opentext™

SUCCESS STORY

MAD Security

Industry

- Information Technology

Products

- Bricata Network Detection & Response

Solutions

- Integrated network detection and response capabilities into MAD Security MSSP offering.
- Enables analysts to rapidly visualize activity across complex network environments and identify potential threats.

Results

6.5 minutes to detect and respond to cyber incidents—less than half the company's SLA.

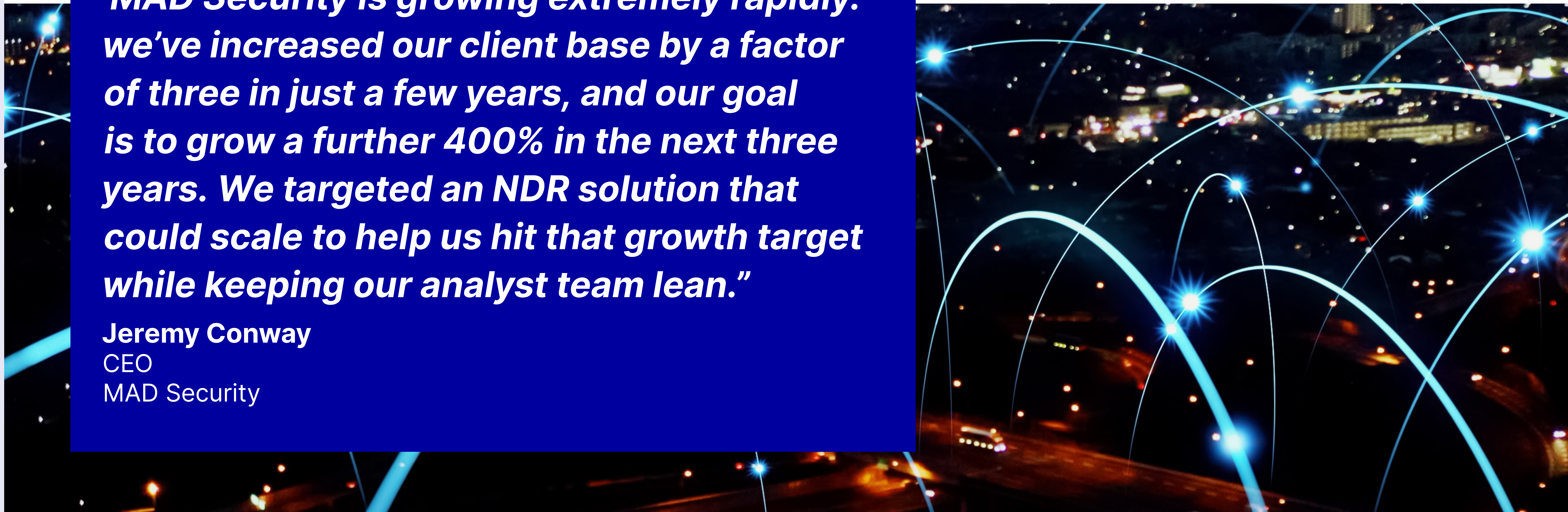
Significant reduction in false positives, saving time on investigations and improving operational efficiency.

Delivers rapid onboarding for new clients, enabling MAD Security to continue its fast-paced business growth.

MADSecurity

MAD Security protects sensitive government data against advanced cyber threats

Managed security service provider cuts false positives significantly to support a fast-growing client base with network detection and response from Bricata.



> ***"MAD Security is growing extremely rapidly: we've increased our client base by a factor of three in just a few years, and our goal is to grow a further 400% in the next three years. We targeted an NDR solution that could scale to help us hit that growth target while keeping our analyst team lean."***
>
> **Jeremy Conway**
> CEO
> MAD Security

In the United States, government contractors are becoming a prime target for cyber attacks, ranging from phishing and social engineering to malware and ransomware. Leading the fight against cybercriminals is MAD Security: a managed security service provider (MSSP) that helps contractors and other small and medium sized enterprises [SMEs] detect potential breaches and prevent attackers from disrupting operations or exfiltrating data.

Jeremy Conway, CEO at MAD Security, explains, ***"information security is a key priority for our clients because many of them must comply with stringent requirements set by the Federal government. We help our clients protect their systems so they can focus on their core competencies—a big advantage for organizations with lean IT departments."***

MAD Security offers MSSP services in multiple tiers, ranging from foundational capabilities such as antivirus scanning, central logging and user-awareness training to more advanced services such as real-time monitoring and threat response.

"In the past, we relied on an anomaly-based intrusion detection system to find indicators of compromise [IOCs]," continues Conway. ***"While this approach was effective for analyzing north-south traffic across small networks, it was a challenge to pinpoint IOCs across larger networks with significant volumes of east-west traffic. If we could reduce the time our analysts spent drilling down into the data, we could accelerate our response and improve cost-efficiency—ultimately providing a more competitive service."***

To sharpen its visibility of cyber threats, MAD Security decided to augment its offering with network detection and response [NDR] capabilities. The aim was to continuously monitor and analyze raw enterprise network traffic, creating a baseline of network behavior that would help analysts hunt down emerging threats faster.

