SMART iT

YOUR TRUSTED IT ADVISOR

Who We Are

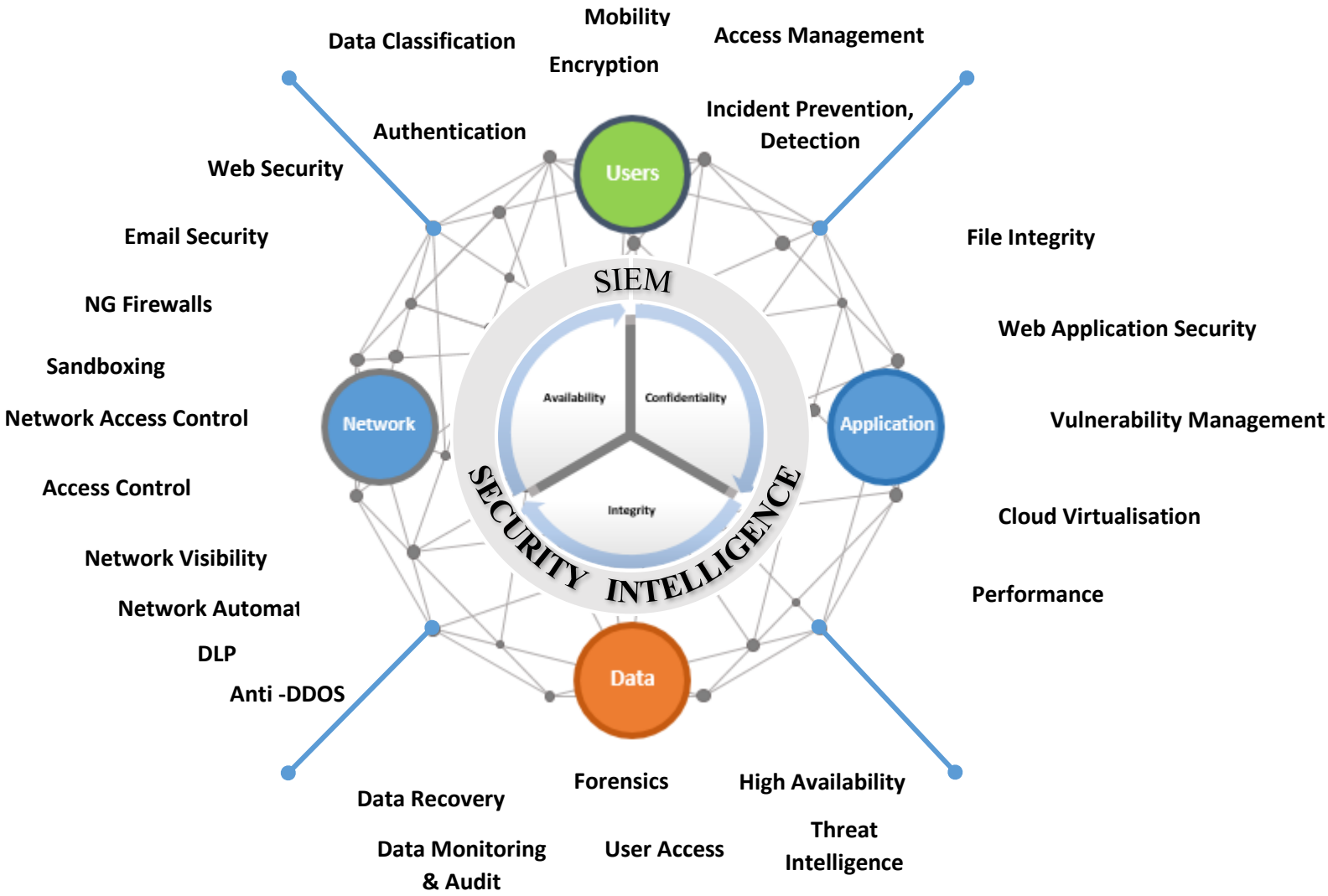
SMAR IT is one of the first Tunisian companies speaking Cyber Security.

With our business model and strategy based on "win-win-win" relation, between Partners-SMART iT and customers, we deliver best performance and solutions, which best meet client requirements and achieve compliance.

We assist our customers in building secure networks; guarantee Confidentiality; assuring Data Integrity and availability by offering them integrated solutions **Data center & Cloud, Governance, Risk Assessment, Threat Protection, Securing Mobility, Security Intelligence, Vulnerability Management and Incident Handling.**


Presales Representative
Presales Representative
Head Office (Sousse, Tunisia)

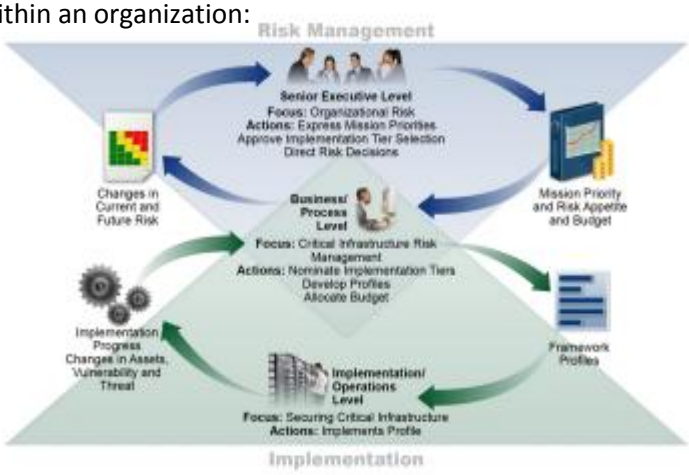
SECURITY FRAME WORK OVERVIEW



Security Frame Work

IT Security is a fragmented market, proliferated with many point products that are designed to address specific risks, and which may meet targeted compliance goals, but these solutions typically fail to provide a comprehensive, integrated picture of the threat landscape. Instead of organizations becoming more relevant and agile in their response to security challenges, increased complexity is created that can overwhelm IT Security teams. The challenge is compounded by patient attackers, sophisticated advanced threats, and the increasing use of cloud and mobile technologies, which expand the potential attack surface.

SMART iT Framework provides a common language for understanding, managing, and expressing cyber security risk to internal and external stakeholders. Help to identify and prioritize actions for reducing cyber security risk, and it is a tool for aligning policy, business, and technological approaches to managing that risk. It can be used to manage cyber security risk across entire organizations or it can be focused on the delivery of critical services within an organization:



SMART iT solutions cover all IT Security domains and corner stone giving our customers the ability to achieve their Security objectives and visions. Our Security Framework deliver a comprehensive security approach by delivering solutions covering major IT actors: Users, Network, Application and finally Data.

SMART iT simplify security risk management by implementing the required security controls and ensure their efficiency.

The Framework Core provides a set of activities to achieve specific cyber security outcomes, we define five activities:

SMART IT SOLUTIONS

A new mindset for data security is required if organizations are to stay ahead of the attackers and more effectively protect their intellectual property, employee, data and customer information against data breaches in the future.

Daily efforts to reduce exposer areas, effective controls, compliance, risk management, incident response, putting results into context, managing the IT security platform etc… is only increasing management complexity and time waist.

SMARRT iT portfolio incorporate solution translated into life cycle delivering a complete security approach composed of : Data Center, Access Control, Network Security, Mobility, Risk Assessment, Threat & Endpoint protection and Security Intelligence.

Every solution carefully chosen to cover customer IT Security gaps delivered with high expertise from our team and Technologies supplier support to achieve an effective application performance and traffic visibility, implementing critical controls, verification of those controls, zero-day malware protection, securing data, remediation of next-generation threats, automation and orchestration etc…

Data Center

IT technology advances at an ever neck-breaking pace. IT managers are burdened with the responsibility to keep up while providing a great user experience and simultaneously reducing costs. A continuous need for increasing performance and accelerating delivery, storage requirement, quick issues detection, securing data, minimizing risk and guarantee business continuity.

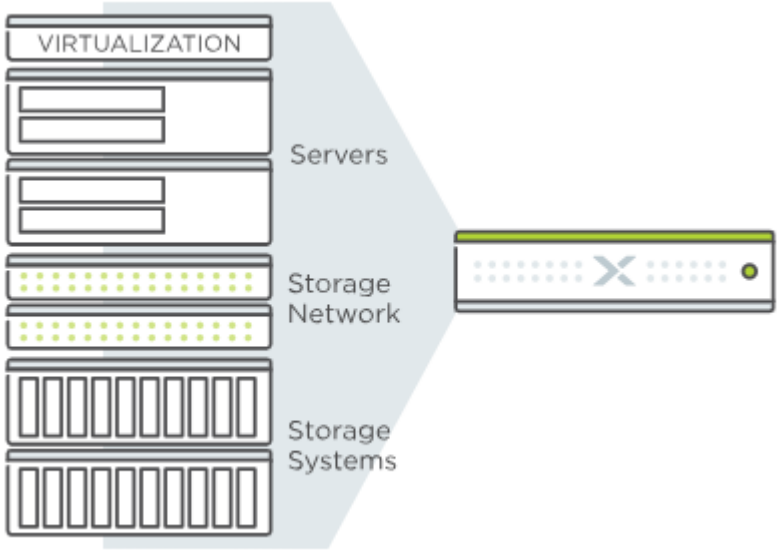
Data Centers are full of equipment different sources Network, Storage, Security, creating more risks and more management complexity from that emerge the need for automation and orchestration.

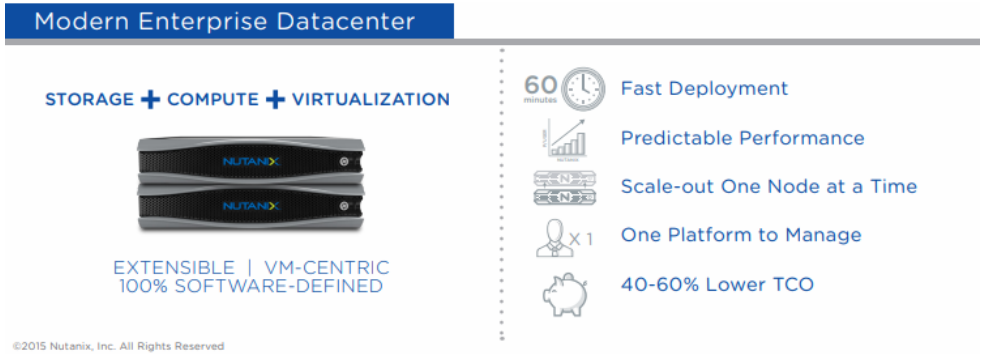
Hyperconverged Infrastructure (HCI)

The Nutanix Xtreme Computing Platform is a 100% software-driven infrastructure solution that natively converges storage, compute and virtualization into a turnkey appliance that can be deployed in minutes to run any application out of the box. Datacenter capacity can be easily expanded one node at a time with no disruption, delivering linear and predictable scalability with pay-as-you-grow flexibility.

