TABLE OF CONTENTS

SONICWALL®

HOW TO USE THE SALES PLAYBOOK

1. This is a document to help you better understand SonicWall Capture Client solutions and how to discuss security with partners/customers

2. Use this as a reference tool not an external presentation:

   - Other tools, resources, and external-facing assets are linked within this documentation

   - Please keep in mind most slides are marked as "FOR INTERNAL / PARTNERS ONLY", so feel free to use non-marked slides for end-customer presentations

3. Ensure you have the most updated/refreshed version of the Capture Client Sales Playbook by downloading from CC Resource Folder (SFDC)

SONIC**WALL**®

CAPTURE CLIENT POSITIONING AND VALUE PROP

A **unified and advanced** endpoint security solution… → …that stops breaches faster than humanly possible. → Download Datasheet

Advanced Endpoint Protection

+

Proactive Endpoint Detection & Response

+

Threat Hunting with Deep Visibility

w/ optional

SonicWall Ecosystem Integrations

1 Continuous behavioral monitoring to protect against both file-based and fileless threats
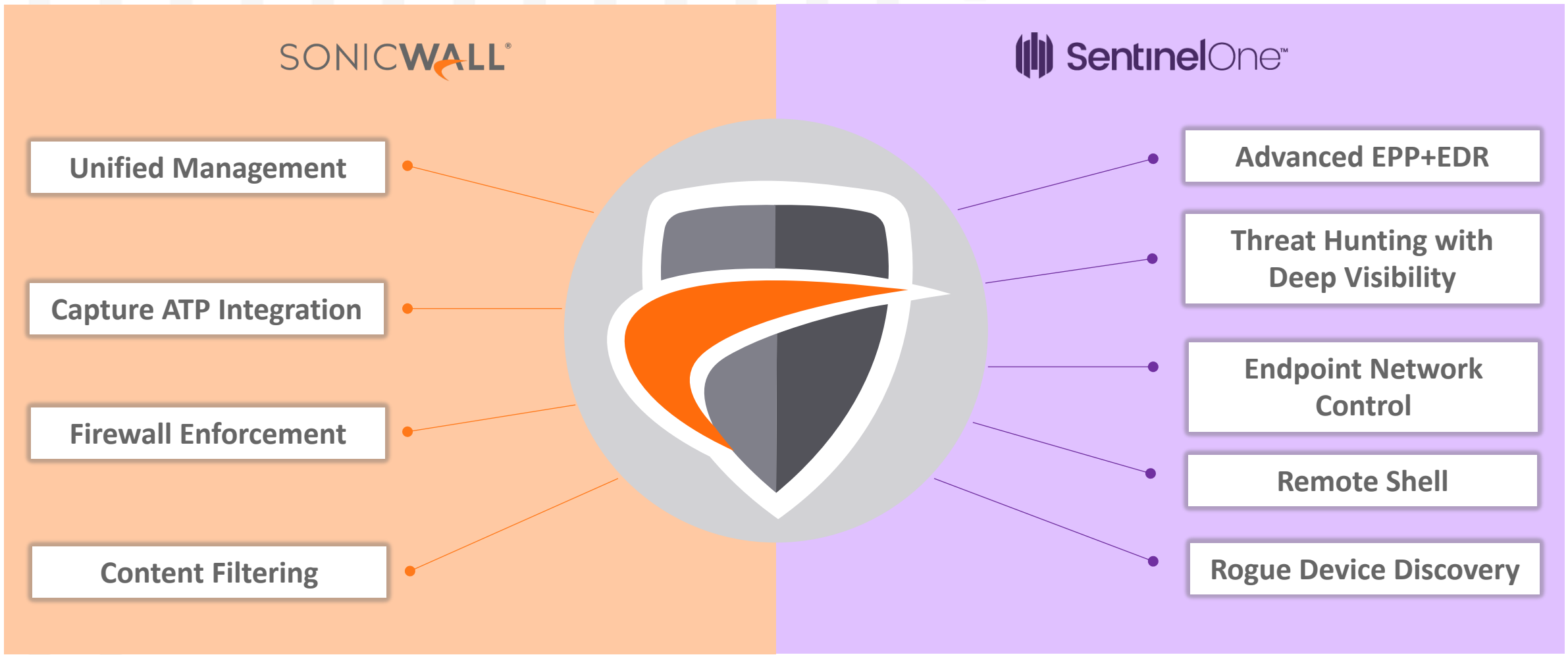
2 Simple one-click remediation that restores endpoints back to previous known good state

3 Automated Threat Hunting with easy to create custom rules and alerts

4 Enforcement of protection policies / restrictions and visibility into encrypted traffic (w deep packet inspection)

SONIC**WALL**®

THE "ANATOMY" OF CAPTURE CLIENT CAPABILITIES

SONICWALL®

SentinelOne™

- Unified Management
- Capture ATP Integration
- Firewall Enforcement
- Content Filtering

- Advanced EPP+EDR
- Threat Hunting with Deep Visibility
- Endpoint Network Control
- Remote Shell
- Rogue Device Discovery

Capture Client combines SonicWall Security Platform with SentinelOne so that endpoints are secured with defense-in-depth and seamless multi-layered security postures.

