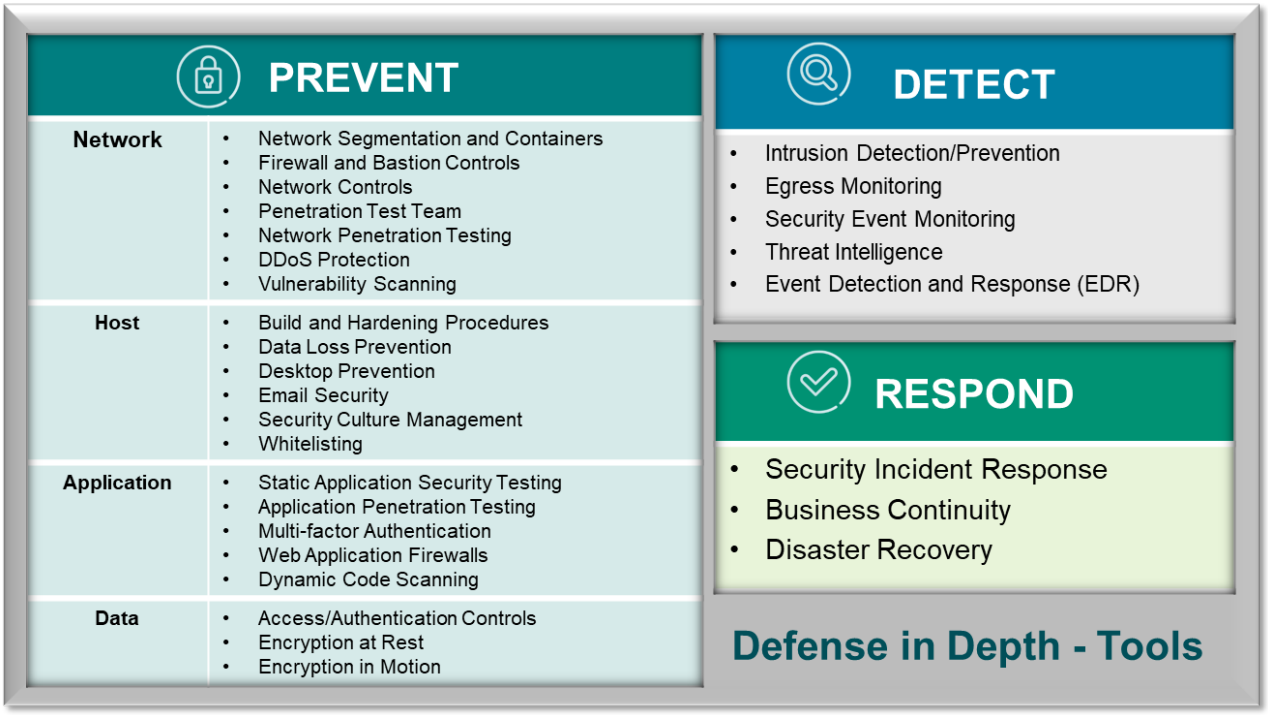
Defense in Depth Strategy

2021

At FIS, our priority is to protect our clients' data and financial interactions. We realize cybersecurity has no end state and are constantly improving our services and security to stay in front of the ever-changing industry threats.

FIS employs a defense-in-depth strategy by putting multiple compensating controls into place to protect our clients' data from malicious activity. These combined efforts, sorted by their purpose to prevent, detect, and respond, demonstrate our approach to threat mitigation.

These activities are monitored and governed by our Risk, Information Security and Compliance (RISC) organization. For more information on the FIS RISC group, see the RISC Overview document on the FIS Client Portal Vendor Management Resource Center.



Prevent

Network Segmentation and Containers

Network segmentation segregates production networks from non-production networks

FIS utilizes a container model for segmenting network environments from each other. Each container provides a separate set of security zones (e.g. DMZ, Application, Data) so that all aspects of the container are separate from each other. FIS has two different business models that drive our container strategy: an application service provider and a hosting provider. In the application service provider example, we host a variety of products and applications to service multiple customers. FIS creates containers for these various applications either by likeliness or by financial risk. On the hosted model, each customer resides within its own dedicated risk container for delivery of their products and services. This model reduces risk between products and delivers a more secure environment for our customers.