Nutanix eliminates complexity and allows IT to drive better business outcomes. Nutanix is built with the same web-scale technologies and architectures that power leading Internet and cloud infrastructures, such as Google, Facebook, and Amazon – and runs any workload at any scale. The Xtreme Computing Platform brings together web-scale engineering with consumer-grade management to make infrastructure invisible and elevate IT teams so they can focus on what matters most – applications.

At the heart of the Xtreme Computing Platform are two product families: Nutanix Acropolis and Nutanix Prism. Acropolis provides a distributed storage fabric delivering enterprise storage services, and an app mobility fabric that enables workloads to move freely between virtualization environments without penalty. Nutanix Prism, a comprehensive management solution for Acropolis, delivering unprecedented one-click simplicity to the IT infrastructure lifecycle.



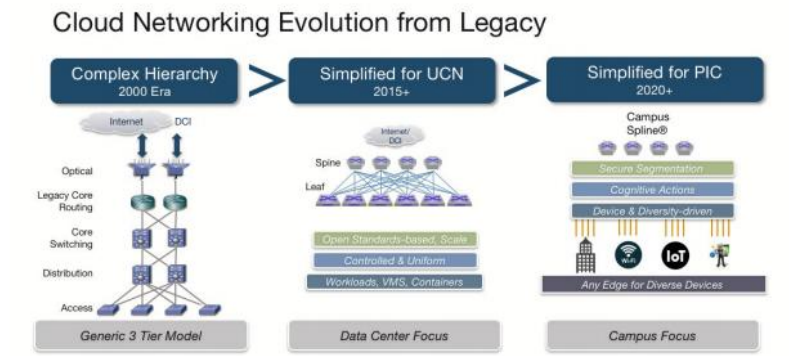


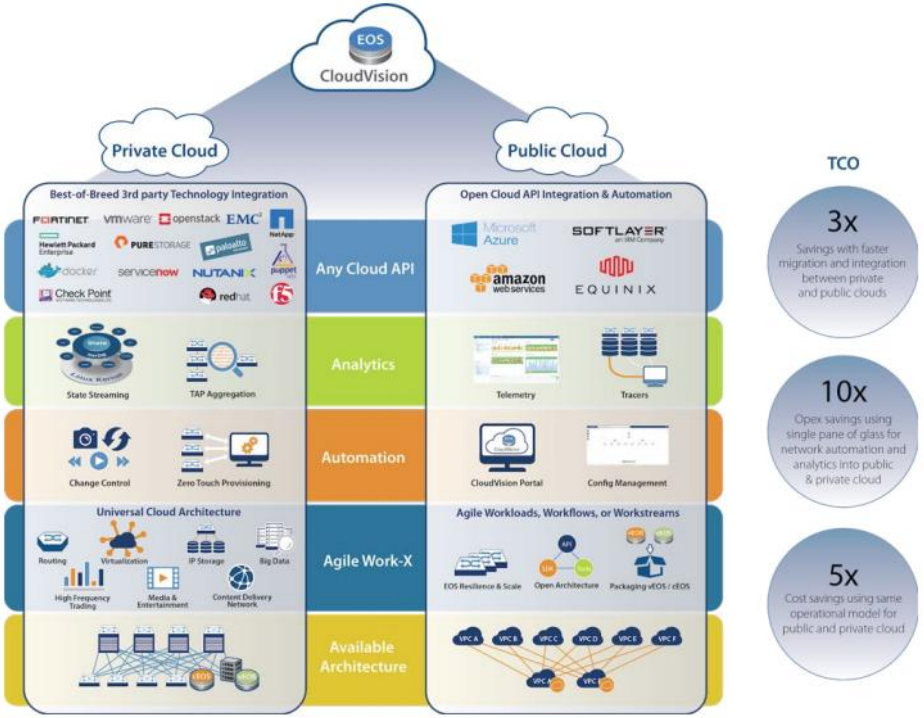
SOFTWARE-DRIVEN CLOUD NETWORKING

Arista Networks was founded to pioneer and deliver software-driven cloud networking solutions for large data center storage and computing environments. Arista's award winning platforms, ranging in Ethernet speeds from 10 to 400 gigabits per second, redefine scalability, agility and resilience. Arista has shipped more than 20 million cloud networking ports worldwide with CloudVision® and Arista EOS, an advanced network operating system.

Arista EOS, is the most advanced network operating system to enable open third party development. The award-winning software is built upon a stable, open source Linux core with a central state-oriented database that makes EOS inherently self-healing, in-service upgradeable and extremely robust. Arista EOS Central offers web-based access to development tools, scripting examples, and support to deliver real-world solutions that bridge the gap between what vendors build and what users want. Arista actively shares code samples, engages in collaborative forums, and posts works in progress to get early insight into use cases.

Arista Networks is the leader in building scalable, high-performance and ultra-low latency cloud networks with low power consumption and a small footprint for modern data center and cloud computing environments. Purpose-built hardware with Arista 7000 and 7500 families Arista EOS and CloudVision, maximize system uptime, stateful fault repair, Advanced Event Management, Zero Touch Provisioning, latency analysis and a fully accessible Linux shell. Arista's programmable platforms include native support for VMware, network-virtualization and hundreds of applications. Arista's solutions are designed to meet the stringent power and cooling requirements of today's most demanding data centers, proven advantages already in use in many of the largest cloud data centers around the world.

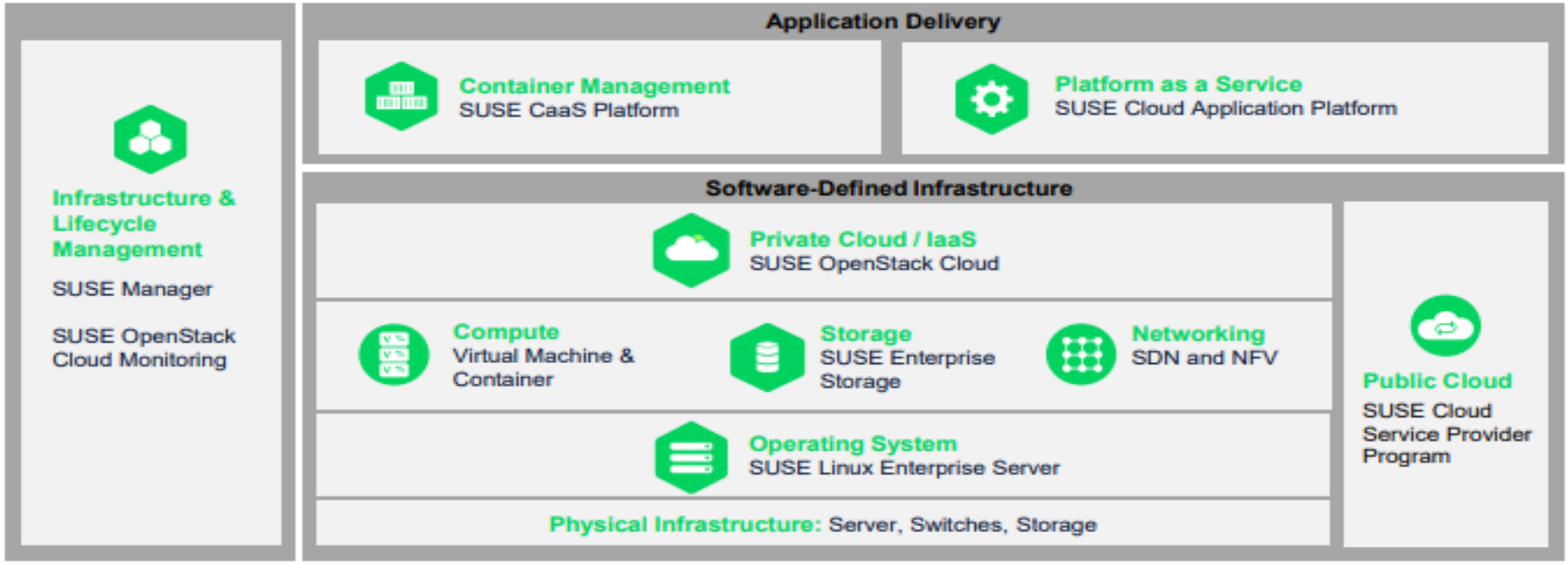




SOFTWARE-DEFINED INFRASTRUCTURE SDI

SUSE, a pioneer in open source software, provides reliable, software-defined infrastructure and application delivery solutions that give enterprises greater control and flexibility. More than 25 years of engineering excellence, exceptional service and an unrivaled partner ecosystem power the products and support that help our customers manage complexity, reduce cost, and confidently deliver mission-critical services. The lasting relationships we build allow us to adapt and deliver the smarter innovation they need to succeed – today and tomorrow.

SUSE Software-defined Infrastructure and Application Delivery Approach



Network Virtualization Platform for the Software-Defined Data Center

NSX software-defined networking (SDN) is part of VMware's software-defined data center (SDDC) concept, which offers cloud computing on VMware virtualization technologies. VMware's stated goal with NSX is to provision virtual networking environments without a command-line interface (CLI) or other direct administrator intervention. Network virtualization abstracts network operations from the underlying hardware onto a distributed virtualization layer, much like server virtualization does for processing power and operating systems (OSes). VMware vCNS virtualizes Layer 4-7 (L4-L7) of the network. Nicira's NVP virtualizes the network fabric, Layer 2 (L2) and Layer 3 (L3).

NSX exposes logical firewalls, switches, routers, ports and other networking elements to enable virtual networking among vendor-agnostic hypervisors, cloud management systems and associated network hardware. It also supports external networking and security ecosystem services.

Security: VMware NSX Data Center delivers consistent, automatable network security to workloads no matter where they live -- from the data center, to the cloud, to the edge. With NSX Data Center, network security policies can be defined based on application contexts and enforced on every individual workload, without the need to touch the physical network.