5

BEST-IN-CLASS PROTECTION & DETECTION
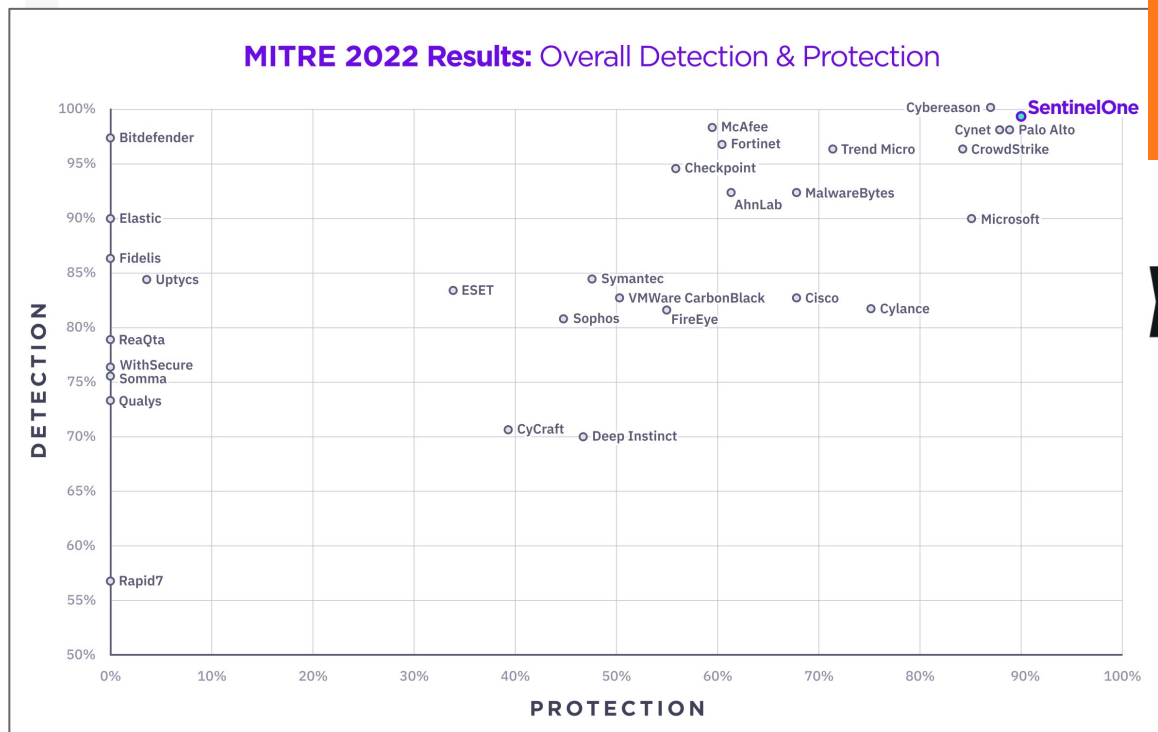
SentinelOne

100% Protection
9 of 9 MITRE ATT&CK Tests

100% Real-Time
0 Delays

100% Detection
19 of 19 Attack Steps

99% Highest Analytic Coverage
108 of 109 Detections

99% Visibility
108 of 109 Attack Sub-Steps

The MITRE ATT&CK Evaluation is important to partners and customers because it analyzes the effectiveness of EDR solutions based on:

- Ability to Protect and Detect
- Detection Delays and Visibility
- Analytic Coverage vs Telemetry

MITRE 2022 Results: Overall Detection & Protection

(Scatter plot — X axis: PROTECTION (0% to 100%), Y axis: DETECTION (50% to 100%). Data points:)

- Cybereason
- SentinelOne
- McAfee
- Fortinet
- Cynet
- Palo Alto
- Trend Micro
- CrowdStrike
- Bitdefender
- Checkpoint
- MalwareBytes
- AhnLab
- Elastic
- Microsoft
- Fidelis
- Uptycs
- Symantec
- ESET
- VMWare CarbonBlack
- Cisco
- Sophos
- FireEye
- Cylance
- ReaQta
- WithSecure
- Somma
- Qualys
- CyCraft
- Deep Instinct
- Rapid7

Capture Client includes SentinelOne's Industry-winning technology!

