accenture | Google Cloud

Building a Future-Ready Defense:

The Key to Cyber Resilience in the Financial Services Industry

Executive Summary

The financial sector is the most targeted industry for cyberattacks, with threat actors leveraging tactics like phishing, ransomware, and credential theft to exploit vulnerabilities and gain access to critical systems. These challenges are amplified by evolving compliance demands and the growing complexity of hybrid cloud environments. To stay secure and resilient, financial institutions need more than traditional defenses; they require an integrated, intelligence-driven security strategy that provides real-time visibility and rapid response capabilities.

Google Unified Security brings together a suite of cloud-native solutions across threat intelligence, security operations, cloud risk management, and secure enterprise browsing. Through our partnership with Google and Accenture's deep experience in the financial sector, we help clients implement and scale these tools to reduce risk, improve compliance readiness, and strengthen cyber resilience. Together, we empower financial institutions to protect sensitive data, accelerate secure innovation, and maintain trust in an increasingly complex threat landscape.

Cybersecurity Challenges in the Financial Industry

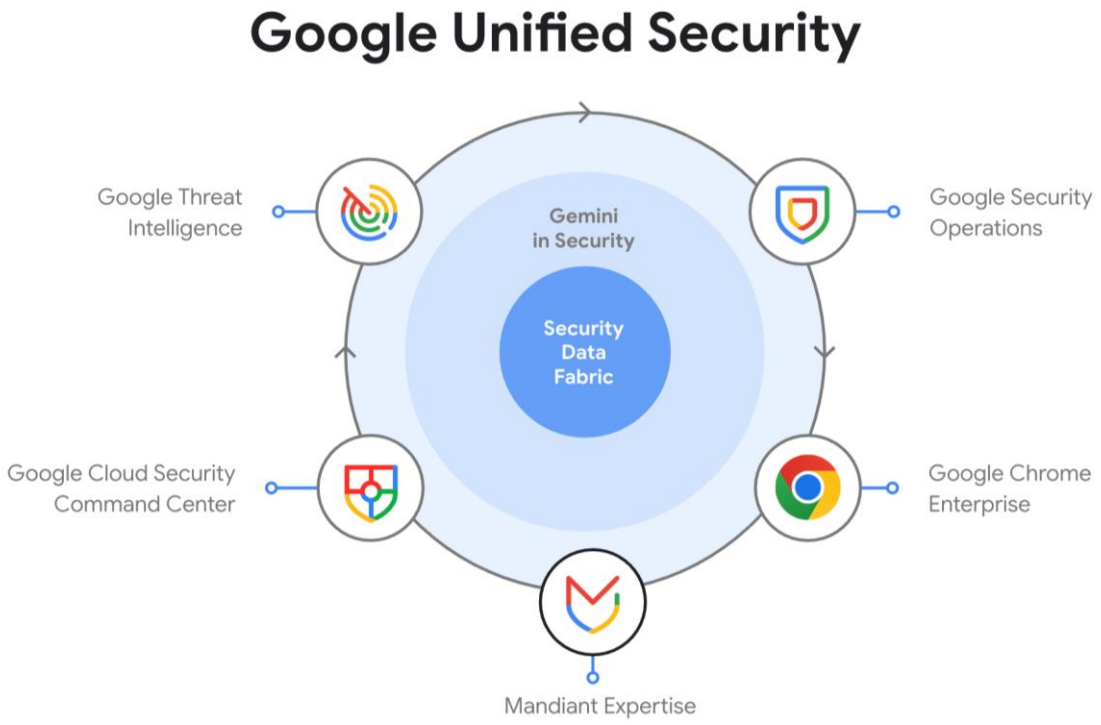
The financial industry faces a variety of cybersecurity threats, such as supply chain attacks, fraud, ransomware and DDoS attacks. According to Mandiant's M-Trends 2025: Data, Insights, and Recommendations From the Frontlines Report, the financial industry is the industry with the highest rate of targeted attack activities (17% of reported activity). Financial gain continues to be the greatest motivator, representing 35% of all Mandiant incident response investigations in 2024 and due to their high concentration of valuable financial data and sensitive data, financial organizations continue to be a prime target for cyberattacks. Implementing and enforcing appropriate security measures is a critical, ongoing challenge that is compounded by the burden of complex, stringent regulatory requirements. Organizations need to ensure that sensitive assets remain protected to ensure the security and resilience of the vital infrastructure and services they provide.

