MSP
Barracuda
Your journey, secured.

Stories from the security operations center (SOC): The importance of comprehensive XDR coverage

By Adam Khan, VP of Global Security Operations, Barracuda XDR

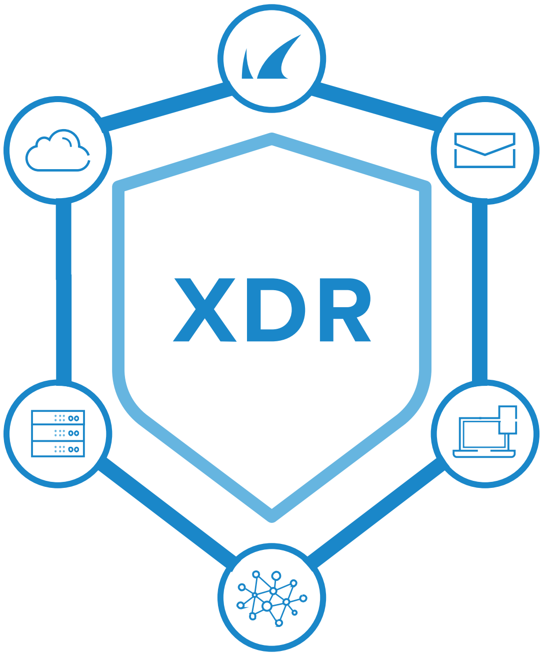
SOLUTION BRIEF

Introduction

Imagine being a cybersecurity analyst working in a security operations center (SOC), the first line of defense for many organizations. Every day, alarms and events are bombarding the team, and the team must piece together the puzzle of potential threats across the attack surfaces of networks, endpoints, cloud applications, email, and servers. What happens when one or more of the puzzle pieces are missing?

In the ever-evolving cybersecurity landscape, the need for comprehensive security measures has never been more critical. Extended Detection and Response (XDR) offers a holistic approach to security, integrating various tools and technologies to provide a unified defense mechanism.

This solution brief delves into real-life cyberattacks witnessed by Barracuda XDR's SOC teams, highlighting the critical role a comprehensive security strategy plays in mitigating these attacks. Below are behind the scenes tactics, techniques, and procedures (TTP) that adversaries have used. This will showcase how limited security subscription can leave an organization vulnerable, and the effectiveness of complete XDR coverage to protect against today's advanced threats.



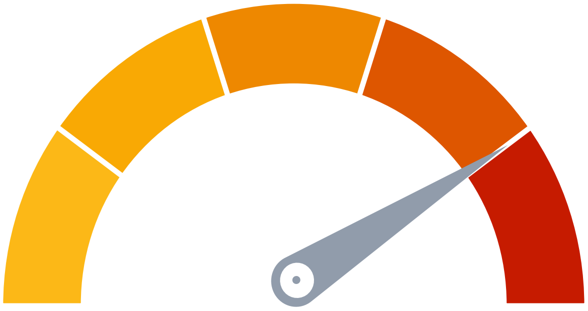
Scenario 1

Industry: Information Technology

Barracuda XDR coverage: Managed Endpoint Security

Incident classification: Ransomware and data breach

Risk level:



○ XDR Cloud Security

○ XDR Email Security

● XDR Endpoint Security

○ XDR Network Security

○ XDR Server Security

What happened:

The customer subscribed to Barracuda XDR Managed Endpoint Security only for devices that they already have visibility to. This created a significant gap which was ultimately used as the exploitation point during the ransomware incident. While XDR Managed Endpoint Security's EDR, SentinelOne, effectively detected and neutralized the threat on devices with active agents, it left numerous machines unprotected and susceptible to ransomware attack. This incident was further exacerbated by the absence of a comprehensive security strategy which should include XDR Network Security, Server Security, Cloud Security, and Email Security. This reduced SOC's visibility into critical threat indicators.