MITRE ENGENUITY ATT&CK® EVALUATIONS
Enterprise
WIZARD SPIDER & SANDWORM
2022

Learn More about the MITRE ATT&CK Framework and Evaluations:

- SonicWall MITRE ATT&CK Framework Blog Part 1
- SonicWall MITRE ATT&CK Framework Blog Part 2
- Intro to MITRE ATT&CK video
- MITRE ATT&CK Technique Matrix
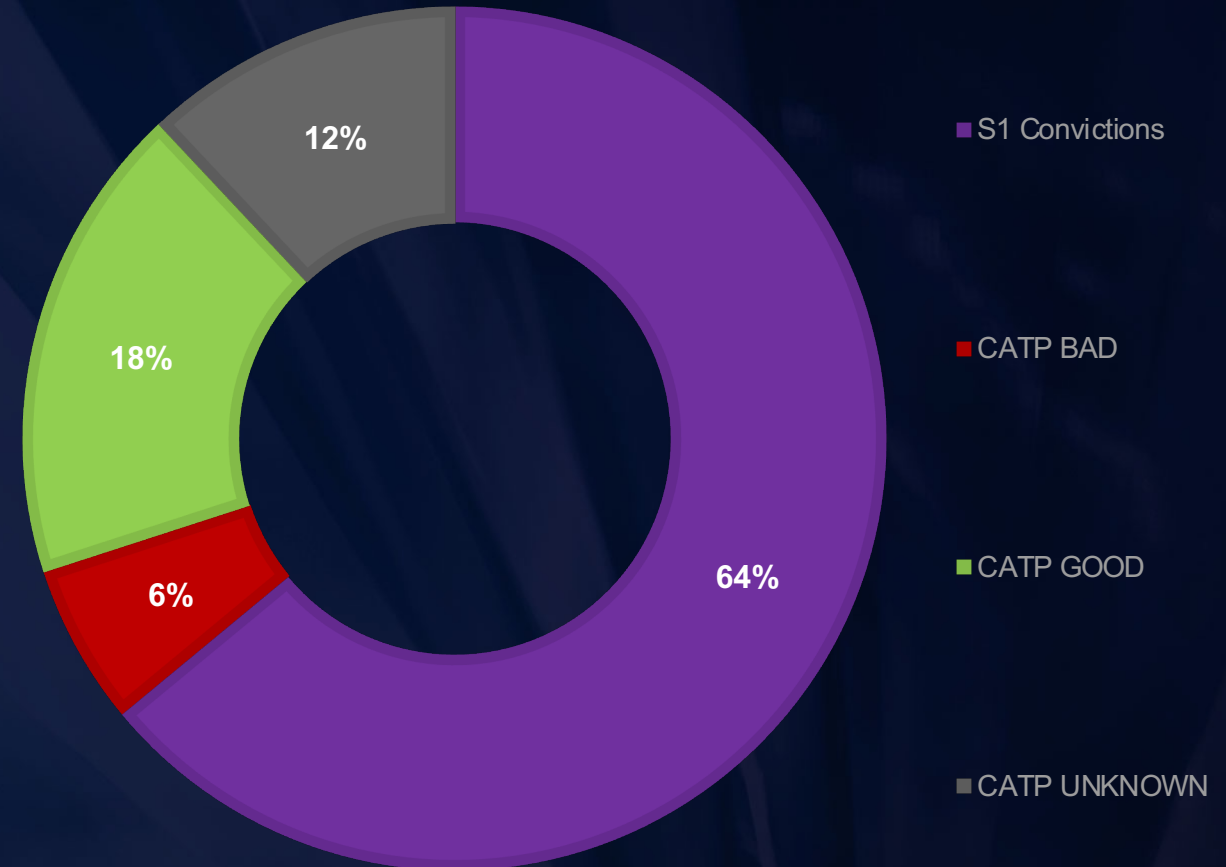
Capture ATP

+ **SentinelOne**™

Capture ATP reduces false positive alerts by 18% and identifies true threats.

The results? **Less false alerts and accurate threat classification for best mitigation actions.**

COMPOSITE RESULTS: Dec 2021 – May 2022

- 73.0K # of total threats*
- 32.9K # of suspicious threats**
- 26.2K # of total threats processed by C-ATP

*detected by S1 across our customer base (grouped by hash)
**detected by S1's On-Write Static AI – Suspicious engine

