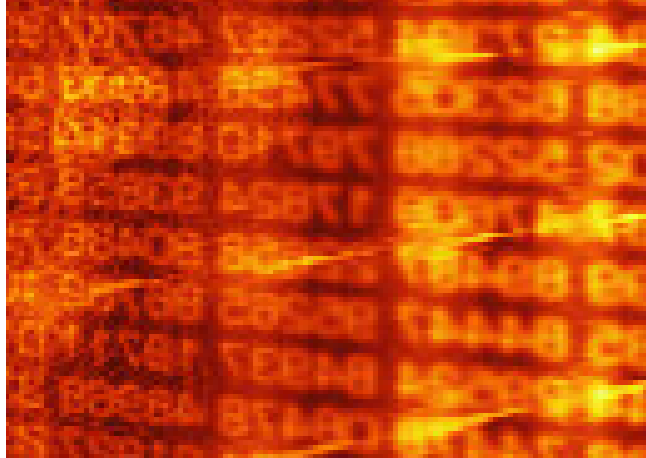


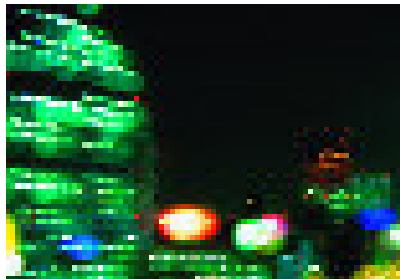
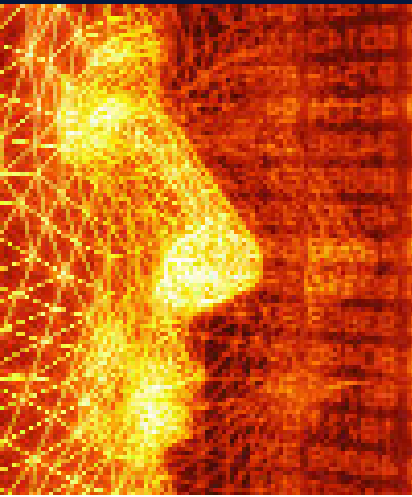
ENTERPRISE SECURITY SERVICES



Your core business depends on information technology. This dependence places demands on management to address data security (customer and corporate), regulatory requirements and Sarbanes Oxley accountability, among other issues. Fidelity Information Services executes a comprehensive security program that assures the integrity, confidentiality, availability and control of company and client data.

BUSINESS CHALLENGES

- Balancing interoperability and security for access to corporate assets
- Looming external (e.g., Internet) and internal (e.g., disgruntled employee) threats
- Regulatory mandates require substantive action
- Exponential increase in the number of individuals determined to exploit your corporate assets
- Reactive mitigation assures imminent failure, and is no longer an acceptable business practice
- Uncontrolled access or misplaced corporate assets leave your most valuable resources exposed
- Protecting information for an increasingly mobile workforce presents new and unique threats to guard against



ENTERPRISE SECURITY SERVICES

THE SOLUTION

Fidelity's Security Services ensure the availability and integrity of systems supporting some of the nation's top financial institutions. Other commercial enterprises dependent on data security for their reputation and viability of their core business also rely on Fidelity's Security Services. Staffs certified in multiple disciplines combine to provide a secure environment for your company's vital data resources. This includes expertise in information security, network and internet security, project management, RACF and other security applications. Proven processes and disciplines include: security patch management, directory authorization and authentication, firewall and router management, scanning and remediation, and intrusion detection.

Experience and infrastructure allow Fidelity to:

- Centrally deploy and manage anti-virus applications
- Firewall architecture, deployment, configuration, management and reporting
- Monitor and manage network and host intrusion sensors
- Proactive vulnerability scanning, reporting and mitigation management
- Manage mainframe RACF logical security access instances
- Manage UNIX & Windows servers for logical security access

DESCRIPTION OF SERVICES

• **Architecture, Design, Management, Implementation of:**

- Network and Host Intrusion Detection
- Penetration Testing
- Scanning and vulnerability reporting
- Automated virus protection
- Proactive security industry awareness
- Incident Management

• **Scanning, assessments and reporting.** Periodic vulnerability scanning and remediation management of servers located in Fidelity technology centers and on customer networks.

• **Firewalls and Perimeter Protection.** Best practices in design, implementation and security protection for all devices. These include leveraging existing firewalls, Internet DMZ modules, Intrusion Detection systems, anti-virus and patch management.

• **Incident Handling.** Fidelity stands accountable on all incidents (virus, email, network, worms, etc) of security penetration risk. This includes assessment, trouble shooting, mitigation and event analysis.

• **Auditing.** Fidelity leadership for all activities regarding audits and/or customer security inquiries.

• **Critical Vulnerability Remediation.** Fidelity Security manages critical vulnerability remediation alerting, procedures, process and timelines to limit data loss or damage that result from virus, worms or malicious intent.

• **EPO, Anti-Virus.** Fidelity provides expertise to plan, architect, deploy and manage an automated virus protection solution.

• **SOX and Regulatory Management.** Fidelity Security works as a key participant and contributor to customers' Sarbanes Oxley and other regulatory remediation projects. Our experience in the heavily regulated banking industry uniquely positions Fidelity to understand and solve your business challenges.