

## White Paper

# How Corelight Smart PCAP gives defenders 100% visibility

## Introduction

When security investigations require packets, defenders have traditionally turned to full packet capture. This approach, however, often leaves analysts with only a few hours or days worth of traffic to analyze due to prohibitive storage costs. With average attacker dwell times measured in months not minutes, this limited lookback window kneecaps an analyst's ability to go back in time and understand what happened. Moreover, full packet capture does not integrate well with modern SIEM workflows, forcing analysts to "chair swivel" from their SIEM into another pane of glass to locate and retrieve packets.

Corelight Smart PCAP for the [AP 3000 Sensor](#) delivers a superior *and* more cost-effective solution for security teams, offering up 50% cost savings and 10x longer retention vs. full packet capture, with 1-click SIEM packet retrieval for streamlined investigations. How? Through Corelight's Zeek-based protocol analyzers that give defenders comprehensive, yet compact [network log evidence](#) and the ability to easily configure precise packet captures. With Corelight logs and captured packets, defenders can achieve 100% visibility and investigate network activity that occurred months, even years, in the past.

## Capturing the packets that count

What makes Corelight Smart PCAP so smart? First, it does not waste energy capturing encrypted or file-based traffic since Corelight can already extract files and generate rich, actionable visibility around encrypted traffic without decryption. How? By parsing and logging the observable characteristics of encrypted protocols (e.g. SSH, RDP and SSL) and enriching these logs with [powerful encrypted insights](#) that reveals inferred behaviors such as large file transfers over SSH or RDP brute forcing activity.

Thus, with Corelight Smart PCAP analysts can dramatically extend their packet lookback window vs. full PCAP by targeting just the 10-20% of their traffic that contains unencrypted, non file-based packets. This

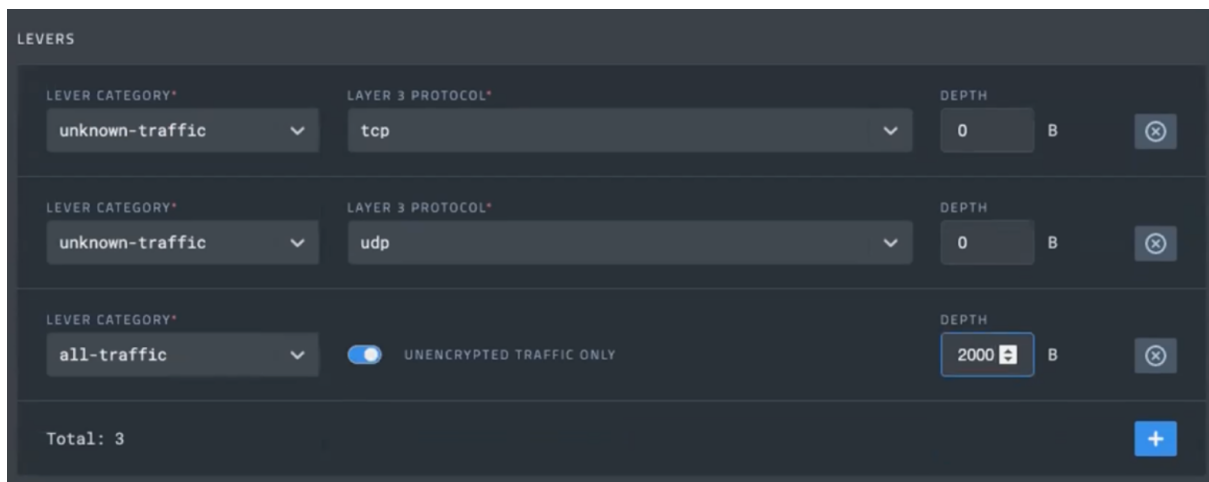
solution is also smart in that it tracks traffic across port and protocol and allows analysts to quickly build robust packet capture rules using capture levers tied to protocols, anomalous activity, alerts, and more.

Figure 1: Packet capture levers supported by Corelight Smart PCAP:

- all
- all-unencrypted
- dce-rpc
- dhcp
- dnp3
- dnp3-tcp
- dnp3-udp
- dns
- dtls
- encrypted-rdp
- filetransfer
- ftp
- ftp-data
- gtpv1
- http
- imap
- irc
- modbus
- mqtt
- mysql
- notice
- ntlm
- ntp
- protocol-violation
- radius
- rdp
- rfb
- smb
- smtp
- snmp
- socks
- syslog
- teredo
- sip
- ssl
- unknown-dns-reply
- unknown-tcp
- unknown-udp
- weird

Corelight recommends a baseline capture rule for Smart PCAP (see Figure 2 below) that combines the unknown-tcp, unknown-udp, and all-unencrypted capture levers and configures the capture byte depth for the latter (all-unencrypted traffic) to capture only the first 2,000 bytes of those connections.