% by C-ATP Threat Classification

- ■ S1 Convictions
- ■ CATP BAD
- ■ CATP GOOD
- ■ CATP UNKNOWN

64%
6%
18%
12%

SONIC**WALL**®

'PERFECT' THREAT DEFENSE
5 QUARTERS IN A ROW

Capture ATP
+ RTDMI™

SonicWall Capture ATP with patented Real-Time Deep Memory Inspection™ faced 160 total days of rigorous testing by ICSA Labs during five straight certifications in 2021 and 2022.
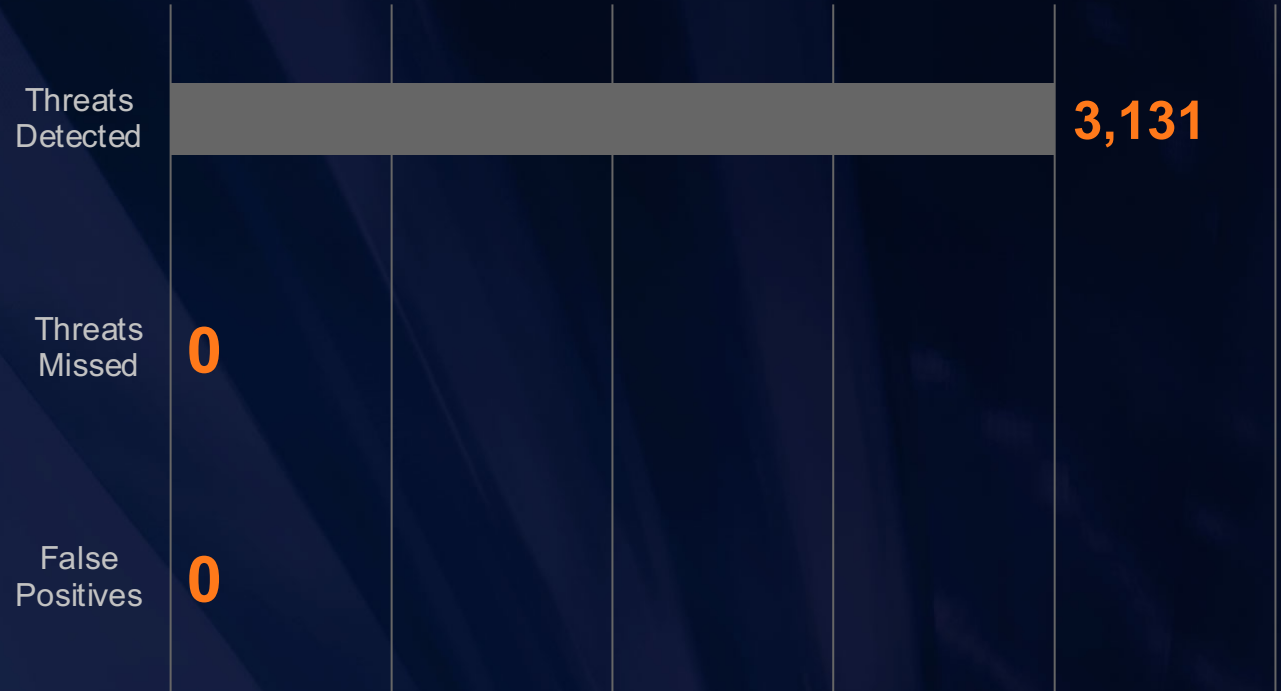
The results? **Five 'perfect' scores in a row.**

Threats Detected — 3,131

Threats Missed — 0

False Positives — 0

Capture ATP detected 3,131 of 3,131 new and unknown malicious samples during 160 total days of ICSA laboratory testing in 2021 and 2022. SonicWall is the only vendor in ICSA Labs ATD certification history to receive five consecutive perfect scores.

COMPOSITE RESULTS

- 160 Days of Testing
- 6,719 Total Tests
- 3,131 New & Little-Known Samples
- 3,588 Innocuous Applications

2021-22 OVERVIEW

- *Only* Vendor Ever with Five Straight 'Perfect' Scores
- 100% Detection of Unknown Threats
- Zero False Positives
- Nine Consecutive ICSA Labs ATD Certifications

ICSAlabs
CERTIFIED   ADVANCED THREAT DEFENSE

SONICWALL®

COMPETITIVE LANDSCAPE

Link to Battlecards (Internal ONLY)

Link to Battlecards (Partner site)

✓ Available   ✗ Unavailable   ◐ Partially Available or Not Included with EPP

Feature	Capture Client (S1)	Crowdstrike	Microsoft	Sophos	Kaspersky	Carbon Black	Symantec
Advanced Endpoint Protection + EDR	✓	◐	✓	◐	◐	◐	✗
One-Click Rollback Response	✓	✗	✗	✗	✓	✗	✗
Device Control	✓	◐	✓	✓	◐	◐	✓
Application Vulnerability Intelligence	✓	✓	◐	✓	✓	✓	◐
Endpoint Network Control	✓	◐	◐	✓	✓	✗	✓
Threat Hunting with Deep Visibility	✓	✓	◐	◐	✗	✓	◐
Rogues	✓	✓	✓	✗	✗	✗	✓
Remote Shell	✓	✓	✓	✗	✗	✓	✗
Capture Advanced Threat Protection (ATP)	✓	✓	✓	✓	✓	✗	✓
Content Filtering	✓	✗	✗	✓	✓	✗	✗
SonicWall Firewall Integration – DPI-SSL, Visibility & Telemetry	✓	✗	✗	◐	✗	✗	✗
Cloud Management, Reporting & Analytics (Unified Management)	✓	◐	◐	✓	◐	◐	◐