Compliance: VMware NSX Data Center changes the way applications in data centers are secured by enabling a zero-trust security model through micro-segmentation inside data centers and clouds. NSX Data Center reduces the scope of compliance by isolating the systems that store, process or transmit sensitive data. This enables a fundamentally more secure environment and helps to ensure and demonstrate compliance with many regulations such as PCI DSS, HIPAA, FedRAMP, SOC, CJIS, DISA STIG and more.

Automation: VMware NSX virtualizes all networking and security functions to enable faster deployment through automation by reducing manual, error-prone tasks. Complete lifecycle automation of applications ensures that policy is provisioned, managed, and retired in lock step with workloads, eliminating operational bottlenecks in the application lifecycle.

Web-Scale Networking

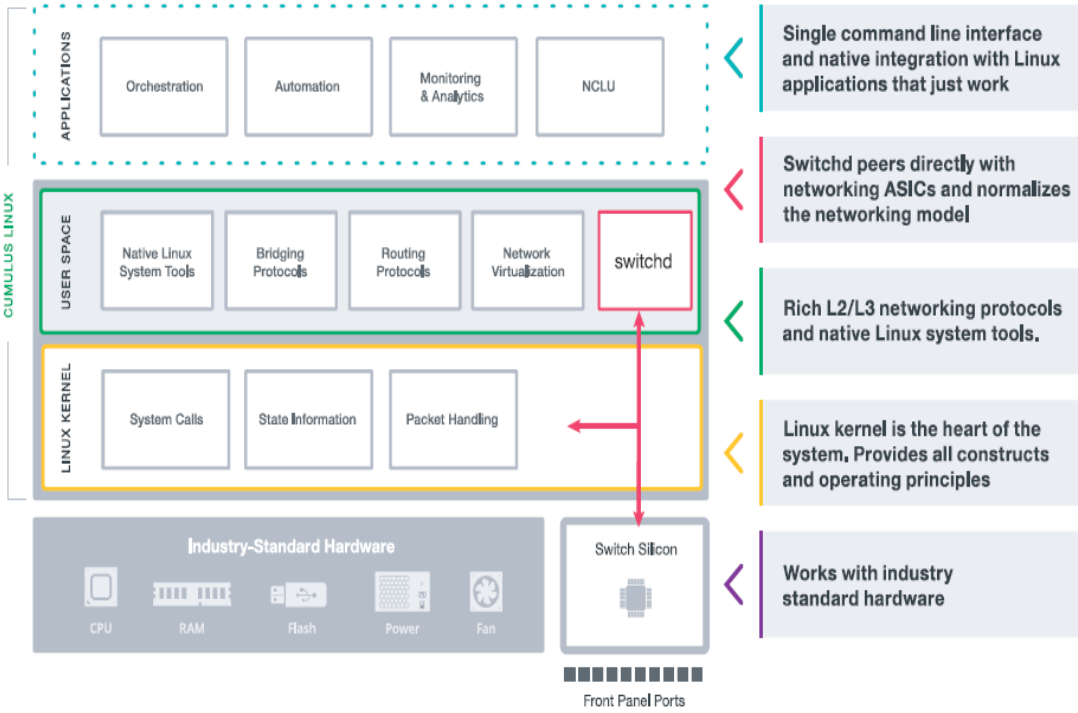
Cumulus is leading the transition of the data center market from a closed and proprietary environment to one that embraces open, standards-based systems. Unlike anyone else in the market, we build networking products purely with Linux. Our customers can leverage its standard interfaces and rich ecosystem to achieve a new level of control of cost and operations — previously accessible only to the largest web-scale operators.

By transitioning to open networking, we believe organizations of all sizes can affordably build and efficiently operate your network like the world's largest data centers. Our customers can run their data center networks the way Google and Facebook have done for years — highly automated, flexible and efficient, without all the development time or expensive, specialized hardware. We call it web-scale networking.

Instead of focusing on siloed solutions, at Cumulus Networks, we transform every stage of the networking lifecycle — from architecture, design, build, deployment and operations — with our two core products, Cumulus Linux and Cumulus NetQ. Cumulus Linux is the most flexible network operating system available because it runs on Linux. Our customers access flexibility, efficiency, speed and choice with a unified stack and a feature set designed for the digital age. With Cumulus NetQ, we empower organizations with full network validation and reduced downtime and even extend network visibility into containers.

The network is a critical part of the data center that has traditionally been a bottleneck for rapid deployment of applications. From provisioning and deployment to monitoring and operations, we believe in completely transforming the industry by enabling a web-scale IT architectural approach.

THE ARCHITECTURE OF CUMULUS LINUX



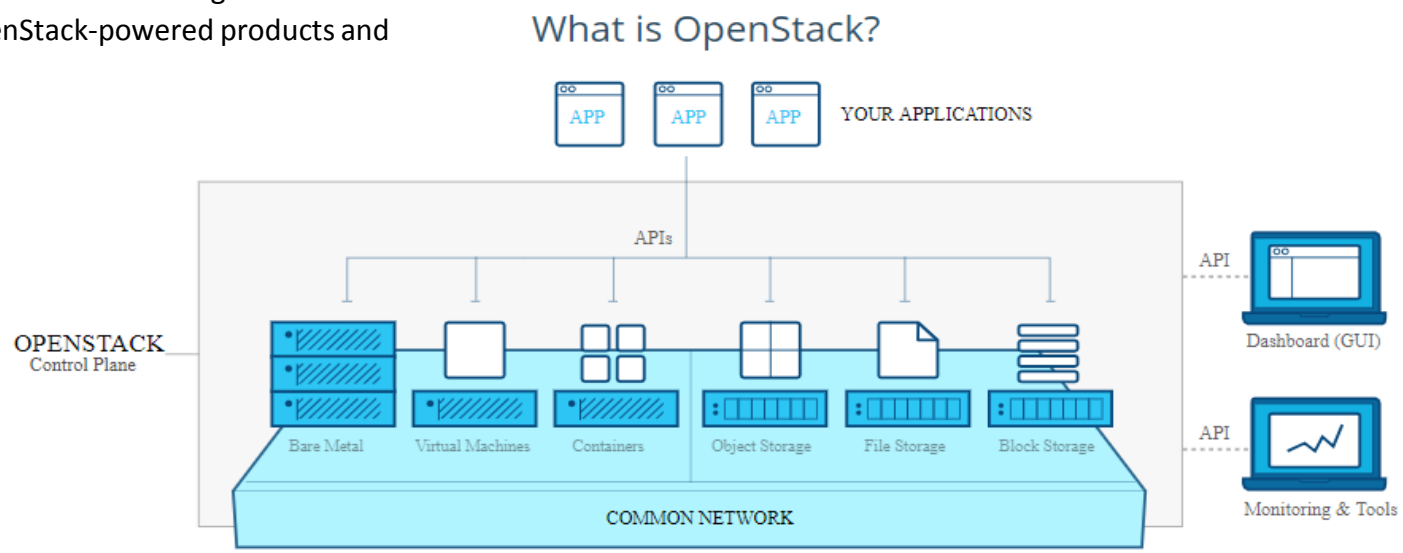
Cloud Operating System

OpenStack software controls large pools of compute, storage, and networking resources throughout a datacenter, managed through a dashboard or via the OpenStack API. OpenStack works with popular enterprise and open source technologies making it ideal for heterogeneous infrastructure.

Hundreds of the world's largest brands rely on OpenStack to run their businesses every day, reducing costs and helping them move faster. OpenStack has a strong ecosystem, and users seeking commercial support can choose from different OpenStack-powered products and services in the Marketplace.

.

OpenStack is a cloud operating system that controls large pools of compute, storage, and networking resources throughout a datacenter, all managed through a dashboard that gives administrators control while empowering their users to provision resources through a web interface



Access Control

Access control is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimizes risk to the business or organization.

There are two types of access control: physical and logical. Physical access control limits access to campuses, buildings, rooms and physical IT assets. Logical access control limits connections to computer networks, system files and sensitive data.

Access control systems perform identification authentication and authorization of users and entities by evaluating required login credentials that can include passwords, personal identification numbers (PINs), biometric scans, security tokens or other authentication factors.

Finally, the required processes and procedures to achieve continuous compliance are automated so that human error or risk of insider threats are minimized.

Enterprise-Class Access Control Solutions

avigilon™
a Motorola Solutions Company

Avigilon, a Motorola Solutions company, provides trusted security solutions to the global market.

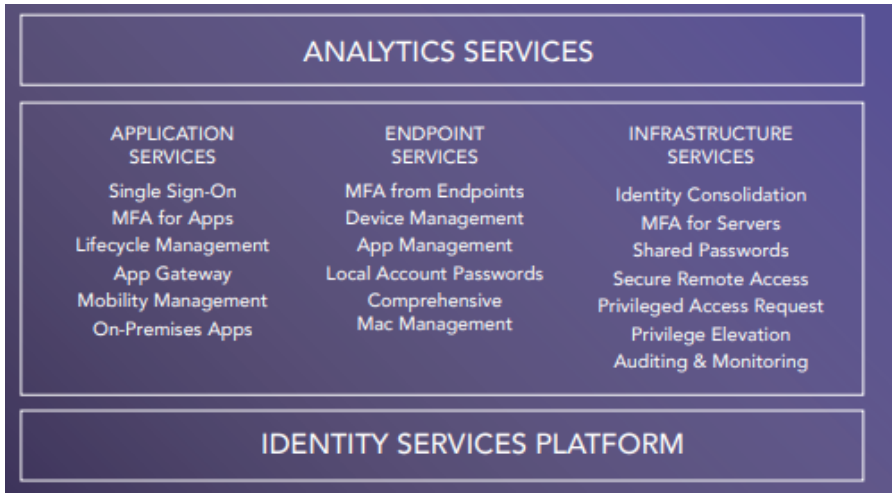
Avigilon designs, develops, and manufactures video analytics, network video management software and hardware, surveillance cameras, and access control solutions. Avigilon's solutions have been installed at thousands of customer sites, including school campuses, transportation systems, healthcare centers, public venues, critical infrastructure, prisons, factories, casinos, airports, financial institutions, government facilities, and retailers.

