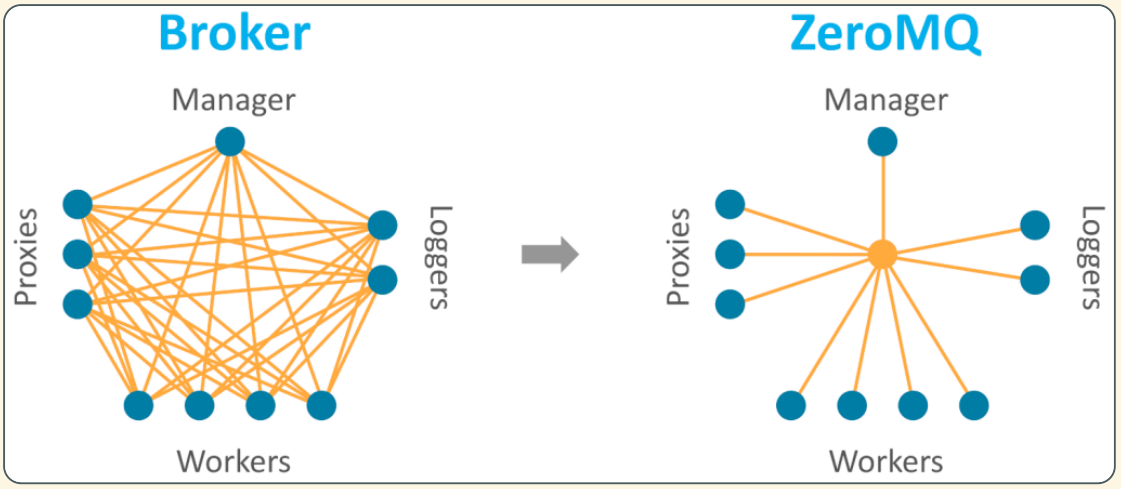
```
$ zeek -i udp::0.0.0.0:4789:vxlan
policy/frameworks/conn_key/packet_source/udp/vxlan_vni
```

— Runnable command plus policy script for VNI tracking `launch-20260917-0d171be8` `v9.0.0`

02 ZeroMQ as default cluster communication backend BREAKING

88

Zeek 9 switches the default cluster communication backend from Broker to ZeroMQ, enabling direct worker-to-worker eventing, cluster-wide event publishing, and single-point cluster event tapping; scripts relying on Broker-specific eventing must re-enable it explicitly. Broker's legacy embedded WebSocket server is fully removed — `Broker::BrokerProtocol`, `Broker::default_port_websocket`, `Broker::default_listen_address_websocket`, `Broker::web_socket_buffer_size`, and `Broker::web_socket_overflow_policy` no longer exist, and the `BrokerProtocol` enum and the Broker manager's Listen() C++ method argument are removed — use Cluster::listen_websocket() and the `ZEEK_WEBSOCKET_*` environment variables instead. `zeromq/main.zeek` options are split into a separate `zeromq/options.zeek` file so standalone Zeek processes can connect to the ZeroMQ layer without participating in cluster node events.



— Named migration API and env vars, but no runnable migration command

`launch-20260917-0d171be8` `v9.0.0`

03 TLS analyzer ECH logging and new extension events NEW

85

Adds `ech_kdf_id` and `ech_aead_id` fields to `ssl.log` (via the `protocols/ssl/ssl-log-ext.zeek` policy script) reporting HPKE KDF and AEAD identifiers from the TLS 1.3 ECH extension. Adds a new `ssl_extension_encrypted_client_hello` event carrying information about the TLS `encrypted_client_hello` extension, and a new `ssl_extension_signature_algorithms_cert` event raised for the `signature_algorithms_cert` extension.

Enable ECH extension logging in ssl.log to capture HPKE KDF and AEAD identifiers from TLS 1.3 Encrypted Client Hello handshakes.

```
$ @load protocols/ssl/ssl-log-ext
```

— Load command given for the policy script `launch-20260917-0d171be8` `v9.0.0`

04 **Configurable binary-data escaping in JSON logging** NEW

83

Adds multiple configuration options for handling binary data in JSON logging, resolving a long-standing ambiguity, including `Log::json_string_escape_policy` (type `JSON::STRING_ESCAPE_POLICY_*`) to make control-character and invalid UTF-8 escaping configurable; the default remains `JSON::STRING_ESCAPE_POLICY_HEX`.

Switch JSON log escaping to TSV-style (reversible) encoding instead of the default hex encoding, so downstream SIEM parsers can round-trip binary fields correctly.

```
zeek
redef Log::json_string_escape_policy =
JSON::STRING_ESCAPE_POLICY_TSV;
```

— Config example with exact key and enum values `launch-20260917-0d171be8` `v9.0.0`

05 **Optional ZIP file analyzer** NEW

76

Adds a new, optional ZIP file analyzer that reports contained files to `files.log`; `policy/files/zip/register.zeek` maps the bundled Spicy ZIP analyzer to the `application/zip` MIME type, with recursive ZIP depth controlled by `Spicy::max_file_depth`.

— Named script, MIME type and depth control key `launch-20260917-0d171be8` `v9.0.0`

06 **SHA256 ticket hashes in kerberos.log** BREAKING

73

Replaces the MD5-hashed `auth_ticket` and `new_ticket` fields in `kerberos.log` with `auth_ticket_sha256` and `new_ticket_sha256` (via `protocols/krb/ticket-logging.zeek`); load the `protocols/krb/md5-ticket-logging.zeek` policy script to restore the original MD5 fields.

— Migration script named, clear before/after fields `launch-20260917-0d171be8`

07 **SHA256 SSH host key fingerprint in ssh.log** BREAKING

73

Replaces the `host_key` fingerprint field in `ssh.log` with a new `host_key_fingerprint` field using SHA256 in the same format as `ssh-keygen -l`;

the `protocols/ssh/md5-host-key-logging.zeek` policy script restores the old field.

— Migration path and exact format named `launch-20260917-0d171be8`

---

08 **Nine new HTTP analyzer weirds** NEW 73

Extends the HTTP analyzer with nine new weirds — `HTTP_bad_chunk_size`, `HTTP_chunked_multi`, `HTTP_content_length_0_and_expect_100_cont`, `HTTP_content_length_leading_zeros`, `HTTP_bad_content_length`, `HTTP_obsolete_line_folding`, `HTTP_content_length_and_chunked`, `HTTP_content_range_and_chunked`, and `HTTP_expect_not_100_continue` — for unusual Content-Length, Transfer-Encoding, and Expect header usage.

— All nine weird names given, no filtering example `v9.0.0`

---

09 **Storage-framework persistence for known-* scripts** NEW 71

Extends the `known-certs`, `known-hosts`, and `known-services` scripts with storage-framework options including `enable_hosts_persistence`, `host_store_prefix`, `host_store_backend_type`, and `host_store_backend_options`, using a SQLite backend under `Cluster::default_store_dir` by default.