Firewall Controls

Firewall Controls

FIS has implemented a layered approach to our firewalls to control communication between environments. Firewalls define what communication is allowed or blocked to assist in controlling access to Company or client data. FIS blocks all communication by default, and then only allows what

communication is needed between environments. FIS meets industry or regulatory review requirements by performing periodic rule-recertification to identify unused or permissive rules that are no longer warranted for refinement or remediation purposes. This approach ensures implementation of least privileged network access with appropriate reviews for oversight and governance.

Bastion Controls

Bastion Networks and Hosts

FIS utilizes a bastion model to support the various segmented network environments which FIS calls containers. This bastion model is not only used for support purposes but also management and monitoring of privileged access to systems residing within the segmented environments. Bastion access is provisioned on a principle of least privilege in that only appropriate personnel are authorized to authenticate and utilize bastions for the specific segmented network. This model ensures a secure access method to support our various customers' production environments by eliminating the risk of direct access from our internal corporate network.

Network Controls

FIS Utilizes Various Network Controls

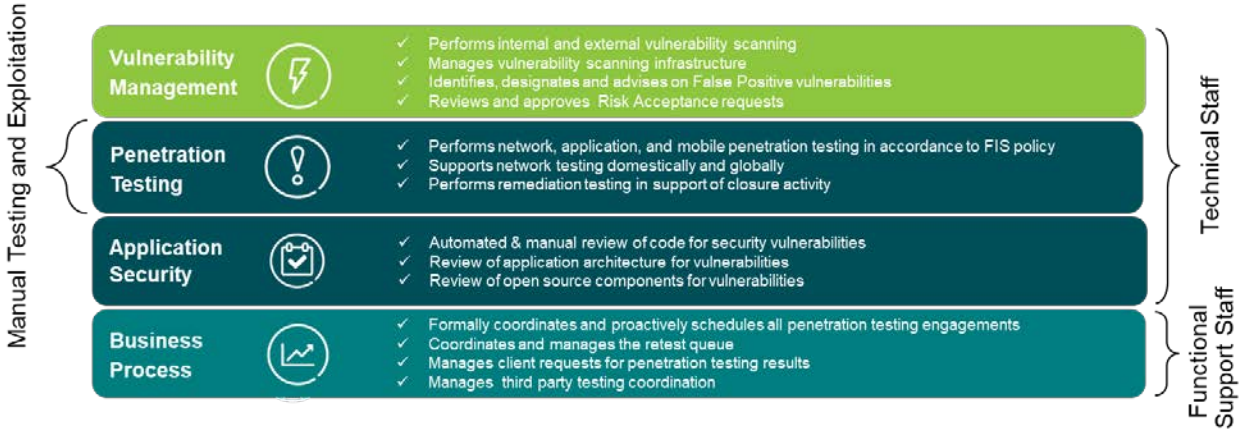
FIS deploys a variety of network controls such as IDS/IPS, IP reputation, NAC, incident response, behavior analysis, as well as forward and reverse proxies among others. In addition to the network segmentation and firewall controls, these combined tools provide additional defense in-depth to policing the network transport for inappropriate or malicious intended traffic.

As a complementary control beyond the intrusion prevention system technology, FIS regularly monitors several security industry sources that track known malicious IPs /address ranges. These IP ranges are regularly added to a blocking rule in the network perimeter firewalls as an added security measure.

Penetration Test Team

PTT program focuses on FIS network segments and applications

Reporting by the Chief Information Security Office, the FIS Penetration Test Team (PTT) has responsibilities ranging from functional program management to advanced penetration testing. The Penetration Test Team is responsible for testing the enterprise-wide deployment of network and application environments to identify current and emerging vulnerabilities. This program focuses on FIS network segments and applications and prioritizes systems that are internet-facing, perform electronic delivery of sensitive information, and/or process payment transactions.