Figure 2: Corelight Smart PCAP UI showing lever configurations for a new capture rule



This specific Smart PCAP rule depicted above takes just a minute to configure and gives organizations 100% network coverage by capturing packets for all connections not already parsed and logged by

Corelight, along with the first 2,000 bytes of all unencrypted traffic to supplement Corelight logs. This means analysts will have a source of network evidence for every connection that crosses the wire, whether that's in the form of a Corelight log, captured packets, or both!

### 1-Click SIEM Retrieval Drives Efficient Investigations

To support incident response and threat hunting organizations can stream Corelight's logs to their SIEM of choice. Smart PCAP integrates seamlessly into this workflow by appending a URL for the captured packets to Corelight's conn.log (See *URL highlighted in Figure 3 below*), giving analysts the ability to 1-click retrieve and load the packets in Wireshark for further analysis.

Figure 3: A Corelight conn.log viewed in Splunk with its 1-click packet retrieval URL highlighted

```
4/23/21 { [-]
5:52:07.205 PM
  _path: conn
  _system_name: smartpcap-lab
  _write_ts: 2021-04-23T17:52:07.205380Z
  community_id: 1:zxNXAE/Cme5fQhh6sJLs7GItc08=
  conn_state: RSTR
  duration: 0.0182631015775879
  history: ShAddFar
  id.orig_h: 192.168.10.50
  id.orig_p: 46785
  id.resp_h: 192.168.10.31
  id.resp_h_name.src: NTLM_AUTH
  id.resp_h_name.vals: [ [+]]
  id.resp_p: 445
  local_orig: true
  local_resp: true
  missed_bytes: 0
  orig_bytes: 8471
  orig_ip_bytes: 10455
  orig_l2_addr: 08:00:27:a1:b6:e6
  orig_pkts: 38
  proto: tcp
  resp_bytes: 2812
  resp_ip_bytes: 4628
  resp_l2_addr: 08:00:27:7f:b5:8b
  resp_pkts: 35
  service: ntlm,dce_rpc,gssapi,smb
  spcap.rule: 1
  spcap.trigger: notice
  spcap.url: https://192.168.5.1/spcap/v1/?uid=CUIPR04C10N2QVBZR9
  ts: 2021-04-23T17:52:07.187078Z
  uid: CUIPR04C10N2QVBZR9
}
Show as raw text
host = smartpcap-lab | source = smartpcap-lab | sourcetype = corelight_conn
```

Corelight's SIEM workflow integration can save analysts considerable time that would otherwise be spent in another UI locating and pulling the packets needed for an investigation. With Smart PCAP, analysts can pivot from an alert, to a connection log, to captured packets right from their SIEM in less than a minute.

## Up to 10x Longer Retention with Flexible Storage Options

Corelight Smart PCAP stores packets on external Dell PowerVault storage arrays, with a range of supported configurations (see tables below), giving security teams flexibility and offering considerable cost savings (up to 50%) compared to full PCAP. With Corelight Smart PCAP and max storage, analysts gain weeks to months of packet look back capability and months to years worth of logs in their SIEM.

*Table 1: Corelight Smart PCAP storage configuration for 12TB drives*

	Config 1	Config 2	Config 3
Dell Model	PowerVault ME4012 (iSCSI)		
# of drives/unit	12 x 12TB		
Expansion units (ME412)	0	1	3
Storage Capacity	120TB	240TB	480TB
Rack Space	2RU	4RU	8RU
Estimated Retention (10% of 10G)	11 days	22 days	44 days
Estimated Retention (10% of 15G)	7 days	14 days	29 days

*Table 2: Corelight Smart PCAP storage configuration for 8 TB drives*

	Config 4	Config 5	Config 6
Dell Model	PowerVault ME4012 (iSCSI)		
# of drives/unit	12 x 8TB		
Expansion units (ME412)	0	1	3
Storage Capacity	80TB	160TB	320TB
Rack Space	2RU	4RU	8RU
Estimated retention (10% of 10G)	7 days	14 days	29 days
Estimated retention (10% of 15G)	4 days	9 days	19 days

## Conclusion

Elite defenders report that they can resolve the vast majority of their investigations with just Corelight's logs, but some investigations will invariably require packet-level visibility to resolve. The challenge here is that legacy PCAP solutions were designed primarily around the needs of IT teams where network problems are usually identified in real-time (e.g. DNS requests failing) and their short packet lookback windows (hours to days worth of visibility) satisfy most IT use cases.

Security teams are built differently and need to be able to investigate network events in real time as well as events that happened months in the past for deep investigations. With Smart PCAP, Corelight has designed an elegant and purpose-built packet capture solution for security teams that can extend their packet lookback window up to 10x with 50% cost-savings vs. full packet capture solutions. Moreover, Corelight's solution interlinks the captured packets with Corelight's alerts and log evidence to accelerate investigations, with embedded PCAP URLs in Corelight's conn.log that give investigators a 1-click packet retrieval option during an investigation.



Defenders have always sought the high ground in order to see farther and turn back attacks. Corelight delivers a commanding view of your network so you can outsmart and outlast adversaries. We capture, interpret, and connect the data that means everything to defenders.

**info@corelight.com | 888-547-9497**