Trend Micro™ Deep Discovery Uncovers Targeted Attacks

The operations behind Motel 6 are better protected from APTs and cybercrime.

> “Deep Discovery is not just a step forward–it is a big leap forward... Deep Discovery gives us a line of defense against targeted attacks. We can now shut them down quickly.”
>
> - **Andrew McCullough, Lead Information Security Architect, IT**
> Motel 6, Dallas, Texas

EXECUTIVE SUMMARY

Customer Name: Motel 6

Industry: Hospitality

Location: Dallas, Texas

Web site: www.motel6.com

Number of Employees: Approximately 7,500

CHALLENGE:

- Prevent infections, especially malicious code that can steal sensitive data, and remain hidden for long periods of time
- Maximize return on investments in systems
- Integrate and coordinate multiple lines of defense
- Improve visibility over security, and reduce complexity for management
- Strengthen compliance (PCI and more), and ultimately maximize protection of customer information

SOLUTION:

- Uncover hidden threats with Trend Micro Deep Discovery
- Switch endpoint security to Trend Micro™ Enterprise Security for Endpoints
- Introduce Trend Micro™ Deep Security modules to boost protection for mission-critical applications and high-risk servers
- Support from security experts (Trend Micro Technical Account Management Services)

BUSINESS RESULTS:

- Significant reduction in infection rates, with “eye-opening” discovery of malicious threats attempting to “phone home”
- Major improvement in system resource utilization, with in-the-cloud protection
- IT time savings (4–8 hours/week, for 2–6 technicians and engineers)
- Boosted confidence in protection of customer information and corporate reputation
- Alignment between company vision and security vendor’s directions

Challenge

The Motel 6 network consists of 1,100 properties under the Motel 6 and Studio 6 brands. The company’s primary and back-up data centers serve an extensive network of approximately 5,000 endpoints throughout the continent.

Like retailers, hospitality companies must manage and secure sensitive customer data including credit card numbers and personal identification information. As an employer, the company also handles personal health information. Compliance and risk management go hand in hand, as top corporate priorities.

“Everything comes down to risk—how the business might be impacted and how we can minimize risk while maximizing the returns from our security dollars,” said Andrew McCullough, the lead information security architect for Motel 6.

“In the hospitality industry, security is important to everyone. Credit card or identification or health information—these are all synonymous because of the challenge and cost of recovery from data theft. We can’t afford to have our brands publicly associated with any breach of security. The reality is that people don’t trust their information being given to a company that has been compromised, especially if it happens more than once.”

Industry efforts to improve security, with regulations and guidelines promoted by the Payment Card Industry (PCI) and various government agencies, have changed operating practices and policies for companies like Motel 6.

“For retail and hospitality, PCI has made companies wake up and think about security,” said McCullough. “The guidelines are not perfect, but they are a step in the right direction and especially important in our business. Hospitality has been targeted over the last few years. I pay close attention to the threat activity in our industry as well as the bigger retail landscape.”

Solution

When Motel 6 began to see an increasing number of threats making it through the company’s multiple layers of security, they acted swiftly to find and deploy a solution with more advanced global threat intelligence. Of particular concern was the rise of advanced persistent threats (APTs), including targeted attacks on businesses that handle credit card information.

The deployed security solutions for Motel 6 included endpoint and perimeter security products from multiple vendors. “Security is always about defending; we don’t trust anyone and don’t rely on any one solution or vendor,” explained McCullough. “We had one vendor for endpoint security—desktops and servers—and it was this layer that was our primary concern.”

Step 1: Threat Discovery

The concern stemmed from the rising numbers of infections. As a first step towards improving security, Motel 6 decided to introduce Trend Micro™ Threat Management System, now Trend Micro™ Deep Discovery.

“The numbers of Trojans and BOTs that were discovered by the Trend Micro solution opened our eyes,” said McCullough. “We were really impressed with the detection rates. Threat Management System warned us of malware that was gathering information and attempting to pull in malicious payloads from ‘command-and-control’ or CNC servers. If they had gone undetected, many of these threats have been known to operate for months or years. With the Trend Micro solution, we were detecting them and stopping them before they caused any breaches.”

Motel 6 became a loyal Threat Management System customer, and actively partnered with Trend Micro during the development and introduction of the next-generation Trend Micro Deep Discovery solution. One of the first beta deployments of Deep Discovery has been actively protecting Accor North America since its introduction.

Steps 2: “Thinking Outside the Box” About Endpoint Security

“The fact that our previous vendor’s endpoint solution was not effectively blocking even generic malware was very troubling,” said McCullough. “That’s when we evaluated what else was available and decided to think outside the box about a more effective strategy, one that would better protect server endpoints mobile users, and desktops, as well as incorporate more advanced threat detection.”

Motel 6’s security team considered several leading security vendors in terms of their threat detection technologies and overall directions for endpoint security. Basically, they wanted it all:

- A dashboard “that everyone dreams of,” one that enables true central management of company-wide security
- Integrated point products that provide multi-layered protection
- Support for compliance
- Additional types of protection and capabilities for higher-risk endpoints, such as point of sale (POS) systems and data base servers
- Security tailored for mission-critical applications
- A small security footprint

The security team found that the company’s security requirements could best be met by switching to Trend Micro Enterprise Security for Endpoints, including the flagship product Trend Micro™ OfficeScan™ solution for protecting servers, desktops, and laptops. Trend Micro Deep Security was also chosen, to introduce advanced capabilities such as file integrity monitoring, log inspection, intrusion defense, and more to supplement server security.

“We were looking for the big picture, and Trend Micro was going in the right direction,” said McCullough. “Our visions definitely aligned.”

