Time to Play Offense with Your Data Protection Strategy

Ed Koorsgard
Sophos
Senior MSP
Sales Engineer

Chris Rudnik
Sophos
Channel Sales

Randy O'Donnell
Prodatix
CTO

Matt Bullock
Prodatix
CEO

SOPHOS + prodatix DATA MANAGEMENT

February 12, 2025

Ed Koorsgard

Sophos
Senior MSP Sales Engineer

Total data security with Sophos MDR and Prodatix

sophos.com

Agenda

- Data Defense versus Offense
- Why Complete Data Lifecycle Protection?
- Sophos as an Offensive strategy
- How Managed Detection and Response will save your company
- Demo of Sophos MDR
- Wrap-up

Defensive Data Protection

- Immutable data backup
- On-premises and Cloud backup
- Data replication (DRaaS)

Offensive Data Protection

- Stop the malware/ransomware before it gets into your data

- Scanning backups for “sleeper” ransomware

- Follow the flow of the data

Complete Data Lifecycle Protection

1. From the time it enters your business until it’s deleted or archived
2. How many potential points of failure exist in your data lifecycle?
3. How do you “close the holes” in your data security and protection environment?

People

4 Million

The global shortage of cybersecurity practitioners currently needed

(ISC)^2, 2023 Cybersecurity Workforce Study

Process

59%

Of organizations were hit by ransomware in the last year

Sophos, 2024 State of Ransomware Report

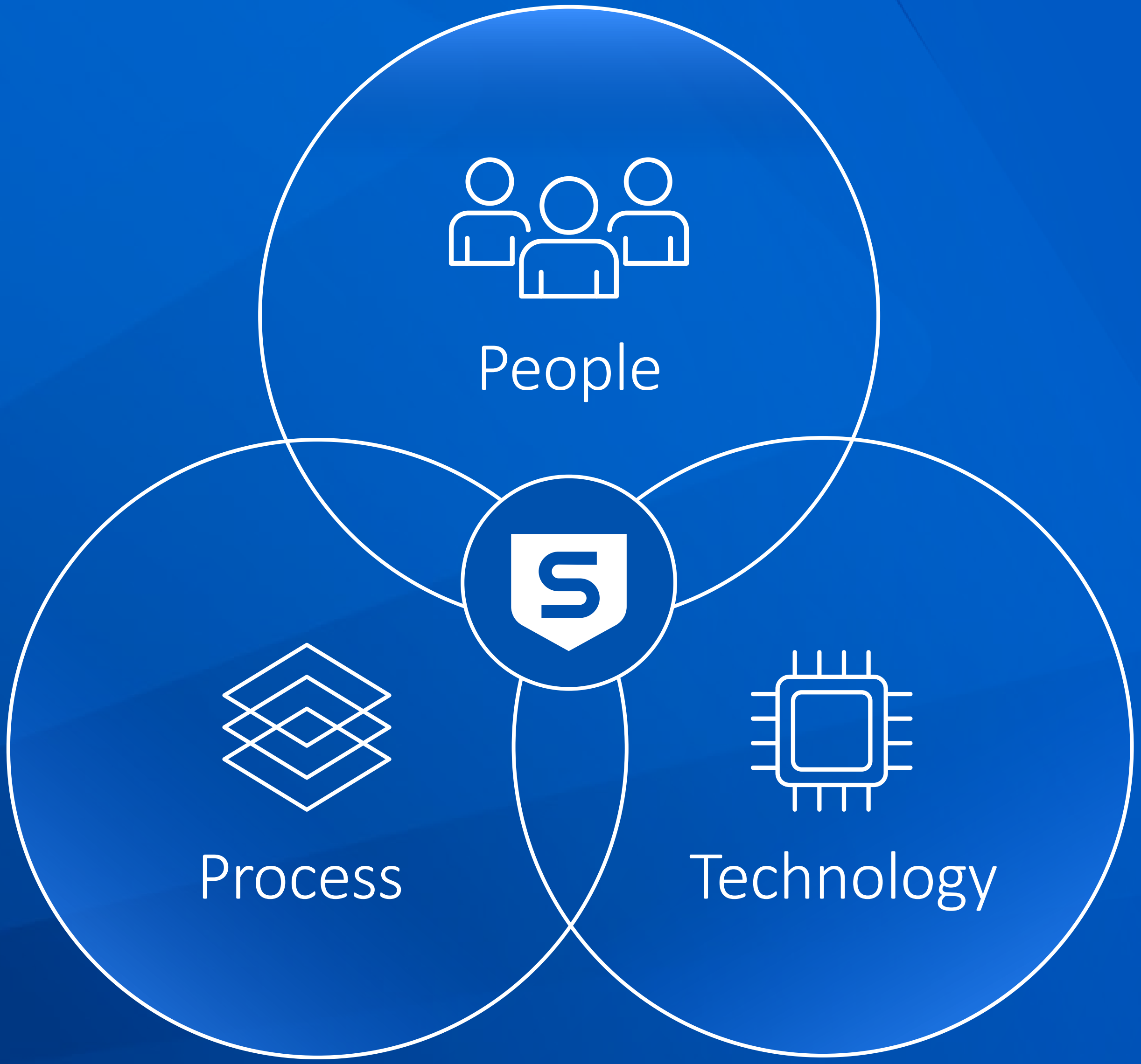
Technology

95%

Of organizations find it challenging to investigate and respond to security alerts generated by their tools

Source: The state of Cybersecurity 2023, Sophos