The impact of a successful cyberattack can be severe, resulting in significant financial loss due downtime, failure to meet regulatory or industry requirements, penalties associated with an incident, and loss of customer trust. Financial institutions must adopt a proactive approach to prevent and mitigate cybersecurity risks, using a multi-layered solution that incorporates threat detection, incident response, security controls and monitoring.

Protecting Against Data Exposure with Google Unified Security

For the financial industry, data exposure is a critical concern. Various factors such as deliberate attacks, human error, misconfigurations (e.g., access controls and encryption for storage, databases, or network), and vulnerabilities can ultimately result in unintended data exposure. Additionally, both malicious or accidental insider threats may result in the disclosure of sensitive customer data, intellectual property, or other financial information. According to Mandiant's M-Trends 2025 Report, exploits (33%) and stolen credentials (16%) are responsible for almost half of the initial infection vector for cyberattacks. Once attackers have compromised the environment, misconfigurations or unmitigated vulnerabilities may result in the exposure of sensitive information and data exfiltration.

Announced at Google Cloud Next 25, Google Unified Security combines threat intelligence, security operations, cloud security and secure enterprise browsing into a comprehensive security offering, enabling stronger security outcomes for customers. These products and services equip customers with the tools and knowledge they need to remain agile in the ever-evolving threat landscape, as well as have confidence in their ability to have visibility, context and control over the security risks most critical to their industry. Google Threat Intelligence, Google Security Operations, Google Security Command Center, and Google Chrome Enterprise work together within the Google Unified Security platform to provide secure solutions across various domains, including unintended data exposure. Together, Accenture and Google Cloud are using their combined expertise and technology to provide a complete security suite to enable protection and resilience against cyberthreats throughout the financial industry.



Google Security Command Center

Securing the Future of Finance with Google Cloud and Accenture

Google Security Command Center (SCC) is a native risk management platform that enables financial institutions to detect, assess, and respond to security issues across their Google Cloud environment. With continuous monitoring of assets, configurations, and access, SCC helps banks, insurers, and FinTech's protect sensitive data, demonstrate compliance, and reduce operational risk. When paired with Accenture's deep financial industry expertise, SCC becomes a foundational control for secure, scalable digital transformation.

Core Capabilities of Google SCC

Real-Time Asset Inventory

Automatically discovers and catalogs all Google Cloud resources—providing full visibility across production, dev, and hybrid environments.

Risk-Based Threat Detection

Identifies misconfigurations, exposed services, suspicious activity, and vulnerabilities using Google's native and third-party detectors.

Compliance Mapping & Monitoring

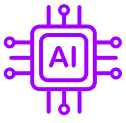
Aligns findings to frameworks like PCI-DSS, GLBA, FFIEC, and NIST to streamline audit readiness and reporting.

Path Simulation

Models lateral movement and privilege escalation scenarios to surface high-impact vulnerabilities before they are exploited.

Integrated Remediation Workflows

Delivers actionable fixes with one-click integrations to tools like Security Command Center dashboards, Cloud Console, and Security Command API.



AI Protection

Discover AI assets, implement security controls to safeguard AI systems and models, and detect and responds to threats targeting AI systems.

Addressing a Critical Challenge: Strengthening Cloud Resource Protection

In complex cloud environments, visibility gaps and misconfigurations are common culprits behind security incidents. Google Security Command Center helps proactively identify and mitigate these issues by continuously scanning for:

- Misconfigured storage buckets or compute resources
- Excess IAM privileges that exceed least-privilege principles
- Publicly exposed APIs and endpoints

By surfacing these risks in real time, SCC enables financial institutions to tighten their security posture, reduce compliance gaps, and maintain trust across digital services.

How SCC Helps

- Detects Public or Overexposed Resources SCC scans for assets like cloud storage buckets or databases that are inadvertently made accessible to the public or unauthorized users.
- Monitors Access Permissions Continuously It identifies when IAM (Identity and Access Management) roles grant excessive privileges, reducing the risk of privilege misuse.
- Delivers Real-Time Alerts and Fixes When exposure risks are detected, SCC provides instant alerts along with prescriptive remediation steps to close the security gaps quickly.
- Enterprise-Wide Visibility For organizations with multiple departments or business units, SCC provides consistent policy enforcement and security posture monitoring across all projects.

