CASE STUDY

Red Bull and Fortinet Join Forces to Improve Security with FortiEDR

Red Bull, a global brand known for its energy drinks, media, technology, and sports business gives wiiings to people and ideas since 1987. Many of the organization's employees engage in creative work, which means they need freedom to access a wide range of webservices. This complicates life for Red Bull security teams, who are responsible for protecting more than 330 corporate locations. "Security needs to cover almost every area of the company," explains the head of Red Bull's security operations center (SOC). "We have a big footprint, and the nature of the company means we need to do everything fast."

Another wrinkle in Red Bull's security landscape is the fact that cybersecurity requirements vary across the 175 countries where the company operates. These range from the General Data Protection Regulation (GDPR) in the European Union to India's requirement that security incidents be reported to the government within six hours after discovery.

Together, these factors mean Red Bull needs an endpoint security solution that enables the team to centrally manage companywide security policies, while remaining flexible enough to accommodate the diverse needs of Red Bull staff and business units in every region of the world.

Endpoint Security That Simply Works

For the past seven years, Red Bull has relied on Fortinet's endpoint detection and response (EDR) solution, FortiEDR, to protect endpoints around the world. In early 2017, when the solution's deployment to client systems was still in progress, the company experienced a ransomware attack in a "smaller satellite office" that was not yet using FortiEDR. The incident strengthened the company's resolve to finish the FortiEDR deployment.

Since client implementation was completed, the scenario has not repeated. "I cannot remember any malware-related security event that significantly impacted us resulting from threats getting through FortiEDR," says a Red Bull IT infrastructure security architect. "We have seen over the years that it is super difficult for threats to bypass FortiEDR."

In a multivendor defense-in-depth approach, Red Bull runs a classic, signature-based antivirus solution as a frontline defense of its client systems. "Every month, dozens of relevant events get past our perimeter security and the antivirus solution," the security architect adds. "FortiEDR is our final line of defense—and it works."

FortiEDR is particularly crucial for picking out emerging threats that are not yet recognized by other security solutions. "FortiEDR is built for detecting zero-day threats, and Fortinet updates it frequently," says the security architect. "The ability to detect zero-day threats, out of the box, is the main benefit of FortiEDR."

"Having the FortiEDR solution, with the FortiGuard MDR Forensic On-Demand Service behind it, gives us a very effective two-layer operations team. The tool is powerful, and this partnership prepares us to respond quickly and effectively if there is an attack."

Head of Security
Operations Center,
Red Bull

Details

Customer: Red Bull

Industry: Consumer Goods

Global Locations: 300+

Fortinet-Secured Endpoints: ~16,500

Business Impact

- Greatly enhanced security posture companywide: No serious malware-related security incidents have gotten past FortiEDR
- Enhanced detection of zero-day threats, and faster staff response in the event of an attack

FortiEDR also differs from other products in its support for threat response. “We know that we cannot prevent every possible security event. But FortiEDR, with its post-infection prevention, is very good at hindering malicious consequences.”

FortiEDR and FortiGuard MDR Forensic On-Demand Service Are Protecting 16,500 Endpoints Companywide

Red Bull recently expanded its use of FortiEDR to include all servers as well. “We use FortiEDR on every client, which totals more than 15,000 workstations, both Mac and Windows,” says the security architect. “We also have it on all 1,300 servers. We have a very heterogeneous environment, with every variant of Windows Server and Linux, including Red Hat, CentOS, and Amazon Linux. And we are running multiple versions of each of these. FortiEDR works on all the operating systems in our environment.”

Before expanding the FortiEDR installation, Red Bull ran penetration testing. “When we are choosing a security solution, we usually do a pen test,” says the SOC leader. “We were satisfied customers with FortiEDR on our workstations, but the testing is part of our standard decision process. Our pen testers looked at what FortiEDR detected. We were impressed with the visibility and forensic capabilities that we saw in FortiEDR, so we rolled it out to our servers as well.”