— All config keys named, no worked config sample `v9.0.0`

---

10 **Software detection cache tuning options** NEW 70

Adds `Software::parse_cache_interval`, `Software::found_cache_interval`, and `Software::max_software_cache_size` tunables to the software framework for finer control over version-detection caching.

Cap the software framework's detection cache to limit memory use and reduce noisy software-version log churn in high-volume environments.

zeek

```
redef Software::max_software_cache_size = 5000;
redef Software::parse_cache_interval = 1min;
redef Software::found_cache_interval = 5min;
```

— Config example with exact keys and file location `launch-20260917-0d171be8`

---

11 **Declarative zeek.conf cluster orchestration** NEW 65

Adds a new declarative `zeek.conf` cluster configuration file consumed by Zeek's `systemd` generator (`zeek-systemd-generator`) to produce systemd unit files for orchestrating Zeek clusters, including multi-machine deployments; later extended to support multiple interfaces and multi-host deployments.

– Names config file and generator but no example unit file `launch-20260917-0d171be8` `v9.0.0`

12 **`?as` safe type-cast operator and expanded `as` casting** NEW 65

Adds the `?as` operator to Zeek's scripting language for safely checking type-conversion compatibility at runtime, and extends the `as` casting operator to cover all type conversions previously requiring explicit BiFs such as interval_to_double(), plus additional natural companions.

– Named operator and replaced BiF, no code sample `launch-20260917-0d171be8` `v9.0.0`

13 **Thread-safety enforcement for zeek::fmt()** BREAKING 65

Calling zeek::fmt() from non-main threads now emits a warning (and aborts in debug builds); plugins spawning threads must switch to threading::BasicThread::Fmt() or std::format().

– Names replacement APIs plugin authors must adopt `v9.0.0`

14 **Reporter::limit_reached_weird() BIF for size-limit violations** NEW 62

Adds `Reporter::limit_reached_weird` BIF to report size-limit violations, logging a named weird and appending `X` to the connection `history` field.

– Named BIF and history field marker, no call example `v9.0.0`

15 **DNS opcode fields for RFC 1996 notifications** NEW 60

Adds `opcode` and `opcode_name` fields to `dns.log` to support DNS notifications (RFC 1996); removable via the `protocols/dns/disable-opcode-log-fields.zeek` policy script.

– Named fields and toggle script, no example `launch-20260917-0d171be8`

THINNER COVERAGE BELOW

16 **Multicast participants log from IGMP activity** NEW 59

Adds a new `multicast_participants.log` (via the `protocols/conn/multicast-participants.zeek` policy script) reporting multicast speakers and hosts participating in multicast connections based on IGMP activity.

– Named policy script and log, no example `launch-20260917-0d171be8` `v9.0.0`

17 **LDAP SASL forwarding to GSSAPI and NTLM** IMPROVED 57

Extends the LDAP analyzer to forward SASL payloads from `bindRequest` / `bindResponse` to GSSAPI and NTLM parsers, enriching logging into

`ntlm.log` and `kerberos.log`.

— Names messages and target logs but no example `launch-20260917-0d171be8` `v9.0.0`

---

18 **Bundled Spicy 1.17.0 with optimizer and Windows support** IMPROVED 55

Ships Spicy 1.17.0 with a control-flow-graph-based optimizer delivering 20–60% microbenchmark performance improvements and Windows (MSVC) build support.

— Concrete numbers but no user action described `launch-20260917-0d171be8`

---

19 **Non-final OpaqueType with plugin hooks** NEW 55

Makes `OpaqueType` non-final and adds hooks for hashing, casting, and default initialization, enabling plugins to introduce new scripting types storable in sets/tables and castable to existing Zeek types (experimental).

— Experimental plugin hook, no code sample given `v9.0.0`

---

20 **TCP support in Syslog analyzer** NEW 54

Extends the Syslog analyzer to support TCP via Octet Counting and Non-Transparent-Framing on port 514/tcp.

— Names framing modes and port but no config example `launch-20260917-0d171be8` `v9.0.0`

---

21 **dce_rpc_auth() event for DCE-RPC authentication context** NEW 54

Adds dce_rpc_auth() event for script-level access to the security provider, per-message protection, and authentication context in DCE-RPC PDUs.

— Named event and payload contents, no example handler `v9.0.0`

---

22 **QUIC DPD signatures for non-standard ports** NEW 54

Adds DPD signatures for QUIC version 1 and QUIC version 2 to attach the QUIC analyzer on non-port-443 UDP connections on signature match.

— Names protocol versions but no config detail `v9.0.0`

---

23 **Kerberos analyzer field and event enhancements** IMPROVED 52

Extends `kerberos.log` AP entries to populate the previously-unset `service` and `cipher` columns, and extends the krb_ap_request() event with an `in_kdc_padata` parameter indicating whether the AP-REQ is embedded in KDC/TGS pre-authentication data.

— Named fields and event parameter but thin usage guidance `v9.0.0`

---

24 **Case-insensitive and single-line pattern modifiers in Input Framework**

NEW

52

Extends the Input Framework to read pattern values with case-insensitive (`/foo/i`) and single-line (`/bar/s`) modifiers.

– Exact modifier syntax named, no full config `v9.0.0`

25 **NTP control and private mode logging** NEW

50

Adds new `ntp_control.log` and `ntp_private.log` logs covering NTP modes 6 and 7 respectively, which were previously unlogged.

– Names two new logs but no usage detail `launch-20260917-0d171be8` `v9.0.0`

26 **Build and platform support changes** BREAKING

50

The ZeekJS plugin now requires `std::format` from C++20, dropping support for older distributions using GCC 12.x such as Debian 12. FreeBSD is no longer officially supported with CI testing; it moves to the same community-patch model as OpenBSD.

– Named platforms and requirement but no migration step `v9.0.0`

27 **$attributes field on script_id records** NEW

48

Adds a `$attributes` field to `script_id` records returned by the global_ids() BiF, exposing identifier attributes.

– Named field and BiF, no usage example `v9.0.0`

28 **Multicast DNS logged as separate transactions** IMPROVED

30

Logs multicast DNS transactions as separate transactions since they occur on separate network flows.

– Bare behavioral note, no field or script named `launch-20260917-0d171be8`

29 **FTP sessions with only login and logout logged** NEW

23

Logs FTP sessions that feature only login and logout.