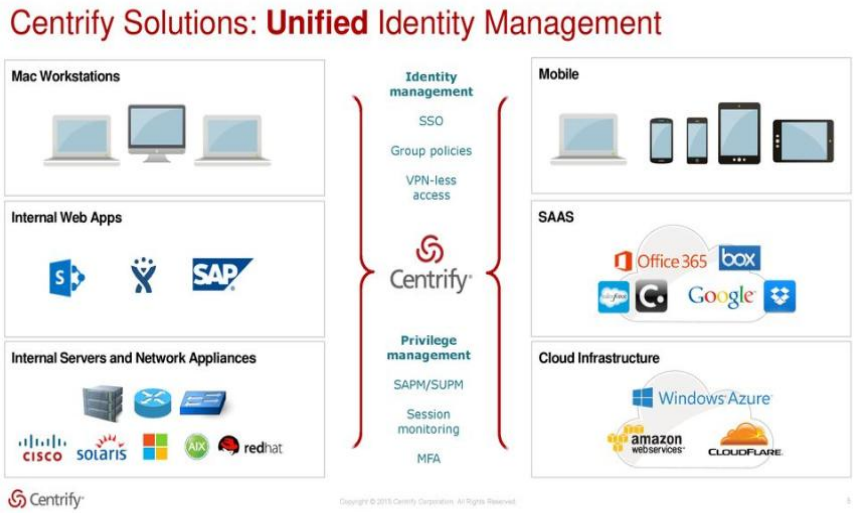
Better information, faster response times.
Integrated graphic mapping.

With our enhanced graphic map support, you get real-time visual information for all of your alarms and doors in the context of your floor plan. This enables you to respond to trouble faster.

Identity and Access Management

Centrify is the leader in securing enterprise identities against cyberthreats that target today's hybrid IT environment of cloud, mobile and on-premises. The Centrify Identity Platform protects against the leading point of attack used in data breaches - compromised credentials - by securing an enterprise's internal and external users as well as its privileged accounts. Centrify delivers stronger security, continuous compliance and enhanced user.





Data & Identity Security, Encryption, Multi Factor-Authentication

As the global leader in digital security, Geraldo brings trust to an increasingly connected world. Our know-how helps authenticate identities and protect data so they stay safe and enable services in personal devices, connected objects, the cloud and in between. Our solutions are at the heart of modern life, from payment to enterprise security and the internet of things – enabling our clients to deliver secure digital services for billions of individuals and objects.

Through its acquisition of SafeNet, Gemalto offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of data, digital identities, payments and transactions – from the edge to the core. Gemalto's newly expanded portfolio of SafeNet Identity and Data Protection solutions enables enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters.

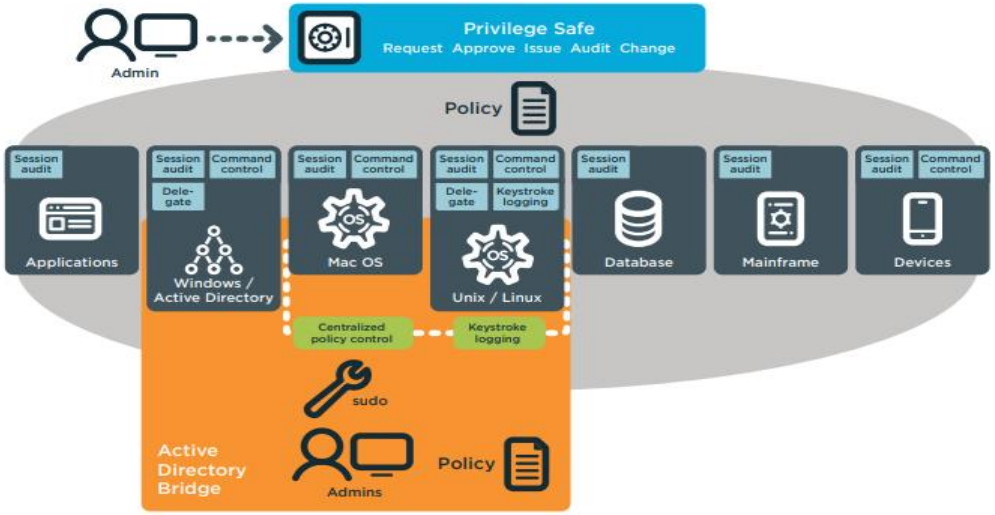
Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.

Identity Management and Access Governance

The One Identity family of identity and access management (IAM) solutions, offers IAM for the real world including business-centric, modular and integrated, and future-ready solutions for identity governance, access management, and privileged access managemenOne Identity identity and access management (IAM) solutions empower you to control administrative access enterprise-wide.

One Identity solutions for privileged access management improve efficiency while enhancing security and compliance; administrators are granted only the rights they need— nothing more, nothing less— and all activity is tracked and audited.

Specifically, One Identity solutions include granular, policy-based delegation for superuser credentials; session audit and replay; keystroke logging; and secure and automated workflows for issuing privileged credentials to administrators and in application-to-application and application-to-database scenarios. The One Identity suite of privileged access management solutions includes both network-based and host-based solutions.



One Identity solutions enable you to secure, delegate, control and audit access for superuser accounts and shared administrative credentials—across a variety of platforms and systems.

Data Protection

Data protection is the process of safeguarding data throughout its lifecycle, from collection and dissemination, all the way to archiving and storage. It relates to data integrity, corruption protection, and overall security of the data. Data protection should always serve as the default policy, in both personal and corporate environments.

This ensure that security mechanisms are in place to analyze the requested traffic, web, email, etc… to identify whether or not traffic contains signature-based or signature-less threats.

Application & Data Security

Barracuda was launched to give businesses an email-security solution that did not cost a small fortune. With more than 1 million cloud-enabled products delivered since, we continue to disrupt the IT-security market with innovative solutions that every business can afford. We're on a mission to protect customers, data and applications from today's advanced threats by providing the most comprehensive and easy-to-use IT-security platform and backing it up with best-in-class customer support.

Barracuda's first spam and virus firewall product became the world's most widely-deployed solution for on-premises email security. Today, we continue to offer easy, comprehensive and affordable solutions for email protection, data protection and network and application security. More than 150,000 global customers put their trust in Barracuda to help safeguard their employees, data and applications.

Barracuda **Solutions**

Network Security

Barracuda CloudGen Firewall
Next generation security and connectivity for distributed enterprise networks and the Internet of Things.

Barracuda Web Security Gateway
Enforces content policies and regulates web activity ensuring user safety.

Application Security & Delivery

Barracuda CloudGen WAF
Comprehensive application security that supports licenseless deployments and complete automation.

Barracuda Web Application Firewall
Comprehensive security specifically designed to prevent malicious attacks targeted at websites.

Barracuda WAF-as-a-Service
Cloud-delivered solution adds enterprise-proven security to your web apps in minutes.

Barracuda Load Balancer ADC
Enhances application scalability, performance, and security with up to 10 Gbps throughput.

Email Protection

Barracuda Essentials
Cloud-based security, archiving and backup for Office 365, Exchange and more.

Barracuda Sentinel
Artificial intelligence for real-time spear phishing and cyber fraud defense.

Barracuda PhishLine
Anti-phishing training and simulation platform.

Barracuda Email Security Gateway
Comprehensive email content security provides inbound/outbound filtering and prevents data leaks.

Email Archiving & eDiscovery

Barracuda Message Archiver
Save copies of emails ensuring quick mobile access and retention for compliance and e-discovery.

Barracuda Cloud Archiving Service
Cloud-based archiving for cloud email services like Office 365.

Barracuda PST Enterprise
Locate, migrate, and eliminate PST files.

Backup and Disaster Recovery

Barracuda Backup
Streamlines backup and recovery with integrated software, local storage, and cloud for offsite replication.

Barracuda Cloud-to-Cloud Backup
Protect Microsoft Office 365 environments by securely replicating to Barracuda Cloud Storage.

Subscription Services

Barracuda Energize Updates
Real-time threat intelligence and firmware updates protect against evolving Internet threats. Also provides access to Tech Support.

Barracuda Instant Replacement
Replacements for failed equipment ship within one business day. Also with an active subscription, after 4 years, receive a new, updated appliance.

Available as: Appliance, Cloud Service, Software-as-a-Service, Virtual Appliance, Software

Visit barracuda.com to try our solutions for free.

Secure Application & Data Security

At Citrix, we focus on a single driving principle: making the world's apps and data secure and easy to access. Anywhere. At any time and on any device or network.

We believe that technology should be a great liberator. Freeing organizations to push the limits of productivity and innovation. Empowering people to work anywhere and at anytime, and giving IT the peace of mind that critical systems will always be accessible and secure.

That is why, at Citrix, our mission is to power a world where people, organizations, and things are securely connected and accessible. A place where all business is digital business. A world where our customers are empowered to make the extraordinary possible. We will accomplish this by building the world's best integrated technology services for secure delivery of apps and data – anytime, anywhere.

Digital Workspace

Networking

Analytics

As businesses of all kinds become digital, organizations depend on the ability to create new disruptive business models, new ways to engage employees and customers, and new ways to work. Yet, the complexity and limitations of legacy systems and concerns over security are hindering enterprises from moving fully into the digital future.

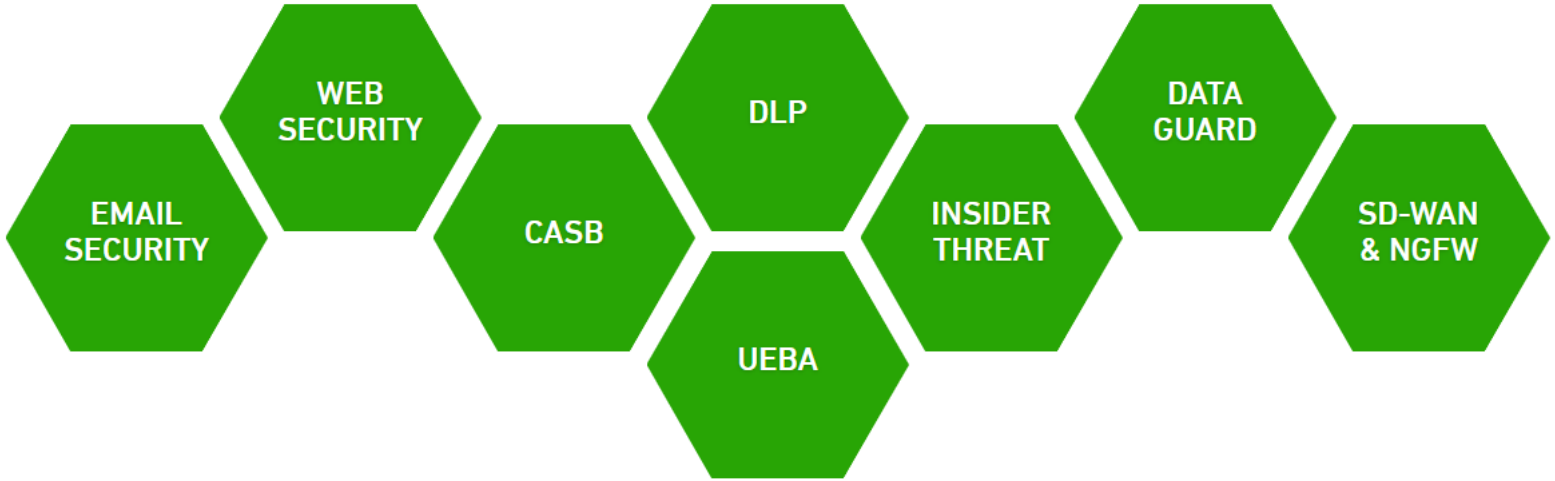
Citrix (NASDAQ:CTXS) aims to power a world where people, organizations and things are securely connected and accessible to make the extraordinary possible. We help customers reimagine the future of work by providing the most comprehensive secure digital workspace that unifies the apps, data and services people need to be productive, and simplifies its ability to adopt and manage complex cloud environments. With 2017 annual revenue of $2.82 billion, Citrix solutions are in use by more than 400,000 organizations including 99 percent of the Fortune 100 and 98 percent of the Fortune 500.