FEATURES AND PLANS

Feature	Definition	CC Advanced	CC Premier
Cloud Management, Reporting & Analytics (Unified Management)	Access Capture Client reporting and management within the Capture Security Center (CSC) single pane of glass management console.	✓	✓
SonicWall Firewall Integration – DPI-SSL, Visibility & Telemetry	Enable enforcement of deep packet inspection of encrypted traffic (DPI-SSL) on endpoints and easily deploy trusted certifications to each endpoint.	✓	✓
Content Filtering	Allows organizations to block malicious sites, as well as increase user productivity by throttling bandwidth or restricting access to objectionable or unproductive web content.	✓	✓
Capture Advanced Threat Protection (ATP)	Discovering, quarantining, and removing undercover threats before the execute saves time for end users and administrators.	✓	✓
Advanced Endpoint Protection + EDR	Full featured enterprise-grade EPP+EDR – including NGAV and behavioral AI to stop known and unknown threats. Built on the SentinelOne anti-malware engine, Capture Client requires no signatures, daily/weekly updates or cloud lookups/databases for detection.	✓	✓
One-Click Rollback Response	Resolve threats with 1-Click and without scripting on one, several, or all devices across the entire estate.	✓	✓
Device Control	Prevent infected devices like USBs from connecting to endpoints, device control can lock out unknown devices.	✓	✓
Application Vulnerability Intelligence	Administrators can catalog every application on each protected endpoint with information on known vulnerabilities within them.	✓	✓
Threat Hunting with Deep Visibility	Deep Visibility allows the security admins to easily find related IOCs, using an intuitive UI and queries can be customized as needed to allow for quick, repeatable Threat Hunting process.	✗	✓
Endpoint Network Control	Allows for transfer of firewall rules into the endpoint, therefore ensuring optimal security, regardless of user's location. If an endpoint is discovered to be infected, they can be quarantined, until an admin can remedy the issue.	✗	✓
Rogues[1]	Helps identify dark and hidden endpoints to reduce the network attack surface	✗	✓
Remote Shell[2]	This allows the admins to access endpoints without the need for a third-party application and troubleshoot configuration or security issues. It allows them to gather forensics evidence after an attack and even clean up the endpoint, if necessary.	✗	✓

1 Rogues is only available for users with Account scope
2 Remote shell will be made available on demand in a new user account (with 2FA enabled) directly on the S1 console

CC PREMIER VALUE MATRIX

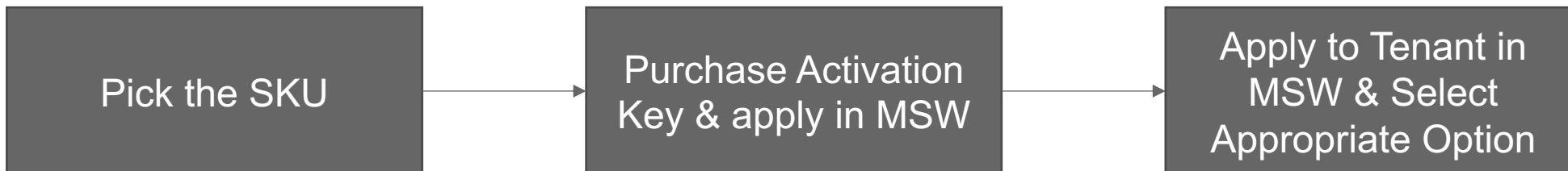| Feature	Value Add	Use-case Examples
Threat Hunting with Deep Visibility	• Easily find "related" IOCs using Storyline-based hunting • Deeper visibility of events related to files, processes, scripts and network connections • Powerful attack visualization capabilities • Out of the box queries to get you started • Custom rules and alerts to automate hunts	• Deletion of VSS shadow copy across endpoints • Identification of policy/task changes • Identification of obfuscated PowerShell scripts • Identification of threat/risk landscape
Endpoint Network Control	• Reduce the Attack Surface by controlling inbound and outbound network traffic for Windows, Mac, and Linux • Host firewall with ACL-based rules to allow/disallow traffic • Customize quarantine options and allow trusted connections	• Block traffic to malicious URLs/IPs on different ports and protocols • Quarantine infected endpoints and allow them to connect to selected web address
Rogues	• The Rogues feature identifies the unprotected endpoints and provide enterprise wise visibility • No additional software or hardware required • No network changes required	• Identify endpoints that are not protected by Capture Client
Remote Shell	• Remote forensics • Remote troubleshooting • Remote threat eradication	• List live network connections on the endpoint • List running processes, their location, installed path, signature etc • Remove malicious values from the registry • Remove malicious schedule tasks

SONICWALL®

CC Premier delivers full parity with SentinelOne Singularity Complete

SKU OPTIONS FOR PURCHASE

Bands For Advanced & Premier	Term Options
BAND 1 - 5 - 24 ENDPOINTS	1 YR or 3YR
BAND 2 - 25 - 49 ENDPOINTS	1 YR or 3YR
BAND 3 - 50 - 99 ENDPOINTS	1 YR or 3YR
BAND 4 - 100 - 249 ENDPOINTS	1 YR or 3YR
BAND 5 - 250 - 499 ENDPOINTS	1 YR or 3YR
BAND 6 - 500 - 999 ENDPOINTS	1 YR or 3YR
BAND 7 - 1000 - 4999 ENDPOINTS	1 YR or 3YR
BAND 8 - 5000 - 9999 ENDPOINTS	1 YR or 3YR
BAND 9 - 10000+ ENDPOINTS	1 YR or 3YR
MSSP PROTECT	1 YR or Monthly
MSSP POWERED	1 YR or Monthly
MSSP POWERED+	1 YR or Monthly

Competitive Displacement SKUs available ONLY for Advanced
- *2YR for 1YR*
- *3YR for 2YR*

