CASE STUDY

Global Entertainment and Resort Company Continues to Slash Time to Protect, Detect, and Correct

Adding innovative security technologies boosts security posture and mitigates risk

MGM Resorts International

Customer Profile
Multinational hospitality and entertainment company

Industry
Gaming, hospitality, entertainment, food and beverage, and retail

IT Environment
20,000 nodes across 20 resort entities worldwide, including more than 340 bars and restaurants and 170 retail outlets

By leveraging the Open Data Exchange Layer (OpenDXL) and solutions such as McAfee® Investigator, which uses machine learning and artificial intelligence to cut incident response time, this company has significantly reduced—and continues to shrink—the time needed to block and remediate threats, making its businesses and customers safer.

MGM Resorts International is a large and growing hospitality and entertainment company based in Las Vegas, Nevada. The company operates 20 resort properties worldwide, which include more than 340 bars and restaurants and 170 retail establishments. Chief Information Security Officer Scott Howitt oversees security for the entire global enterprise, which encompasses 20,000 endpoints, various operating systems, and applications that span the gaming, hospitality, entertainment, food and beverage, retail, and hotel industries.

CISO's Goal: Block Threats and Mitigate Risk as Quickly and Efficiently as Possible

"When customers come to our properties, they are coming to be entertained," says Howitt. "They should not have to think about the security of their data. The big headlines say other companies lost data—I never want that to happen to us."

To keep customer data safe and operations humming, Howitt's overarching goal is to block threats and mitigate risk as quickly and efficiently as possible, especially zero-day attacks and new advanced threats—because there will always be new threats. "To attain that goal, our security infrastructure must continually adapt and get smarter because the bad guys never stop adapting and getting smarter," he adds.

To that end, Howitt has overseen—and continues to oversee—the transformation of MGM Resort International's security ecosystem into one that can continually adapt and learn to protect, detect, and correct faster and faster. "Part of getting smarter is adopting innovative technologies, such as machine learning and AI, at the right time" says Howitt. "We have to keep looking forward."

Incident Response Time Shrinks with Data Visualizations and Expert-Driven Workspaces

A perfect example of how MGM Resort Internationals keeps adapting is its adoption of McAfee Investigator, a SaaS analytics subscription service that automates data collection, organization, and case management for incident response within an expert system-driven workspace. Incorporating machine learning, artificial intelligence, and human expertise, the cloud-based service guides the company's incident response analysts to consider the right questions and hypotheses for the specific situation. Insights with drill downs and visualizations help them explore the most relevant details and subtle indicators as they move rapidly through scoping, validation, documentation, and disposition.

"McAfee Investigator has completely changed the way we do investigations," says Howitt. "I'm definitely much more confident in our investigation results now that we have McAfee Investigator in place, and our incident response team catches things much faster than they did before."

"What makes McAfee Investigator especially valuable is the way it displays data visually," Howitt elaborates. "Human eyes naturally tend to recognize patterns.

Challenges

- Mitigate risks as quickly as possible and block zero-day attacks, today and in the future
- Understand the risk and impact of increasingly complex threats and attack patterns
- Provide 24/7 uptime across multiple industries and applications
- Protect customers' personal data and company's reputation
- Reduce security operations expenditures yet stay current
- Overcome lack of integration between security vendors to assist with operational processes and visibility

It's so much easier to recognize what is happening in the environment by looking at the data visualization that Investigator provides than at a list of log files. The visualization alone reduces investigation time tremendously."

Incident Response Team Experience Greater Continuity, Efficiency, and Maturation

Even after only a few months of using McAfee Investigator, Howitt saw it improved the incident response process. "Before we began using McAfee Investigator, it was hard to get any continuity with our investigations. If an investigator didn't keep clear, concise notes before handing off the investigation, someone might have to track him down to find out how and where to pick up," notes Howitt. "Now my team spends less time trying to get up to speed or switching between tools and more time actually focusing on the investigation. The automated playbook for each case has made handoffs much easier and has increased the efficiency of investigations."

