MICRO FOCUS

Customer Success Story

Security

ITC

ITC Secure Networking slashes time to detect cyber-attacks with Micro Focus® ArcSight.

Challenge

The fast spread of the WannaCry ransomware in 2017 was a reminder of the cybersecurity threats organizations face.

Hospitals and manufacturers were among the many victims of WannaCry, which bypassed corporate security by exploiting a software vulnerability.

London-based managed security services provider ITC Secure Networking understands these threats well. Since 1999, the company has helped many organizations protect their critical data. The challenge for ITC was to recognize vulnerabilities and identify threats as quickly as possible. ITC recognized that the best way to protect clients' data and systems was to collect and analyze logs from firewalls, intrusion prevention systems, security applications, and other systems and devices.

"ArcSight ESM has the best ability to create use cases quickly, easily, and effectively."

KEVIN WHELAN
Chief Technology Officer
ITC Secure Networking

This process could be very time consuming for some organizations. "I heard of one IT manager who had to look at the logs on the train to work, then on the way home," says ITC's Chief Technology Officer, Kevin Whelan.

One solution is to automate this task by using a security information and event management (SIEM) tool. This automatically analyzes the logs, using predefined rules to look for signs of suspicious activity. But not all companies can afford to purchase such a tool or hire staff members with the right skillset to operate it.

Unless organizations address this problem, they are at risk of being targeted by cyber threats. Whelan points out that hacker groups' publication of hacking tools, including a tool used to spread WannaCry, has provided attackers with more ways to infiltrate systems.

"As people start writing exploits, it will be essential to react quickly," Whelan says.

ITC's customers have much to lose if their systems are breached. One financial organization manages transactions each day totaling many trillions of dollars. Other customers include some of the world's largest manufacturers, which need to protect valuable intellectual property. In other cases, ITC protects the

ITC SECURE NETWORKING

At a Glance

- **Industry**
  Software & Technology
- **Location**
  United Kingdom
- **Challenge**
  Protect clients' data from cyber attacks by providing rapid, affordable threat detection.
- **Products and Services**
  ArcSight ESM
- **Results**
  + Reduced time to detect cyber attacks
  + Analyzed 38.6 billion events in a month, identifying 467 security incidents
  + Protected transactions translating to trillions of dollars per day
  + Reduced upfront costs for clients to secure their businesses
  + Improved managers' understanding of regulatory compliance

integrity and availability of websites and systems that process online transactions.

Solution

ITC solves these challenges by hosting and managing a SIEM solution for clients, customizing it to suit their IT environments. This reduces upfront security costs and saves time by identifying critical threats more quickly.

ITC's SIEM must also be capable of ingesting large volumes of data and then correlating it to quickly identify threats.

The solution must also be very customizable. ITC needs to create, apply, and update complex rules that speed up the task of spotting suspicious activity or events.

To achieve this, ITC relies on ArcSight Enterprise Security Manager (ESM). This is the core technology within the company's managed services platform, NetSure360°.

ITC has a dedicated Security Operations Center, manned by a team of experts who manage these systems and monitor security alerts. Customers pay a fixed monthly fee to use the service.

Micro Focus also keeps the company informed about new product developments, supports sales lead generation, and provides technical support.

Results

Cuts Time to Detect and Respond to Cyber Attacks

ITC has reduced the time it takes many of its customers to detect cybersecurity threats, from hours to minutes.

In one case, the company defended a customer in the finance sector from an attack by a notorious threat actor. The customer's employees had previously taken up to five hours to collect and analyze log data for signs of an attack. ITC created a use case and rules within ArcSight ESM, which detected an attack in minutes.

Customers also save time in other ways. For example, online retailers need to respond to alerts and events about threats to their web stores. ITC makes this possible by building an asset model of the customer's IT environment, including the web stores. The company then creates use case rules to prioritize alerts about the web stores.

"ArcSight is flexible enough for us to prioritize which parts of your organization you value more," Whelan says.

He likens some other SIEMs to black boxes, because, he says, they don't allow users to get under the hood and customize alerts effectively. "With a black box, you very quickly get overloaded with too many alerts," Whelan says.

"ArcSight ESM has the best ability to create use cases quickly, easily, and effectively," Whelan says. This allows customers to focus on the alerts that matter most.

ITC can also speed up customers' responses to threats by automatically disconnecting compromised computers from the network. The company does this with ArcSight ESM, which uses scripts to call an Application Programming Interface (API) of networking or network access control equipment, which then disconnects the compromised computer. Not every organization may want to do this, but it's an example of ArcSight ESM's breadth and versatility.

Saves Customers Money

ArcSight ESM's multi-tenancy capability makes it simpler for managed security services providers to reduce their costs by having customers share servers. For example, ITC uses the same infrastructure to host multiple instances of ArcSight ESM, each monitoring a different customer.

This approach is possible because ArcSight ESM can ingest and correlate vast amounts of event and log data from multiple instances of the software. In one month, it analyzed 38.6 billion security events for ITC, correlating 11,681 alerts to identify 467 incidents. One large manufacturing customer has 400 sources of log data in over 100 countries. "ArcSight has phenomenal power to process lists and data. The technology is very scalable," Whelan says.

Some organizations could not afford to purchase, host, and manage an equivalent level of security themselves, says Whelan. "They would have to deploy staff members, software, hardware, and keep the systems updated. It's a 24x7 operation," Whelan says. He points out that many organizations only have one security officer.

Improves Regulatory Compliance

ArcSight ESM also makes it easier for ITC customers to check if they comply with regulations and standards.

For example, ITC uses it to review customers' compliance with the ISO/IEC 27001 standard for information security systems. The company also reviews customers' compliance with the Payment Card Industry Data Security Standard (PCI DSS). The customers can receive reports detailing which areas of their IT environment don't meet required security standards. Micro

> "ArcSight has phenomenal power to process lists and data. The technology is very scalable."
>
> **KEVIN WHELAN**
> Chief Technology Officer
> ITC Secure Networking

Contact us at:
www.microfocus.com

Focus can also provide ArcSight ESM packages that check for compliance with the Sarbanes-Oxley Act and the Health Insurance Portability and Accountability Act in the United States, and regulations in other countries.

"We say it provides our customers with visibility, control, and assurance," Whelan says.