



# Motorola Mobility



motorola  
a Lenovo company

## INDUSTRY

Manufacturing, Semiconductors,  
Mobile Technology

## NUMBER OF ENDPOINTS

69,000

## THE CHALLENGE

- Provide Motorola's SecOps team with the actionable data they need to protect nearly 70,000 endpoints located all over the world.
- Streamline a bloated incident response process that required the manual analysis of multiple spreadsheets along with the forensic images from affected PCs.
- Motorola needed a scalable cybersecurity solution providing a real-time view of activity at all endpoints, along with critical forensic information on malicious incidents.

## SOLUTIONS

- Implement Cybereason Endpoint Detection and Response, providing state of the art real-time visibility into Motorola's entire technical infrastructure.
- ML-powered detection and behavior analysis improves detection speed and accuracy by driving a 1:200,000 analyst-to-endpoint ratio.
- The SecOps team is able to instantly remediate affected devices using an intuitive interface to isolate machines, remove persistent mechanisms, and kill processes with the click of a button.

## CYBERSECURITY OPTIMIZES MOTOROLA MOBILITY'S INCIDENT RESPONSE PROCESS WITH REAL-TIME ACTIONABLE DATA ON ENDPOINT ACTIVITY

Motorola Mobility, a wholly-owned subsidiary of Lenovo, boasts a reputation as a legendary company manufacturing semiconductors and various mobile technologies. A succession of mergers and acquisitions grew the company to over 6,000 employees and their SecOps team is responsible for the company's nearly 70,000 endpoints located across the globe. Needless to say, a scenario such as this requires a best of breed cybersecurity solution.

Prior to their acquisition by Lenovo, Motorola's SecOps team suffered from a bloated, largely manual incident response process. Whenever a malicious incident occurred, the team had to peruse a large number of spreadsheets as well as the forensic images from the affected desktop PCs. As those PCs were locked during the investigation, any incident adversely affected the company's operational efficiency.

The SecOps team also struggled with being located far away from some of the endpoints suffering attacks. The company's Information Protection Principal, Brad Skrbec, felt the team "needed to have a tool that could answer the 'who, what, why, when, and where' questions without a defender needing to be on the scene." The Cybereason XDR Platform provided Skrbec with the solution Motorola needed.

## THE CHALLENGE

Lenovo, one of the most recognizable brands in the world, remains a high value target for cybercriminals and state-sponsored actors. This is especially the case with any organization boasting a large technical infrastructure with tens of thousands of endpoints situated all over the world. In this scenario, a manual incident response process simply won't work for a modern, nimble technology company.

As noted earlier, the Motorola SecOps team dealt with a bloated, manual incident response process. This required cybersecurity engineers to analyze a hoard of data-laden spreadsheets for each malicious incident. Additionally, each affected PC was placed in quarantine, which hampered

employees' ability to perform their duties. This untenable situation needed to be fixed.

Skrbec commented on Motorola's acute need for a cybersecurity tool providing real-time actionable information. "We needed a way to see malicious activities in real time, a looking glass that would let us see the flow of dangerous activities, and most of all, allow us to respond just as quickly," he said. It was a critical scenario, considering that cyber attackers find endpoints to be an attractive target, since they tend to be more vulnerable compared to servers or other components within an enterprise technical infrastructure.

In fact, Skrbec noted cybercriminals tend to attack servers by using another trusted endpoint as a pivot to access the server. It's a situation requiring a cybersecurity tool with real-time visibility that lets a SecOps team monitor an entire technical infrastructure.

## THE SOLUTION

Before deciding on the Cybereason XDR Platform, Skrbec's team first needed to conduct a thorough proof of concept project. A detailed POC is essential to truly vet the capabilities of any cybersecurity tool used by his team. "Vendors must deliver on what they say. We maintain a certain amount of flexibility in our tool belt, because to stay onboard with us, delivering on promises is paramount," added Skrbec.

Lenovo deployed Cybereason Endpoint Detection and Response without any issues. More importantly, it also caused no friction within the enterprise's environment, which is a critical issue when building trust between an organization and their cybersecurity vendor. "We've seen wild amounts of friction with some tools, and that is a significant issue for us. A successful security program requires trust between the security team, SLT, and users. Anything that erodes that trust is generally disposed of like a hot potato," Skrbec said.

After the deployment of the new SecOps tool, Cybereason easily met Skrbec's demand for a frictionless implementation. "In the security world, that's exceedingly rare. In addition the overall maintenance of the tool has not required FTEs, which is always a boon," he added.

The Cybereason XDR Platform served as a game changer for Lenovo. Cybereason EDR provides threat intelligence which aggregates multiple threat feeds using machine learning analysis to quickly determine the maliciousness of a threat. Finally, they had the ability to monitor Motorola's entire technical infrastructure in real time. They receive critical actionable information on any malicious incidents from the MalOp™, a valuable feature provided by the platform. This data includes story visualizations, including an attack timeline, infected machines, the root cause, tools the attackers used, and other relevant information.

Lenovo's cybersecurity team is responsible for nearly 70,000 endpoints dispersed all across the planet. Cybereason's cross-machine correlation engine easily handled these workloads by driving a 1:200,000 analyst-to-endpoint ratio. With a reduced workload, their security team can now identify threats quickly with a higher degree of accuracy.



"Cybereason's growth, added functionality and usability have given us significantly better capabilities to improve our team and security posture"

**BRAD SKRBEK**

Information Protection  
Principal,  
Motorola Mobility



LEARN MORE AT [CYBEREASON.COM](https://www.cybereason.com)



The Cybereason XDR Platform provides instant remediation powered by AI that allows them to kill processes, quarantine files, remove persistent mechanisms, prevent file execution, and isolate machines from a single, intuitive interface.

According to Skrbec, malicious operations now “get addressed in a timely manner and we’re well aware of the dangers and risks of the attack.” Ultimately, implementing Cybereason made his team more effective and efficient when compared to the earlier manual incident response process.

## THE OUTCOME

The deployment of Cybereason EDR provided Skrbec with the visibility to monitor Lenovo’s enterprise technical infrastructure like never before. Skrbec feels the amount of information provided by Cybereason allows his team to decide to quarantine an infected machine with confidence. “We’re looking at more than just the sum of our network’s parts. We now have an elevated picture; a view from all perspectives, all from a single vantage point,” he added.

Another significant benefit – especially to the Lenovo C-Suite – involves the enhanced reporting provided by the Cybereason XDR Platform. The reporting engine provides live statistics instead of outdated metrics. “When the CIO comes to us and asks what we’re doing with a ransomware attack, we need to be able to respond with actions that resolve and close that case in an easy way. And Cybereason has been an extraordinary help in this,” noted Skrbec.

In the end, Cybereason EDR provides Lenovo with a state of the art tool to monitor and protect their widely-dispersed technical infrastructure. It’s now an essential piece in the company’s SecOps tool belt. Cybereason enabled an overburdened cybersecurity team to truly make a difference for their organization.



LEARN MORE AT [CYBEREASON.COM](https://www.cybereason.com)

