blackpoint

BRANDX CASE STUDY:

STOPPING A VPN BREACH IN MINUTES FOR A FINANCIAL SERVICES FIRM

When attackers struck twice in one morning, Blackpoint's SOC neutralized both threats long before traditional endpoint tools raised the alarm.

As Scott Werner, owner of BrandX IT, put it: *"This just illustrates the point that it's not a single point of attack anymore, it's almost like a pre-attack attack. They went after the firewall first, then the computer."*

THE INCIDENT

A financial services firm came dangerously close to a serious breach when attackers launched two compromise attempts within minutes of each other. Blackpoint Cyber's Response Operations Center (BROC) moved fast, detecting and acting on the first VPN attack in just four minutes by immediately working with partner BrandX IT to shut it down.

But the attackers weren't finished. While remediation was still in progress, a second account was compromised. This time, within six minutes, Blackpoint had identified and contained that threat too, stopping it before it could spread. Meanwhile, the client's additional endpoint detection and response (EDR) tool didn't raise an alert until nearly an hour later, long after the SOC had already secured the environment.

"The EDR didn't alert me until 10:30, almost an hour later. Blackpoint had already seen the firewall issue and called me 10–15 minutes before anything else happened."

Because Blackpoint was watching and responding in real time, the firm walked away from the incident untouched: no downtime, no data loss, and no compliance fallout. Scott summed it up simply: "Disaster averted, no doubt.

FROM THE EYES OF THE BLACKPOINT SECURITY OPERATIONS CENTER

116

VPN-related incidents Blackpoint's SOC responded to from January to August 2025.

Attackers love VPNs because one device means instant, stealthy access.

PARTNER PROFILE

Company: BrandX IT

Type: Managed Service Provider (MSP)

Location: Evanston, Chicago

KEY DATA AT A GLANCE

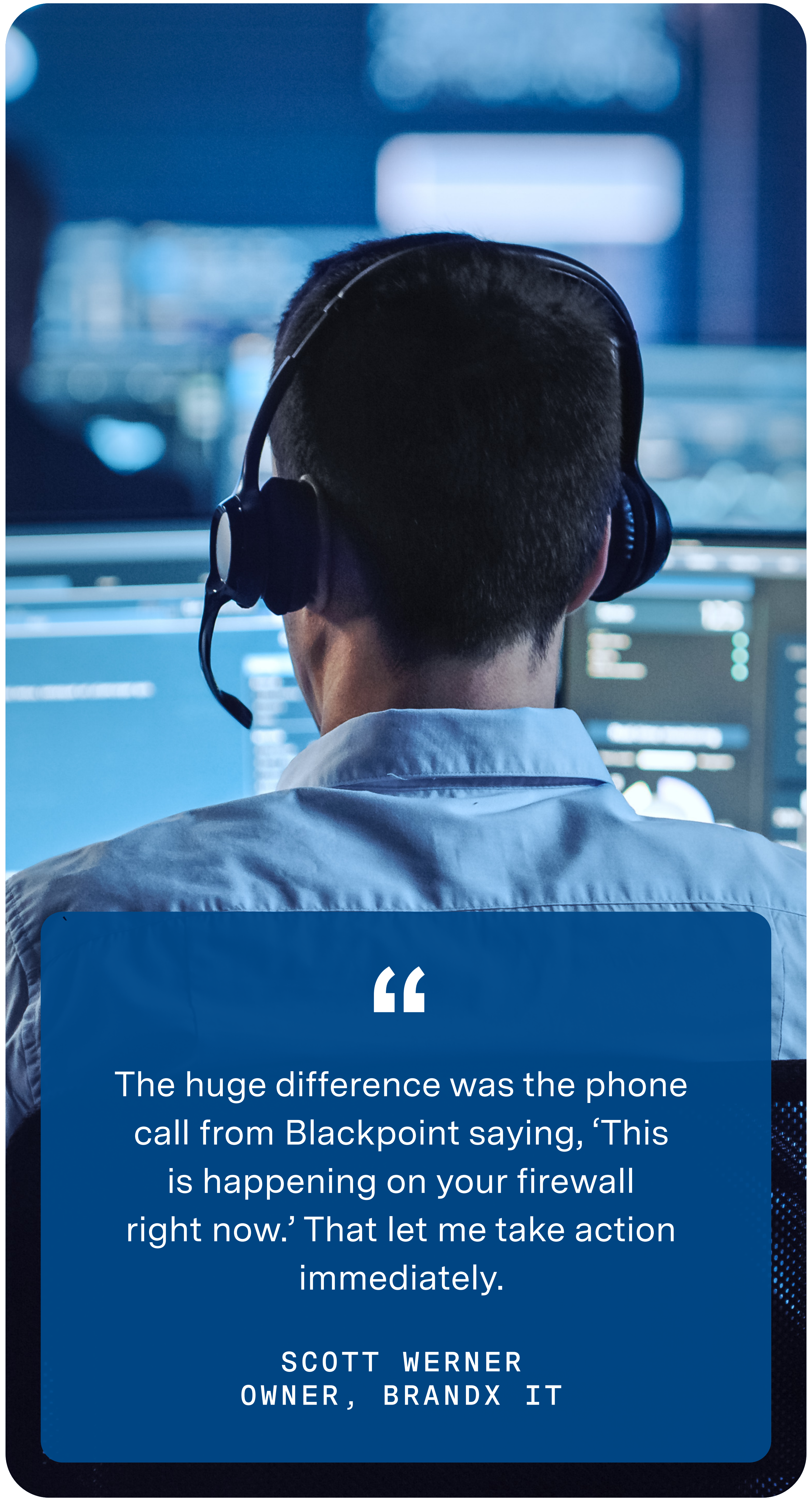
Date: August 24, 2025

Industry: Financial Services

Threat Type: VPN Compromise

Initial Access: Brute force login attempts via exposed SSL VPN

Outcome: No data exfiltration, no persistence, no downtime or disruption



> “
>
> The huge difference was the phone call from Blackpoint saying, ‘This is happening on your firewall right now.’ That let me take action immediately.
>
> SCOTT WERNER
> OWNER, BRANDX IT

