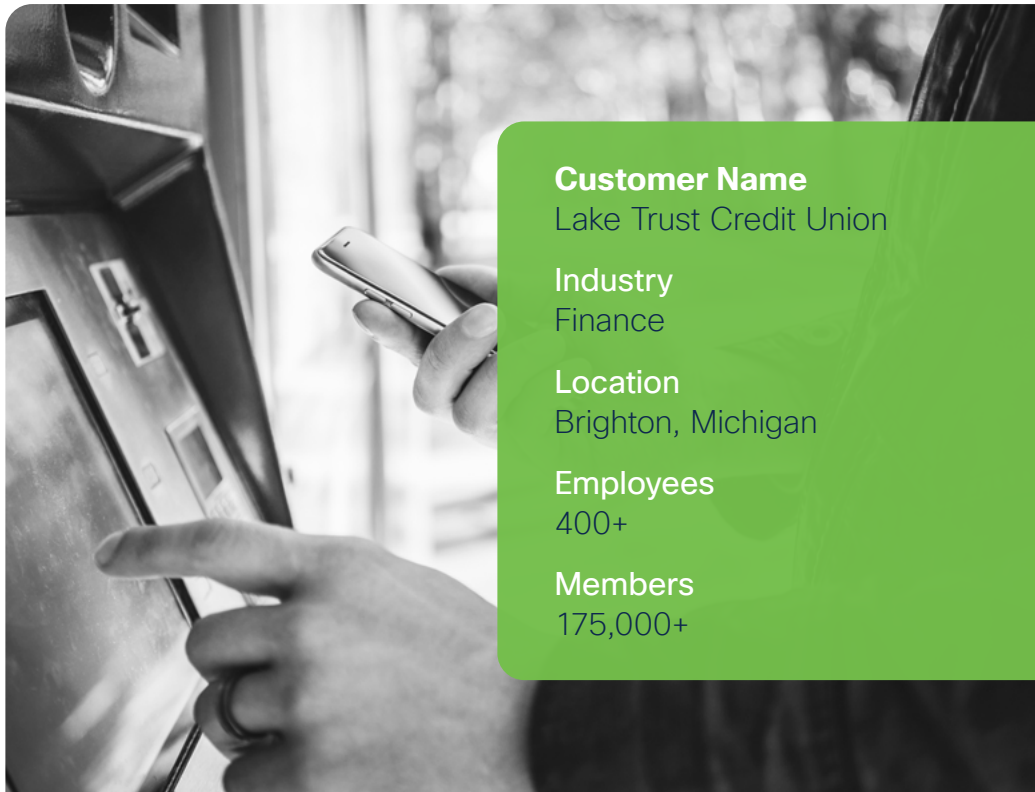
CISCO
SECURE

Securing a distributed network and ensuring compliance with Cisco Secure Network Analytics

Lake Trust Credit Union is a community-based credit union headquartered in Brighton, Michigan, with around $1.8 billion in assets, ranking it in the top 1% of credit unions nationwide. It has 22 branches and over 175,000 members across Michigan.



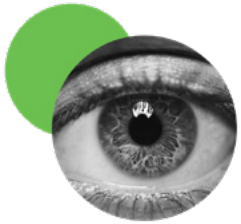
Customer Name
Lake Trust Credit Union

Industry
Finance

Location
Brighton, Michigan

Employees
400+

Members
175,000+



Challenges

- Protecting a variety of sensitive member data and financial assets
- Being able to prove audit requirements and ensure other internal business and security policies are being enforced
- Monitor a distributed network spread across 22 branches and multiple ATM locations
- Maintaining a first-class security strategy and infrastructure with a lean team

Solutions

- Secure Network Analytics (Stealthwatch)
- Identity Services Engine (ISE)
- Secure Firewall (Firepower)
- Secure Endpoint (AMP for Endpoints)
- Umbrella
- Secure Email (Cloud Email Security)
- AnyConnect
- Secure Malware Analytics (Threat Grid)

Results

- Unprecedented threat visibility with actionable alerts infused with context
- Ability to easily prove audit requirements like cryptographic compliance, and to monitor for any business or security policy violations with custom alerts
- Achieved automated detection and response across the network, endpoints and web, and extended investments with an integrated security architecture
- Transitioned to a remote workforce without compromising on security and infrastructure uptime

Key challenges

Being a financial institution, Lake Trust is very concerned about ensuring the security of their assets and their members. Additionally, Lake Trust needs to ensure certain regulatory as well as some internal business compliance requirements.

The Lake Trust network is spread across multiple branches, ATMs, as well as data centers. They needed a solution that could effectively monitor this spread-out network. The team comprises of four people, responsible for the entire platform infrastructure and its security, so automation and ease of deployment of solution was also a priority.

Lake Trust previously had a product to monitor their network that wasn't meeting their requirements. The product needed to have a single chokepoint to install a device and collect the network telemetry from. But as mentioned above, the Lake Trust network is highly distributed across multiple branches. The older product also lacked the flexibility to define custom security alerts in order to monitor for any specific policy violations.

