DESERT RESEARCH INSTITUTE ELEVATES DATA SECURITY IN A DYNAMIC THREAT ECOSYSTEM WITH CHECK POINT

DRI
Desert Research Institute

Customer Profile

Desert Research Institute is a world leader in investigating the effects of environmental changes.

Challenge

- Protect sensitive data against email and other attack vectors
- Enable dynamic defenses to keep pace with evolving threats
- Maximize team productivity and efficiency

Solution

- Check Point Quantum Security Gateway
- Check Point Quantum NGFW
- Check Point R80

Results

- Prevented advanced unknown attacks daily
- Aligned policy to project contract parameters and gained ability to adapt policy on the fly
- Saved hours of time managing hundreds of policies with automated traffic and log analysis

> "Check Point Next Generation firewalls with SandBlast Network give us universal, automatic protection that stops threats every day—before we even know they're here."
>
> —Ryan Coots, Senior Network Engineer, Desert Research Institute

Overview

Desert Research Institute

The Desert Research Institute (DRI) leads global efforts to investigate environmental changes and their impact. The institute increases scientific knowledge and pioneers environmental assessment technologies in projects on every continent.
Its goal: To promote ecosystem preservation, enhance resource management, and improve human health and welfare.

Business Challenges

As a nonprofit research arm of the Nevada System of Higher Education, DRI conducts research projects spanning land, air, and sea. The institute supports main campuses in Reno and Las Vegas and at three remote locations. It employs 550 people who travel globally, involved in projects in most of the world's countries.

A wide range of governmental agencies, such as the Department of Energy, the Department of Defense and the Navy, and other organizations grant research contracts to DRI. As its primary funding source, these contracts come with specific sets of data protection guidelines. Some client relationships have been in place for more than 50 years, so adhering to contract security parameters is critical to retaining those agreements.

"Securing project data is instrumental in keeping these projects," said Brandon Peterson, Chief Security Officer for DRI. "We must protect information and intellectual property that rogue nations and cybercriminals would love to access. Data protection is of paramount importance."

The Institute has been a Check Point customer for more than a decade. Recently, rapid growth added new locations, much higher network traffic volumes—and a larger attack surface to protect. Besides needing greater security capacity, the DRI team is small. They wanted to standardize security across all locations to save time, optimize their resources, and simplify management. With much at stake, DRI conducted an extensive evaluation of security solutions, which included Check Point, Cisco, and Fortinet.

"We chose Check Point again," said Peterson. "Its broad range of protection and high performance made the choice easy. Check Point also made it easy to standardize our security infrastructure, regardless of the size of a remote location."

> "We chose Check Point again..Its broad range of protection and high performance made the choice easy. Check Point also made it easy to standardize our security infrastructure, regardless of the size of a remote location."
>
> —Ryan Coots, Senior Network Engineer, Desert Research Institute

Solution

Smart, Multi-Vector Protection

The institute deployed a Check Point 15,600 Next Generation firewall at its primary locations. Five Check Point 3200 Security firewalls enable secure VPN connectivity to DRI for mobile employees located around the world. The firewalls provide high performance, reliability, and uncompromised security to protect users, traffic, and data from sophisticated Gen V threats. DRI uses the built-in application control, URL filtering, IPS, antivirus, and anti-bot capabilities to defend against multi-vector attackers.

SandBlast Network is built into the firewalls, providing zero-day protection with Threat Emulation and Threat Extraction capabilities. SandBlast Threat Emulation performs deep CPU-level inspection to stop attacks before they can evade detection and deploy payloads. SandBlast Threat Extraction analyzes files and documents to remove potentially malicious elements before delivering safe content to users.

Management for the entire infrastructure—systems, policies, and configurations —is all centrally managed from a single pane of glass in the Check Point R80 SmartConsole. With global locations to monitor, Check Point R80 cyber security management makes it easy for the small team to work concurrently from the same rule base without conflict.

"Check Point is an all-in-one solution with advanced protection at the click of a button," said Peterson. "Integrating all of these solutions and bringing them together in a single management tool has been really helpful."

"Check Point is an all-in-one solution with advanced protection at the click of a button. Integrating all of these solutions and bringing them together in a single management tool has been really helpful."

—Ryan Coots, Senior Network Engineer, Desert Research Institute

Results

Smarter Defenses

Email threats represent a large attack vector for DRI. SandBlast Network scans the institute's high volumes of email for malicious attachments, URLs, and other content, preventing threats from getting to users' mailboxes.

"Our researchers receive files and software from many different sources," explained Peterson. "SandBlast Network has detected—and stopped—malware that evaded controls at several large federal agencies. We sleep better knowing that if something tries to enter the network, SandBlast Network will find it."

A Smart Single Pane of Glass

The engineering team uses Check Point R80 security management, with its SmartEvent and SmartLog features. SmartEvent correlates logs from all enforcement points to identify suspicious activity, track trends, and mitigate threats. It delivers full threat visibility into security risks through a single dashboard.

With rapidly changing threat environments across global locations, the team makes many policy changes each day. The team relies on SmartEvent to manage the gateways and make rule changes on the fly. At the same time, SmartLog converts and analyzes log data to deliver split-second search results, giving the team real-time visibility into billions of log records over multiple time periods and domains. Team members use SmartLog to troubleshoot connectivity errors and ensure researchers are properly connected.

"Check Point firewalls are already easy to manage, but having everything visible in a single pane of glass makes it even simpler," said Ryan Coots, Senior Network Engineer at DRI. "I use SmartLog every day to analyze inbound and outbound traffic and mitigate threats. It's fast and easy, making efficient use of our time."

Check Point R80 enabled DRI to apply the most appropriate firewall and application policies to each traffic segment. For example, policies for traffic from a researcher working on a public project or shared weather data will be different than policies for traffic from researchers working on a sensitive military application.
The team can visually see segmented traffic and policies in Check Point R80 and manage them properly.

"Check Point is a tremendous partner," said Peterson. "We're confident that they're already working on securing us against tomorrow's threats, as well as today's."

—Ryan Coots, Senior Network Engineer, Desert Research Institute

Automatic Zero-Day Protection

Check Point SandBlast Network has been a lifesaver for stopping threats from reaching users' mailboxes. SandBlast Network detects suspicious email attachments and URLs and analyzes them before delivery. If the file is safe, it's delivered to the end user. If it's a threat, it's stopped before it reaches the end user.

"Users don't have an easy way to confirm if files they receive are safe," said Coots. "Check Point Next Generation gateways with SandBlast Network give us universal, automatic protection that stops threats every day—before we even know they're here."

Dynamic On-the-Fly Protection

Ease of use goes a long way toward protecting DRI data and researchers in a constantly changing environment. The ability for multiple administrators to work in R80 concurrently—from anywhere in the world—enables the lean team to continuously adapt policy and address dynamic threat environments.

"We make multiple policy changes a day," said Coots. "Concurrent management, in addition to Check Point automation, multiplies our efficiency even more."

Next Stop—the Cloud

DRI plans to move some workloads to the cloud, creating a hybrid cloud environment. The team will be able to continue using their Check Point solutions to secure both—cloud and premises—environments with a single set of integrated capabilities.

"Check Point is a tremendous partner," said Peterson. "We're confident that they're already working on securing us against tomorrow's threats, as well as today's."

For more information, visit:
https://www.checkpoint.com/products/