Google Security Operations

Strengthening Financial Security Operations with Google Cloud and Accenture

Google SecOps is a cloud-native, comprehensive service that helps organizations improve their threat detection, investigation and response activities to drive security operations center (SOC) modernization and adapt to the ever-evolving cyber threat landscape. Google Cloud and Accenture have partnered to develop solutions that leverage Google SecOps at its core. Through this collaboration, Google and Accenture empower financial services with a secure foundation for security operations, enabling agility and resilience while accelerating digital transformation.

Core Capabilities of Google SecOps

Google SecOps provides SOCs with a unified, proactive approach to incident response:

Data Collection

Ingest and normalize large scale raw, unprocessed network and security telemetry to enable the enrichment of events.

Threat Detection

Offers configuration and monitoring of indicators of compromise (IOCs) through curated and custom detections to provide MITRE ATT&CK coverage and enable security teams with the flexibility to adapt detections based on organizational threat model requirements.

Threat Hunting and Threat Intelligence

Leverage intelligence from Google, Mandiant and VirusTotal for threat context, enrichment, and risk scoring analytics-based alert prioritization to enable security analysts to proactively identify and quickly investigate incidents. Utilize Gemini-powered AI for natural language queries and investigation summaries with recommended actions.

Automated Response

Leverage real-time dashboards and reporting for performance and operation analytics as well as compatibility with various vendor security product integrations via the Marketplace. Utilize Gemini-powered AI for Playbook Assistant and Investigation Assistant for automated SOAR remediation playbook creation and guidance for response activities.

Addressing a Critical Challenge

Financial industry SOCs often face high data ingestion costs, slow alert response speed, and alert fatigue due to false positive rates. Delays in generating meaningful and actionable alerts leave financial institutions vulnerable to undetected threats that could result in a data breach, while excessive costs impact profitability and allocation of funds which could be used for business growth or improved security measures.

How Google SecOps Helps

Google SecOps enhances SOCs by processing petabytes of data to generate context-rich threat findings and IOCs, while offering competitive and predictable pricing to aid cost forecasting. Businesses can reduce alert fatigue through Google curated detections, high fidelity detection rules developed and tuned using best-in-class threat intelligence with mapping to the MITRE ATT&CK framework. Custom detections can be created to identify potential threats and IOCs specific to business threat model requirements. Detections provide security operations teams with actionable context and enable optimization of critical SLA/SLO response metrics, such as Time to Detect and Time to Contain, to minimize the impact of potential breaches.

Further enhancing efficiency, Google Cloud is integrating Gemini-based agentic AI solutions which will offer AI-based alert triage agents. The offering builds upon existing features like Google Threat Intelligence Endpoint Insights, Investigation Assistant, and Playbook Assistant which provide alert context, playbook and remediation automation, and guided response. With the volume of threats financial institutions are facing and the prevalence of financially motivated attacks, the operational efficiencies gained through using Google SecOps can ensure the industry remains resilient and competitive in the future.

Google Threat Intelligence

Securing the Future of Finance with Google Cloud and Accenture Google

Google Threat Intelligence delivers timely, actionable insights that financial institutions can leverage to detect, understand, and defend against emerging cyber threats. It draws on the unparalleled scale of Google's threat visibility — including insights from billions of devices and user interactions, giving security teams a real-time edge. Together, Google Cloud and Accenture enable firms to anticipate attacks, reduce risk, and protect what matters most: customer trust, sensitive data, and operational continuity.

Core Capabilities of Google Threat Intelligence

Real-Time Threat Feeds

Access tailored industry threat data — including emerging zero-day vulnerabilities, malware signatures, phishing domains, ransomware indicators, and more — sourced from Google's global infrastructure..

Threat Actor Attribution

Uncover tactics, techniques, and procedures (TTPs) used by threat actors to better understand intent and prioritize defenses.

Mandiant Intelligence Integration

Gain access to in-depth threat reports, attack patterns, and adversary insights curated by Mandiant analysts—renowned for their work in high-profile breach response.

SIEM/SOAR Integration

Integrates directly with tools like Google Chronicle to automate detection, alerting, and incident response workflows.