Step 3: Minimizing the Security Footprint

Achieving a small security footprint was of particular interest to Motel 6. Having seen how traditional threat signatures and patterns could quickly become unwieldy and severely impact system performance during scans, they wanted a more resource-conservative approach for security. Powered by Trend Micro™ Smart Protection Network™ infrastructure, Trend Micro enterprise security solutions have the benefit of in-the-cloud protection that keeps on-premise solutions lightweight and efficient.

> “The numbers of Trojans and BOTs that were discovered by the Trend Micro solution opened our eyes. We were really impressed with the detection rates.”
>
> - **Andrew McCullough, Lead Information Security Architect, IT**
> Motel 6, Dallas, Texas

DEPLOYMENT ENVIRONMENT:

Primary and DR data centers

1100+ hotels/motels in U.S. and Canada

400 servers; 5,000 endpoints

Trend Micro Deep Discovery 3.0

Trend Micro Deep Security 8.0

Trend Micro OfficeScan 10.0

"When dealing with POS or servers, we don't replace assets often," said McCullough. "Management wants to maximize ROI and extend asset life. This makes processor and memory very valuable resources. Even so, we needed to add in more protection for higher-risk endpoints such as POS systems and the large servers hosting mission-critical applications and databases. We were using homegrown logging functions to protect those assets, and assist with compliance efforts as well.

"We thought that there had to be something that would consolidate all of these security functions and minimize the impact on memory and processors. That something was Trend Micro Deep Security. It does many things in a single package, and provides us with a better dashboard. This means better risk management and better visibility for higher-risk systems where we have our critical business data."

Results

The combination of Trend Micro solutions and service has changed the threat landscape for Motel 6.

"We are not seeing the infections we saw before we introduced Deep Discovery, OfficeScan, and Deep Security," said McCullough. "We used to call our previous vendor on a weekly basis, it seemed, reporting new infections. It was frustrating to be told often that the threat was known but that the signature was no longer included in the pattern files. This is what you have to do to keep pattern file sizes down.

"That's the advantage of Trend Micro Smart Protection Network — threat information is collected in the cloud to reduce the footprint on the client side. To the best of my knowledge, Trend Micro was the first to leverage the cloud in this manner. As a result, they get higher detection rates and don't have to drop signatures."

Higher detection and better endpoint protection has translated to saved time for Motel 6. The security team estimates that they save four to eight hours per week troubleshooting security issues. These hours are multiplied, since efforts are usually required from two members of the team; a complex issue can take five or six members of the IT staff away from other work. The relationship with Trend Micro has also led to early access to the new Deep Discovery product.

"Threat Management System, the predecessor, was a good step in the right direction," said McCullough. "It gave us the ability to be alerted to certain conditions without forcing processes or traffic to stop in every case.

"Deep Discovery is not just a step forward — it is a big leap forward. With the new 'sand box' capability, Deep Discovery can evaluate a suspicious java applet or code snippet and help us make the right decision. After all, it is not always the broad-scale threats that represent the biggest danger to our business. Today, it could be a targeted attack—a piece of code crafted just to get at our data. Deep Discovery gives us a line of defense against targeted attacks. We can now shut them down quickly."

> "Everything combined–Trend Micro solutions and service–reduces our risk and really improves our security posture. We have a lot of confidence now. Trend Micro has made a massive difference in our security."
>
> - **Andrew McCullough, Lead Information Security Architect, IT**
> Motel 6, Dallas, Texas

Company Profile:

Motel 6 offers the lowest price of any national chain at more than 1,100 company-owned and franchised locations throughout the United States and Canada. For 26 years, Motel 6 has used the tagline, "We'll leave the light on for you®," earning the chain the highest brand recognition in the economy lodging segment. Motel 6 was the first national pet friendly chain, welcoming pets since 1962. Standard amenities include free local phone calls, no long distance access charges, free morning coffee and expanded cable channel line-up. Most locations offer Wi-Fi Internet access, swimming pools and guest laundry facilities. For more information, visit www.motel6.com.

Trend Micro solutions have given Accor North America many new security capabilities.

"We have gained several things, compared to our previous solutions," said McCullough. "Sandboxing is just one thing. Another is browser filtering. We can catch a piece of malicious Java code or an ActiveX script when it is running in a browser session. Now we can stop that code without blocking legitimate web activity. The majority of infections come in this way, and now we have the capability to stop them."

McCullough went on to comment on the improved interface, better alerting, and "fantastic" reporting. On top of the product features, he credits the Trend Micro Technical Account Manager (TAM) with their improved security position. "Having access to an expert TAM really makes a difference. When something goes wrong, he immediately alerts us. If it is critical, we'll get a phone call. Everything combined — Trend Micro solutions and service — reduces our risk and really improves our security posture. We have a lot of confidence now. Trend Micro has made a massive difference in our security."

Trend Micro Products

- **Trend Micro Deep Discovery**
  http://www.trendmicro.com/us/enterprise/security-risk-management/deep-discovery/index.html
- **Trend Micro Deep Security**
  http://www.trendmicro.com/us/enterprise/cloud-solutions/deep-security/index.html
- **Trend Micro OfficeScan**
  http://www.trendmicro.com/us/enterprise/product-security/officescan/index.html
- **Trend Micro TAM Services**
  http://www.trendmicro.com/us/enterprise/consulting-support-services/technical-account-management/index.html

> "That's the advantage of Trend Micro Smart Protection Network– threat information is collected in the cloud to reduce the footprint on the client side. To the best of my knowledge, Trend Micro was the first to leverage the cloud in this manner."
>
> - **Andrew McCullough, Lead Information Security Architect, IT**
> Motel 6, Dallas, Texas

TREND MICRO™

Securing Your Journey to the Cloud