– Single-sentence bare description `launch-20260917-0d171be8`

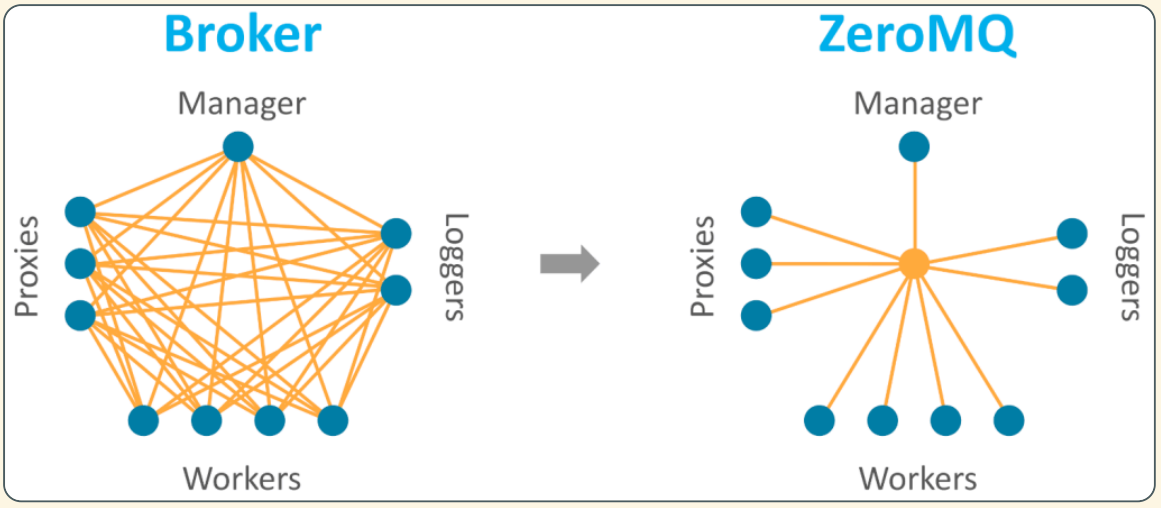
└──▷ **BREAKING ON UPGRADE**

! The `host_key` field in `ssh.log` is replaced by `host_key_fingerprint` (SHA256, `ssh-keygen -l` format); any pipeline keying on `host_key` will break unless the `protocols/ssh/md5-host-key-logging.zeek` policy script is loaded to restore it.

- ! The `auth_ticket` and `new_ticket` fields (MD5 hashes) in `kerberos.log` are replaced by `auth_ticket_sha256` and `new_ticket_sha256` (SHA256) via `protocols/krb/ticket-logging.zeek`; load `protocols/krb/md5-ticket-logging.zeek` to restore the original fields.
- ! The default cluster communication backend is now ZeroMQ instead of Broker; scripts or packages that rely on Broker-specific eventing must re-enable the Broker backend explicitly.
- ! Broker's legacy embedded WebSocket server is fully removed: `Broker::BrokerProtocol`, `Broker::default_port_websocket`, `Broker::default_listen_address_websocket`, `Broker::web_socket_buffer_size`, and `Broker::web_socket_overflow_policy` no longer exist. Use Cluster::listen_websocket() and the `ZEEK_WEBSOCKET_*` environment variables instead.
- ! The `BrokerProtocol` enum has been removed and the Broker manager's Listen() C++ method no longer accepts its optional `BrokerProtocol` argument; it always uses Broker's native protocol.
- ! Calling zeek::fmt() from non-main threads now emits a warning (and aborts in debug builds); plugins spawning threads must switch to threading::BasicThread::Fmt() or std::format().
- ! The ZeekJS plugin now requires `std::format` from C++20, dropping support for older distributions using GCC 12.x such as Debian 12.
- ! FreeBSD is no longer officially supported with CI testing; it moves to the same community-patch model as OpenBSD.

`announced · Sep 17, 2026`

Zeek 9 ships ZeroMQ cluster comms by default, native encapsulated-traffic ingestion, systemd orchestration via zeek.conf, and new log fields.



└──▷ **TRY IT**

Enable ECH extension logging in ssl.log to capture HPKE KDF and AEAD identifiers from TLS 1.3 Encrypted Client Hello handshakes.

```
$ @load protocols/ssl/ssl-log-ext
```

Cap the software framework's detection cache to limit memory use and reduce noisy software-version log churn in high-volume environments.

```
/etc/zeek/local.zeek
redef Software::max_software_cache_size = 5000;
redef Software::parse_cache_interval = 1min;
redef Software::found_cache_interval = 5min;
```

- Adds a new declarative `zeek.conf` cluster configuration file consumed by Zeek's `systemd` generator to produce systemd unit files for orchestrating Zeek clusters, including multi-machine deployments.
- Adds `Software::parse_cache_interval`, `Software::found_cache_interval`, and `Software::max_software_cache_size` tunables to the software framework for finer control over version-detection caching.
- Adds `ech_kdf_id` and `ech_aead_id` fields to `ssl.log` (via the `protocols/ssl/ssl-log-ext.zeek` policy script) reporting HPKE KDF and AEAD identifiers from the TLS 1.3 ECH extension.
- Adds new `ntp_control` and `ntp_private` logs for NTP modes 6 and 7 respectively.
- Adds a new `multicast_participants.log` (via the `protocols/conn/multicast-participants.zeek` policy script) reporting multicast speakers based on IGMP activity.

+14 more

BREAKING ON UPGRADE

- The `host_key` field in `ssh.log` is replaced by `host_key_fingerprint` (SHA256, `ssh-keygen -l` format); any pipeline keying on `host_key` will break unless the `protocols/ssh/md5-host-key-logging.zeek` policy script is loaded to restore it.
- The `auth_ticket` and `new_ticket` fields (MD5 hashes) in `kerberos.log` are replaced by `auth_ticket_sha256` and `new_ticket_sha256` (SHA256) via `protocols/krb/ticket-logging.zeek`; load `protocols/krb/md5-ticket-logging.zeek` to restore the original fields.
- The default cluster communication backend is now ZeroMQ instead of Broker; scripts or packages that rely on Broker-specific eventing must re-enable the Broker backend explicitly.

GOOD PICK? 👍 👎 GOOD REASON? 👍 👎

02 Qualys

1 RELEASE · 2026-09-15 → 2026-09-17

Vulnerability Management

Qualys is a cloud-based security and compliance platform that continuously monitors, detects, and helps remediate vulnerabilities across IT assets and infrastructure.

// WHY IT MADE THE LIST

DEPTH 5/5 IMPACT 5/5

Automated host isolation now fires natively through the Qualys Cloud Agent when a QQL policy matches — quarantining hosts with overdue CISA KEV vulnerabilities within seconds, no EDR integration required — paired with AI-powered patch reliability scoring that grades each patch before deployment.

> Qualys expanded Policy Audit with AI-assisted policy creation, continuous compliance monitoring, automated remediation, and risk-based finding prioritization, while TruRisk Eliminate gained AI-powered patch reliability scoring and Cloud Agent-native automated host isolation for overdue CISA KEV vulnerabilities.

└──▷ WHAT SHIPPED · 7 FEATURES most completely described first ? what's the number?

01 AI-powered patch reliability scoring NEW

95

TruRisk Eliminate adds AI-powered Patch Reliability Scoring that combines LLM-analyzed public sentiment with Qualys telemetry on patch rollback and vulnerability reopen rates to produce a pre-deployment reliability score (Low / High) for each patch. In the Patch Management app (Patches > Windows), the `patch.kb` QQL filter surfaces Patch Reliability assessments for specific KBs, and clicking `Patch Reliability: Low` opens an AI Assessment window showing known issues and source links via Detailed Report.