Now, for every endpoint across the company, Red Bull’s external SOC teams use the FortiEDR event viewer to understand the threats the solution has detected and prevented. “We also really like the incident response capabilities,” the security architect says. “When we see something suspicious on a specific machine, we put that endpoint on the highest logging setting so that we can watch everything going on with that system. We can also use the communication control module to isolate a system, or to block certain applications from communicating. And if we find out about a vulnerability in a certain version of an app that some Red Bull users have, we can use the virtual patching feature to block the affected version and allow all the versions that do not have the issue to function as usual.”

The Red Bull security team is also using FortiEDR to detect applications that have not been properly registered. “We are managing security operations across 300-plus locations, and because we give people freedom, some of them install unwanted apps,” says the SOC leader. “With FortiEDR, we can detect those unauthorized apps and react. We can even use FortiEDR to block a specific minor version of an app that is not secure, whilst allowing the safe ones.”

The security architect says Red Bull relies on the FortiEDR forensics module, as well. “We use it to do deeper research into interesting incidents,” he says. “Our SOC team uses the threat hunting nearly every day to get more context around the events in the event viewer. The forensics module is a powerful tool that provides essential details.”

If the team cannot fully explain the details of a security event, even after delving into the forensics module, they may turn to the FortiGuard MDR Forensic On-Demand Service. “For example, when suspicious PowerShell scripts are executed and it is unclear whether they are malicious, we usually invoke the MDR consulting team,” says the security architect. “That team will do a full analysis by retrieving the file, looking through the code of the PowerShell, and giving a recommendation for whether we should isolate the client or, alternatively, whether it is a false positive.”

“Having the FortiEDR solution, with the FortiGuard MDR Forensic On-Demand Service behind it, gives us a very effective two-layer operations team,” adds the SOC chief. “We can delve as deeply as we want to investigate an event. But to fully understand the data in FortiEDR, we would have to be forensics experts, which is why we sometimes turn to Forensic Hours. The tool is powerful, and this partnership gives us excellent visibility into threats and prepares us to respond quickly and effectively if there is an attack.”

Business Impact (cont.)

- No endpoint performance degradation, a persistent issue with the company’s previous endpoint security solutions
- Protection for all clients and servers across a heterogeneous environment (including Windows, macOS, different Linux variants, and Windows embedded systems)
- Visibility into unauthorized applications users have installed, and streamlined ability to block any unsecure app

Solutions

- FortiEDR

FortiGuard Security Services

- FortiGuard MDR Forensic On-Demand Service

“We aim for partnership with our vendors. We need a solution that works for us and has actual results. We also want to work with a vendor that will listen if we have a request. We have always had that kind of relationship with Fortinet.”

Security Architect,
IT Infrastructure,
Red Bull

Extreme Security That Is Easy to Manage

The FortiEDR solution has proven simple to manage, even across Red Bull's widely dispersed global network infrastructure. "We need a tool that is both extremely secure and very lightweight," the security architect says. "The Fortinet EDR solution fits that bill." Its high throughput performance means FortiEDR does not get in the way of end users getting their work done.

"A lot of our users are working in areas like video rendering," says the SOC leader. "Noticeable latency is not acceptable. Before we had FortiEDR, we would get complaints about security systems impacting endpoint performance. FortiEDR has solved that problem." Even when the security team rolls out an update, it usually has no user impact at all.

Excellent Support Builds a True Partnership

For seven years, Red Bull security teams have had a close relationship with the FortiEDR support and development groups. "Our relationship with Fortinet is very good," says the security architect. "The FortiEDR support team takes our feedback seriously. Dozens of times, we have requested a feature that made it into the FortiEDR product."

This is how Red Bull likes to do business. "We always aim for partnership with our vendors," the security architect concludes. "We are not necessarily looking to purchase the cheapest solution or work with the biggest vendor in the market. We need a solution that works for us and has actual results. We also want to work with a vendor that will listen if we have a request. We have always had that kind of relationship with Fortinet."

FORTINET

www.fortinet.com

September 5, 2024 11:01 AM

2619020-0-0-EN