

A SECURE DESTINATION FOR CONFIDENTIAL DATA

Evolving technology makes it increasingly easy to do more with less, particularly with cloud based services. As organizations consider new cloud options, which vendor can be trusted with the most confidential data and what should be looked for in terms of security in the cloud?

Data growth and associated storage costs are becoming increasingly problematic to organizations that are coming to the conclusion that maintaining their own storage infrastructure is not sustainable in the longer term.

Understanding how data and services are secured in a cloud based IT environment is of great importance to organizations if they are to benefit from the new cloud possibilities on offer. Moreover different cloud vendors approach and commitment

to security should be high on the list of qualifying factors in the decision making process.

nScaLED is committed to providing a secure destination for the most confidential of client data and our commitment to this goal is a key differentiator over competitive offerings.

Physical Data Centers

nScaLED only makes use of SAS-70 (Type 11) certified data center providers for physical infrastructure. Each provider is carefully selected based on strict criteria for service levels, financial stability, equipment choice, security protocols and certification, service outage history and other factors.

SAS-70 Certification (Type II)

Statement on Auditing Standards (SAS) No. 70, Service Organizations, is a widely recognized auditing standard developed by the American Institute of Certified Public Accountants. A service auditor's examination performed in accordance with SAS No. 70 represents that a service organization has been through an in-depth audit of their control objectives and control activities. In a Type II report, the service auditor will express an opinion on whether the controls that were tested were operating with sufficient effectiveness to provide reasonable assurance that the control objectives were achieved during the period specified.

Physical Security of Data Centers

- All data centers employ biometric scanning protocols and round the clock interior and exterior surveillance monitoring
- Only authorized personnel are granted access credentials
- All personnel undergo thorough background security checks before they are hired
- Data centers are unmarked buildings to maintain a low security profile

All hardware within data centers is 100% dedicated to our services. Collocation personnel do not have password access, do not do any software based maintenance and are not aware of where or how nScaLED provisions clients or data across physical resources.

Connectivity

nScaLED data centers do not serve web applications to the public Internet. The only way to access the nScaLED cloud is through either dedicated private lines, or over secure IPsec VPN connections. Our data centers are an extension to each customer's internal LAN environment.

This is a key differentiator over other public cloud providers that commonly serve thousands of applications to the Internet and present a different security profile to the common, internal LAN environment.

IPsec

Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPsec can be used to protect data flows between a pair of hosts (e.g. computer users or servers), between a pair of security gateways (e.g. routers or firewalls), or between a security gateway and a host.

All access to nScaLED facilities is provided either through encrypted, industry standard (IPsec) VPN connections or through dedicated private lines (MPLS etc).

Private Lines

Many clients use MPLS/MPVS or other private lines to connect different office LAN's into one distributed network. Multiprotocol Label Switching (MPLS) is a mechanism in high-performance telecom networks which directs and carries data from one network node to the next. MPLS makes it easy to create "virtual links" between distant nodes. It can encapsulate packets of various network protocols.

nScaLED clients can elect to terminate MPLS networks directly into our data center facilities eliminating the need for IPsec connectivity (or use a combination of both).

Client Divisions

Cost efficiencies with cloud computing are attained partially through operating shared physical resources across a number of clients with different demand requirements. Careful provisioning across clients allows cloud data centers to operate at 80% efficiency or better, as opposed to 10% - 15% of typical private data centers.

Shared physical resources require strict attention and adherence to client separation of data to prevent any comingling (and disclosure) of client data. Intra-client data separation occurs at multiple levels. All clients receive a dedicated layer 2 VLAN specifically for them. All resources are provisioned into this network. This means that each client's network traffic has its own logical partitioning from any other client.

Perimeter Firewalls

nScaLED makes use of high quality Cisco ASA (Adaptive Security Appliances) for perimeter protection. No traffic comes into the networking environment without passing through our array of perimeter security devices.

Intrusion Detection

An Intrusion Detection System (IDS) detects network traffic that attempts to circumvent or destroy the security policy of a networked computer environment in attempt to deteriorate the integrity, confidentiality, and availability of computer resources.

nScaLED uses sophisticated intrusion Detection Systems (IDS) as part of our overall security suite. An IDS sits outside the clients network and continually scans all incoming traffic for signatures of possible cyber threats. Since the sensor is outside the network, it does not add any points of failure that could cause network downtime.

When traffic is detected that appears malicious or threatening the firewall is immediately warned to block the traffic while allowing legitimate traffic to continue.

An IDS is an important piece of equipment and we invest significant time and money into this layer of our network architecture.

Comprehensive Protection & Security Review

- Detects and alerts you of network threats in real time
- Leverages thousands of threat signatures
- Can automatically block attacks
- Increased accuracy through 7 factor scenario modeling
- Real-time signature-based alerting plus review by security engineer every 12 hours

Correlation Capabilities

- Correlates threats with host vulnerabilities (generic exploits are ranked lower in priority than exploits matching your specific vulnerabilities)
- Correlation of disparate event sources to detect complex attack patterns

Personnel and Procedures

nScaled personnel are screened by background security checks before hiring.

Client Passwords

nScaled personnel do not require password access to client operating environments and are therefore unable to authenticate beyond the Operating System.

Client Names and Codes

nScaled makes use of codes to obfuscate client names and compute resources such that different storage volumes, networks, and compute resources cannot be easily traced back to specific client data.

Encryption

All data transmitted over IPsec is encrypted using industry standard, strong encryption algorithms. At the client's request, data protected within nScaled can be encrypted at source during the setup process. This optional procedure means that volumes stored within the cloud remain encrypted at all times.

Data Scrubbing

nScaled makes of (Department of Defense) standard disk scrubbing before returning previously utilized storage disks into production (or retirement). This means that no residual data can be identified or read across disk resources.

Conclusion

nScaled cloud data centers are designed to be at least as secure as our clients internal LAN environments, and are in many cases more so. We understand that the security of our client's data is paramount, and we continually seek to improve our design and service levels in consultation with client requirements.