The PTT is continually trained and educated in the latest techniques and technologies. Team members hold many of the top industry certifications (Certified Information System Security Professional, Certified Ethical Hacker, Certified Information Security Auditor, Global Information Assurance Certification Penetration Tester, etc.) and are active participants in the Information Security community. Where appropriate, FIS employs outside testers and expertise.

Application and Network Penetration Testing

FIS follows penetration testing industry best-practices including NIST, OWASP and PCI

Penetration testing is designed to demonstrate risk realization of security vulnerabilities by attempting to exploit them from the perspective of a malicious attacker. Penetration testing includes leveraging automated and manual tools to attempt to find complex and obscure vulnerabilities. This activity allows FIS to proactively respond to web application, network, and system level threats by identifying how single vulnerability instances can be further exploited.

Our network penetration testing includes internal and external assets and are conducted annually. Our methodology is based on the NIST standards and SANS guidelines.

Our application penetration testing includes web-based, internet or internal facing, 3rd party owned or hosted applications, FIS hosted, Critical or High-risk applications where FIS owns the control testing responsibility. The application penetration testing program was developed in accordance with industry wide best practices, including those detailed by National Institute of Standards and Technology (NIST), the Open Web Application Security Project (OWASP), the Payment Card Industry (PCI) Security Standards Council, and FIS' own risk assessment.

Penetration testing is performed, at a minimum, annually for all in scope applications and network infrastructure.

DDoS Protection

DDoS mitigation includes Internet service provider engagement, third party scrubbers and intrusion prevention system adjustments

FIS' systems are continually evolving in their sophistication for log and event correlation and analysis. It is widely known that all Internet-facing infrastructures are under a constant onslaught of attack from a variety of automated tools, as well from targeted attacks. When a real and credible alert is received, it is evaluated, and FIS assembles the appropriate response teams. During this phase, technical and communication bridge lines are initiated to identify mitigation and communication steps to client. Steps to alerts include:

- Identify intended targets
- Notify intended targets
- Block traffic
- Engage Mitigation Steps
- Monitor and adjust

Mitigation steps can include engaging appropriate Internet Service Providers (ISPs), third party DDoS scrubbers, adjusting our intrusion prevention systems (IPS) and contacting law enforcement. FIS has worked with our Internet Service Providers to insure our border gateway protocol (BGP) peer addresses are not accessible on the general Internet to prohibit distributed denial of service attacks against our peering routers.

For more information on FIS DDoS Protection, see the DDoS Preparedness document on the FIS Client Portal Vendor Management Resource Center, under the RISC category, Information Security section.

Build and Hardening Procedures

FIS engineered interoperability between four key enterprise functions surrounding the management of a hardened device. We then call that device “hardened” against attack.

FIS has an enterprise build standard and hardening procedures for networks, Windows, UNIX and Linux. We enforce these standards through layered controls. In general, the build process requires a series of checkpoints where validation of the key controls are vetted by external groups and scanning. These newly built devices are released into operation only after validation. Once in operation and on the network, these devices are scanned and interrogated regularly to sustain a hardened environment. The scanning checks include vulnerability detection, operating system end of life, anti-virus, anti-malware, white listing, security logging, local account compliance, and patch currency. Group policy is used to facilitate centrally managed settings like domain password policy compliance/enforcement, and the global remediation of configuration related vulnerabilities. These central global policy objects are reviewed and updated quarterly to ensure compliance with FIS security policies and principles.

FIS has engineered interoperability between several key enterprise functions surrounding the management of a hardened device. Asset management, endpoint controls, the product, application, and services inventory, vulnerability management, and change and incident management are all integrated to provide a 360-degree view throughout the life of an asset. With this deployment, management and reporting for business lines are centralized, facilitating the use of common process and best practice across the enterprise.

FIS’ build standards and procedures are based around the Center for Internet Security (CIS) benchmark standards. The content surrounding configuration and build practices are treated as confidential to protect against exploitation of our security and the security of our clients and their customers. Therefore, FIS does not distribute these standards externally.

Data Loss Prevention (DLP)

FIS deploys a Data Loss Prevention (DLP) tool to not allow writing out to external media.