Data Security

Forcepoint was created to empower organizations to drive their business forward by safely embracing transformative technologies – cloud, mobility, Internet of Things (IoT), and others – through a unified, cloud-centric platform that safeguards users, networks and data while eliminating the inefficiencies involved in managing a collection of point security products. The Forcepoint platform will protect against threats from insiders and outsiders, rapidly detect breaches, minimize "dwell time" – the period between compromise and remediation – and stop theft.

With Forcepoint, organizations can protect users, networks and data in the cloud, on the road, and in the office. We simplify compliance, enable better decision-making and streamline security so that our customers can concentrate on what's important to them

Forcepoint provide a unified cloud-centric platform to defend against attacks, detect suspicious activity sooner, and give the context needed to decide what actions to take to defeat the attack and stop data theft. Defend, detect, decide, defeat



Network & Infra Protection

Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.

It consists in the implementation of adequate Hardware, software, policies, and procedure in order to guarantee full network visibility of traffic in/out

Most definitions of network security are narrowed to the enforcement mechanism. Enforcement concerns analyzing all network traffic flows and should aim to preserve the confidentiality, integrity, and availability of all systems and information on the network.

Enterprise Security

The rules of engagement in today's threat landscape are changing rapidly and as cyber-crime evolves, there is a security gap that can be exploited. As our dependency on technology further permeates our daily habits, the threats that exploit the security gap will have graver consequences.

Every day at FireEye, we see firsthand the impact of cyber-attacks on real people. This is what inspires us to fulfill our mission to relentlessly protect our customers from the impact and consequences of cyber attacks.

We have learned that technology alone is not enough to combat cyber attackers. Our fundamental belief is that hands-on front-line expertise and intelligence, combined with innovative technology, provides the best means to protect our customers from cyber threats

FireEye has created a unique learning system. Our real-time knowledge of the threat landscape ensures that our offerings provide the best means to protect our customers. We are constantly guided by our frontline expertise as we build our products, deliver threat intelligence and arm our services team to prepare for, respond to and prevent breaches.

The FireEye Innovation Cycle was created by product teams embracing our world-class frontline threat expertise AND our frontline experts embracing our solutions. We use this innovation cycle to create the most effective cyber defense platform – a seamless, on demand extension of our customers security operations.

Network Visibility & Tests

Ixia provides testing, visibility, and security solutions, strengthening applications across physical and virtual networks.

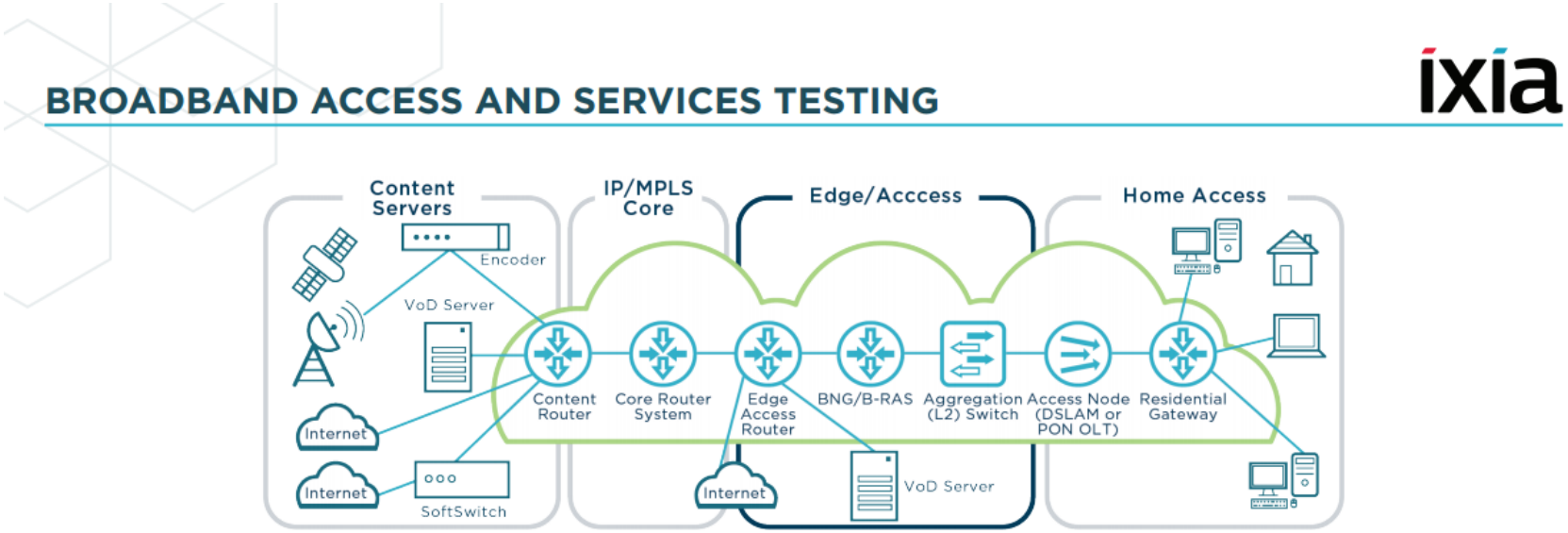
Ixia's solutions emulate realistic media-rich traffic and network conditions so that customers can optimize and validate the design, performance, and security of their pre-deployment and production networks. Ixia's solutions flow across all network types and designs: from enterprises and government agencies to service providers and network equipment manufacturers (NEMs).

Applications do great things, but they all have bugs and blind spots. Making them stronger means better testing, security resilience, and monitoring ability. Ixia takes a three-pronged approach to making applications stronger with IxTest™, IxSecure™, and IxVision™ architecture capabilities.

Ixia's customers benefit from faster time-to-market, optimized application performance, and higher-quality deployments, ensuring that their applications run stronger.

HIGHER SPEED ETHERNET SOLUTIONS

Ixia is the leading provider of test solutions for higher speed Ethernet (HSE) components, networks, devices, and systems. Our load modules operate within our standard Ixia Chassis that support 1 to 12 load modules each, depending on chassis features.



Enterprise Security

Palo Alto Networks provides an enterprise security platform that help its customers protect and defend their data assets with highly effective tools at the network, data center, and endpoint levels. Palo Alto Networks commissioned Forrester Consulting to conduct this Total Economic Impact™ (TEI) study to examine the potential return on investment (ROI) enterprises may realize by deploying a spectrum of Palo Alto Networks products. This case study offers readers with a framework to evaluate the potential financial impact of the offering on their organizations.

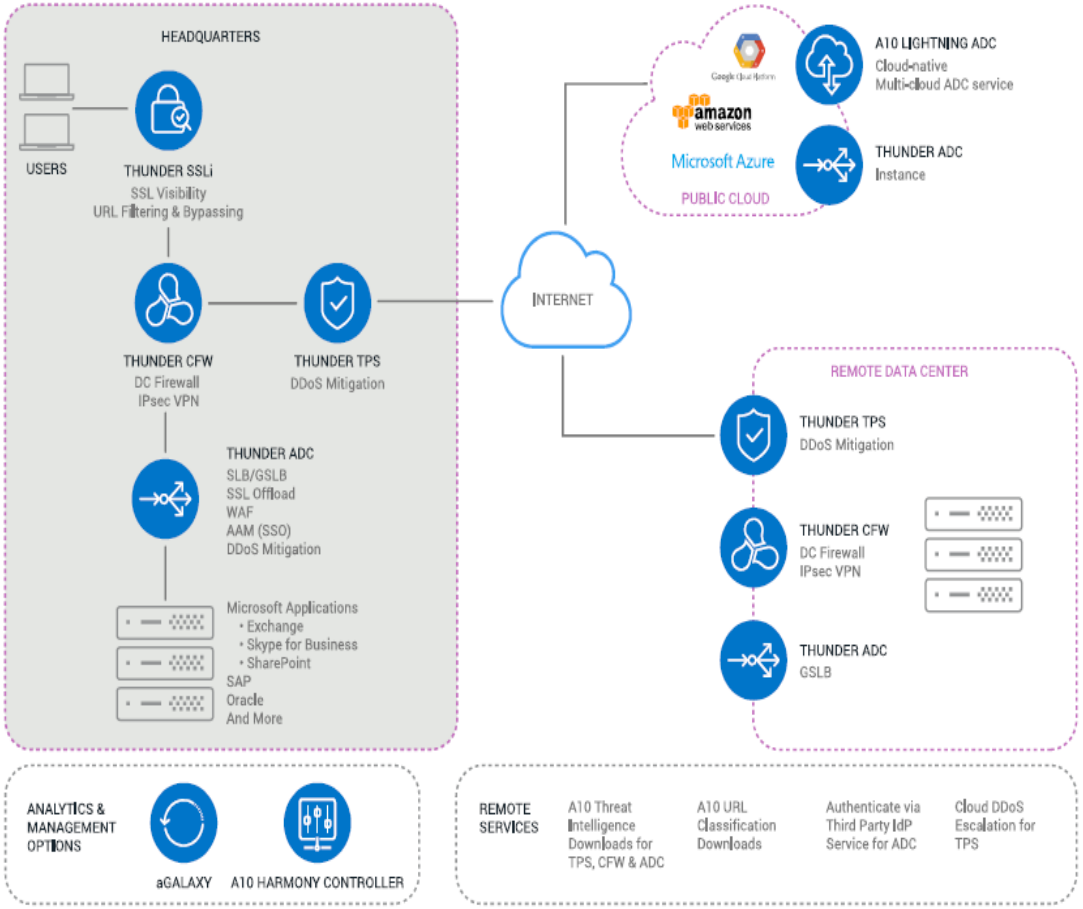
Our deep cybersecurity expertise, commitment to innovation, and game-changing security platform are helping bring an end to the era of breaches by delivering highly automated, preventive measures against cyberthreats at all stages in the attack lifecycle and ensuring protection that is superior to legacy security technologies. With our unique platform, organizations can confidently pursue a digital-first strategy and embark on technology initiatives, like cloud and mobility, that help grow their business and empower their employees while maintaining complete visibility and the control needed to protect their most valued data and critical control systems.