Check patch reliability before deploying a Patch Tuesday update — filter to specific KBs in the Patch Management app to see whether Qualys rated them Low or High reliability before pushing to production.

> 📍 In the Patch Management application, go to Patches › Windows and enter the QQL query: patch.kb: [KB5124008 , KB5124012] — then click 'Patch Reliability: Low' on any result to open the AI Assessment window and review known issues and source links via 'Detailed Report'.

— Names exact QQL filter, UI path, and runnable example 2026-09-15-2b585d21

02 Automated host isolation via Cloud Agent NEW

95

TruRisk Eliminate can automatically isolate a host natively through the Qualys Cloud Agent when a user-defined QQL policy is met, with no EDR integration required,

quarantining the host within seconds and writing a timestamped audit record of which rule, host, and deadline triggered the action. A built-in CISA KEV isolation use case applies the QQL `vulnerabilities.status:[ACTIVE,NEW,REOPENED]`, `vulnerabilities.riskFactor.cisaKEVDueDate < 'now-1s'`, and `vulnerabilities.riskFactor.cisaKnownExploits:TRUE` to isolate hosts where a KEV remediation deadline has passed and the vulnerability remains open.

Automatically isolate any host where a CISA KEV remediation deadline has passed and the vulnerability is still open, preventing exploitation while patching continues.

```
$ vulnerabilities.status:[ACTIVE,NEW,REOPENED] AND
vulnerabilities.riskFactor.cisaKEVDueDate < "now-1s" AND
vulnerabilities.riskFactor.cisaKnownExploits:TRUE
```

— Names exact QQL fields and a runnable isolation query `2026-09-15-2b585d21`

03 **AI-Powered Policy Creation for Policy Audit** NEW 60

Teams can upload frameworks, benchmarks, vendor guidance, or internal policies and use AI assistance to map controls to policy logic, assessment criteria, and expected values, with human review and approval required before the mapped policy is published.

— Describes mechanism but no named config or endpoint `2026-09-17-5c9e514a`

THINNER COVERAGE BELOW

04 **Ring-based phased patch deployment** NEW 55

TruRisk Eliminate Patch Management supports ring-based phased deployment, letting low-reliability patches be progressively validated through Test → Staging → Production environments before broader rollout.

— Names deployment stages but no config or command `2026-09-15-2b585d21`

05 **Audit Fix automated remediation** NEW 45

Audit Fix streamlines correction of compliance findings through pre-built remediation content and automated workflows, and validates that fixes remain in place over time.

— General mechanism described, no named commands or config `2026-09-17-5c9e514a`

06 **Risk-based prioritization for Policy Audit findings** IMPROVED 45

Policy Audit findings are now prioritized by incorporating asset criticality, threat exposure, business context, ransomware relevance, and security risk indicators.

— Names several risk factors but no UI or query detail `2026-09-17-5c9e514a`

07 **Audit Insights continuous compliance monitoring** NEW

40

Audit Insights continuously monitors controls, detects compliance drift, and automatically collects evidence throughout the year instead of relying on point-in-time assessments.

— What it does is clear, no concrete surface or steps given 2026-09-17-5c9e514a

└──▷ **ALSO FROM THESE RELEASES**

changelog · Sep 17, 2026

Qualys adds AI-Powered Policy Creation, Audit Insights continuous monitoring, and Audit Fix automated remediation to Policy Audit

- Adds AI-Powered Policy Creation for Policy Audit, enabling teams to upload frameworks, benchmarks, vendor guidance, or internal policies and use AI assistance to map controls to policy logic, assessment criteria, and expected values — with human review and approval before publication.
- Introduces Audit Insights to continuously monitor controls, detect compliance drift, and automatically collect evidence throughout the year instead of at point-in-time assessments.
- Introduces Audit Fix to streamline correction of compliance findings through pre-built remediation content and automated workflows, validating that fixes remain in place over time.
- Adds risk-based prioritization to Policy Audit findings by incorporating asset criticality, threat exposure, business context, ransomware relevance, and security risk indicators.

GOOD PICK? 👍 👎 GOOD REASON? 👍 👎

03 Aviatrix 10.1.0

Firewalls & Network Defense

Aviatrix is a cloud networking platform that simplifies multi-cloud connectivity, security, and operations across AWS, Azure, and Google Cloud.

// WHY IT MADE THE LIST

DEPTH 5/5 IMPACT 4/5

Adds Distributed Cloud Firewall East-West Layer 7 inspection and intra-cluster enforcement for EKS plus Premium ET Pro IPS rule feeds, letting teams catch lateral movement across cloud boundaries that was previously invisible, alongside FIPS 140-3 validated IPsec and end-to-end VRF multi-tenancy.

> Aviatrix 10.1.0 ships FIPS 140-3 validated IPsec , end-to-end VRF multi-tenancy, DCF East-West Layer 7 inspection and Premium ET Pro IPS feeds, alongside Flexible Gateway Deployment, independent gateway sizing, and previews for private-Kubernetes-cluster firewalling, make-before-break gateway replacement and Smart Gateways; Private Mode is removed and Controller UI management moves fully to CoPilot.

└──▷ **WHAT SHIPPED · 22 FEATURES** most completely described first ? what's the number?

01 Premium IPS rule feeds in DCF NEW

90

Adds `Security > Distributed Cloud Firewall > IPS > Rule Feeds` (labeled ET Pro in CoPilot) as a Premium IPS feed applied alongside custom Suricata rulesets, with traffic actions governed by severity thresholds in the active IPS Profile.

Activate the Premium ET Pro IPS rule feed so that matched traffic is handled according to your active IPS Profile severity thresholds, without replacing any custom Suricata rules you have uploaded.

> 📍 In CoPilot, go to Security › Distributed Cloud Firewall › IPS › Rule Feeds; the ET Pro feed is listed as the default entry — confirm it is enabled, then verify or adjust severity thresholds in your active IPS Profile.

— Exact CoPilot path plus step-by-step example given `10.1.0`

02 DCF intra-cluster enforcement for EKS NEW

90

Adds DCF intra-cluster enforcement, enabled per-cluster from CoPilot under `Security > Distributed Cloud Firewall > Settings > Intra-Cluster`, supporting Calico, Cilium, Antrea, AWS VPC CNI (v1.14+), Weave Net, and Canal.

Enable DCF intra-cluster policy enforcement on an EKS cluster so that Distributed Cloud Firewall controls all east-west pod traffic via existing CNI NetworkPolicy support.

📍 In CoPilot, go to Security › Distributed Cloud Firewall › Settings › Intra-Cluster, select the target EKS cluster, and enable enforcement.

— Named path, supported CNIs, and worked example `10.1.0`

03 **Independent gateway instance sizing** NEW 90

Adds independent gateway instance sizing, allowing a single instance to be resized from CoPilot at `Cloud Fabric > Gateways > (transit or spoke) > gateway group > Instances` tab without affecting HA or the group default size; surfaces a 'Multiple Sizes' label when a group has diverged.