The initial breach was facilitated through a compromise of a firewall's SSL VPN that did not have multi-factor authentication (MFA) enabled. This initial penetration method was observed in prior incidents, often used by Akira ransomware actors, who use compromised VPN credentials to enter networks. In this instance, the threat actors also targeted vulnerabilities in Cisco VPNs to establish their initial foothold, specifically exploiting CVE-2023-20269, a zero-day vulnerability affecting Cisco ASA and FTD devices.

Following the breach, the threat actors leveraged their position to conduct lateral movements across the network. This led to the compromise of victim's servers, where the threat actors escalated their privilege, manipulated admin accounts and groups, and set up unauthorized communication channels with a malicious command and control (CNC) server. The lack of robust security measures across multiple layers of the network infrastructure allowed the threat actors to exploit various vulnerabilities that resulted in a successful compromise.

Attack tools used:

The threat actors employed a variety of tools to compromise the system, execute malicious activities, and evade detection. Below is a table explaining the purpose and function of each tool used during the attack:

TOOL NAME	DESCRIPTION
MeshAgent.exe	Part of the MeshCentral remote management platform. In this context, it was likely used for remote control and command execution, allowing the threat actor to execute commands and scripts remotely.
Mesh.exe	Associated with MeshCentral, this executable could be a component or variant used for similar purposes as MeshAgent.exe, such as remote access or command execution.
Meshnet.exe	Potentially another variant or component related to MeshCentral, possibly used for establishing a persistent network connection back to the attacker, facilitating lateral movement or data exfiltration.
1.exe	A generic executable name; its purpose in the attack would depend on the specific payload it contained. Often used by attackers to avoid detection by blending in with regular files or using nondescript names.
Turnoff.bat	A batch script used to disable various services on the compromised system. This could include security software, updates, or other system protections to maintain persistence and avoid detection or remediation efforts.
Psexesvc.exe	A component of PsExec, a legitimate Microsoft Sysinternals tool used for executing processes on remote systems. In this context, it was likely used to execute malicious payloads or scripts remotely without user interaction.
Netscan.exe	A network scanning tool that can be used to identify open ports, running services, and other network attributes. In an attack, it could be used to map the internal network for further exploitation or to find additional targets.
api.playanext[.]com	Identified as a command-and-control (C2) server for the Akira ransomware, orchestrating the attack by issuing commands to infected systems.
AnyDesk	While AnyDesk is a legitimate remote desktop application widely used for legitimate access, it is frequently exploited by attackers for unauthorized remote control, facilitating rapid lateral movement across an organization's network.

The impact:

The ransomware attack coupled with data exfiltration had profound implications for the customer. The customer experienced operational disruption since their critical systems and data were rendered inaccessible, bringing a halt to their services.

The selective deployment of XDR Managed Endpoint Security agents meant that not all devices were protected. This allowed the ransomware to infiltrate and compromise unprotected systems. This partial coverage proved to be a critical gap in the customer's defense strategy.

Moreover, the exploitation of a vulnerability in the SSL VPN without MFA allowed initial network access that led to widespread network compromise. The lateral movement within the network, privilege escalation, and manipulation of administrative controls further exacerbated the situation. Unauthorized communication with a malicious command and control server likely resulted in sensitive data being exfiltrated. This compounded the damage with potential data breach implications, including loss of intellectual property, customer data, and compliance violations.

Lessons learned:

This incident highlights the critical need for a comprehensive security strategy that encompasses a holistic approach. The security posture should extend well beyond endpoint protection to include network, server, cloud, and email security. The gaps in coverage served as exploitable points for attackers, resulting in a compromise that led to financial loss and potential reputation damage. Full spectrum XDR coverage would have alleviated the risks by effectively detecting and counteracting threat vectors. This underscores the importance of uniform protection across all devices to ensure consistent deployment of security agents to prevent vulnerabilities.