Small- and midsized businesses lack the resources to stop today's cyber attacks



Sophos Detection and Response Solutions

MDR

Defend against sophisticated novel threats and advanced active adversaries
Superior outcomes delivered as a service 24/7 by highly-skilled experts

XDR

Tools for practitioners: Investigate and respond to complex multi-stage threats across all key attack surfaces that technology alone can’t block

EDR

Tools for practitioners: Investigate and respond to complex threats on endpoints and servers that technology alone can’t block

Ep

Strong protection is critical. Stopping more threats upfront reduces the investigation and response workload for IT and security teams

Managed Detection and Response (MDR)

A fully-managed, 24/7 service delivered by experts who specialize in detecting and responding to cyberattacks that technology solutions alone cannot prevent

MDR Sophos MDR

Threat Hunting
Proactive threat hunts performed by highly-trained analysts uncover and rapidly eliminate more threats than security products can detect on their own

Threat Detection
Enabled by extended detection and response (XDR) capabilities that detect known threats and potentially malicious behaviours wherever your data reside

Incident Response
Our analysts respond to threats in minutes whether you need full-scale incident response or assistance making more accurate decisions

26,000+ MDR Customers

99.98% of threats automatically blocked

Average Sophos MDR Threat Response Times

Time to Detect	Less than 1 Minute
Time to Investigate	Less than 25 Minutes
Time to Respond	Less than 12 Minutes

This is a lot to manage.