In addition, using McAfee Investigator has matured the team, helping them learn from each other. "In the past, if one investigator who was exceptionally skilled at thinking through all the aspects of a certain attack handed off the investigation to another whose skills were different, the investigation might slow or stall," explains Howitt. "Now, with automated playbooks, the receiver of the handoff—and others—can learn from the earlier investigator. Everyone gets a much clearer view of every stage of the investigation. It's also easier to transfer new-found knowledge to similar incidents. The ability to learn from each other via the tool, rather than relying on people to be good teachers, advances the entire team much faster."

Completeness of Vision Drives Transformation from Antivirus Protection to Integrated Security Ecosystem

When MGM Resorts International first implemented McAfee antivirus protection approximately seven years ago, the McAfee solution was just one of many point solutions within the enterprise security environment. As the company began to think longer term and build a more comprehensive, layered defense architecture, it wanted to consolidate vendors to save money and simplify operational overhead. The broad portfolio of security solutions offered by McAfee enabled consolidation, but that wasn't the main reason for partnering with McAfee.

"One of the things I constantly preach is that I don't care about the individual products. I care about the big picture, about how all the tools work together to make us safer," notes Howitt. "Completeness of vision is why we keep coming back to McAfee. McAfee envisions an adaptive ecosystem of interconnected security solutions and services that work together to make real-time, optimized security decisions. As time has passed, we

McAfee Solutions

- McAfee® Advanced Threat Defense
- McAfee Endpoint Security
- McAfee Enterprise Security Manager, McAfee Enterprise Log Manager, McAfee Event Receiver
- McAfee Investigator
- McAfee Threat Intelligence Exchange
- McAfee Data Loss Prevention (McAfee DLP)
- McAfee Endpoint Threat Defense and Response
- McAfee Web Gateway
- McAfee Professional Services

have continually seen McAfee executing on that vision—for example, by introducing McAfee Threat Intelligence Exchange and opening up DXL [the Data Exchange Layer] to allow collaboration with other vendors."

McAfee Threat Intelligence Exchange Plus McAfee Advanced Threat Defense Revolutionizes Defenses

Adding McAfee Threat Intelligence Exchange and McAfee Advanced Threat Defense to its security infrastructure bolstered MGM Resort International's defenses exponentially. Leveraging the Data Exchange Layer (DXL), McAfee Threat Intelligence Exchange instantly shares local and global threat data to all DXL-connected security solutions, including McAfee Endpoint Security and third-party solutions. "With McAfee Threat Intelligence Exchange, going from discovery to blocking across our entire environment takes literally two clicks," says Joshua McKiddy, an MGM Resorts International senior cybersecurity engineer.

Furthermore, the combination of McAfee Threat Intelligence Exchange and McAfee Advanced Threat Defense sandbox appliances, which provide sophisticated static and dynamic behavioral analysis, dramatically enhanced the protection provided by the company's existing McAfee Web Gateway appliances. For example, if a user attempts to click on an embedded .exe file on a web page and the web gateway doesn't know if the file is malicious, the appliance in question immediately checks the file against the McAfee Threat Intelligence reputation database. If no match is found, the file is automatically sent to the McAfee Advanced Threat Defense appliance for analysis. If McAfee Advanced Threat Defense convicts it, the reputation database is immediately updated, and the file becomes blacklisted throughout the enterprise.

Adding Behavioral Detection and DXL Integration Improves Endpoint Protection

To move from signature-based antivirus detection to behavioral detection and to take full advantage of McAfee Threat Intelligence Exchange, MGM Resorts International became one of the first McAfee customers to migrate from McAfee VirusScan® Enterprise to McAfee Endpoint Security. In addition to the Threat Prevention module of McAfee Endpoint Security, the company migrated the Adaptive Threat Prevention module, which contains Dynamic Application Containment (DAC), to quarantine unknown files at the endpoint while they are analyzed, and cloud-based Real Protect machine learning technology.

