# MUTTII

# MUTTII Advanced Security + Endpoint Detection and Response (EDR) For service providers

### Simplify endpoint security

With more than 60% of breaches now involving some form of hacking<sup>1</sup>, businesses must now turn to advanced security solutions and providers to help them combat today's sophisticated threat landscape. However, most market-leading EDR solutions capable of countering these threats introduce:

- High costs and complexity, making them inaccessible downmarket
- A long time to value, high training and onboarding requirements



- Incomplete protection, requiring additional integration for business continuity
- Scalability challenges requiring large teams
   of security professionals to operate

Unfortunately for service providers just starting a practice, the skills and expenses required to run their own EDRbased service may be out of reach. For providers with established security specialization, they may find trying to build their detection and response services with market-leading solutions prices them out of their midmarket or SMB customers — only to find themselves also competing with the MDR services of their solution vendor.

# Muttii<sup>®</sup> Advanced Security + EDR, designed for service providers

Muttil® understands that service providers need to balance offering effective services with meeting different client requirements and budgets.

We also know that they need an advanced security solution that can rightsize margins and in-house skills, is multitenant, SaaS based, offers better security outcomes — and — focuses on the right amount of automation and ease of use for rapid turn up and scale across multiple clients and their unique environments.

Designed for service providers, Muttil® Advanced Security + EDR enables you to simplify endpoint protection — rapidly detect, analyze and remediate advanced attacks while ensuring unmatched business continuity. Eliminate the cost and complexity of multiple point products and enable your team with one complete cyber protection solution that is simple to manage and deploy.

### Streamline your detection and response services with Muttii®

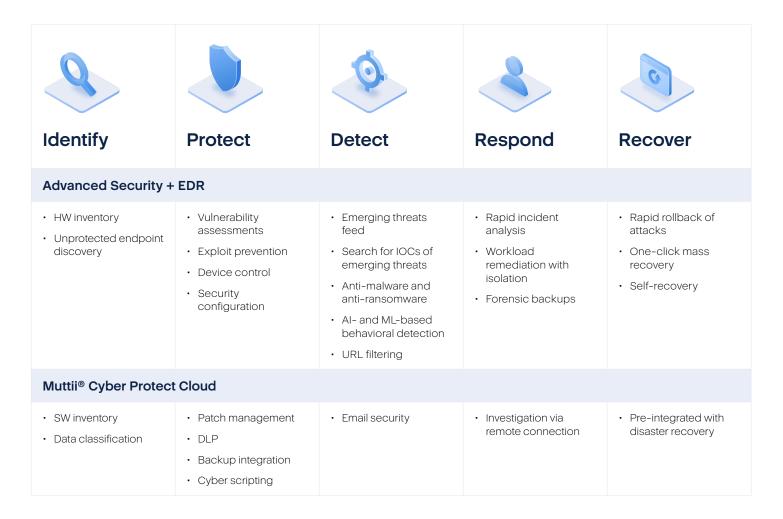
Incidents > 27									88 (?) (2)
Threat status Severity Investigation		Created Apr 19, 2023 10:53:52:092	Updated Apr 19, 2023 10:57:52:060					Pos	t comment 🛛 😔 Remediate entire incident
CYBER KILL CHAIN ACTIVITIES									
Legend	· 🗉						O	Ø patch.exe	×
Workload	1	Smss.exe Create process	m.exe					OVERVIEW RESP	ONSE ACTIONS ACTIVITIES
Process	8	Create pr	opess						
File	1574 🔹		Create process	powershell.exe				Security analysis for	process
Network	6 🔹			Read file				Verdict	(Malicious threat)
Registry	9 🔹			Create process	• +4 >			Severity	• HIGH
Involved	1641 🔹				Read file		•		Data Encrypted for Impact
Suspicious activity	2		Create process			EDRTestEvents		Reason of detection	Impact Adversaries may encrypt data on target
Malicious threat	8 🔹		create process	Ø powershell.exe	·			Reason of detection	systems or on large numbers of systems in a
Incident trigger	1			Read file	• + 272 ~		•	•	network to interrupt availability to system an network resources. They can attempt to
000000000					Read file	En Conhost.exe			render stored data inaccessible by encrypting
ttack stages	~				Read file	ATL.DUL			files or data on local and remote drives and withholding access to a decryption key. This
vecution 0					Read file	ATL.DLL			may be done in order to extract monetary
Apr 19, 2023 10:39:56:300					Read file	mscoree.dll			compensation from a victim in exchange for decryption or a decryption key (ransomware)
Suspicious activity detected with process pow	ershell.exe ).				Read file	(a propsys.dll)			or to render data permanently inaccessible in
Apr 19, 2023 10:39:56:382 Suspicious activity detected with process pow	and a line of the				Read file	the mscoree.dll			cases where the key is not saved or transmitted.
Apr 19, 2023 10:39:56:616	rishen.exe .				Read file	IMM32.DLL		Detection date	Apr 19, 2023 10:40:29:839448
Suspicious activity detected with process pow	ershell.exe).				Read file	propsys.dll			
Apr 19, 2023 10:40:29:270					Read file	IMM32.DLL		Reputation	
Process powershell.exe is abusing PowerShell scripts for execution.	commands and				Read file			VirusTotal	C Go to VirusTotal
					Read file	b propsys.dll		Google	C Go to Google
Apr 19, 2023 10:40:29:839					Read file	b powershell.exe			
Process patch.exe is encrypting data and files	on specific systems.				Read file	propsys.dll		Details	
						The rpcss.dll		Туре	Process
Apr 19, 2023 10:51:45:188					Read file	propsys.dll		Name	patch.exe
Suspicious activity detected with process pow	archell ave				Read file	(E rpcss.dll		PID	13208