Resize a single gateway instance without touching HA peers or changing the group default size, useful when one instance needs more capacity after a traffic spike.

📍 In CoPilot, go to Cloud Fabric › Gateways › (transit or spoke) › gateway group › Instances tab, select the individual instance, and choose a new size.

— Exact CoPilot path plus example steps given `10.1.0`

04 **VRF multi-tenancy end-to-end propagation** NEW 85

Adds VRF for multi-tenancy with end-to-end propagation across transit-to-transit peering, BGP-spoke-to-transit peering, and intra-group backup links; enabled by a Controller feature flag (off by default) plus per-attachment opt-in, supporting up to 200 network domains.

— Flag and scope named but no exact toggle command `10.1.0`

05 **DCF for Private Kubernetes Clusters (Preview)** NEW 85

Adds DCF for Private Kubernetes Clusters (Preview), enabled per cluster in CoPilot or Terraform, supporting EKS, AKS, and GKE; requires an Aviatrix spoke gateway in the same VPC with a security-group rule allowing TCP port 443 to the Kubernetes API server.

— Named requirements and port, no exact command `10.1.0`

06 **DCF Spoke Local Breakout** NEW 80

Adds DCF Spoke Local Breakout, recording the egress path taken in every DCF log entry; requires Single IP SNAT (or customized SNAT), the 10.1 gateway image, and a supported instance size on Aviatrix Transit (FireNet) and AWS TGW centralized topologies.

— Detailed requirements but no exact config steps `10.1.0`

07 **DCF Quick Time-to-Value dashboard** NEW 80

Adds DCF Quick Time-to-Value dashboard with a system-defined, Aviatrix-managed read-only threat intelligence ruleset (defaults to Watch Mode) and ten Recommended Security Control cards covering ToR traffic, sanctioned-country traffic, cleartext legacy protocols, cryptomining pools, and outbound proxy/relay; requires Controller 8.2+ and CoPilot 4.37.

— Version requirements named but no navigation steps `10.1.0`

---

08 **DCF East-West Layer 7 inspection for AWS** NEW 70

Adds DCF East-West Layer 7 inspection for AWS, with symmetric routing enabled per spoke group in CoPilot or Terraform, also reducing cross-AZ data transfer cost and latency.

— Names scope and tooling, lacks exact command `10.1.0`

---

09 **GCP Global VPC Regional Spoke Egress (Phase 2)** IMPROVED 70

Adds GCP Global VPC Regional Spoke Egress (Phase 2), letting operators choose which regions egress locally vs. through FireNet, with both modes coexisting in the same Global VPC; the CoPilot Egress page now shows Global VPCs in a nested tree displaying each region's egress mode.

— UI location named, mechanism explained, no exact steps `10.1.0`

---

10 **Smart Gateways Phase 3 (Preview)** NEW 70

Adds Smart Gateways Phase 3 (Preview) covering transit gateways, Edge as Spoke, Edge as Transit, and BGP spoke gateways, controlled by three tiered feature flags (fabric-wide kill switch, per-group underlay flag, per-group route-resolver flag) all off by default.

— Flags named but no exact toggle steps `10.1.0`

---

11 **Flexible Gateway Deployment (no public IP)** NEW 65

Adds Flexible Gateway Deployment (private subnet, no public IP), enabled per gateway group at creation time on AWS (including GovCloud) and Azure, via CoPilot and Terraform.

— Names platforms and tools but no exact steps `10.1.0`

---

12 **Transit peering options: AZ affinity and jumbo frames** NEW 65

Adds AZ Affinity Across Transit, enabled per peering (disabled by default) on AWS same-region HPE peerings, and opt-in AWS inter-region jumbo frame support for transit peering (AWS only, excluding partitions such as AWS GovCloud that do not support jumbo frames).

— Both peering settings named with scope, no exact command `10.1.0`

13 **FIPS 140-3 validated IPsec data plane** NEW 60

Adds FIPS 140-3 validated IPsec data plane as a separate FIPS-validated gateway build; existing gateways must be replaced (not toggled) to enter FIPS mode.

— Migration note given but no exact command 10.1.0

14 **SNAT and HPE support on Azure spokes** NEW 60

Adds SNAT and HPE support on Azure spokes with subnet groups for both HPE and non-HPE deployments, configurable via the existing Controller API/CLI or Terraform.

— Names tooling paths, no exact command 10.1.0

THINNER COVERAGE BELOW

15 **Make Before Break Gateway Replacement (Preview)** NEW 50

Adds Make Before Break Gateway Replacement (Preview), preserving the gateway's external IP through cut-over so partners and firewalls need no reconfiguration, with automatic eligibility checking per gateway.

— Explains benefit, lacks named config surface 10.1.0

16 **Private Mode removed, requires rebuild** BREAKING 50

Private Mode is fully removed; deployments still on Private Mode cannot upgrade in place and must be rebuilt as Flexible Gateway deployments.

— Clear migration note, no exact command 10.1.0

17 **Kubernetes Discovery and SmartGroups reach GA** IMPROVED 45

Promotes Kubernetes Discovery and SmartGroups to general availability, enabling DCF rules to enforce policy across both Kubernetes Pods/Services and VM workloads.

— States GA status and scope, no config detail 10.1.0

18 **AKS onboarding with Microsoft Entra ID** NEW 45

Adds AKS onboarding with Microsoft Entra ID, with the Controller auto-detecting the Entra ID setting on the AKS cluster.

— Describes auto-detection, no config steps 10.1.0

19 **Azure v6 instance support for gateways** NEW 35

Adds Azure v6 instance support for gateways on Controller 10.1.0 and later.

— Names version requirement only, no further detail 10.1.0

20 **Controller UI management moves to CoPilot** BREAKING 35

Controller UI features formerly managed in the Controller UI are now managed exclusively from CoPilot; onboarding flows for new and existing deployments now route through CoPilot.

— States change of location, no specifics of affected features `10.1.0`

21 **DCF CSP Exclusion List reaches GA** IMPROVED 25

Promotes DCF CSP Exclusion List to general availability.

— Bare GA announcement with no further detail `10.1.0`

22 **Universal Installer for OpenVPN Client** NEW 25

Adds Universal Installer for the Aviatrix OpenVPN Client.

— Name only, no mechanism given `10.1.0`

└──▷ BREAKING ON UPGRADE

! Private Mode is fully removed; deployments still on Private Mode cannot upgrade in place and must be rebuilt as Flexible Gateway deployments.

! Controller UI features formerly managed in the Controller UI are now managed exclusively from CoPilot; onboarding flows for new and existing deployments now route through CoPilot.

`10.1.0`

Aviatrix 10.1.0 adds FIPS 140-3 IPsec , end-to-end VRF multi-tenancy, DCF East-West L7 inspection, Premium IPS feeds, and Flexible Gateway Deployment.

└──▷ HOW TO FIND IT

Enable DCF intra-cluster policy enforcement on an EKS cluster so that Distributed Cloud Firewall controls all east-west pod traffic via existing CNI NetworkPolicy support.

