Latest Information Security Identity & Mobility Solutions
About Us

Shifra is a value added distributor founded in 2007 out of Dubai Internet City with a partner network covering the Middle East region. Shifra provides expertise to enterprise customers around the Middle East in three main areas: Information Security, Identity Protection and Enterprise Mobility. The name Shifra originates from the word “Sifr”, the Arabic numeral zero which was later used to describe a cipher that then created a coded message, thus forming the basis of encryption as we know it today.

With an extensive experience in channel development for multi-national vendors the Shifra team has the perfect aptitude to understand the needs of the market and satisfy them. Our team consists of information technology experts that hold a cumulative experience of over 100 years in the field. Shifra professionals bring international experience from across the world; the US, Europe, Asia and the Middle East region.
security

With the ever increasing amount of data being compromised due to inefficient and backward security solutions, importance of effective data protection became undeniable. Shifra offers a variety of information security and authentication services that helps organizations to protect and manage their logical, physical, and cloud-based data assets.

Proofpoint solutions:

Stop advanced threats before they get to people over email, social media and mobile apps

Protect the information people create to reduce the attack surface and compliance risk

Enable their teams to respond quickly when things go wrong

Proofpoint solutions protect your people, data, and brand from advanced threats and compliance risks with cybersecurity solutions that work. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them via email, mobile apps, and social media. But since some attacks get through even the best defenses, our solutions proactively protect the critical information people create and equip security teams with the right intelligence and tools to respond quickly.
Protecting people from targeted attacks

Well over 90% of targeted attacks use email, social media, or mobile apps to compromise your endpoints, steal your credentials, and steal your data. Our solutions detect and block these threats with a powerful blend of:

- Cloud-powered tools to detect and block malicious email attachments, links, social media posts, and mobile apps, updated in real time as the threat landscape changes
- A massive threat graph composed of observed attacker tradecraft built into a with hundreds of billions of data points, helping stop attack campaigns both with and without malware
- Analysis by a dedicated team of over 100 threat researchers

Today’s attackers target users everywhere they work—on and off your network, across a wide mix of devices, and through new communications channels. Our advanced threat solutions work in the email flow via a gateway, on social platforms, and across the worlds’ app stores to detect advanced threats everywhere they target people.

Next-generation solutions powered by threat intelligence
Securing The Digital Transformation

ABOUT THALES E-SECURITY
Thales e-Security is the leader in advanced data security solutions and services that deliver trust wherever information is created, shared or stored. We ensure that the data belonging to companies and government entities is both secure and trusted in any environment – on premise, in the cloud, in data centres or big data environments – without sacrificing business agility. Security doesn’t just reduce risk, it’s an enabler of the digital initiatives that now permeate our daily lives – digital money, e-identities, healthcare, connected cars and with the internet of things (IoT) even household devices. Thales provides everything an organization needs to protect and manage its data, identities and intellectual property and meet regulatory compliance. Security professionals around the globe rely on Thales to confidently accelerate their organization’s digital transformation.

COMPREHENSIVE DATA SECURITY SOLUTIONS
Thales e-Security provides companies everything they need to protect and manage their data and scale easily to new environments and requirements — encryption, advanced key management, tokenization, authorization, privileged user control and Hardware Security Modules (HSMs).

DATA SECURITY LEADERSHIP
With strong engineering expertise and real world experience, Thales e-Security has been a leader in protecting data in mission-critical environments — finance, government, manufacturing, technology & enterprise for over four decades.

GLOBAL SECURITY ORGANIZATION
Thales e-Security is part of Thales Group, a €19 billion Fortune 500 organization that provides a complete spectrum of security infrastructure solutions and services.
SOLUTIONS TO YOUR DATA PROTECTION CHALLENGES

Delivering security and trust in data wherever data is created, shared or stored without impacting business agility.