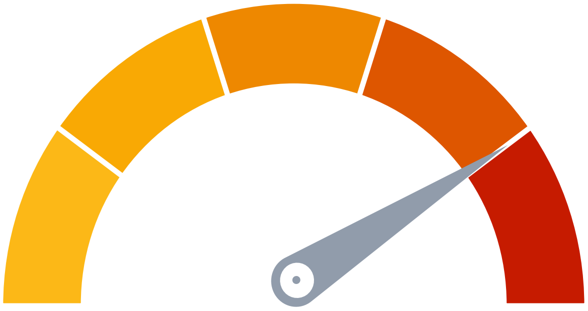
Scenario 2

Industry: Manufacturing

Barracuda XDR coverage: Cloud Security

Incident classification: Ransomware

Risk level:



● XDR Cloud Security
○ XDR Email Security
○ XDR Endpoint Security
○ XDR Network Security
○ XDR Server Security

What happened:

A threat actor exploited compromised credentials to gain unauthorized entry into a Remote Desktop Protocol (RDP) server. The attacker utilized the well-known tool, Hydra, to perform a brute-force attack on a user's account through an SSL VPN. The absence of MFA on the VPN made it easy for the attacker to penetrate the environment. The customer had independently purchased SentinelOne EDR and had it in place. However it had many misconfigurations, including the improper exclusion of essential system directories. These critical oversights resulted in over 100 devices being compromised. It impacted laptops, workstations, and servers, and causing significant disruption to their enterprise resource planning (ERP) system. Additionally, the threat actor deleted the organization's backup data, adding to the gravity of the breach.

Despite the customer's implementation of XDR Cloud Security, with Microsoft 365 integration, the absence of XDR Network Security, Server Security, Email Security, and Managed Endpoint Security resulted in significant blind spots for Barracuda XDR's SOC teams. The SOC teams' capacity to detect and respond to threats was critically weakened due to the lack of visibility across essential data sources. Moreover, since the attack occurred outside of the Microsoft 365 environment, the SOC's monitoring scope was insufficient, further hindering the SOC's ability to identify and mitigate the threat effectively.

Attack tools used:

The threat actor employed a variety of tools to compromise the system, execute malicious activities, and evade detection. Below is a table explaining the purpose and function of each tool used in the attack:

TOOL NAME	DESCRIPTION
Hydra	A well-known network logon cracker that supports many different protocols and can perform rapid brute-force attacks on user accounts.
Mimikatz	A tool that can extract plaintexts passwords, hash, PIN code, and kerberos tickets from memory. It can also perform pass-the-hash, pass-the-ticket or build Golden tickets.
Metasploit	A comprehensive framework that provides information about security vulnerabilities and aids in penetration testing and IDS signature development.
Ncrack	A high-speed network authentication cracking tool designed to help companies secure their networks by proactively testing all their hosts and networking devices for poor passwords.
PowerShell Empire	A post-exploitation framework that allows attackers to manage compromised systems using PowerShell. It can be used to move laterally through networks.
smbexec.[py]	A component of the Impacket suite, smbexec.[py] provides a method for remote code execution, leveraging service creation to execute attacker-specified commands. This script is particularly effective for enabling lateral movement within a network, as it offers a semi-interactive shell environment to the attacker.
crackmapexec.[py]	Also a part of the Impacket collection, it's a versatile post-exploitation tool that facilitates lateral movement across networks. It specializes in exploiting Active Directory environments, providing capabilities for credential harvesting and manipulation, thereby undermining network security protocols.
PyPyKatz	PyPyKatz, a Python implementation of the well-known Mimikatz utility, is adept at extracting a variety of authentication credentials. This includes plaintext passwords, hashed passwords, PINs for smart cards, and Kerberos ticket caches, making it a formidable tool for attackers seeking to escalate privileges or access sensitive information.

The impact:

The security breach significantly disrupted the customer's operations, leading to major financial losses. The compromise of the network halted production activities, derailing the customer's manufacturing schedules. Further, the loss of backup data prolonged the downtime and recovery process, which resulted in more than two months for the customer to resume full operation.