Customized Threat Detection

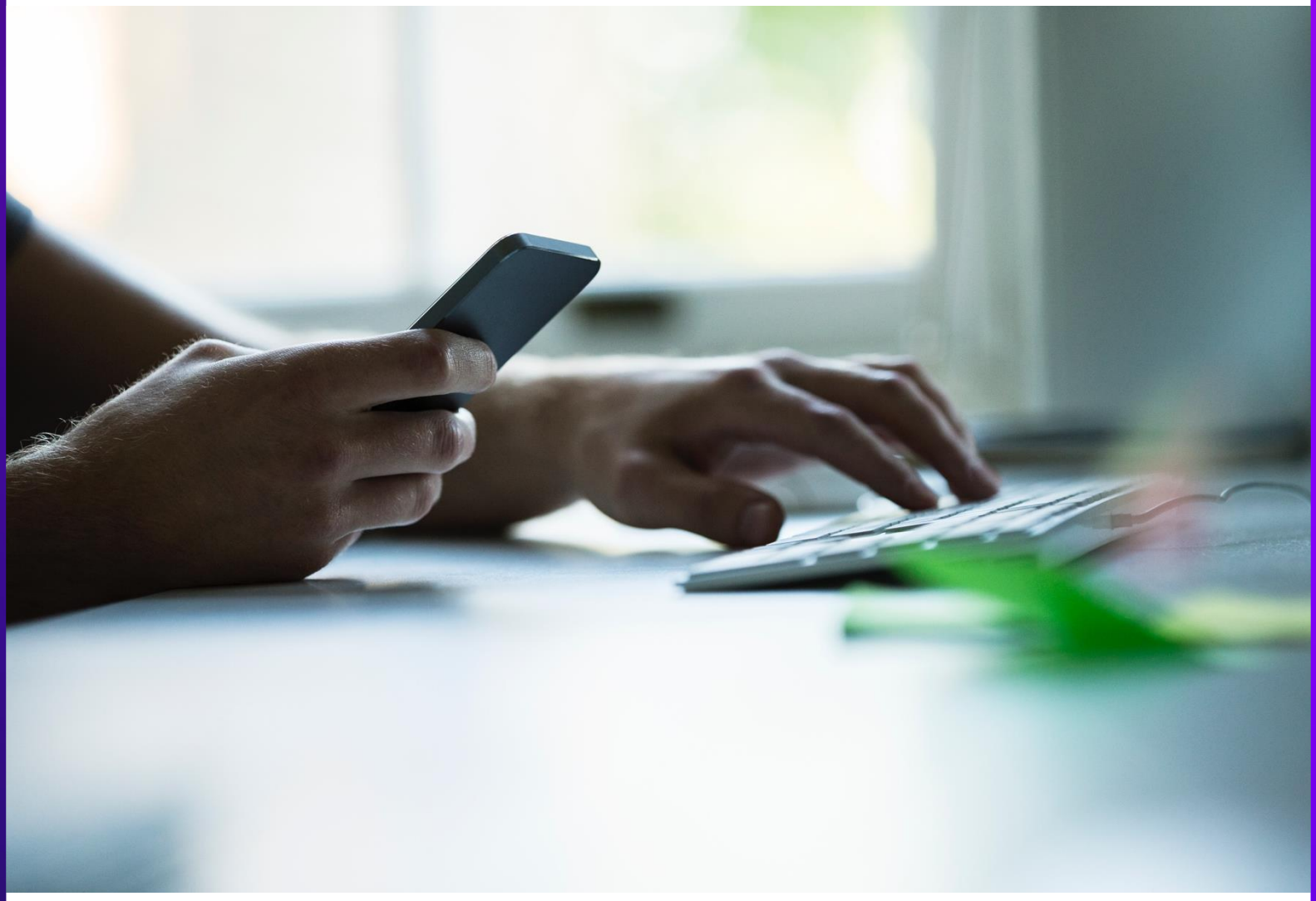
Build tailored detection rules for your environment, enhanced by Google's AI and contextual threat intelligence.

Addressing a Critical Challenge

Modern attackers use phishing, credential abuse, and zero-day exploits to move laterally and exfiltrate data — often without triggering traditional alerts. According to Mandiant's M-Trends 2025 Report, the average external entity compromised and dwelled in an organization's environment for an average of 26 days before they were detected. Security teams need real-time intelligence that reflects current threat behavior, not static rule sets.