GLOBAL
Thales e-Security is an integral part of a global security giant that is making the world safer through comprehensive infrastructure solutions and services to governments and corporations of all sizes

DEDICATED
Our passion, commitment and focus on ensuring that the data that builds business is trusted, wherever it’s created, shared or stored drives everything we do

TRUSTED
Our customers include 19 of the world’s 20 largest banks, four of the world’s five largest oil companies and 27 NATO country members
SECURITY AUTOMATION AND ORCHESTRATION PLATFORM

Challenge

Some of the long-term secular trends in IT such as mobility, virtualization and cloud has resulted in significant productivity gains for organizations — but at the at same time, they have presented extraordinary challenges for the CIO and CISO’s to secure the organization’s network. The collective consequence of these trends has resulted in a diminished network perimeter and expanded attack surface of an organization’s network — making it ripe for cyber thieves to infiltrate an organization’s network and gain access to sensitive data.

Solution

Network Sentry offers a policy-based security automation and orchestration platform that enables discovery of every endpoint and network infrastructure device, provides contextual awareness for implementing dynamic network access control, and the ability to contain a cyber breach through automated threat response. By automating the complex threat triage process and rapidly responding to security alerts, Network Sentry minimizes the risk of unauthorized access to corporate assets and intellectual property, protects the brand, and reduces the impact, time, and costs of containing cyber threats.

Benefits

Visibility

Gain Unprecedented Network Visibility

Fundamental to the security of a constantly changing network is an understanding of its makeup: switches, routers, wireless controllers and access points as well as VPN concentrators. Network Sentry provides a real-time view into dynamic network infrastructure so that risky changes are detected and prevented. Network Sentry provides centralized administration and reporting from a single console and visibility of all network devices, users and endpoints across all locations.
Identify and Classify Every Endpoint on the Network

With the growth in BYOD and the IoT, managing device types and ownership is a significant challenge when securing a network. Network Sentry automatically discovers and profiles endpoints, classifying them by type and determining if the device is corporate-issued or employee-owned. The user is also identified and the appropriate role-based network access policies are implemented within Network Sentry to protect critical data and sensitive assets while ensuring compliance with internal, industry and government regulations and mandates.

Automate and Simplify Network Access for Guests

Network Sentry streamlines the secure registration process of guest users. When appropriate, users can self-register their own devices — laptops, tablets or smartphones — shifting the workload away from the IT staff. Or, the simplified task of onboarding guests can also be delegated to designated network administrators.

Control

Assess Risk of Every Endpoint on the Network

Ensuring the integrity of wired and wireless devices before they connect to the network minimizes the risk of vulnerability and the spread of exploits and malware. Network Sentry validates a device’s configuration as it attempts to join the network. If the configuration is found to be noncompliant, the connection is prevented or the device is forced to an isolated or limited-access VLAN. Users are warned that their device must be remediated. This can be done automatically through integration with a vulnerability assessment, patch management system or by following manual instructions delivered to the user's device. Access is granted once corrective measures are successfully undertaken.

Automate Onboarding Process for Large Numbers of Endpoints

BYOD and guest-network environments using 802.1X can leverage Network Sentry's EasyConnect feature to simplify the onboarding process by dynamically configuring security settings on Windows, Mac OS X, iOS and Android devices. In the event that a device initially connects to an open (unsecured) wireless SSID, Network Sentry automatically configures its security settings by seamlessly moving the connection to a secure SSID.
PREVENTATIVE SECURITY FROM THYCYCOTIC

SECURE PASSWORDS
Secret Server
Creates a fundamental security layer - managed from a single console - to protect against cyberattacks that use privileged accounts to strike at the core of the enterprise. Available for OnPremise, Cloud, or Hybrid deployments.

Password Reset Server
Provides simple, self-service password management to free up IT help desk staff from timeconsuming and inefficient processes, and enforces stronger end-user password controls

ENDPOINT & PRIVILEGED ACCESS SECURITY SUITE

EPAS Suite Provides an unmatched combination of Secret Server, Privileged Manager for Windows, and Privileged Manager for Unix that enables you to control privileged accounts, restrict privileged access on servers and clients, and improve users' ability to run approved Windows applications.
PROTECT ENDPOINTS & CONTROL ACCESS
Privilege Manager for Windows & UNIX Provides advanced security to manage application rights with a combination of privilege management, application whitelisting, and real-time application reputation and threat intelligence.
Local Security Solution Delivers comprehensive endpoint security by limiting privileges for business and admin users, groups, and applications, and enforces policies to remove administrator rights from unauthorized accounts.
Security Analysis Solution Remediates OS configurations risks by identifying security configuration issues using the Security Content Automation Protocol (SCAP), and addressing vulnerabilities with automated remediation.
Group Management Server Empowers non-IT personnel to securely manage their department's Active Directory Groups without assigning them a privileged account.