Lessons learned:

The partial deployment of security solutions left this customer vulnerable to cyberattacks. The breach underscored the critical importance of comprehensive cybersecurity measures. In the wake of the breach, the customer recognized the necessity of a more robust defense strategy and opted to subscribe to the full suite of XDR services for complete protection across network, endpoints, servers, cloud, and email. By leveraging complete XDR coverage, the XDR's SOC team will gain full visibility to not only detect suspicious activities, but also prevent unauthorized access, and enable the SOC teams for swift response times to mitigate threats in a timely manner. This strategic shift towards a comprehensive XDR approach marks a significant step forward in fortifying the customer's cybersecurity defenses and resilience against future attacks.

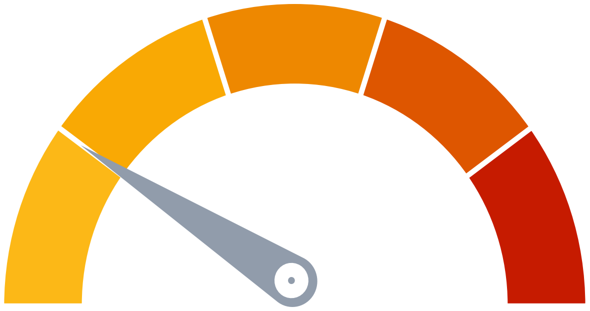
Scenario 3

Industry: Retail

Barracuda XDR coverage: Cloud Security, Email Security, Network Security, and Managed Endpoint Security

Incident classification: Ransomware

Risk level:



● XDR Cloud Security

● XDR Email Security

● XDR Endpoint Security

● XDR Network Security

○ XDR Server Security

What happened:

Despite the XDR coverage, the customer's servers were unfortunately not protected by XDR, and it became their Achilles' heel. An oversight left a critical server with its Remote Desktop Protocol (RDP) exposed to the public internet allowed attackers to open RDP channel to infiltrate the network. Upon gaining access, they targeted the domain controllers (DCs), where they created and subsequently deleted accounts to obscure their tracks. This level of access granted the attackers the ability to compromise the integrity and confidentiality of the network. Since the XDR's SOC teams lacked visibility into the customer's servers, the threat actor's activities were not detected. This allowed the threat actor to exfiltrate sensitive data from the file servers and proceeded to sell the stolen information on the dark web.

Attack tools used:

The threat actor employed a variety of tools to compromise the system, execute malicious activities, and evade detection. Below is a table explaining the purpose and function of each tool used in the attack:

TOOL NAME	DESCRIPTION
RDPWrap	This tool allows multiple RDP sessions on Windows workstations or servers that don't support it by default, used by an attacker to create multiple stealthy sessions without alerting the legitimate user.
BloodHound	Utilized post-exploitation to understand and analyze privilege relationships within an Active Directory environment, facilitating the discovery of paths an attacker can traverse to gain elevated privileges.
Cobalt Strike	A threat emulation tool that could be used post-exploitation to maintain persistence, escalate privileges, and move laterally, as well as exfiltrate data.
John the Ripper	Often employed in password cracking, this tool could be used to decipher passwords obtained during the breach, particularly useful if the threat actor has gained access to hashed passwords.
ADFind	A command-line utility used to extract information from Active Directory, which could help attackers understand the environment and plan further exploitation.

The impact:

The breach of the critical file servers had profound ramifications as it exposed valuable intellectual property and sensitive customer data which were sold on the dark web. The unauthorized disclosure led to reputational damage and undermined client trust. While the operational aspects of the business remained largely uninterrupted, the focus shifted to damage control and managing the fallout from the data breach. The company was compelled to rebuild their file servers and domain controllers from the ground up to ensure the eradication of any lingering threats and to fortify their defenses against future attacks. The incident highlighted the necessity of comprehensive server security and the potential consequences of neglecting any aspect of the cybersecurity framework.

