FORTRA™

How Finance Companies Bank on Tripwire ExpertOps
Four Managed Services Use Cases for Cybersecurity and Compliance

Finance companies opt for managed services to stay compliant, bolster overburdened security teams, and get ongoing support in keeping their data safe from damaging breaches. The finance sector regularly finds itself on the front lines of emerging attack techniques; attackers commonly search for edge vulnerabilities and test new malware variations against financial systems. According to the Verizon *2020 Data Breach Investigations Report*, 63 percent of attacks in this sector were coordinated externally, 18 percent were coordinated internally, and nine percent resulted from human error[1].

However, most breaches are entirely preventable. Your security team can drastically reduce your attack surface and stay audit-ready by implementing fundamental security controls like security configuration management (SCM), file integrity monitoring (FIM), and vulnerability management (VM). All three of these core processes can be managed on your behalf with Fortra's Tripwire® ExpertOps℠, so your team can use their expertise to help run the business instead of managing security tools.

Four Tripwire ExpertOps Use Cases for Finance

Tripwire ExpertOps automates the essential processes finance entities rely on, including expert-provided configuration hardening recommendations and audit evidence. With the largest available library of supported policies and platforms and coverage for an array of OS versions and devices, there are numerous use cases large financial institutions can find in Tripwire ExpertOps.

Here are four of the most common ways Tripwire ExpertOps helps financial customers.

1. **Bolstering small security teams**
   Choosing managed services is an efficient way to quickly relieve overburdened security staff. Stretched security teams are common due to the cybersecurity skills gap. Tripwire's *2020 Cybersecurity Skills Gap Report* found that larger organizations, which one might assume have more resources, are experiencing a strain on their cybersecurity team even more acutely than smaller organizations. Ninety-four percent of

CONSOLIDATE YOUR SCM AND VM TOOLS

Financial institutions often have the same personnel on both their VM and SCM tools. Why not let a dedicated Tripwire expert manage both of these foundational cybersecurity controls? Companies using Tripwire ExpertOps receive continuous support for both controls at once, with key insights and customized guidance for the whole security picture.

> *"THE RELIABILITY OF THE FIM PRODUCT GIVES US THE CONFIDENCE TO FULFILL JUST ABOUT ANY REPORTING REQUEST COMING FROM OUR STAKEHOLDERS AND AUDITORS, WHICH MAKES OUR AUDITS GOES VERY SMOOTHLY AND QUICKLY."*
>
> **—IT VICE PRESIDENT,** FORTUNE 500 FINANCIAL SERVICES COMPANY
> TVID: 896-715-6EC

surveyed organizations said they would benefit from outside help with security processes like VM and SCM2.

The maintenance work of keeping consoles up and running day to day can exhaust a security team's time, keeping them from taking on other important tasks. Even with highly mature security teams in place, the demand for talent creates an ongoing vacuum for change as there always remains a need to train administrative staff.

When security experts leverage their expertise running your security solution, your team no longer needs to spend long hours training up or sifting through data to determine which actions to take. Instead, they can focus on more advanced practices like threat hunting, endpoint detection and response (EDR), and penetration testing.

Tripwire ExpertOps is the perfect fit for organizations that want to offload the work of console maintenance to a trusted Tripwire Managed Service Engineer (MSE). It provides stretched security teams with continuous staffing to operate and manage your Tripwire solution at peak efficiency. Your security team can perform at a much higher capacity thanks to ongoing support, guidance, and customized reporting that adapts to meet continuous objectives.

2. **Securing network device configuration**
Financial organizations have to take a particularly judicious approach when it comes to securing the configurations of their network devices. It's not uncommon for large enterprises to have individual solutions and tools for each type of endpoint on their systems.

Managing multiple databases and operating systems with various tools only complicates system hardening and attack surface reduction. If your security team currently uses solutions that only work with one type of endpoint, it may be time to consider the consolidation advantage of a managed solution. Tripwire ExpertOps, with its broad platform coverage, eliminates the need to deploy multiple tools for different endpoints

Vendor and tool consolidation is another reason outsourced managed services are becoming increasingly useful in sizable organizations. In many cases, Tripwire ExpertOps is a more cost-effective option than implementing a new tool or vendor for different types of assets and environments—including both on-premise and in the cloud.

Organizations with broad network infrastructures require continuous monitoring for unexpected changes from a known and secure system baseline. Devices like routers, firewalls, switches, servers, load-

balancers, and intrusion detection systems all require consistent management. Tripwire ExpertOps will not only keep you from needing to switch between tools to conduct this management, but also place the day to day management in the hands of a dedicated MSE.

3. **Automating reconciliation workflows**
Audit fatigue is all too common among financial institutions as well, with audit preparation and response eating up a substantial amount of security teams' time. Much of the painstaking and time-consuming work required to pass an audit comes down to change reconciliation.

The sheer volume of change occurring on enterprise-scale systems calls for automated reconciliation. Automation can greatly reduce the number of changes that need to be singled out for manual review. This means your staff will have more time to focus on those particular changes that can't be automated—drilling down into the biggest potential threats and letting an advanced tool automatically reconcile changes that don't merit a closer examination.

Automation not only aids in the more strategic use of security teams' time. It also helps create a detailed audit trail. Tripwire ExpertOps allows you to show auditors specifically which changes were associated with which tickets and what patching results were achieved as well. This makes for a smooth audit process because the documentation is generated automatically.

4. **Maintaining Continuous Compliance**
Continuous policy monitoring for critical assets keeps them safer from potential breaches and aligned with regulatory compliance frameworks. Financial entities often experience difficulty with the operational aspects of compliance.

Tripwire ExpertOps covers a wide array of compliance requirements across the globe, such as Sarbanes-Oxley Act (SOX), Payment Card Information Data Security Standard (PCI DSS), Society for Worldwide Interbank Financial Telecommunication (SWIFT), Ontario Superintendent of Financial Institutions (OSFI), and the Monetary Authority of Singapore. Additionally, it allows you to create custom policies to keep your systems in alignment with internal governance frameworks.

Summary

Financial organizations have many challenges to contend with that can be assuaged by a managed services solution like Tripwire ExpertOps. It quickly addresses their challenges at scale and with a lower total cost of ownership.

Sources

1   "2020 Data Breach Investigations Report." Verizon Enterprise, 2020.

2   Tripwire, Inc. and Dimensional Research. 2020, Cybersecurity Skills Gap Report 2020, www.tripwire.com/misc/skills-gap-survey

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.