Leading companies, including those in Financial Services, Health Care, Retail, Telecommunications, Manufacturing, Media, Government, Defense, Oil and Gas, and Education, use Voltage solutions for:

Founded:
1996

Funding:
Insight Venture Partners 2015

Products:
• Thycotic Secret Server
• Thycotic Privilege Manager for Windows
• Thycotic Password Reset Server
• Thycotic Group Management Server
• Thycotic Local Security Solution
• Thycotic Security Analysis Solution

Acquisitions:
Arellia acquired 2016 Microsoft Windows end-point security and application control solutions that stop the progress of malware-based attacks at the endpoint, limiting an attacker's ability to move beyond their initial point of entry.

Customers:
More than 7,500 organizations worldwide, including Fortune 500 enterprises.

Used by more than 180,000 IT admins and security pros.

OUR AWARDS & RECOGNITIONS

Inc. 500
BNC. 5000 Fastest Growing Companies In America: 2013, 2014, and 2015

Best of VMWorld
- Security and Compliance 2014 & 2016; Finalist / runner up

SC Magazine Awards Europe 2015: Finalist, Best Customer Service

Washington Business Journal Best Places to Work 2015: #17 Medium Sized Biz Category

identity

Identity management is one of the most important components of any organization’s security infrastructure. In any organization information assets must be accessible only to individuals who are granted explicit entitlements to specific information. Shifra has a strong IAM solutions portfolio which will help to set and improve the mechanisms by which organization digitally identifies individuals, assigns privileges, monitors access and data usage, maintains separation of duties, and provides end-to-end audit-ability of this infrastructure.

**Solutions we provide:**
- Strong Authentication
- Secure Online Banking
- Privileged Access Management
- Single Sign On
- Identity-as-a-Service (IDaaS)
- Ideal Lifecycle Management
Identity and Access Management

Versatile Security is an Identity and Access Management (IAM) provider focusing on management of access enabling devices: smart cards, mobile, tablets, virtual and RFID/NFC devices.

Solutions:
- vSEC:CMS
- vSEC:ID
- vSEC:MAIL
- Smart Cards
- Virtual Smart Cards

Versatile Security provides enabling IT security products centered on the usage of security devices such as smart cards. Company’s solutions enable the customers to securely authenticate, issue and manage user credentials more cost efficiently than other solutions on the market.

Versatile Security focuses on developing products with the following attributes:
- Fast installation and integration
- No or limited need of dedicated hardware
- Intuitive and efficient user interface
- Highest security levels
- No hidden costs
The leader in cloud security
Understand activities, protect data, stop threats and respond to incidents

Trusted by the world’s largest companies, our cloud-scale security platform enables security professionals to understand risky activities, protect sensitive data, stop online threats, and respond to incidents in a way that fits how people work. Netskope — security evolved.

Unique Capabilities

- **Advanced Enterprise DLP:**
  With Netskope, you have comprehensive cloud DLP that covers all cloud traffic, from mobile apps, sync clients and native apps to off-premises devices, allowing you to inspect all traffic for potential DLP violations.

- **Architected for Any Use Case:**
  Netskope is architected to cover all cloud security use cases in comprehensive manner. Flexibility starts with the option of being deployed as a 100 percent cloud services, as an on-premises appliance, or in a hybrid manner that includes both.

- **Granular Policies for All Services:**
  Netskope sees and decodes all cloud traffic, not just sanctioned browser traffic like most CASBs. Our patented, all mode architecture gives you visibility and control over sanctioned services whether users and on a web browser, mobile app, or sync client.