Only for Qualified MSSPs

- All SKUs are priced Per Endpoint

- Ordering via non-MSSP SKUs
  - Minimum order - 5 Endpoints
  - Per Endpoint price varies by Band
  - SKU usage based on order quantity
    - *If customer needs 75 endpoints, use Band 3*
    - *If customer wants to increase from 75 to 77, use Band 1 (5+ Only)*
    - *If customer wants to increase from 75 to 100, use Band 2*
    - *If customer wants to increase from 75 to 175, use Band 4*

- Ordering via MSSP SKUs
  - No minimum order
  - Flat per endpoint price for any quantity
  - SKU usage based on MSSP Tier

SONIC**WALL**®

Always encourage buying 10% additional licenses up front for growth

RENEW, EXPAND, UPGRADE

Pick the SKU	→	Purchase Activation Key & apply in MSW	→	Apply to Tenant in MSW & Select Appropriate Option

To	Select SKU from	Select on activation	
Renew Only	Same Plan & Band	Renew	
Expand within Plan	Option 1: Band based on Total	Renew	Effective expiry date based on co-terming logic
	Option 2: Band based on difference	Upgrade	
Upgrade Plan	Preferred Plan & Band based on Total	No action needed (automatic upgrade)	

SONICWALL®

13

HOW DOES CO-TERMING WORK

- Effective plan is based on the new key applied

- Effective quantity is based on activation option – Renew vs Upgrade

- Effective Validity is based on new term, remaining term, effective plan & effective quantity

Calculated based on "Credits" for the effective plan

- 1 Advanced License for 1 Month = 1 Credits

- Combine credits from old key(remaining term) & new key

- Divide by effective quantity to get validity (from activation date)

- Use multipliers to prorate remaining term when changing plans

Pro-ration Multipliers for upgrade across Tiers

↓ From / To →	Basic	Advanced	Premier
Basic	1	0.7	0.5
Advanced	N/A	1	0.8
Premier	N/A	1.3	1

SONICWALL®

SonicWall uses co-terming to make sure the customer is always whole

EXAMPLE WITH BILL OF MATERIALS

1. Initial Purchase - Displacing customer's 125 licenses of Sophos Intercept X with 1 Yr of term remaining

SKU CODE	SKU DESCRIPTION	Qty
02-SSC-6769	SONICWALL CAPTURE CLIENT ADVANCED 100-249 COMPETITIVE DISPLACEMENT 3YR	125

Activation Date: 1st May 2022
Expiry Date: 30th April 2025

2. 6 Months Later – Customer has expanded to protect 70 more servers

SKU CODE	SKU DESCRIPTION	Qty
02-SSC-1522	SONICWALL CAPTURE CLIENT ADVANCED 50-99 3YR	70

Activation Date: 1st Nov 2022
Effective Plan: Advanced
Effective Quantity: 195
Prorated Expiry Date: 4th July 2025

3. 18 Months Later – Customer has had a breach and, as part of improvements, wants to upgrade to Premier

SKU CODE	SKU DESCRIPTION	Qty
02-SSC-9843	SONICWALL CAPTURE CLIENT PREMIUM 100-249 1YR	195

Activation Date: 1st May 2024
Effective Plan: Premier
Effective Quantity: 195
Prorated Expiry Date: 6th April 2026

SONICWALL®

WHO ARE YOUR CUSTOMERS

Sally IT
(Small End Customer)

Key Challenges
- Limited resources / IT budget
- Difficulty managing product licenses
- Critical vulnerabilities on endpoints without knowing scope of remediation
- Issues with current EPP
- Lack of time to deploy full security stack
- Unsure of suspicious files

CC Benefits
- Centralized cloud management for license management and reporting
- AI-powered malware/ransomware detection and roll-back
- App vulnerability scanning
- Capture ATP integration
- Content Filtering

Capture Client **Advanced** makes IT and Security as easy as possible without high cost

Lisa IT Director
(Large End Customer)

Key Challenges
- Too many endpoint security updates
- Technical concerns for DPI-SSL deployment
- Frequent attacks attempts
- Overload of false positive alerts
- Lack of visibility of attack forensics and centralized management of endpoints

CC Benefits
- Automated and continuous behavioral scanning to detect threats
- Advanced and one-click remediation capabilities
- Robust threat intelligence and deep visibility with Threat Hunting

Capture Client **Premier** levels up security teams and empowers them to confidently threat hunt
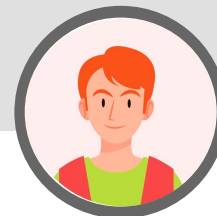
Tony Channel
(Transactional Reseller)

Key Challenges
- Taking on new vendors and solutions can be complicated and resource intensive
- Need more education and training of how to sell and market solutions
- Focus on growing business and customer demand for products/solutions

CC Benefits
- Best in Class Endpoint Security capabilities by combining SentinelOne and SonicWall
- Industry leader reputation
- Robust CC Training and Co-marketing resources for resellers
- Easy and Flexible

Bundle **Capture Client** to make your IT offering more competitive with best-in-class Endpoint Security that grows your margins

Vince CISO/CIO
(Vertical End Customer)

Key Challenges
- To secure business flow with minimal overhead or excessive budgets
- Protect all assets including Endpoints
- Maintain organizational connectivity and productivity
- Reduce TCO

CC Benefits
- Unified Management-Consolidate security to manage fewer vendors
- Beyond signature-based Protection
- Improved Threat Visibility
- Secure Remote Workforce-Employees working remotely and connecting to organizational resources

Increase protections to combat new and greater threats with **Capture Client** and reduce IT staff workload with unified management.