"MAD Security is growing extremely rapidly. We've increased our client base by a factor of three in just a few years, and our goal is to grow a further 400% in the next three years," comments Conway. ***"We targeted an NDR solution that could scale to help us hit that growth target while keeping our analyst team lean."***

MAD Security selected an NDR solution from Bricata, an OpenText company. An end-to-end network security platform, Bricata simplifies network protection by combining smart packet capture (SmartPCAP) and rich network metadata generation, delivering a clear view of even the most complex networks. The solution enables MAD Security to gain insights faster than ever through deep packet inspection, behavioral anomaly detection, IOC matching and AI-powered analytics.

Gaining a clearer view

Conway recalls that, ***"one of the main reasons we selected Bricata is the level of visibility it gives us. We can now look beyond individual subsets of endpoint and log data to build up a clear picture of what happened and when during an attack—even if the network traffic is encrypted. Crucially, we can use the solution to make sure that our remediation efforts are successful, for example, by monitoring for new IOCs during our cleanup effort to detect whether the attacker is changing tactics or switching to an alternate toolset."***

Working with a team from Bricata, MAD Security performed a thorough proof of concept before deploying the solution into production.

> ***"Thanks in large part to Bricata, we can now detect and correlate events, investigate the data, and notify the client in an average of just 6.5 minutes—less than half our SLA."***
>
> **Jeremy Conway**
> CEO
> MAD Security

"The support and guidance we've received from the Bricata team have been excellent," comments Conway. ***"The team ran multiple demos with us, allowing us to get deep into the technical capabilities of the solution and explore its potential to the full. During the actual implementation, the team went above and beyond to help us by running formal and informal training and support sessions to answer our questions and walk us through specific use cases."***

Sorting the signal from the noise

Equipped with NDR capabilities from Bricata, MAD Security analysts can now more effectively sort the signal from the noise when analyzing massive volumes of network events. By minimizing false positives, analysts can focus on the most serious threats—helping to drive down response times.

"We are very pleased with the Bricata product development roadmap, which is perfectly aligned with our own long-term strategy," explains Conway. ***"Bricata is continually improving the solution, and we've been particularly impressed with the enhancements they've made to the user interface and data visualization capabilities. It's getting easier and easier to surface the insights we need, and Bricata is always willing to listen to our feedback and incorporate feature requests into new versions."***

Today, Bricata is one of the core enabling technologies of MAD Security's advanced MSSP service offering. The solution allows the company's analysts to visualize activity across north-south and east-west network traffic, identify potential threats and anomalies, and drill down to determine the best response.

Responding faster to cyber threats

Since it started its journey with Bricata, MAD Security has slashed its response times for alerting clients to cyberattacks.

Conway confirms: ***"We have a 15-minute service-level objective [SLA] for notifying clients of a critical cyber security incident. Thanks in large part to Bricata, we can now detect and correlate events, investigate the data, and notify the client in an average of just 6.5 minutes—less than half our SLA. The insight we're getting from Bricata has also cut down our false-positive rate significantly, saving time and freeing our analysts to focus on the real threats."***

Shrinking the attack surface

By incorporating Bricata into its MSSP offering, MAD Security empowers its clients to strengthen their security posture.

"One of the first clients we onboarded onto the NDR solution was an organization that reached out to us after suffering a major ransomware attack," recalls Conway. ***"They had a complex network infrastructure, and their central logging tool had already been compromised. With the NDR solution, we quickly gained a clear view of all the affected systems, which helped us to plan, execute and monitor the effectiveness of our response. Since we cleaned up the ransomware infection, the organization has been subjected to a number of other attacks—but with Bricata, we were able to shut them down before they could take hold."***

As MAD Security adds more clients to the NDR solution, it will be able to offer increased protection to all. Conway comments: ***"Attackers tend to try out new techniques on high-profile targets such as***

aerospace and defense contractors first, but once the toolsets become widespread, we start to see them used against a broad range of organizations. We can extend the lessons we learn in protecting high-profile clients to cover everyone on our NDR platform—delivering better security for all our clients.”

Planning for the future

Looking ahead, MAD Security plans to complement its NDR solution with OpenText™ EnCase™ Forensic—improving its approach to collecting, preserving and analyzing digital forensics data.

Conway elaborates: ***“We currently use software agents as part of our remote incident response process, but agentless triage via EnCase Forensic promises to be much more efficient. I worked with EnCase Forensic during a previous role at a U.S. Federal agency, and found it to be a highly reliable and capable solution. There’s a large user community and great training resources on offer, and we’re looking forward to taking the next step.”***

He concludes: ***“By building NDR capabilities into our MSSP offering with Bricata, we’re offering our clients greater protection against cyber threats and helping them respond to attacks faster.”***

About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on-premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit opentext.com.

Customer stories

opentext.com/contact

Twitter | LinkedIn