- **Advanced Threat Protection:**
  Netskope is the only CASB with comprehensive, advanced threat protection for cloud services, combining a unique cloud vantage point with multi-layered threat detection and remediation capabilities.
Our Vision

Peace of mind for all global businesses and government entities with complete and proven digital security solutions. When it comes to online security, most organizations seek to strike the right balance of protection with an optimal user experience. With this in mind, VASCO developed an innovative platform along with patented security technologies, utilizing the strongest encryption and latest in biometrics, that enable custom tailored solutions to meet the unique needs of each customer. This translates into more focus on the business and less on security vulnerabilities and compliance exposure.
VASCO is a global leader in trusted security with two-factor authentication, transaction data signing, document e-signature and identity management solutions designed for all businesses and government agencies. VASCO also secures access to data and applications in the cloud and provides a robust toolset for application developers to easily integrate security functions into their web-based and mobile applications. More than 10,000 customers in 100 countries rely on VASCO to secure access, manage identities, verify transactions, simplify document signing and protect high value assets and systems.
Identity and Access Management

Evidian offers a complete, integrated and modular solution for digital identity management and access governance compatible with their security policies and the new regulatory requirements.

Solutions:

- Enterprise Single Sign-On - Strong passwords with no password-typing
- Enterprise SSO for mobile - Solution for Android SSO and IOS SSO
- Web access management - Portal security and web single sign-on
Evidian sectoral approach offers organizations from all sectors an implementation of solutions that is adapted to each profession.

For Evidian identity and access management is a major building block to ensure the security of information systems. To get the full benefit of it, the identity and access management system must gain adherence from users and professions and offer tools for technical managers that are adapted to new usage scenarios and to the development of cloud services.
As businesses develop, their networks must grow with certain priorities in mind: core efficiency, vigilant security and the ability to go wireless and mobile. Shifra offerings help organizations to unify their business network, maximize security and efficiency.

Solutions we provide:
- Enterprise Wireless Access
- Bring Your Own Device
- Wifi Monetization
- Guest Access Management
- Network Access Control
Controller-less Wi-Fi and Cloud-enabled Networking for the Enterprise

Aerohive is an innovative enterprise mobility company. Aerohive solutions enable enterprises to leverage the power of mobility to increase productivity, engage customers and grow their business. Companys’ proprietary mobility platform utilizes the cloud and a distributed, controller-less architecture to deliver unified, intelligent, simplified networks that can be cost-effectively deployed. The scalability and flexibility of the platform makes enterprise mobility available to organizations regardless of their level of IT resources and enables a consistent network architecture to be deployed across enterprises of all sizes.

Mobility has become too complicated for many organizations and to address this Aerohive has focused on simplifying enterprise mobility with cloud-managed, unified mobility platform and built out a broad, integrated platform that includes:

• A complete, mobility-centric network access infrastructure including Controller-less Wi-Fi, access switches, branch routers, and client management agents

• Cloud-based management that dramatically simplifies IT operations

• Mobility applications that capture important contextual end-user data from our mobility platform and provide new business insights and analytic capabilities

Products:

› Access Points
› Routers
› Switches
› Network Management
› Cloud Services Platform
› Applications
Cloud4Wi provides an innovative cloud Wi-Fi platform for managing and monetizing Wi-Fi services.

Cloud4Wi’s platform enables venues to be rewarded for Wi-Fi services offered to customers by providing access to the world’s first Wi-Fi marketplace. It includes every tool that venues need to manage and monetize their Wi-Fi services. Using an easily customizable splash portal and powerful proximity, advertising, social media and analytics applications, venues can engage their customers and generate additional revenues over their Wi-Fi network.

**Solutions:**
- Wi-Fi Hotspot Management
- Engaging Marketing Apps
- Powerful Analytics

Leading telecommunications and networking players, system integrators and Wi-Fi vendors have chosen Cloud4Wi to better serve their most demanding and enterprising customers who are searching for ways to maximize and/or offset their Wi-Fi investments.

**How Cloud4Wi works**

1. Configure the guest Wi-Fi access
2. Define engaging marketing strategies
3. Collect and analyze visitors’ behavior