WHY THREAT ACTORS TARGET FINANCIAL SERVICES:

- Average data breach cost for financial firms: USD 6.08 million, 22% higher than the global average of USD 4.88 million. [1]
- Malicious attacks remained the top attack vector in finance, at 51%. [1]
- Vulnerability exploitation as an initial vector rose to 20% of breaches, nearly matching credential abuse, the most common vector. [2]
- Edge devices and VPNs were involved in 22% of exploit-based breaches, an almost eightfold increase from 3% in the prior year. [2]

[1] Cost of a data breach 2024: Financial industry

[2] Verizon 2025 Data Breach Investigations Report

THE TWO-PART ATTACK TIMELINE

Part 1: The VPN Compromise

09:44ET Blackpoint SOC alerts on failed share attempts from compromised account, sourcing from SSL VPN.

09:45ET Escalation for suspicious scanning activity begins.

09:46ET Senior MDR analyst initiates investigation.

09:48ET SOC calls BrandX, confirms compromised account, recommends disabling account and taking down VPN.

[Time Elapsed: 4 Minutes]

At this stage, the threat actor had not yet succeeded in gaining access. Blackpoint SOC quickly engaged the partner to secure the environment, but the attack was far from over.

Part 2: The Account Compromise

11:00ET SOC detects second compromised account

11:04ET SOC isolates to contain the intrusion.

11:06ET SOC updates BrandX, confirms workstation isolation, and coordinates next steps.

[Time Elapsed: 6 Minutes]

As the attacker pivoted to a second account, Blackpoint immediately isolated the impacted device, cutting off the intrusion before it could spread. Working side by side with the partner, the SOC contained

Result

The financial services client remained essentially unaffected; no downtime, no data loss, and no compliance impact. By identifying suspicious activity in motion, neutralizing the threat, and then isolating a compromised endpoint, Blackpoint protected both the partner’s reputation and the client’s critical operations.

> “
>
> Blackpoint gives me peace of mind. I tell clients, you want me to sleep at night, this lets me do that.
>
> SCOTT WERNER
> OWNER, BRANDX IT

LESSONS LEARNED

- VPNs are still a leading attack vector. Even patched devices are vulnerable to credential-based attacks.
- Traditional EDR alone isn't enough. Alerts after-the-fact don't prevent compromise.
- Real-time SOC response saves businesses. By isolating and containing threats without requiring client involvement, Blackpoint drastically reduces downtime and risk.

This incident proves that while VPNs aren't going away, neither are the attackers targeting them. For MSPs, relying solely on endpoint detection or patch management leaves clients exposed. With Blackpoint Cyber's SOC watching 24/7, threats are stopped before they spread, protecting client trust, compliance, and business continuity.

THE BLACKPOINT DIFFERENCE

With Blackpoint SOC watching around the clock, businesses gain real-time protection that goes beyond alerts to full containment and recovery.

DETECTION

Rapid detection enables the Blackpoint SOC to secure faster than any other SOC available, drastically reducing downtime.

RESPONSE

Blackpoint SOC isolates on your behalf to ensure no matter what time of day, your business and the clients you protect are safe.

TRUE PARTNERSHIP

Blackpoint SOC works as a true partner in protection. Isolating on your behalf and working through remediation with you.

OUTCOMES THAT MATTER

With Blackpoint, MSPs avoid downtime and brand impact from a breach. Operating as a true extension of your team without the overhead.

THIS IS WHY MSPS TRUST BLACKPOINT TO HAVE THEIR BACK WHEN IT MATTERS MOST.

blackpoint

ABOUT BLACKPOINT CYBER

Blackpoint Cyber's mission is to provide 24/7, proactive, nation-state-grade cybersecurity to organizations of all sizes around the world. Through a unique combination of advanced proprietary technology and human-powered active-SOC services, Blackpoint empowers IT professionals with the industry's fastest Managed Detection, Response, and Remediation (MDR) solution, eliminating cyber threats in real time and mitigating any potential risks. Founded in 2014 by former Department of Defense security and intelligence experts, Blackpoint is deeply committed to the growth and success of the managed IT and security community and believes sophisticated cybersecurity is a necessity and should be accessible to all.

Learn more at: blackpointcyber.com

VULNERABILITY MANAGEMENT

EXTERNAL SCAN

Latest External Scan was on September 18, 2024

INTERNAL SCAN

Address vulnerabilities with Microsoft Defender for Endpoint

41% Microsoft Secure Score
2% Active Devices
404 Known Vulnerabilites

CLOUD SCAN

8 Compliant
6 Action Recon

MDR

● 4 Active
● 2 Idle
● 0 Inactive