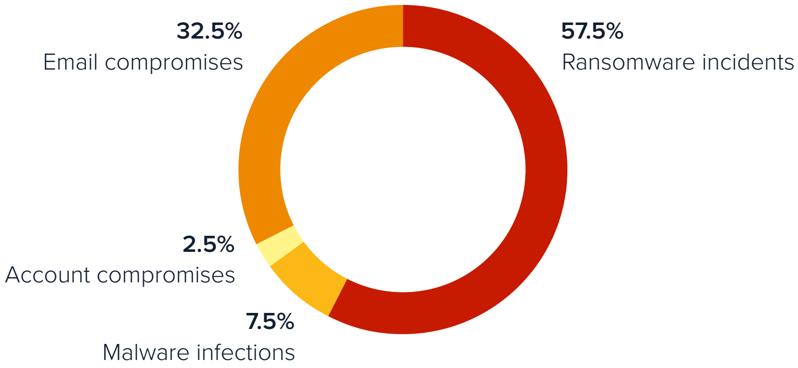
Lessons learned:

This breach underscored the imperative for a holistic cybersecurity strategy, emphasizing that comprehensive protection across all facets of the IT infrastructure is nonnegotiable. Leaving any single element, such as unmonitored servers, creates a gap that can be exploited. The incident is a reminder of the interconnected nature of cybersecurity defenses, where the strength of the system is determined by its most vulnerable point.

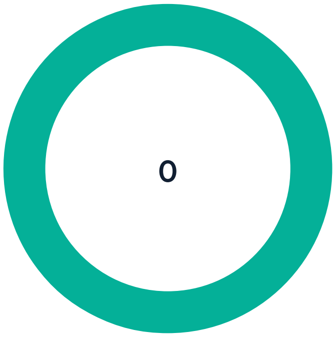
The proven impact of comprehensive cybersecurity coverage

What impact does comprehensive cybersecurity coverage have on organizations? The answer is in the data. Data collected in the past three years shows that customers with complete Barracuda XDR coverage experienced a significant decrease in security breaches, with an outstanding record of zero major incident responses required.

Incidents without full XDR coverage



Incidents with full XDR coverage



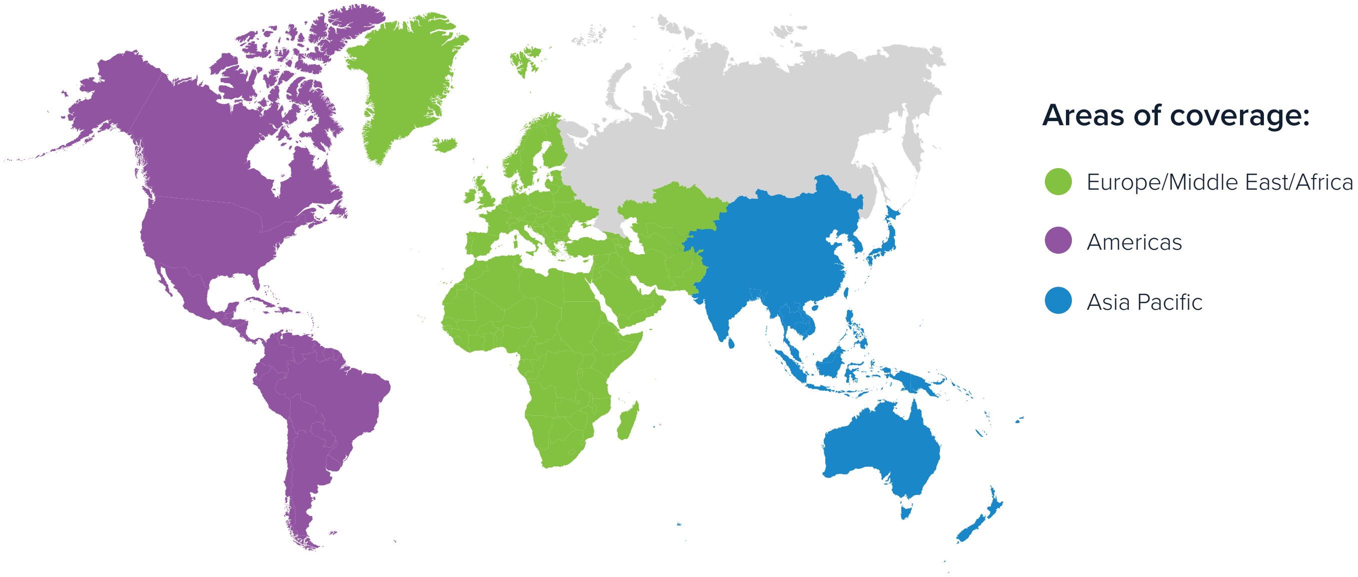
In 2023, Barracuda's findings reflect a strong contrast in the security posture between those with and without full XDR coverage. Without full XDR coverage, the SOC teams observed various incidents, including email compromise, account compromise, malware infections, and ransomware incidents. On the flip side, clients who employed full XDR coverage experienced zero incidents. This is a testament to the robust protection that a comprehensive XDR solution offers.