MULTISTAGE ATTACKS

Attacks that end in a different place than they started

LIVING OFF THE LAND ATTACKS

Attacks that blend in by using legitimate tools in malicious ways

UNKNOWN VULNERABILITIES

Attacks that leverage a weakness, flaw, or error in software

CREDENTIAL ABUSE

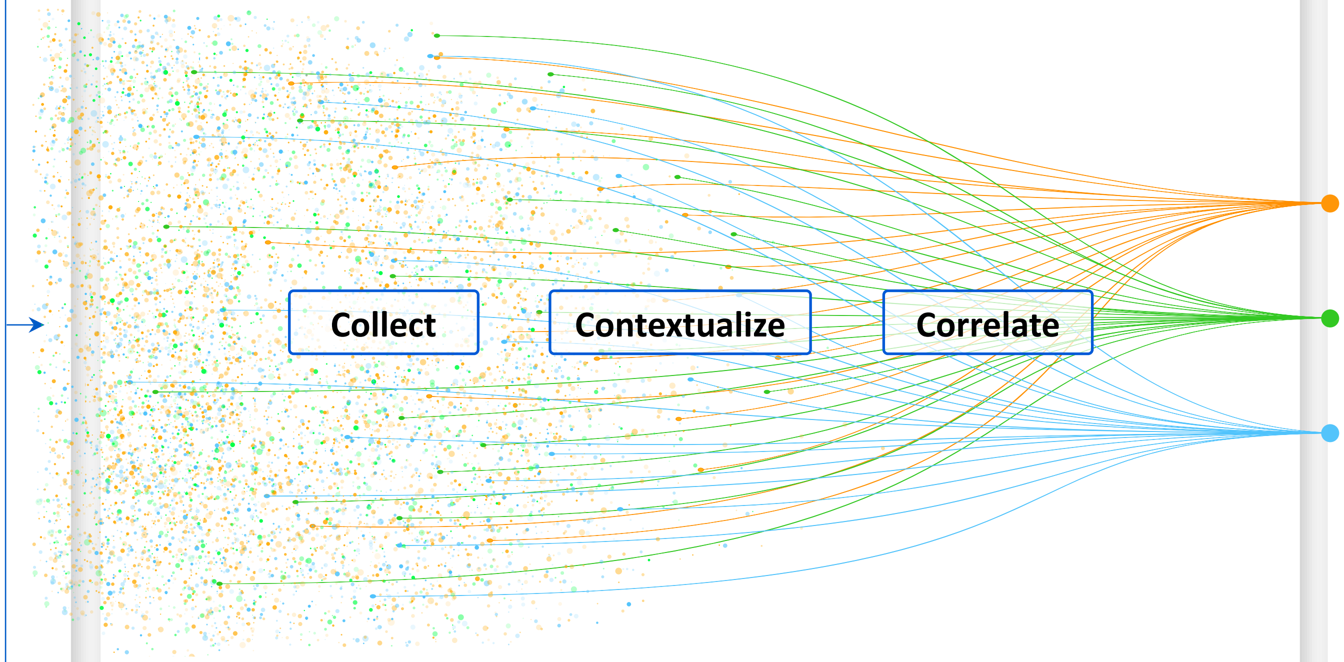
Attacks that start with an adversary logging in instead of breaking in

Event Sources

- Endpoint
- Firewall
- Email
- Cloud
- NDR
- Identity
- Network
- Backup

Threat Analysis and Correlation

Sophos XDR Data Lake



Collect

Contextualize

Correlate

Threat Intelligence + **Automated Response** + **Advanced Threat Analytics**

Sophos MDR Complete

24/7 Managed Detection and Response Services

Full-Scale Incident Response

Root Cause Analysis and Remediation

$1M Breach Protection Warranty

Proactive Threat Hunting

Expert-Led Threat Investigation

Example Sophos MDR Response Actions

Sophos MDR Essentials – Threat Response

Example Response Actions:

- Isolate host(s) utilizing Sophos Central
- Apply host-based firewall IP blocks
- Terminate processes
- Force log off user sessions
- Disable user accounts
- Remove malicious artifacts
- Add malicious hash to blocked items in Sophos Central

Sophos MDR Complete – Full Incident Response

Example Response Actions:

All MDR Essentials Response plus:

- Dedicated incident response lead and process management
- Root cause analysis to identify initial access
- Identification of compromised assets with remediation support
- Malware triage and analysis with SophosLabs
- Review of all relevant logs to assist with response and remediation

SOPHOS MDR ESSENTIALS

A full-featured MDR service that’s compatible with what you have

GET MORE FROM TOOLS LIKE MICROSOFT DEFENDER

Our analysts can leverage your existing technology investments to detect and respond to threats.

STOP ACTIVE ATTACKS

Human-led response actions disrupt and contain active threats, preventing spread.

STOPS WHAT SECURITY TOOLS MISS

Detect and stop more cyberthreats than security tools can identify on their own.

GET ON-DEMAND IR EXPERTISE

The Sophos Incident Response Retainer puts our IR experts on standby to get you back to business quickly in the event of a breach

It’s Time To Play Offense With Your Data

Ed Koorsgard
Sophos
Senior MSP Sales Engineer
ed.korsgaard@sophos.com
sophos.com

Randy O’Donnell
Prodatix
CTO
randy.odonnell@prodatix.com
prodatix.com

Matt Bullock
Prodatix
CEO
matt.bullock@prodatix.com
prodatix.com

Thank you for taking your time to join us!

SOPHOS + prodatix DATA MANAGEMENT