Fully Automated DDoS Defense

A10 Networks' range of leading secure application services ensure users, applications and the customer experience are optimal.

A10 application delivery controllers (ADC) offer data center or cloud-native service options for critical applications. SSL Insight® solutions eliminate the SSL blind spot, so security devices can better protect internal users. DDoS protection, and edge firewalls with IPsec VPN, help safeguard networks from internet threats and DDoS attacks.

Over 3,000 enterprises and service providers have chosen A10 for their Application Delivery, Security and Next Gen Networking needs. A10 has risen to become the number 1 market share leader in Japan and number 3 worldwide. Multiple solutions and benefits have driven A10's impressive growth; this white paper maps out why A10 is the preferred choice.

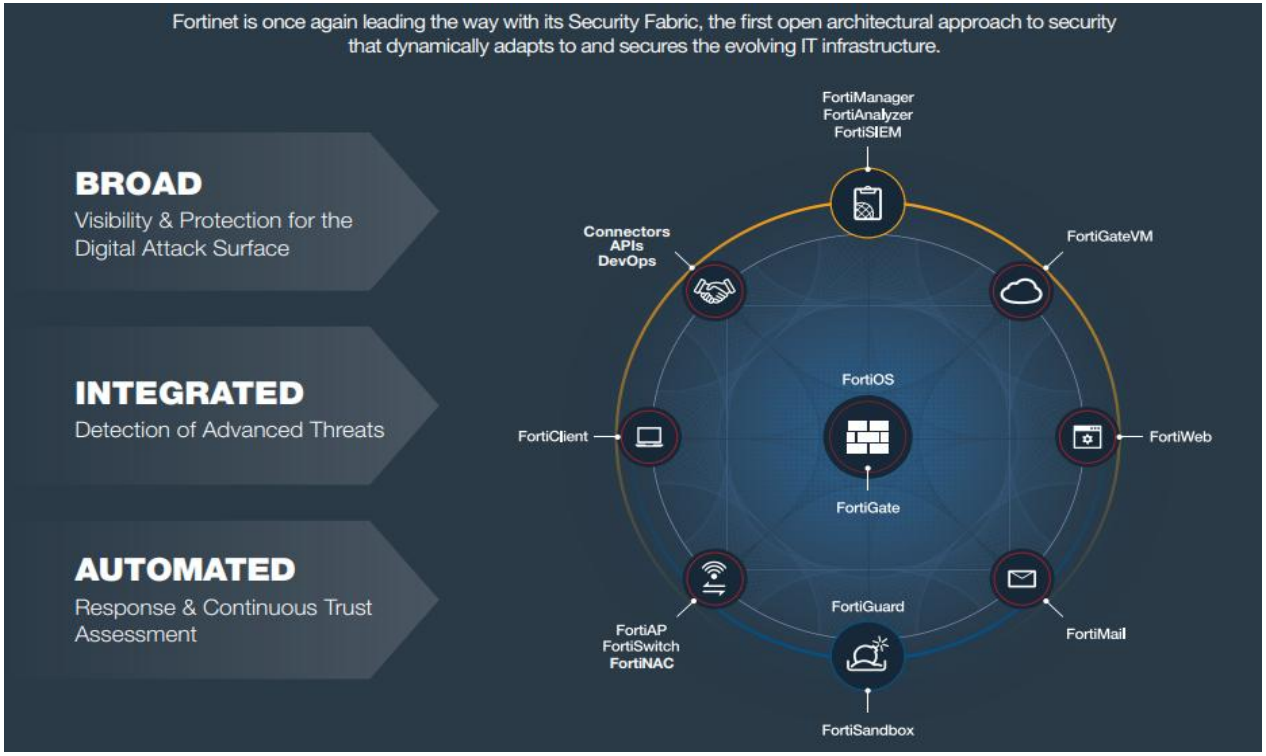


Comprehensive Network, Endpoint, Application and Access Security

Fortinet's mission is to deliver the most innovative, highest-performing network security fabric to secure and simplify your IT infrastructure. We are a leading global provider of network security appliances for carriers, data centers, enterprises, and distributed offices.

We provide top-rated network and content security, as well as secure access products that share intelligence and work together to form a cooperative fabric. Our unique security fabric combines Security Processors, an intuitive operating system, and applied threat intelligence to give you proven security, exceptional performance, and better visibility and control--while providing easier administration.

Our products covers: Network security, Multi-Cloud security, Web Application Security, Email security, Advanced Threat Protection, Secure Unified Access, Endpoint security, Management and Analytics



Threat Protection

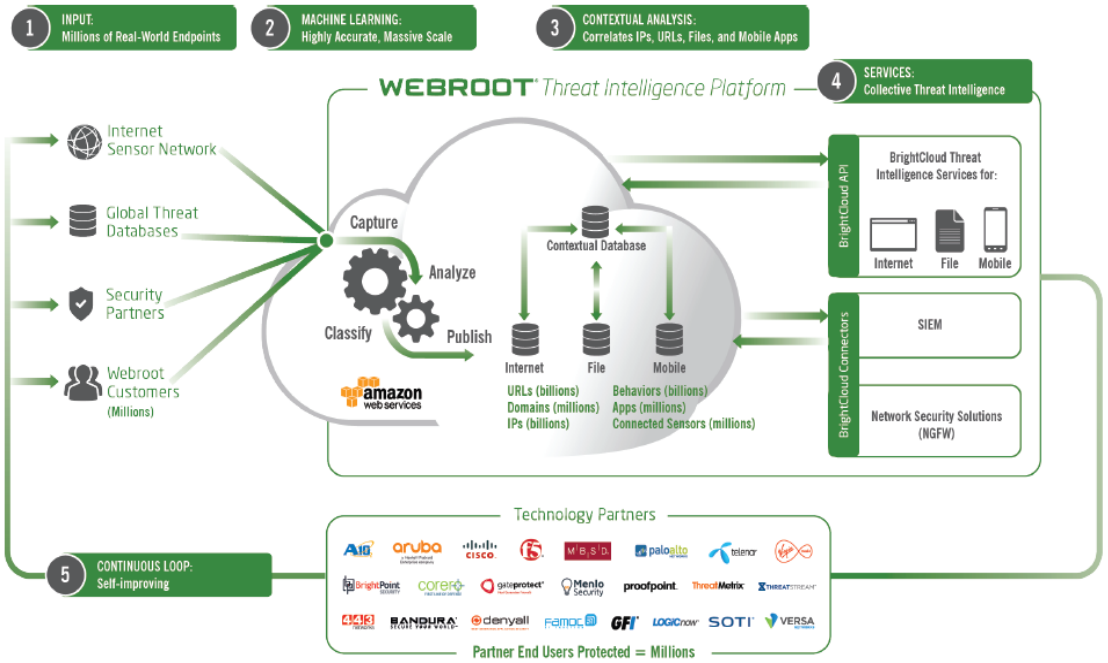
Threat Protection is the way to defend network by security solutions against sophisticated malware or hacking-based attacks targeting sensitive data. Advanced threat protection solutions can be available as software or as managed services.

Generally solutions include some combination of endpoint agents, network devices, email gateways, malware protection systems, and a centralized management console to correlate alerts and manage defenses. Therefore, we have three major functions: real-time visibility, context and Data awareness, with three key areas: Halting or mitigating threats before they breach systems, disrupting activity in progress or countering actions that have already occurred as a result of a breach and Interrupting the lifecycle of the attack to ensure that the threat is unable to progress or proceed

Next-generation Protection Endpoints, Networks and End-Users

Webroot delivers network and endpoint security and threat intelligence services to protect businesses and individuals around the globe. Our smarter approach harnesses the power of cloud-based collective threat intelligence derived from millions of real-world devices to stop threats in real time and help secure the connected world. Webroot maximizes your security, cuts bandwidth utilization, reduces resource loads on PCs, and shrinks cybersecurity disk space use. All the while, its centralized console streamlines management, saving you time and money on administration of your endpoint devices; while the agent itself automatically remediates infections.

Equally important to its functionality, Webroot protection provides you with the enterprise-level security without requiring on-site enterprise-level security expertise. Small and medium sized businesses have reported not only significantly better infection statistics since deploying Webroot solutions, but also saving 50% or more money than with their previous solutions.



Hadoop® nodes for massive transaction processing with high performance, ultra-fast response times

Cassandra™ Ring – for worldwide high availability Big Data analytics

Big Data Drives Predictive Identification of Malware by the Webroot Threat Intelligence Platform

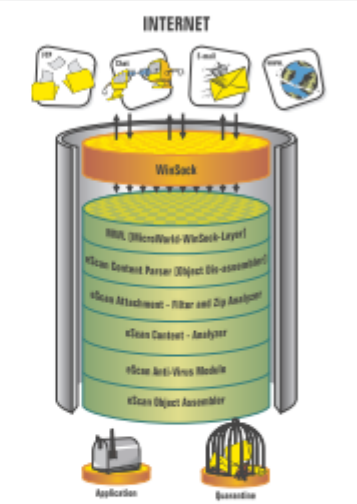
Enterprise Endpoint & Mobility Security

MicroWorld develops Information Security solutions that provide protection against current and evolving cyber threats. Our product portfolio includes eScan and MailScan that encompass Anti-Virus, Anti-Spyware, Content Security, Anti-Spam and Network Intrusion Prevention solutions. Incorporated in the USA with offices worldwide, we are represented by our partners across the globe.

eScan's Enterprise Endpoint Protection (EPP) provides an unified security solution to protect and manage enterprise data, systems and network in a platform agnostic environment. eScan's EPP uses a combination of advanced technologies to provide real time monitoring and protection against evolving cyber threats such as Ransomware, DDoS, APT or targeted attacks.