This unparalleled level of security isn't a product of chance. Full XDR coverage means that every aspect of the environment, from all major attack vectors, is monitored and protected with the most advanced security measures. Having a centralized, full spectrum of defensive tools at work, combined with proactive threat hunting and response strategies, creates a fortified barrier against the increasingly sophisticated attacks.

In-depth analytics and real-time monitoring enable the XDR's SOC teams to detect and neutralize threats before they escalate into incidents. The absence of major incidents among fully covered clients speaks volumes to the efficacy of a comprehensive XDR strategy. It underscores that complete visibility and integrated defense mechanisms are not just ideal but essential for modern cybersecurity.

A follow-the-sun SOC model

Barracuda XDR's SOC operates on a 24/7/365 basis, across the Americas, Europe, Middle East, and Africa, and Asia Pacific regions. This ensures continuous vigilance and rapid response to threats anywhere in the world.



SOC dedicated teams include:

TEAM COLOR	RESPONSIBILITIES
Blue Team	Cybersecurity Analysts focused on defending against cyber threats.
Green Team	Endpoint Security Engineers specializing in securing endpoints against attacks.
Purple Team	Security Automation Engineers working on the integration of security processes with automated tools.
Red Team	Cyber Security Engineers who simulate cyberattacks to test and improve security.

The dedicated teams boast a comprehensive skill set, covering all aspects of defensive and offensive security tools along with development and AI/ML expertise. We engage in research and development (R&D) practices for new security advancements & optimizations. Barracuda XDR's SOC teams hold prestigious certifications such as CISSP, AWS, Azure, CISA, CSAP, ISO 27001, AWS Security, GCIH, C|EH, GIAC, CySA+, Security+, Network+. We utilize advanced runbook mapping, engage in attack and defense exercises, provide incident response guidance, and conduct thorough threat hunting. The automated 'Allow' and 'Blocklist' capabilities ensure faster zero-day coverage. With state-of-the-art security information and event management (SIEM), security orchestration automation and response (SOAR), and threat intelligence platform (TIP) equipped with 10B+ IOCs, 800+ ML-based detections, and MITRE ATTACK framework mapping, alongside attack labs and automated threat defense, Barracuda XDR's SOC technological prowess is unmatched.