WHO ARE YOUR MSSPS

**Mary MSP
(Transitioning MSP)**

**Mark MSSP
(Large Partner)**

Mary MSP — Key Challenges

- Never-ending security updates
- Customer environment reports and analysis
- Unable to thoroughly remediate and restore from attack
- Too many manual tasks
- Need support developing new security services offering
- Co-Marketing needs
- Wants more training /education
- Desires more flexible payment options

Mary MSP — CC Benefits

- Rule/Policy enforcement
- Easy DPI-SSL Certificate management
- Detailed on-going reporting and analysis
- Unique rollback (self-service) capabilities
- Easy-to-understand error reporting and remediation
- MSSP Program delivers:
  - o Flexible monthly pricing
  - o Co-marketing support
  - o Security service packages for easy bundling with current IT offering

Mark MSSP — Key Challenges

- Must manage and understand different environments
- Operational cost and time lost when endpoint remediation
- Issues with current EDR
- Lack of robust incident forensic
- Targeted attacks
- Company reputation on the line
- Customer retention / Competitors
- Growing / defending market share
- Seamless and frictionless
- Lack of complete MDR capabilities

Mark MSSP — CC Benefits

- Centralized cloud-based management for multi-tenants
- Deployment of baseline policies
- Simplified one-click remediation
- Threat attack visuals and storylines for effective Threat Hunting
- MSSP Program delivers:
  - o Best in Class Endpoint Security capabilities by combining SentinelOne and SonicWall
  - o Industry leader reputation

Partner with Capture Client **Advanced** to securely and effortlessly protect customers while growing your recurring revenue

Partner with Capture Client **Premier** for intrinsic security and resiliency for your customers and your business

SON

17

CAPTURE CLIENT CAN BE DEPLOYED TO MEET YOUR CUSTOMERS / PARTNERS NEEDS

For Customers Who Self-Manage Security or Transactional Partners/Resellers (SECURITY STACK FOCUS)

Hybrid work becoming the norm and we're seeing an uptick in threats to organization's expanding attack surface. This means to fortify your security perimeter, every endpoint – inside and outside of your network walls – requires multilayer endpoint security.

SonicWall Capture Client is a light-weight unified client platform that delivers advanced best-in-class endpoint security with threat hunting. The behavior-based anti-malware, powered by SentinelOne constantly looks at changes in system behavior to stop attacks before and during execution. If malware does damage the system or data as in ransomware, easy one-click rollback makes remediation easy.

Do you have a couple more minutes so we can talk a little more about your current security needs?

For Customers Who Self-Manage Security or Transactional Partners/Resellers (BUSINESS IMPACT FOCUS)

Given hybrid work is becoming the norm, companies are plagued with increasing cyberattacks with most data breaches starting at a compromised endpoint.

SonicWall Capture Client, powered by SentinelOne, delivers advanced best-in-class endpoint security. What this means is that CC can instantaneously rollback ransomware deployment and stop malware from spreading.

With the ability to quickly detect and remediate breaches, it minimizes downtime, prevents need to payout ransomware demands, and saves your company's reputation.

Do you have some time to dive a little deeper on Capture Client's key features?

SONIC**WALL**®

CAPTURE CLIENT CAN BE DEPLOYED TO MEET YOUR MSSP NEEDS

For Transitioning MSP

Increasing ransomware, malware and other malicious attack vectors has evolved the threat landscape. And with hybrid work becoming the norm, we're seeing the attack surface expand rapidly – so with all this, many MSPs are making the transition to an MSSP.

By deploying SonicWall Capture Client, you can customize endpoint security service models and pricing seamlessly with your current MSP service bundles.

In addition to the wide range of service offering, SonicWall MSSP solutions and program provide: Simplified operations, Flexible pricing, Priority Tech Support and Go-To-Market collaboration.

Have you considered if your MSP is ready to have a competitive advantage and grow rev/margin?

For Mature MSSPs

With the proliferation of new cyber threats, it's advantageous to future-proof your customer's IT environment – ransomware attacks happen to any size organization.

By leveraging best-in-class cybersecurity tools and a modern security approach, endpoints are secured so that data is protected. Additionally, SonicWall Capture Client enables you to drive high efficacy and efficiency for your MSSP business by:

- *Shortening downtime and increasing continuity for customers*

- *Automating threat detection and roll-back capabilities*

- *Proactively finding hidden threats with robust threat hunting and intelligence reporting*

Let me send you some additional details of how we can partner with your MSSP to drive higher revenue and secure your customers.