"With the addition of these three products—McAfee Threat Intelligence Exchange, McAfee Advanced Threat Defense, and McAfee Endpoint Security—we significantly improved our overall security posture across the entire environment," claims Howitt. "We transformed our defenses to become more behavior-based on ingress and egress points as well as on endpoints themselves."

Results

- Improved security posture through well-orchestrated integration and intelligence sharing
- Increased confidence in investigation quality without sacrificing speed
- Accelerated time and reduced effort to contain, investigate, and remediate advanced threats
- Consolidated security vendors, simplifying administrative overhead
- Creating adaptable security infrastructure
- Improved collaboration and skills of security investigation team

"With DAC and Real Protect and integration with DXL, McAfee Endpoint Security is a far superior product to what we had before," adds Howitt. "When there's a zero-day announcement, we no longer have to scramble to make sure that all the .DAT files have been pushed out correctly; we know that the endpoints are covered. We have also eliminated the network chatter of multiple signatures being disseminated. Users are happier too because endpoint security is now transparent to them."

OpenDXL Aids Orchestration and Collaboration with Partners to Improve Efficiency and Protection

"For years, those of us in the security industry have been looking for a way to tie everything together, an orchestration framework, if you will," states Howitt. "OpenDXL is that framework, that fabric that ties all the tools together and makes them work together more efficiently and effectively, and McAfee is embracing it. Seeing this messaging bus concept applied to security is very exciting. I knew that we had to have it in our environment."

Now, once a quarter, MGM Resorts International gathers representatives from McAfee and its three other major security partners—Palo Alto Networks, Cisco, and Okta—in the same room to discuss possible use cases to leverage OpenDXL. "Together, we figure out how to use open APIs to get all our tools working together better and create a more powerful security platform," explains Howitt.

"Not surprisingly, our partners entered into this arrangement hesitantly at first, unsure about working so closely with their competitors, but once they realized that together they were making their own tools more efficient and powerful by collaborating, they embraced it," he continues. "Our own security operations team was also a bit hesitant about using open source code, but the more collaboration you have, the more likely you are to find better ways to use a tool or make it work better and be more secure. So now everyone is on board with this strategy of using the community to create solutions faster. To quote McAfee, 'Together is power.'"

This OpenDXL collaboration among vendors resulted in the integration of the threat information from its firewall vendor into McAfee Threat Intelligence Exchange. Howitt also looks forward to the coming integration of the Cisco Platform Exchange Grid (pxGrid) with DXL so that McAfee Threat Intelligence Exchange can share its information as well. "It's simply a matter of exercising your imagination as to how your tools might work together and then using the OpenDXL fabric to make it happen," he declares.

> "...Today my organization spends less than my predecessor CISO did, but we are getting a lot more out of our program. The key is leveraging our tools better and intelligently orchestrating them with one another."
>
> —Scott Howitt, Chief Information Security Officer, MGM Resorts International

Company Spends Less but Protects Better

For CISO Scott Howitt, a good day is when he gets to spend time with the company's business leaders thinking about how to help them do what they need or want to do faster and better. "A bad day, on the other hand, is when something gets past our defenses," he says. "But thanks to orchestrating our tools so much better now, there are a lot fewer bad days and many more good days. I am spending more time with business and less with operations."

"CIOs and CISOs are under a lot of pressure to reduce their spend," adds Howitt. "So, in addition to thinking of how to help business improve processes, we need to be wise about expenditures. Today my organization spends less than my predecessor CISO did, but we are getting a lot more out of our program. The key is leveraging our tools better and intelligently orchestrating them with one another."

> "McAfee Investigator has completely changed the way we do investigations. I'm definitely much more confident in our investigation results now that we have McAfee Investigator in place, and our incident response team catches things much faster than they did before."
>
> —Scott Howitt, Chief Information Security Officer, MGM Resorts International

McAfee
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com