MicroWorld Winsock Layer (MWL) Technology

MicroWorld-WinSock Layer (MWL) is a revolutionary concept in scanning Internet traffic on a real-time basis. It resides on the Winsock Layer of the OS and scans all incoming and outgoing traffic from the Internet. It checks for any security violating content, passing all clean data packet, else removed before reaching the application layer.



MWL Technology

MWL, which is placed above the WinSock layer and acts as a 'Transparent Gatekeeper' on the WinSock layer of the operating system. All data packets coming on different TCP/IP ports are assembled. It then decodes e-mail and web traffic, FTP and ICQ traffic along with all the attachments and passes them through numerous filters such as Virus Filters, Content Filters, Attachment Filters, etc. These filters check validity of the file's content and issue dynamic notifications.

Proactive & Multi-Layered Security

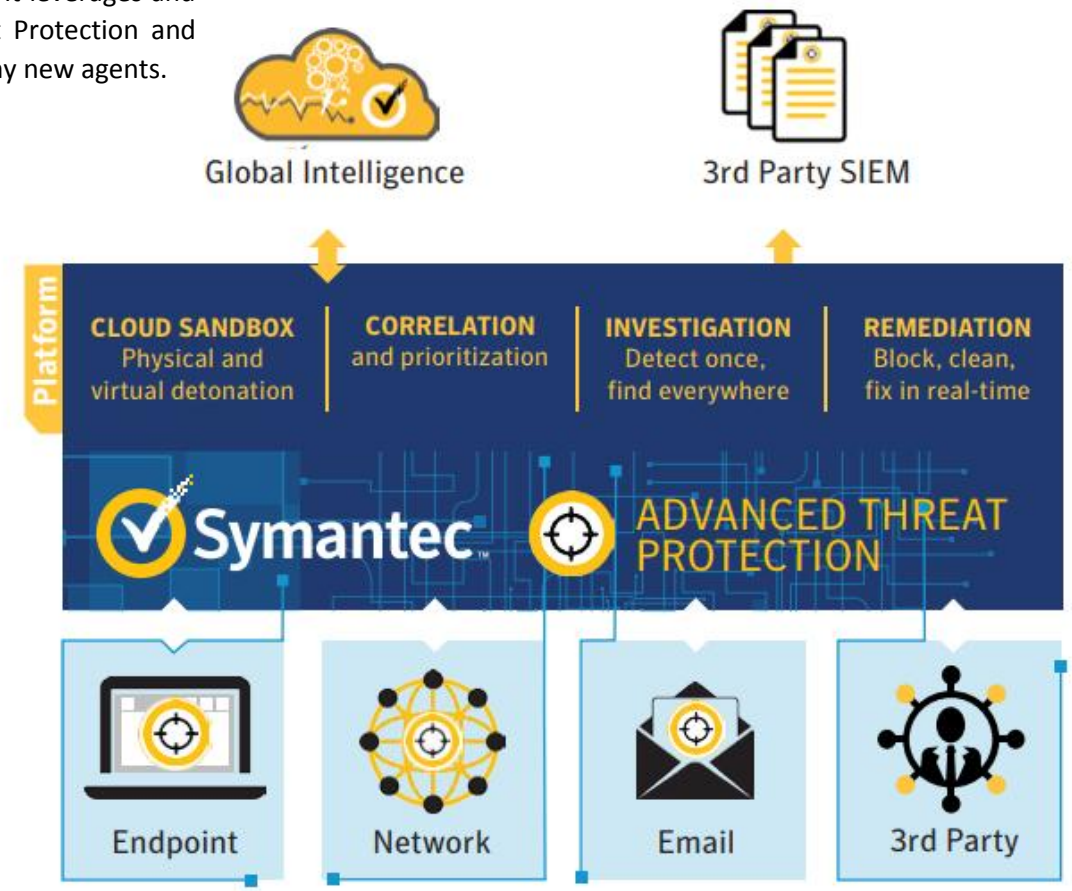
Since 2011, Heimdal Security has been developing new technologies and providing intelligence to protect over 350,000 users against cyber-criminal attacks and data security breaches.

Heimdal has been specifically designed to protect you from financial and data stealing malware, while doing banking operations and keep you safe from Zero Hour malware and security exploits frequently employed by IT criminals.

Heimdal is a proactive security solution that filters cyber threats before they reach your system, but also during and after cyber attacks. It does not work like a traditional antivirus, but rather complements it. Heimdal is focused on proactive Internet security, while antivirus is focused on reactive security.

ADVANCED THREAT PROTECTION

Symantec™ Advanced Threat Protection is a new unified solution to help customers uncover, prioritize, and quickly remediate today's most complex advanced attacks, across endpoints, networks and email. It leverages and enhances existing deployments of Symantec™ Endpoint Protection and Symantec™ Email Security. Cloud, and does not require any new agents.



Risk Assessment & Mitigation

Information technology, as a technology with the fastest rate of development and application in all branches of business, requires adequate protection to provide high security. The aim of the safety analysis applied on an information system is to identify and evaluate threats, vulnerabilities and safety characteristics. IT assets are exposed to risk of damage or losses. IT security involves protecting information stored electronically.

In the process of risk identification, its sources are distinguished by a certain event or incident. In that process, the knowledge about the organization, both internal and external, has an important role. Besides, experiences from this or a similar organization about risk issues are very useful.

Reduce Risk

Rapid7 (NASDAQ:RPD) powers the practice of SecOps by delivering shared visibility, analytics, and automation so that security, IT, and Development teams can work together more effectively. The Rapid7 Insight platform empowers these teams to jointly manage and reduce risk, detect and contain attackers, and analyze and optimize operations. Rapid7 technology, services, and research drive vulnerability management, application security, incident detection and response (SIEM), orchestration and automation, and log management

Advanced vulnerability assessment analytics and reporting

The modern network is no longer simply composed of servers and desktops; remote workers, cloud and virtualization, containers, and mobile devices mean your risk exposure is changing every minute. Utilizing the power of Rapid7's Insight platform and the heritage of our award-winning Nexpose solution, InsightVM provides a fully available, scalable, and efficient way to collect your vulnerability data from this modern environment, turn it into answers, and minimize your risk.

Continuously Assess & Identity Risk

SecureAuth addresses the missing link – continuous identity security – by creating intelligent intersections between security and identity. We help leading companies, their employees, their customers and their partners eliminate identity-related breaches. As a leader in access management, identity governance, and penetration testing, SecureAuth is powering an identity security revolution by ensuring the continuous assessment of risk and enablement of trust. Our highly flexible Identity Security Automation (ISA) Platform enabling people and devices to intelligently and adaptively access systems and data, while effectively keeping bad actors from doing harm. We make it easier for organizations to prevent the misuse of credentials and exponentially reduce the enterprise threat surface

SecureAuth is focused on solving the #1 problem in cybersecurity – Eliminating Identity-Related Breaches. We're constantly raising the bar by continuously assessing risk and enabling trust to improve identity security.

Penetration testing assessments are also useful in validating the efficacy of defensive mechanisms and determining how well end-users adhere to security policies.

SecureAuth is recognized in Gartner Magic Quadrants for Identity Governance and Administration, and Access Management, and is named leader in multiple categories by KuppingerCole. SecureAuth has also named a 2018 Gartner Peer Insights Customers' Choice for Access Management, Worldwide. Furthermore, we have received numerous awards including being honored by SC Awards and SC Awards Europe, Best Companies Group: Best Places to Work, Cybersecurity Excellence Award, Stevie American Business Awards, CRN, and Cybersecurity Breakthrough Awards to name a few.

Asset Management, Monitoring, Network & Data Security

With Quest, you and your organization can spend less time on IT administration and more time on business innovation.

Proactive threat detection with Change Auditor Threat Detection: Simplify user threat detection by analyzing anomalous activity to rank the highest risk users in your organization, identify potential threats and reduce the noise from false positive alerts.

Enterprise Reporter Suite helps you keep your Microsoft environment — both on premises and cloud-based — secure and compliant. Comprehensive access assessments and built-in reporting provide deep visibility into Active Directory (AD)/Azure AD, Exchange/Exchange Online, Office 365, Azure, OneDrive for Business, Windows Servers, SQL Servers and NAS/SAN storage, including Azure resources, users, groups, permissions and other configurations.

KACE: Endpoint Systems Management Appliances Provision, manage, secure, and service all network-connected devices

Foglight for Databases: monitoring all your diverse databases centrally, through a single console that increases visibility, you can proactively improve database performance. With alerting, diagnostics, performance analytics and more, you will easily optimize database health – across your entire environment.

NetVault Backup: Protecting enterprise data in complex IT environments can be time-consuming, cumbersome and often incomplete. First, it's not uncommon for backup and recovery solutions to be complicated to install, often requiring help from the vendor's professional services staff, adding to your cost. Then learning to manage and maintain these solutions can take its toll — especially in virtualized environments with multiple operating systems and applications. NetVault Backup simplifies enterprise data protection with powerful, yet easy-to-use features.

Security Intelligence & Incident Response

Involves the real-time monitoring and detection of security events on a computer or computer network, and the execution of proper responses to those events. Computer security incident management is a specialized form of incident management, the primary purpose of which is the development of a well understood and predictable response to damaging events and computer intrusions.