SONICWALL®

STARTING WITH DISCOVERY

	LISTEN FOR KEYWORDS	FOLLOW UP TOPIC
Understanding endpoint security capabilities • How are you defusing threats on endpoints before and during attacks? • What are some endpoint visibility and/or management challenges you face? • Has business continuity and worker productivity been impacted by past breaches? • With the cybersecurity talent shortage, how are you/team dealing with overwhelming false positive alerts and analyst fatigue?	"Legacy" Antivirus Remote or Off-network Ransomware attacks MDR	S1's Signature-less EPP+EDR Cloud-managed ***Rollback & Autonomous Response*** ***MITRE ATT&CK results*** Syslog & API Integrations
Exploring areas of integrated network protection • How do you control threats spreading via unmanaged endpoints? • Do you have visibility of users behind firewalls (as opposed to IP addresses)? • How do you manage network and endpoint security across 2 consoles?	Contractor, BYOD Layers of Defense Single Pane of Glass	Enforcement & SSO Content Filtering ***Capture ATP Integration*** Capture Security Center
Discussing approaches to attacks and vulnerabilities • How did you respond to the Log4j incident? Were you able to identify any exploits in your environment? • When you have a ransomware attack, how do you identify the source and remediate/recover from the incidents? • What steps does your team take to identify and respond to threats or do you work with a SOC/MDR service provider?	IOC / SIEM / SOAR Alert fatigue Cyber Insurance Risk and Threat Intelligence MDR / XDR services	Threat Hunting with Deep Visibility ***Demo / PoC of Threat Hunting*** Syslog & API Integrations

WHEN "NO" REALLY MEANS "TELL ME MORE"

🔓	No thanks. My traditional / signature-based / legacy antivirus is good enough.	➡️	Well, most of today's common attacks can be tweaked or even zero-day / 'Never-Before-Seen' malware that can get missed by static, signature-based antivirus. Capture Client, powered by SentinelOne, uses machine-learning to ensure malware is detected by changes in endpoint behavior and not just rely on a list of viruses to check for.
$$	Capture Client sounds perfect, but I just don't have the budget for it right now.	➡️	We understand that organizations can be challenged with budget constraints, that's why we offer flexible buying options that work for your needs. Plus, a breach could end up costing you exponentially more! So, lets start you with a free trial of CC and discuss how we can work with your budget to get you and your customers data secured.
≠	I'm going to pass – I was told my current NGAV (*from "xyz"*) does the same thing as Capture Client.	➡️	(*if the customer/partner identifies the NGAV solution they are currently using, use available battlecards to provide key advantages of CC vs. competitor*) Each NGAV can be slightly different in how the solution is deployed and managed, it might be worth it to look at how Capture Client stacks up.
+	Capture Client Premier offers some advanced features but we neither have skills nor bandwidth to make use of those features.	➡️	We have partnerships with recognized MSSP partners in each region who can provide managed services.
?	We currently use SonicWall products, but the MDR partner we are considering only uses "xyz" solution for endpoint security.	➡️	SentinelOne delivers the industry-best autonomous protection technology and is integrated with most MDR providers. We'll support this integration so that you can use the best protection and still leverage the services of your provider
📋	Our MSSP is looking for specific security capabilities and integrations with our current technology stack, I'm not sure if Capture Client would align to what we need.	➡️	Capture Client feature/capability enhancements have been consistently delivered every quarter. We are fully on par with Best-in-Class SentinelOne Singularity Complete offering plus we are expanding our integration ecosystem to seamlessly fit with MSSP platforms.

SONIC**WALL**®

OTHER TOOLS AND RESOURCES

SONIC**WALL**®

AVAILABLE RESOURCES AND TOOLS

Tool / Resource Linked	Internal Use	Partner Use	End Customer Asset
Capture Client Customer presentation [SFDC] MSSP Program Customer presentation [SFDC]	X	X	X
Capture Client Sales Aid [SFDC] [Partner Brand Folder]	X	X	
Video: Capture Client Overview	X	X	X
Blog: Capture Client Recent Threat Hunting	X	X	X
Executive Brief: What Administrators Need to Look for …	X	X	X
Executive Brief: How to Set Up Ransomware Protection …	X	X	X
Capture Client Basic EOL Details • End of Sale of Capture Client Basic - Frequently Asked Questions • Difference Between Capture Client Advanced and Basic Licenses	X	X	X
SonicWall University: Capture Client Training [Internal] [Partner] Sales Sprint – Capture Client with Sarah Choi & Shashank Jain [Internal]	X	X	
Individual Sales Plays: FY23 Kaspersky Sales Play [SFDC]	X		
Technical Marketing Video (Feature Clips) – *COMING SOON*	X	X	X
Threat Hunting SQL Cheatsheet (Powered by SentinelOne) [SFDC]	X	X	X
Partner Endpoint Security Marketing Campaign Package [Partner Brand Folder]	X	X	X

SONICWALL®

SONICWALL®

www.sonicwall.com