> 📍 In CoPilot, go to Security › Distributed Cloud Firewall › Settings › Intra-Cluster, select the target EKS cluster, and enable enforcement.

Activate the Premium ET Pro IPS rule feed so that matched traffic is handled according to your active IPS Profile severity thresholds, without replacing any custom Suricata rules you have uploaded.

> 📍 In CoPilot, go to Security › Distributed Cloud Firewall › IPS › Rule Feeds; the ET Pro feed is listed as the default entry — confirm it is enabled, then verify or adjust severity thresholds in your active IPS Profile.

Resize a single gateway instance without touching HA peers or changing the group default size, useful when one instance needs more capacity after a traffic spike.

📍 In CoPilot, go to Cloud Fabric › Gateways › (transit or spoke) › gateway group › Instances tab, select the individual instance, and choose a new size.

- Adds `Security > Distributed Cloud Firewall > IPS > Rule Feeds` (labeled `ET Pro` in CoPilot) as a Premium IPS feed applied alongside custom Suricata rulesets, with traffic actions governed by severity thresholds in the active IPS Profile.
- Adds DCF intra-cluster enforcement for EKS, enabled per-cluster from CoPilot under `Security > Distributed Cloud Firewall > Settings > Intra-Cluster`, supporting Calico, Cilium, Antrea, AWS VPC CNI (v1.14+), Weave Net, and Canal.
- Adds VRF for multi-tenancy (end-to-end propagation) across transit-to-transit peering, BGP-spoke-to-transit peering, and intra-group backup links; enabled by a Controller feature flag (off by default) plus per-attachment opt-in, supporting up to 200 network domains.
- Adds Flexible Gateway Deployment (private subnet, no public IP), enabled per gateway group at creation time on AWS (including GovCloud) and Azure, via CoPilot and Terraform.
- Adds FIPS 140-3 validated IPsec data plane as a separate FIPS-validated gateway build; existing gateways must be replaced (not toggled) to enter FIPS mode.

`+16 more`

└──▷ BREAKING ON UPGRADE

- ! Private Mode is fully removed; deployments still on Private Mode cannot upgrade in place and must be rebuilt as Flexible Gateway deployments.
- ! Controller UI features formerly managed in the Controller UI are now managed exclusively from CoPilot; onboarding flows for new and existing deployments now route through CoPilot.

GOOD PICK? 👍 👎 GOOD REASON? 👍 👎

04 Splunk Security Content

1 RELEASE · 2026-09-10

Detection Engineering

// WHY IT MADE THE LIST

DEPTH 4/5 IMPACT 4/5

Twelve new analytics ship for browser-spawned Unix shells and C2, LOLBAS network abuse on uncommon ports, Socat tunneling, SCCM DLL planting, and macOS AppleScript execution — deployable detection content that catches techniques prior ESCU releases missed.

> Splunk Security Content v6.6.0 ships 12 new detections spanning browser-spawned shells, LOLBAS abuse, macOS AppleScript execution, Socat tunneling and SCCM component abuse, alongside a new NIST AI RMF coverage dashboard and updates improving fidelity across 18 existing analytics.

└──▷ **WHAT SHIPPED · 9 FEATURES** most completely described first ? what's the number?

01 **NIST AI RMF lookups and coverage dashboard** NEW 65

Adds `detection_subcategory_map` and `nist_ai_rmf_subcategories` lookups to support analytic categorization and alignment with the NIST AI Risk Management Framework, plus an alpha `nist_ai_rmf_control_coverage` dashboard mapping AI-related ESCU detections to the NIST AI RMF Govern, Map, Measure, and Manage functions to help identify coverage gaps.

— Names both lookups and the dashboard, marked alpha v6.6.0

THINNER COVERAGE BELOW

02 **LOLBAS and browser-spawned shell detections** NEW 59

Adds `Cisco NVM - Browser Spawned Unix Shell with External Connection` to identify command execution or C2 originating from browsers on Unix endpoints, LOLBAS Network Connection On Uncommon Port to catch rare network activity from trusted system binaries on non-standard ports, and LOLBAS Rare Network Connection to surface anomalous connections from LOLBAS binaries with separate process-group and common-port tuning.

— Three named detections with tuning details, no config surface v6.6.0

03 **Fidelity updates across 18 existing analytics** IMPROVED 50

Updates 18 analytics across Citrix, Windows, Linux, and macOS environments, improving detection fidelity for Citrix ADC exploitation, pipe-based execution, data destruction,

Ghostscript exploitation, PowerShell, event-log manipulation, credential access, and more.

— Lists affected technique areas but no specific analytic names v6.6.0

04 **Socat tunneling and proxying detections** NEW 40

Adds Socat Network Listener Binding an Executable and Socat Remote TCP Connection with Local Echo Disabled detections for network tunneling, proxying, and C2 activity via Socat.

— Two named detections, purpose stated but no mechanism v6.6.0

05 **macOS AppleScript and osascript execution detections** NEW 40

Adds `MacOS AppleScript Shell Execution and Compilation` to improve visibility into script-based execution on macOS, and `MacOS Osascript Displaying Suspicious User Prompt` to catch deceptive user-interaction attacks via osascript.

— Two named detections, thin descriptions v6.6.0

06 **SCCM component abuse detections** NEW 40

Adds Windows SCCM Adsource DLL Was Planted In SMS Provider Directory for DLL planting abuse of SCCM components, and Windows SCCM Smsexec Spawned a Suspicious Child Process for abnormal child-process execution from smsexec.

— Two named SCCM detections, no further mechanism given v6.6.0

07 **Windows builtin account name change detection** NEW 28

Adds Windows Builtin Account Name Was Changed detection to identify account manipulation targeting built-in accounts.

— Single named detection, no mechanism detail v6.6.0

08 **Windows browser-copied content execution detection** NEW 28

Adds Windows Content Copied from Browser was Executed detection to catch suspicious execution workflows involving payloads copied from web content.

— Single named detection, thin description v6.6.0

09 **Linux crontab enumeration detection** NEW 28

Adds Linux Crontab Enumeration detection to identify crontab listing activity used for discovery.

— Single named detection, thin description v6.6.0

GOOD PICK? 👍 👎 GOOD REASON? 👍 👎

05 Dreadnode

3 RELEASES · 2026-08-27 → 2026-09-10

AI-Powered Offensive Security

Dreadnode is an AI-powered security research platform that helps teams build, run, and evaluate offensive AI agents for penetration testing and red teaming.

// WHY IT MADE THE LIST

DEPTH 5/5 IMPACT 5/5

Traditional ML attack targets — extraction, membership inference, evasion, and inversion against fraud, image, and text models — are now provisionable by name across all organizations, extending Dreadnode's agentic red-teaming to classic ML systems.

> Dreadnode opened Web Chat to all users, shipped a Global Tool Registry API and offline/air-gapped deployment support, and added traditional ML attack targets across all organizations, while substantially expanding its AI red-teaming task catalog and web-security capability with HTTP desync detection, geo-distributed DNS resolution, LSB steganography, and IP rotation.