FIS achieves DLP through multiple controls employed in differing combinations across the enterprise. Individual controls are designed to address specific areas of security. Examples of these controls include, but are not limited to, end-user DLP policies that protect against unauthorized data transfers initiated from end user workstations, restrict the use of removable media (for those allowed to use removable media, content policies will block writing of sensitive data to removable media, i.e., non-public information, personal health information, and Payment Card Industry information), and controls around email services to secure and encrypt data. Additional controls include full disk encryption and strict access controls in multiple forms to prevent unauthorized access to data.

Desktop Protection

Desktops are protected by nine different agents

FIS desktops are protected by various PC-based agents that monitor for zero-day attacks and encryption, prevent installation of malicious software, prevent data exfiltration, and create forensic images. Employee Internet access is monitored – even when off the FIS network. FIS desktop security controls include disk encryption, patch management, antivirus, DLP, application whitelisting, NAC, forensics and digital investigations among others.

Email Security

FIS utilizes multiple means to send secure email. As a corporate solution, FIS has deployed Office 365 which allows employees to easily send an encrypted email to deliver confidential business communications with enhanced security. FIS also has established forced TLS partnerships with many of our clients. This gives our clients another secure layer in email communication. TLS is server-to-server session encryption which all modern email security products support. This eliminates the need for any additional encryption mechanism and secures messages in transit.

Security training occurs at relevant touch points

Security Culture Management and Employee Training

The “Think Secure. Be Secure.” campaign promotes the continuation of FIS' risk and security culture and enforces compliance with security standards by integrating baseline secure activities into the everyday lives of employees. Employees are presented with training at relevant touch points throughout the year including online training, phishing exercises, just-in-time training, table-top exercises and printed material.

Whitelisting

Software, when appropriate and available for the different versions of Unix, allows for lockdown of application use and executable files based on appropriate business and operational requirements. Whitelisting is also instituted on Windows servers and desktops. The tool also disallows changes to servers and desktops at an operating system level by blocking unapproved software from executing.

FIS application security controls are tested through a variety of means

Static Application Security Testing (SAST)

Each application contains security controls which are tested through a variety of means, including static code analysis. All code is scanned prior to the release of the code to production. FIS software code is scanned with a top industry static scanning tools that supports industry standard rules which includes Open Web Application Security Project’s (OWASP) Top 10 vulnerabilities, SANS Institute / Common Weakness Enumeration (CWE) Top 25 among others.

Access is reviewed and verified quarterly

Logical Access/Authentication Management

Logical access management plays a key role at FIS. Access to data and information technology resources is restricted through the assignment of user credentials to employees who have been granted authorization privileges by FIS management based on the individual’s job responsibilities. Accounts and their associated rights are created, managed, disabled, and deleted throughout the account’s lifecycle and as accounts are created, access is determined by the principle of least privilege. Password change frequency is maintained and governed according to FIS password requirements. An account’s lifecycle is closely monitored as it advances through many stages from provisioning to authentication, authorization, verification, and de-provisioning. We have oversight of all user’s access through our quarterly access reviews. These entitlement reviews ensure that a user’s access to systems is current and still applicable based on their role and responsibilities. These reviews are conducted by management and/or resource owners, then validated by our Information Security Team. Privileged access is logged and alerted on for all infrastructure using our SIEM.

External environment scanned weekly

Vulnerability Scanning

Vulnerability scanning is primarily focused on identifying insecure system configurations, vulnerabilities due to missing security patches, or the use of outdated software on internal or external hosts. Scanning consists of automated testing targeting internal and external hosts. FIS currently scans external hosts weekly, internal hosts monthly, upon server build request, and ad-hoc to support remediation processes. Over 500,000+ IPs are scanned monthly.

Change Management

FIS employs a systematic approach to implementing system software, infrastructure and application changes. This also includes change to the logical and physical security components of our environment. FIS has developed a standard change process that includes key control points to help ensure changes are controlled and managed in a consistent manner. Additionally, an independent Change Management team exists to oversee and enforce the Change Management process as well as apply final approval of change. The change process and tools support and enforce segregation of roles in the implementation of change.