Optimized attack prioritization and analysis for rapid response	Integrated backup and recovery capabilities for unmatched business continuity	Complete cyber protection solution — designed for MSPs — in a single agent
<ul> <li>Streamline investigations with prioritization of potential incidents and reduced alert fatigue</li> <li>Unlock minutes-not-hours analysis at scale, with automated correlation and Albased guided attack interpretations</li> <li>Increase visibility across MITRE ATT&amp;CK® to rapidly grasp attack analysis and impact, including how an attack got in, what harm it caused, and how it potentially spread</li> </ul>	<ul> <li>Integrated backup and recovery capabilities, providing unmatched business continuity where point-security solutions fail</li> <li>Streamlined single-click remediation and recovery</li> <li>Complete, integrated protection across the NIST Cybersecurity Framework — Identify, Protect, Detect, Respond, and Recover — all from a single solution.</li> </ul>	<ul> <li>Quickly and easily launch new services using a single Muttii<sup>®</sup> agent and console — to deploy, manage and scale</li> <li>Easily scale across multiple clients while preserving healthy margins and minimizing OpEx — no need for a large team of highly skilled people to operate</li> <li>Partner with a vendor focused on your success and enablement — not competing with you for business.</li> </ul>

### Powered by award-winning endpoint protection



### Unmatched business resilience with Muttii® Business continuity across NIST



### **EDR key capabilities**

### **Prioritization of incidents**

Monitor and automatically correlate endpoint events, with prioritization of suspicious event chains in the form of incident alerts.

## Automated interpretation of incidents mapped to MITRE ATT&CK<sup>®</sup>

Streamline response and increase reactiveness to threats, leveraging AI-based interpretations of attacks

mapped to MITRE ATT&CK® to understand in minutes:

- How the attacker got in
- How they hid their tracks
- What harm the attack caused and how it caused it
- · How the attack spread



### Single-click response to attacks for unmatched business continuity

Prevail where point solutions fail — leverage the full power of integration among cybersecurity, data protection and endpoint security configuration management via a single-click response to incidents:

- Remediate by isolating endpoints and quarantining threats
- Investigate further using remote connections and forensic backups
- Prevent future attacks closing open vulnerabilities
- Ensure business continuity with attack rollbacks and integrated backup and recovery

### Simplify endpoint security today

Don't resort to multiple tools and advanced security expertise to protect endpoints. Simplify endpoint security with Muttii<sup>®</sup> EDR.

# Learn more

1. Source: "2022 Data Breach Investigation Report", Verizon



Learn more at www.muttii.com

Copyright © 2020-2023 Muttii Group Pty Ltd. All rights reserved. Muttii® and the Muttii® logo are trademarks of Muttii Group Pty Ltd in the United States and/or other countries. All other trademarks or registered trademarks are the property of their respective owners. Technical changes and Differences from the illustrations are reserved; errors are excepted. 2023–05