└──▷ **WHAT SHIPPED · 35 FEATURES** most completely described first ? what's the number?

01 Global Tool Registry API NEW

90

Adds `GET /api/v1/tools` and `GET /api/v1/tools/{tool_id}` endpoints to query the new Global Tool Registry, giving published capability Python tools and command wrappers stable, organization-scoped identities with immutable revision history.

Enumerate all registered tools in your organization to audit capability surface before a red-team engagement.

```
$ curl -s -H 'Authorization: Bearer <token>' https://<your-instance>/api/v1/tools | jq '.[].id'
```

— Exact endpoints with method, path, and a runnable curl example

Offline SDK and CLI install for air-gapp…

02 Traditional ML attack targets across all orgs NEW

86

Adds three traditional ML attack targets — `fraud tabular`, `MNIST image`, and `IMDB text` — now available across all organizations, covering extraction, membership inference, evasion, and inversion attack types, provisionable by name via the SDK or TUI.

Provision a public ML attack target by bare task name — no org prefix required — to kick off a membership inference campaign.

```
$ dreadnode env provision ml-extraction-fraud-tabular
```

— Named targets and attack types plus a runnable provision command

Traditional ML attack targets now availa…

03 **Air-gap deployment mode** NEW 86

Adds `replicated.isAirgap=true` Helm CLI setting to prevent the Replicated SDK pod from attempting outbound connections to `replicated.app` in air-gapped installs, and a broader air-gap deployment mode that vendors all front-end resources locally, hides the analytics notebook, serves model pricing from a bundled catalog, and pre-bakes capability dependencies into the runtime image so sandbox boot requires no network access.

Prevent the Replicated SDK pod from phoning home during a Helm-based air-gap install in a disconnected environment.

```
$ helm upgrade --install dreadnode ./dreadnode-chart --set
replicated.isAirgap=true
```

— Exact Helm flag with a runnable install command and detailed scope

Web Chat open to all users

04 **Runtime cold-start performance and diagnostics** IMPROVED 83

Runtime cold start reduced by more than 60%, dropping time-to-ready from 18.8s to 6.6s, and now surfaces a full cold-start timing breakdown (total, platform overhead, provider provisioning, boot, installs, slowest step) via `dn runtime start` and `GET /runtimes/{id}`.

Inspect the cold-start timing breakdown on a slow runtime to attribute whether delay is provider provisioning or package install.

```
$ dn runtime start && curl -s -H 'Authorization: Bearer <token>'
https://<your-instance>/runtimes/<id> | jq '.timing'
```

— Concrete before/after numbers plus a named command and endpoint

Traditional ML attack targets now availa… Offline SDK and CLI install for air-gapp…

05 **Self-hosted deployment CA trust and hardening** NEW 82

Adds `caBundle` config key for self-hosted deployments to inject a custom CA bundle into the Node frontend, completing CA trust support across all workloads (API, LiteLLM, and frontend); also adds support to self-hosted Helm charts for non-root container execution and custom CA bundle mounts for outbound TLS trust in private-CA environments.

Inject an internal CA into the Node frontend on a self-hosted air-gapped deployment so TLS to an on-prem model proxy is trusted.

yaml

```yaml
caBundle: |
  -----BEGIN CERTIFICATE-----
  <your-internal-CA-cert>
  -----END CERTIFICATE-----
```

— Named config key with an example YAML snippet plus Helm mechanism

Offline SDK and CLI install for air-gapp… | Web Chat open to all users

06 **TUI theme and slash commands** NEW 80

Adds `DREADNODE_TUI_THEME=light` environment variable to switch the TUI from its default dark palette to a light theme; adds `/reload` slash command to reload the current agent without leaving a chat session; adds `/transcript` command to toggle between compact and full agent transcript views; and adds `/status` slash command showing current session, model, user, org, workspace, and project at a glance.

Check your current session context at a glance in the TUI without leaving the chat interface.

```
$ /status
```

— Names every flag and command but no deeper mechanism

Traditional ML attack targets now availa… | Web Chat open to all users

07 **--mine flag for dn runtime ls** NEW 76

Adds `--mine` flag to `dn runtime ls` to filter runtimes to only those you own; also marks runtimes you do not own in the default listing.

List only the runtimes you own to avoid acting on a colleague's shared runtime in a multi-user workspace.

```
$ dn runtime ls --mine
```

– Exact flag with a runnable command example Web Chat open to all users

08 **HTTP desync and request-smuggling detection** NEW 76

Adds HTTP desync and request-smuggling detection to the web-security capability, covering 11 smuggling families with fingerprinting, payload construction, cache-poisoning detection, and victim-response classification.

– Names 11 families and detection stages but no invocation example

Web Chat open to all users

09 **postMessage handler detection expansion** IMPROVED 76

Expands `postMessage` handler detection in the web-security capability's DOM analysis to cover `window.onmessage`, `MessagePort` / `MessageChannel`, and monitoring-shim wrappers, plus additional origin-validation bypass patterns including unescaped-dot and missing-anchor regex bugs.

– Names exact APIs and bug patterns covered, no example run Web Chat open to all users

10 **Honeytoken and OWASP-ASI attack tooling in SDK** NEW 76

Adds two honeytoken tools to the `ai-red-teaming` capability — mint canary tokens (exfil or RCE variants) and check whether a target agent leaked them across an output boundary; adds algorithmic multi-step tool-attack search to the AI red-teaming agent for finding replay-stable read-then-exfiltrate causal paths across HTTP agent tool call chains; and adds a turnkey OWASP-ASI agentic attack suite runner, argument-aware tool-evidence scoring, and a honeytoken harness for black-box exfil and RCE detection to the SDK.

– Names capability, tool variants and suite components, no runnable example

Offline SDK and CLI install for air-gapp…

11 **Cloudflare Workers OAST support in web-security capability** NEW 73

Adds Cloudflare Workers support via `wrangler` to the web-security capability for deploying programmable OAST endpoints, enabling blind XSS payload hosting, callback logging, and SSRF chain redirection.

– Names tool and three use cases but no runnable example

Offline SDK and CLI install for air-gapp…

12 **Environment-agnostic attack-success detection** NEW 73

Adds environment-agnostic attack-success detection to the `airt` SDK using canary exfiltration, OAST beacons, dataflow taint, LLM judge scoring, and optional customer-defined success policies to produce confidence-rated verdicts.

– Names five detection mechanisms feeding a verdict, no code sample

Offline SDK and CLI install for air-gapp…

13 **Geo-distributed DNS resolution in web-security capability** NEW

72

Adds geo-distributed DNS resolution to the web-security capability, resolving target hostnames through open resolvers in multiple countries (via Shodan or Censys) to detect geo-fenced infrastructure, GSLB routing, and region-locked DNS responses.