Detect

Intrusion prevention systems and Internet egress network analysis services identify malicious traffic

Intrusion Detection/Prevention

FIS has deployed network intrusion prevention and detection systems (IPS/IDS) across the network to monitor network and system activities for malicious activity. The IPS/IDS systems provide a key control layer at the network perimeter and between data centers to identify malicious activity, log information about this activity, attempt to block or stop the activity, and report on it.

Egress Monitoring

FIS subscribes to a service for Internet egress network traffic analysis which helps identify potential intruders' activities in near real-time. The service also provides additional capabilities to detect high-fidelity events or actionable items that may not be detected by other standard security tools including discovering exfiltrated data attempts and command and control attempts.

Security Information and Event Management solution provides correlation and cross reporting capabilities

Security Event Monitoring

FIS collects and stores our systems and network devices logs within a Security Information and Event Management (SIEM) solution. The solution provides correlation and cross reporting capabilities, effectively providing a better means of seeing a holistic picture of security activity. The SIEM enables FIS to proactively investigate security anomalies, malicious and/or out-of-policy activity, and identify potential threats for necessary triage. The SIEM team is a 24x7 operation.

FIS has strong relationships with law enforcement and the FS-ISAC

Threat Intelligence

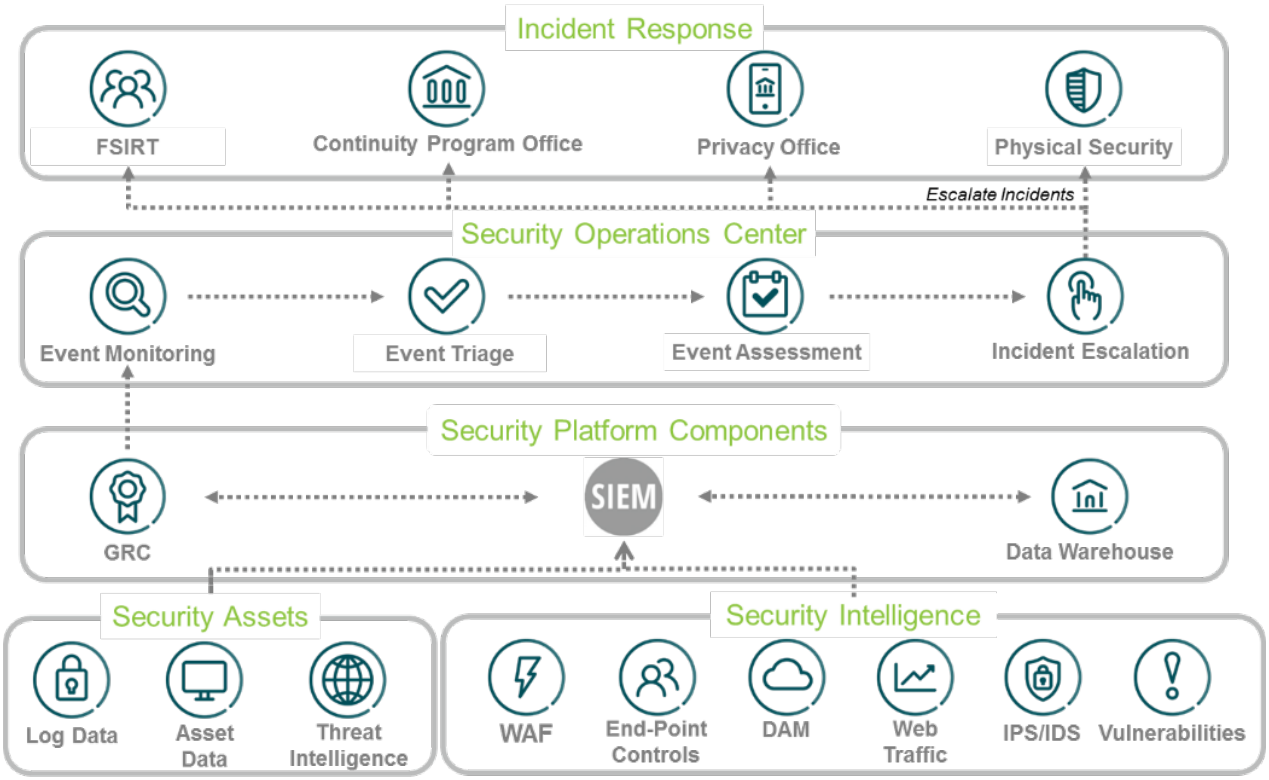
The FIS Threat intelligence unit maintains established relationships with our financial sector partners, the Financial Services – Information Sharing and Analysis center (FS-ISAC), law enforcement, and various intelligence and information security communities. FIS has relationships with the US Secret Service, the Department of Homeland Security National Cybersecurity and Communications Integration Center, Interpol, the United Kingdom's National Crime Agency, the US State Department's International Law Enforcement Academies, the Federal Bureau of Investigation, the Overseas Security Advisory Council, and the Domestic Security Alliance Council. FIS is one of five financial services institutions to formally partner with the Cybercrime Center. The FIS Threat Intelligence Team provides operational, strategic and actionable intelligence to multiple groups within FIS which enables us to prepare for potential future events. Any findings are reported to management and appropriate internal parties, as necessary.