Solution

Lake Trust deployed Cisco Secure Network Analytics (formerly Stealthwatch), a network detection and response (NDR) solution, to monitor their distributed network. The solution can collect traffic from network devices, whether they are in campus or branch locations, without the need of any agents. It then applies a combination of behavioral modeling and machine learning techniques to detect any anomalies and pinpoint critical threats.

> "[Cisco Secure Network Analytics] is truly a great product and I'm not sure how we lived without it."
>
> Steven Cruse
> Platform Engineer at Lake Trust

"Secure Network Analytics is like a microscope with an alarm—alerts have a lot of information."

Steven Cruse
Platform Engineer at Lake Trust

Results

With Secure Network Analytics, Lake Trust was able to achieve the following:

Unprecedented threat visibility

Steven Cruse, Platform Engineer at Lake Trust says, "Secure Network Analytics has really increased our security and operational intelligence. It has helped us see things how they really are as opposed to what we believed them to be. In addition to the team members we have, we now have the Secure Network Analytics "brain" helping us. It has made us smarter!"

Secure Network Analytics has alerted Lake Trust to malware and unwanted applications, even in encrypted traffic. One incident involved a large number of hosts hitting the same external IP address, that Secure Network Analytics alerted as a malware distribution host. Because Secure Network Analytics can store network telemetry for a period of time, it helped identify the activity that occurred just prior to the communication with the malicious IP—it was an external website that was being shared between employees. Lake Trust also has Cisco Umbrella deployed that blocked communication to the malicious IP. Additionally, once Secure Network Analytics identified the source of the malicious activity, Lake Trust was also able to block the external domain using Umbrella. "Secure Network Analytics is like a microscope with an alarm—alerts have a lot of information.", says Steven about the granularity and context provided by Secure Network Analytics alerts that makes them actionable.

Ensuring regulatory and business policy compliance

Lake Trust has to meet certain audit requirements as a financial institution. One of these is to ensure that it's using strong encryption protocols. Secure Network Analytics has a cryptographic compliance dashboard that provides an assessment of the "quality" of

encryption being used such as TLS version, cipher suite and more. It also helps to understand the trends and changes in the amount and type of encryption. Using this feature, Lake Trust is able to prove compliance easily. They are also able to show auditors that they have systems in place to immediately detect any malicious activity like exfiltration of sensitive data, port scanning, etc.

Lake Trust also needed to ensure that their own custom business policies were being enforced. Secure Network Analytics allows the creation of custom alerts that can be defined using multiple attributes related to network metadata and host groups. For example, the “ATM” host group should not communicate to or from the Internet.

Accelerated response with integrated security

Lake Trust has also deployed other Cisco Secure solutions such as Secure Firewall, Endpoint, Email, Umbrella, and Identity Services Engine (ISE). They have enabled the Secure Network Analytics integration with ISE that provides user and device context, and also provides custom and automated remediation right from Secure Network Analytics based on the policies defined within ISE.

Steven mentions that a typical investigation begins with a Secure Network Analytics alert, and then the incident can be narrowed down further and remediated using other tools. And now, with the built-in Cisco SecureX platform experience, Lake Trust is able to correlate and take action on alerts across multiple security controls that are well-integrated with each other. “We are such a small team, it’s not possible to go into all the tools frequently. But all the critical information is now accessible through SecureX.”, says Steven about the simplicity and efficiency of the platform. For more information on the alert seen within SecureX, one can easily pivot into the corresponding solution such as Secure Network Analytics.

> "We were able to transition the employees to work remotely and still had the same level of visibility and protection in place ... Not a lot of companies can say that."
>
> Steven Cruse
> Platform Engineer at Lake Trust

Rapid transition to a remote workforce

Like most organizations, Lake Trust has had to transition to a completely remote workforce immediately. The number of users on VPN grew by more than 20 times overnight. Lake Trust needed visibility into the VPN traffic to determine bandwidth consumption, allocation of resources, heavy VPN users, and what type of traffic or applications didn't need to go through VPN. For example, they were seeing heavy VPN traffic related to video streaming. Using Secure Network Analytics, they found that the weekly communication videos from leadership were taking up a lot of bandwidth because they were being streamed widely, and rightly so. But this type of traffic was safe to not go through VPN and so, they were able to manage the VPN utilization effectively.

Looking back on this, Steven says, "With Secure Network Analytics, we were able to transition the employees to work remotely and still had the same level of visibility and protection in place, as when they were in the office. Not a lot of companies can say that."

Conclusion

Network detection and response (NDR) solutions can uncover threats that other security tools might be missing. They provide unmatched visibility by continuously monitoring all network activities. With Cisco Secure Network Analytics, Lake Trust was able to get industry leading NDR that provided a huge amount of granularity and control over their network traffic, across all their branch locations. And with an integrated approach, they were able to extend their investments in Cisco Secure solutions to achieve end-to-end security across the network, endpoints, web and more.

To learn more, please visit:

cisco.com/go/secure-network-analytics and take our free visibility assessment.