				Barracuda XDR™
LEVEL 1 Basic	LEVEL 2 Intermediate	LEVEL 3 Advanced	LEVEL 4 Optimized	LEVEL 5 Innovative
Blue Team Analysts, business hours coverage	Blue Team, 24x7 Coverage	24x7 SOC team with specialized roles (Blue, Green)	24x7 SOC team with advanced roles (Purple, Red)	24x7 Global SOC Blue, Green, Purple, Red, White Teams with regional presence (AMER, EMEA, APAC)
Network Security, Operating Systems knowledge, Email analysis.	IDS and IPS knowledge. SOC tools such as SIEM.	Cloud Computing, Endpoint security, audit and threat analysis, adversary attack tactics and techniques	Deep experience with live attacks ranging from various ATPs. Advanced SOC tools such as SOAR.	Comprehensive skill set, covering all aspects of defensive and offensive security tools along with development and AI/ML expertise. R&D into new security advancements & optimizations.
Security+, Network+	CIEH, CySA+	AWS Cloud Practitioner, Azure Fundamentals	GIAC, AWS Solutions Architect, AWS Developer	CISSP, AWS, Azure, CISA, CSAP, ISO 27001, AWS Security, GCIH, CIEH, GIAC, and CySA+, Security+, Network+
Simple incident escalation and out of the box rules.	Runbooks/playbooks, threat hunting, basic emerging threats coverage.	Security risk classification, manual allow and blocklist capabilities, custom SIEM rules	Advanced threat hunting, attack and defend exercises, log correlation across multiple data sources	Advanced runbook mapping, attack and defend exercises, incident response guidance and threat hunting. Automated allow and blocklist capabilities. Faster zero-day coverage.
Basic SIEM	Advanced SIEM, Open-source threat intelligence	EDR resources, malware sandbox	SOAR, 300+ signature-based detections mapped to MITRE ATT&CK, cloud lab	State of the art SIEM, SOAR, TIP with 10B+ IOCs, 800+ ML-based detections, MITRE ATTACK framework mapping, attack labs, automated threat defense.

These capabilities elevate the SOC's maturity with robust skillsets and certifications, coupled with the latest technologies. The SOC teams' expertise allows them to serve customers effectively and stop threats in real-time.

Conclusion

The crucial role of comprehensive XDR coverage in contemporary cybersecurity cannot be overstated. Business leaders must view cybersecurity as a strategic imperative, understanding that the cost of comprehensive security is far outweighed by the potential costs of a breach. The incidents discussed above serve as a stark reminder that incomplete security measures can leave organizations vulnerable to attacks that could have far-reaching consequences, both financially and reputationally. The commitment to complete security coverage is not just a technical decision but a business decision, ensuring resiliency in an era of sophisticated cyberthreats.

For technical management, the message is clear: complete XDR security coverage is not merely advantageous but essential. The integration of network, endpoint, cloud, email, and server security enables an unprecedented level of threat detection and response capability. This approach aligns with best practices for modern cybersecurity strategies, allowing for swift action and minimizes the window of opportunity for attackers.

Barracuda's empirical data from the last four years illustrates that customers utilizing a full XDR suite have experienced zero major incidents. This is a direct result of robust detection mechanisms, automated responses, advanced threat intelligence, and the expertise of a mature SOC. This data proves that a well-resourced and intelligently deployed XDR solution not only protects against threats but also provides the ability to adapt to new risks as they emerge.

For business leaders and technical management alike, the path forward is unequivocal. Investing in and advocating for full XDR security coverage is not just about responding to incidents; it's about creating an environment where cyberthreats are managed efficiently to ensure major incidents are prevented before they occur. A proactive and comprehensive approach is the cornerstone of a resilient and secure digital infrastructure for forward-thinking organization.

About the Author

Adam Khan is the VP of Global Security Operations at Barracuda MSP. He currently leads a Global Security Team consisting of highly skilled Blue, Purple, and Red Team members. For more than 20 years, Adam worked at various companies such as Priceline.com, BarnesandNoble.com, and Scholastic. His experience is focused on application/infrastructure automation and security. He is passionate about protecting SMBs from cyberattacks, which is the heart of American innovation.

About Barracuda MSP

As the MSP-dedicated business unit of Barracuda Networks, Barracuda MSP enables IT managed service providers to offer multi-layered security and data protection services to their customers through our award-winning products and purpose-built MSP management platforms. Barracuda MSP's partners-first approach focuses on providing enablement resources, channel expertise, and robust, scalable MSP solutions designed around the way managed service providers create solutions and do business. Visit barracudamsp.com for additional information.

@BarracudaMSP | LinkedIn: BarracudaMSP | smartermsp.com

617.948.5300 | 800.569.0155 | sales@barracudamsp.com