Respond

FSIRT

The FIS Security Incident Response Team (FSIRT) is a specialized group that investigates, contains, prioritizes, mitigates and resolves potential and actual security incidents. FSIRT's mission is to proactively manage cyber risks to improve FIS's security posture. FIS employees are to report security and privacy incidents to the FSIRT, which include violations or imminent threats of violations of security, privacy, acceptable use policies and standard security practices. Security controls also send notifications to the FSIRT. Team members have skills including incident response, computer forensics, malware analysis, code development and data mining. Findings are reported to management and appropriate internal parties, as necessary.

For more information on the FSIRT see the Information Security Incident Response Plan on the FIS Client Portal Vendor Management Resource Center.



Global Business Resilience Program

Recovery plans are exercised and evaluated annually

At FIS, resilience is a continuous process of assessing, planning, training, exercising, and finding new ways to improve how we operate.

FIS' Global Business Resilience (GBR) organization employs a "best-in-class" program that puts seamless continuity of operations at the forefront. The organization's global footprint provides a framework for building organizational resilience and response.

The GBR Program ("Program") is managed and conducted by a team of knowledgeable and experienced staff with a single mission to ensure "business as usual" in unusual times. All FIS entities are required to comply with this global program.

The Global Business Resilience leaders support the Program strategy and execution which is pre-planned; and follows documented procedures. The Policy Owner is the Chief Risk Officer and the Program Owner is the Chief Information Security Officer. FIS' governing committees periodically review and approve the Program's Policy, annual performance, and progress. Oversight of the Program is provided by the Risk Committee of the Board of Directors, and the Enterprise Risk Technology Committee (ERTC). Independent assurance of the Program is provided by internal and external auditors. ISO Audits are conducted annually, and consultants are engaged periodically to assess the program and provide recommendations to raise the program's level of maturity.

Staff and resources are allocated to these disciplines within GBR:

- **Crisis Management (CM)** focuses on emergency response and management of incidents that threaten life, property, operations, our clients, products/services, or FIS' brand.
- **Business Continuity Management (BCM)** prepares for the continuation and recovery of business processes and functions. This discipline ensures that business process dependencies, potential impacts, and risks of a business disruption are identified and mitigated through the development and exercising of robust Business Continuity Plans (BCPs).
- **IT Disaster Recovery (ITDR)** is responsible for alignment of recovery requirements to recovery capabilities, identification and mitigation of IT service recovery risk and exercising.
- **Third-Party Resilience (TPR)** Due to our unique role as a service user and service provider, the third party resilience team covers two areas: 1) they conduct enhanced due diligence of critical third-party vendors and integrate them into FIS' wider continuity recovery testing regimes; and 2) provide Subject Matter Expertise (SME) in representing GBR during interactions with clients, prospects and contract negotiations.

Contact Us

For more information, please visit the FIS Client Portal Vendor Management Resource Center or contact the FIS Client Risk Relations Team at client.risk.relations@fisglobal.com.