How Google Threat Intelligence Helps

In fast-paced environments like financial services, security teams often struggle to translate raw threat data into timely, meaningful action. Traditional tools may surface isolated indicators but lack the broader context needed to prioritize and respond effectively. Google Threat Intelligence addresses this gap by combining global telemetry, behavioral insights, and adversary intelligence empowering teams to understand not just what is happening, but why, and what to do next.



Google Chrome Enterprise

Enhancing Browser Security with Google Cloud and Accenture

Google Chrome Enterprise is an offering for the Chrome browser that provides organizations with advanced security, management, and productivity features. IT teams can easily manage browser policies, settings, applications, and extensions across Chrome-enabled devices through its centralized, cloud-based administrative console, which also provides robust reporting in areas such as browser versioning, installed extensions and security events. Through Google and Accenture's partnership, the financial services industry can access secure solutions to defend against web-based threats while ensuring sensitive data remains protected.

Core Capabilities of Google Chrome Intelligence

Google Chrome Enterprise offers a comprehensive security solution for secure Chrome browser deployment and management with advanced security features and centralized administrative IT controls. There are two tiers available:

Google Chrome Enterprise Core

(no additional cost)

Includes centralized fleet management through the cloud-based Google Admin console, basic browser security controls (e.g., updates, configuration policies, Google Safe Browsing), password protection, basic reporting (e.g., browser versions, installed apps, extensions and security events), and third-party integration compatibility.

Google Chrome Enterprise Premium

(per user, per month billing rate)

Includes Core features, plus enhanced data loss prevention, zero-trust context-aware access, URL filtering, advanced real-time malware and phishing protection with deep scanning, advanced security insights and reporting (e.g., high risk users, suspicious data transfers, and password reuse), and an evidence locker for suspicious files.