– Names data sources and detection targets but no example Web Chat open to all users

14 **Indirect prompt injection web task** NEW

69

Adds an indirect prompt injection web task where agents must detect injections hidden via HTML comments, hidden CSS, off-screen ARIA, white-on-white text, and Unicode tags across a public web page.

– Names five specific hiding techniques, no task identifier

Offline SDK and CLI install for air-gapp…

15 **SDK transforms and scorers for exfiltration and browser attacks**

NEW

69

Adds SDK transforms and scorers covering search-query and trusted-domain image exfiltration channels plus dedicated browser-attack scorers for visual injection, ClickFix execution, navigation hijacking, and domain-validation bypass.

– Names six specific channel and scorer types, no invocation example

Offline SDK and CLI install for air-gapp…

16 **CLI usability in dreadnode env** IMPROVED

67

Adds `provision` as an accepted alias for `create` in `dreadnode env`, and bare public task names (e.g. `ml-extraction-fraud-tabular`) now resolve without requiring an org prefix.

Provision a public ML attack target by bare task name — no org prefix required — to kick off a membership inference campaign.

```
$ dreadnode env provision ml-extraction-fraud-tabular
```

– Names exact alias and example task name Traditional ML attack targets now availa…

17 **Bulk actions for workspace and session management** NEW

67

Bulk workspace member addition now lets you select and add multiple members to a workspace at once from the workspace settings page; adds bulk share-with-workspace action for multiple agent sessions via the floating action bar; and adds bulk archive and unarchive for agent sessions from the Sessions tab, with context-aware actions for active, archived, or mixed selections.

— Names each bulk action and its UI location across releases

Traditional ML attack targets now availa… | Offline SDK and CLI install for air-gapp… | Web Chat open to all users

18 **workspace_mount runtime option becomes a no-op** BREAKING 65

The `workspace_mount` runtime option is now a no-op; `/home/user/workspace` is ordinary sandbox-local storage, and object-storage access must now go through the SDK instead.

— Names the exact option and required migration path

Traditional ML attack targets now availa…

19 **Twelve multi-agent AI red-teaming tasks** NEW 65

Adds 12 multi-agent AI red-teaming tasks covering access-control bypass, indirect injection, memory poisoning, MCP poisoning, reasoning hijack, supply-chain, data exfiltration, DevOps RCE, and sector-specific meshes to the task catalog under the `airt-generative-ai` set.

— Names task categories and catalog set but no task IDs

Offline SDK and CLI install for air-gapp…

20 **Pagination and search in chat session list** IMPROVED 62

Adds pagination and full-text search by title, model, agent, and label to the chat session list, removing the previous 100-session cap.

— Names searchable fields and removed limit but no exact UI path

Web Chat open to all users

THINNER COVERAGE BELOW

21 **Multi-step tool attack sandbox task** NEW 59

Adds a multi-step tool attack sandbox task featuring an over-permissioned agent with file, database, email, and HTTP tools where success requires chaining a sensitive data source to an external exfiltration sink.

— Names the four tool types but no identifier to run it

Offline SDK and CLI install for air-gapp…

22 **Offline SDK/CLI install for air-gapped deployments** NEW 57

Serves the SDK and CLI as self-contained offline bundles from self-hosted deployments, enabling install without reaching PyPI or any external host, and serves documentation at `/docs` inside every deployment for air-gapped and on-prem operators.

– Names the /docs path but no install command shown

Offline SDK and CLI install for air-gapp…

23 **Signup IP allow-list mode** NEW 57

Adds signup IP allow-list mode letting admins restrict new account creation to explicitly approved IPv4/IPv6 CIDR ranges, with deny rules taking precedence.

– Describes precedence rule but no exact config key

Offline SDK and CLI install for air-gapp…

24 **IP rotation tool in web-security capability** NEW 57

Adds IP rotation tool to the web-security capability, deploying Cloudflare Worker proxies on demand for round-robin egress through rotating IPs during engagements.

– Describes mechanism but no invocation shown Web Chat open to all users

25 **LSB steganography support for PNG images** NEW 57

Adds LSB steganography support for PNG images to the web-security capability, enabling payload-smuggling tests and upload pipeline inspection via the built-in Python tool.

– Names format and use case but no example invocation Web Chat open to all users

26 **Failed capability preflight checks surfaced as warnings** IMPROVED 57

Surfaces failed capability preflight checks (e.g. missing `dnsx`, `katana`) as explicit warnings in the agent system prompt and operator logs instead of silently proceeding.

– Names example tools and surfaces but no config to enable Web Chat open to all users

27 **Agentic CI/CD secret-exfiltration task** NEW 57

Adds an agentic CI/CD secret-exfiltration multiagent task simulating hidden instructions in untrusted repo content that cause a CI assistant to leak its deploy secret.

– Describes scenario but no task identifier or run command

Offline SDK and CLI install for air-gapp…

28 **Account Settings additions** NEW 56

Adds a Release Notes section in Account Settings listing the ten most recent changelog entries with links to full docs, on both SaaS and self-hosted installs, and adds a direct link to the system status page in the Support tab of Account Settings on SaaS deployments.

– Names exact UI locations but no deeper mechanism

Traditional ML attack targets now availa…

29 **Lifetime credit cap per member** NEW 53

Adds organization-owner-configurable lifetime credit cap per non-owner member, visible to capped members under Settings → Billing.

– Names UI location but no config surface Offline SDK and CLI install for air-gapp…

30 **Session share attribution** NEW 52

Session responses now include attribution for who shared a session with the workspace and when, covering all share paths including bulk promotion and creation-time visibility.

– Describes mechanism and scope but no field name given

Traditional ML attack targets now availa…

31 **Capability credential visibility before install** IMPROVED 42

Capability detail view and install picker now display which credentials a capability requires before installation.

– States the change but no named surface or example

Traditional ML attack targets now availa…

32 **Assessment and session list display additions** NEW 42

AIRT assessments and findings now display the workspace member who ran each assessment, and each session in the chat session list now displays a message count.

– Two thin UI display additions with no deeper mechanism

Traditional ML attack targets now availa…

33 **Guard invocation highlighting in session transcripts** NEW 39

Adds guard invocation highlighting in session transcripts, showing policy decisions inline within the conversation view.

– Thin description without mechanism or example Web Chat open to all users

34 **Six new Web Chat documentation pages** NEW 35

Adds six new documentation pages covering Web Chat: overview, quickstart, sessions, runtimes, agents and models, and slash commands.

— Lists page topics only, no deeper content `Web Chat open to all users`

35 **Web Chat open to all users** NEW 18

Web Chat is now open to all users.

— Only stated in the release title, no mechanism given `Web Chat open to all users`

└──▷ **BREAKING ON UPGRADE**

! The `workspace_mount` runtime option is now a no-op; `/home/user/workspace` is ordinary sandbox-local storage. Object-storage access must go through the SDK.

GOOD PICK? 👍 👎 GOOD REASON? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · This Week's Highlights · September 18, 2026
The full firehose — every feature release, every day — is in the newsletter.

▷ Subscribe