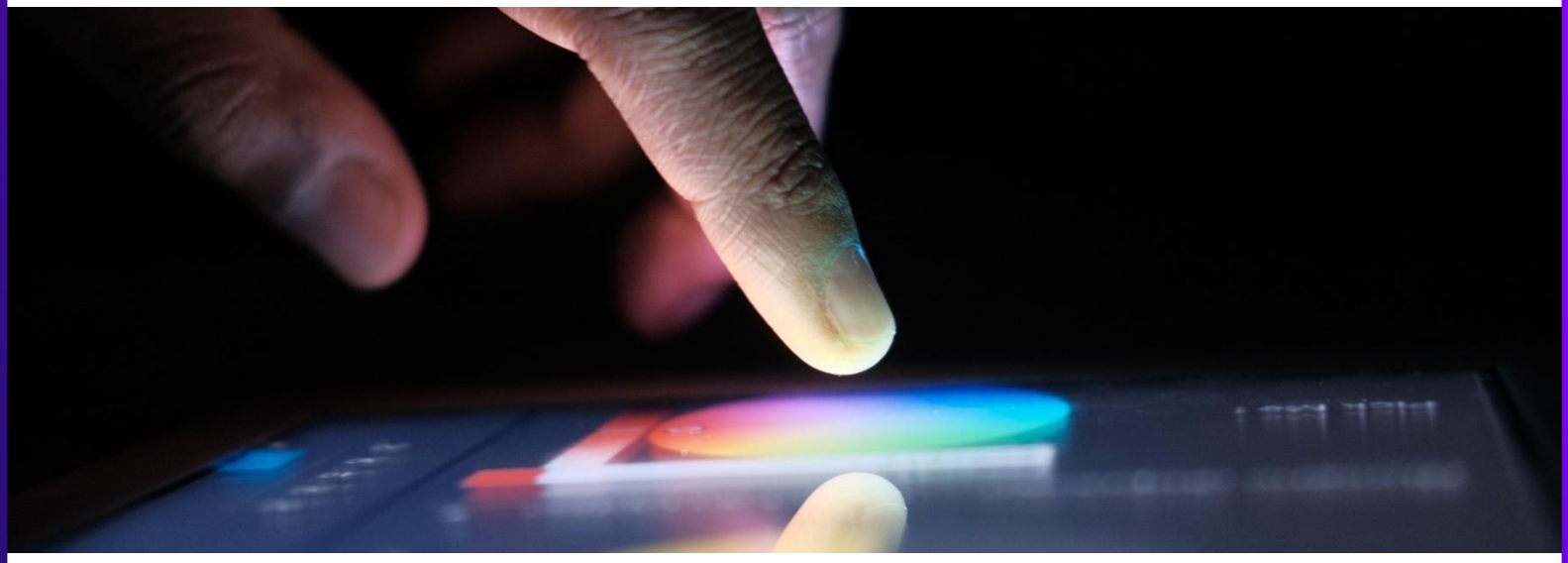
Addressing a Critical Challenge

Financial institutions face an increased threat of sensitive data exfiltration and browser-based attacks. With the prevalence of remote and hybrid workforces, businesses need security solutions that are easy to deploy regardless of location. These solutions must include robust protection and enable comprehensive reporting and response activities to prevent intentional or accidental data exposure. Without sufficient security controls, financial organizations are at an increased risk of costly data breaches, regulatory non-compliance, and loss of customer trust.

How Google Chrome Enterprise Helps

Google Chrome Enterprise provides the financial services industry with solutions to address sensitive data loss and browser-based attacks. Configurable data loss prevention rules combat sensitive data exfiltration by restricting unauthorized actions such as copying data into apps and websites. It enhances security for remote and unmanaged devices through policies to prevent unauthorized file transfers and enabling secure, context-based access to resources without a VPN. With Google Safe Browsing and real-time scanning, Google Chrome Enterprise can proactively warn users of malicious sites and guard against malware, protecting the workforce against potential threats. The offering also provides insight into high-risk users, domains, and data protection events, enabling security operations teams to quickly identify and remediate risky activities that could result in potential data exposure.

When combined with Google SecOps, security operations teams gain deeper visibility into suspicious browser activity, enabling near real-time detection and remediation of threats related to malicious extensions or potential data leakage. With Google Chrome Enterprise, financial institutions can protect sensitive data, defend against cyberattacks, and maintain compliance in a highly regulated environment while minimizing financial and reputational damage from breaches.



Accenture and Google

Accenture is the world's largest security services company, and we have a deep understanding of Google Cloud Security. Accenture aims to help clients in making and executing cybersecurity as an established business priority to enable and protect their business via Google Cloud by leveraging our longstanding partnership with Google Cloud. Earlier this year we were named Google's 2025 Global Service Partner of the Year.

Accenture's vision is to continue to be Google's #1 strategic business partner, helping Google Cloud Security to continue to capture market share and drive material growth in our joint business.

As you consider the insights and content presented in this whitepaper, we invite you to reflect on the following questions to evaluate the suitability of the Google Unified Security Platform for your financial organization and how Accenture can be your trusted partner in this integration.

1. What are the primary cybersecurity challenges your financial institution is currently facing and how can the Google Unified Security platform address those challenges?
2. Are you confident in your organization's ability to meet the complex and evolving cybersecurity challenges and regulatory requirements without gaps in security or compliance?
3. Do your current security solutions provide real-time visibility, actionable insights, and automated remediation capabilities across your environment?
4. Would having an integrated solution that combines threat intelligence, security operations, cloud risk management, and secure browsing streamline your security operations and enhance protection?
5. How could an end-to-end approach to cybersecurity, integrating proactive threat intelligence, AI-powered automation, and cloud-native security solutions, help your organization securely accelerate digital growth?
6. How could partnering with a trusted adviser like Accenture enhance your team's ability to implement, scale, and customize Google Unified Security for your specific needs?
7. Would Accenture's deep expertise in the financial industry and robust managed detection and response (MxDR) capabilities align with your cybersecurity and digital transformation goals?
8. What would be the advantages of leveraging Accenture's MxDR platform, powered by Google SecOps, to modernize your Security Operations Center and reduce costs associated with false positives and slow incident response times?

Conclusion

As cybersecurity threats continue to evolve, financial institutions need trusted partners who can help them stay ahead of risk while enabling innovation. Accenture's deep expertise in Google Cloud security solutions, combined with our proven experience in the financial sector, allows us to guide organizations through complex challenges with clarity and confidence. Together with Google, we deliver integrated, future-ready security strategies that go beyond compliance to support long-term resilience. Our close collaboration ensures clients benefit from cutting-edge capabilities and a higher level of strategic insight helping them protect what matters most while confidently advancing their digital transformation.

What's Next

For more information on Accenture's Managed Detection and Response Offering (MxDR) visit this link.

For more metrics and information from Google's Mandiant M-Trends 2025 Report, visit this link.

To learn more about Accenture and Accenture Security, visit this link.

To learn more about Accenture and Google's partnership, visit this link.