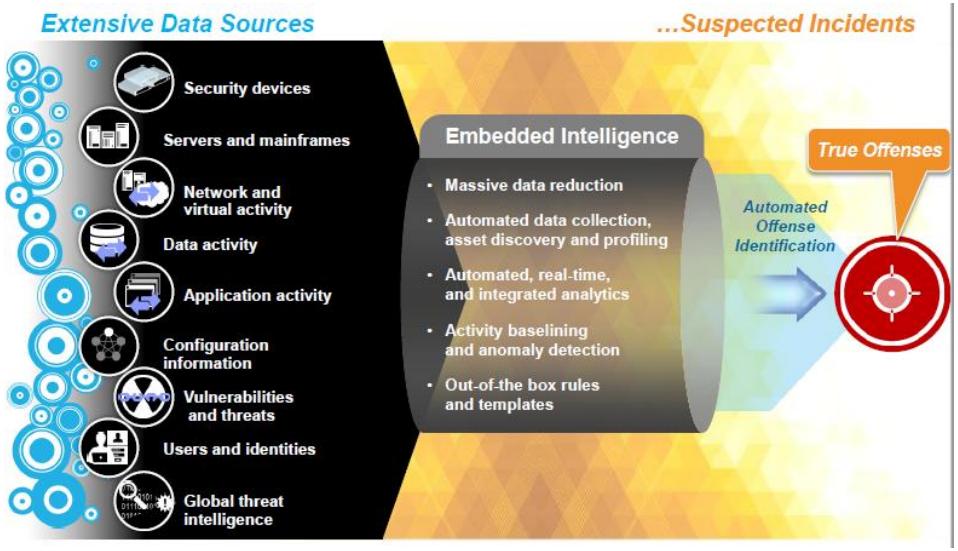
An effective investigation and analysis will lead to determine root cause, attack vectors, data loss and adequate response, finally it enhance the adaptive threat response process to achieve automation.

Integrated Security

IBM integrated security intelligence protects businesses around the world. New technological capabilities come with new vulnerabilities. IBM offers a deep enterprise security portfolio, analytics and real-time defenses customized to your company's needs.

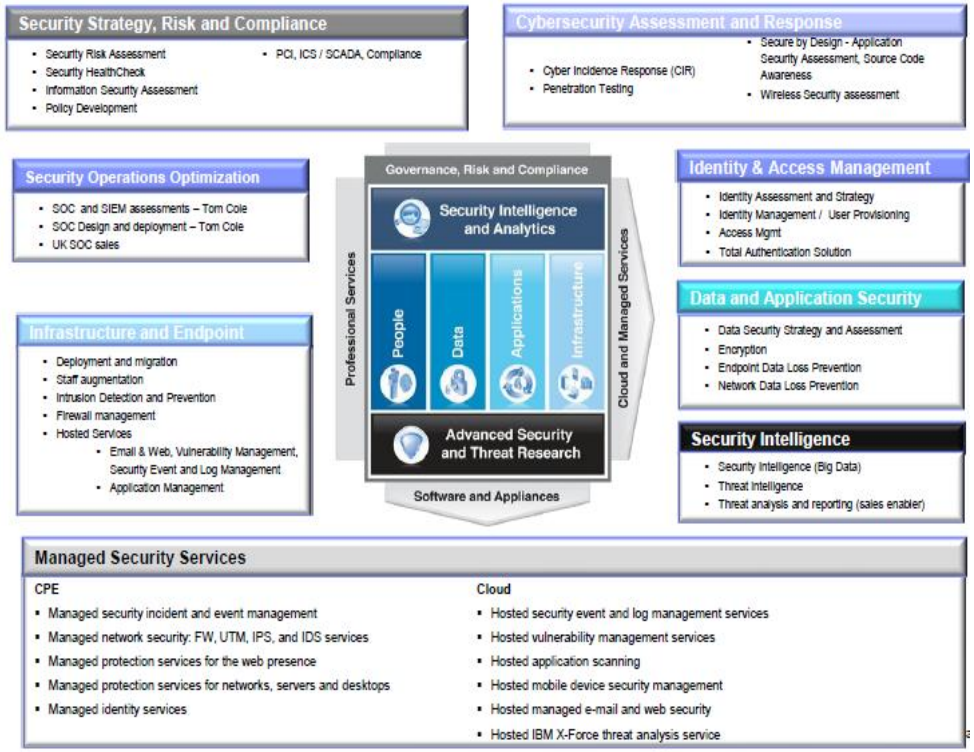
The IBM Security Framework provides a more integrated, intelligent approach to security. The application of security intelligence and analytics along with external threat intelligence helps organizations to detect, analyze and remediate threats that point products will always miss.

Unmatched in ability to help you disrupt new threats, deploy security innovations and reduce the cost and complexity of IT security, IBM can safeguard your most critical data from compromise.



It helps you build a strong security posture that can reduce costs, improve service and enable innovation.

IBM offers a deep enterprise security portfolio customized to your company's needs. Unmatched in ability to help you disrupt new threats, deploy security innovations and reduce the cost and complexity of IT security, IBM can safeguard your most critical data from compromise.



Industrial Control Systems

Nozomi Networks is the leader in Industrial Control System (ICS) cyber security, with the most comprehensive platform to deliver real-time cyber security and operational visibility. Innovating the use of artificial intelligence, our company helps the largest industrial facilities around the world See and Secure™ their critical industrial control networks. Nozomi Networks has been delivering cybersecurity and operational visibility solutions for industrial control systems (ICS) since 2013.

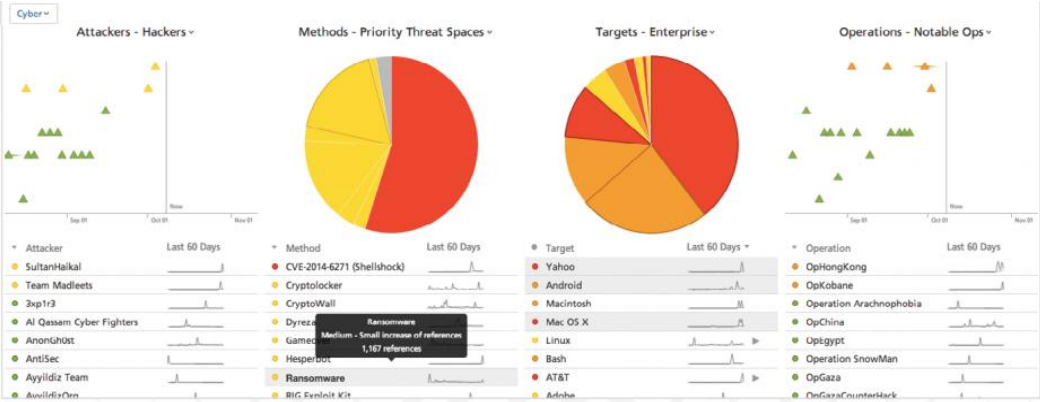
The company was founded by Andrea Carcano, an authority in industrial network security and Moreno Carullo, an expert in artificial intelligence. By applying network behavioral analytics to ICS environments, Nozomi Networks' flagship product, SCADAguardian, delivers real-time visibility into process network communications and configurations. Its ICS network mapping and automated process analysis detects cyber-attacks and operational missteps for immediate remediation.

Threat Intelligence

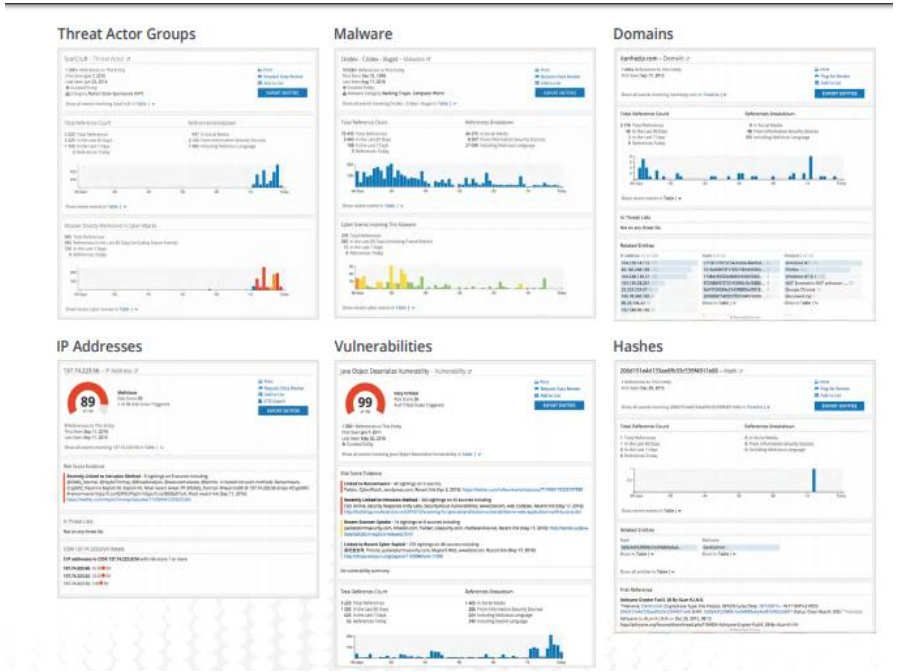
Recorded Future

Recorded Future arms you with real-time threat intelligence so you can proactively defend your organization against cyber attacks. With billions of indexed facts, and more added every day, our patented Web Intelligence Engine continuously analyzes the entire Web to give you unmatched insight into emerging threats. Recorded Future helps protect four of the top five companies in the world. Recorded Future delivers threat intelligence powered by machine learning, arming you to significantly lower risk.

Recorded Future is the only provider offering threat intelligence software powered by patented machine learning and delivered at scale, combined with world-class intelligence services and cyber research expertise to help security professionals identify, prioritize, and quickly respond to relevant threats targeting their organization. Recorded Future is laser focused on delivering actionable threat intelligence while dramatically reducing the time-consuming manual processes of threat intelligence analysis.



Overview of your threat environment tailored to your organization and industry.



Telecom Solutions

A Connected World Needs a New Generation of Telecom Solutions

Telecommunications technologies have undergone enormous changes over the last decades. With the convergence of voice, video and data, the proliferation of internet and IP-based protocols, the unification of fabrics in the data centers, the transformation of telecom hardware -specific devices to software systems, a complete new era of telecom solutions is sweeping the industry. All enterprises must re-evaluate and adapt their telecom infrastructures.

Using best-of-breed products from top-class leading vendors blended with high quality services and custom made telecom solutions; our clients are able to transform their telecom infrastructure, improve offered services and increase client satisfaction and loyalty. Our approach is to view the systems and telecoms infrastructure as a unified environment of integrated systems that constitute the underlying platform for business applications to run smoothly and transparently.

IT /TELCO Solutions and Services

Mediafon group provides various IT and telecommunication services for Lithuanian and foreign business customers, operators and governmental institutions. More than 19 years of experience and customer oriented attitude allows us to offer our customers advanced IT and telecommunication services.

Mediafon Datapro specializes in the development, provision and maintenance of databases and process automation systems and provides such solutions as CEIR, Customer portal, SIM-box and professional services and number portability NPCDB.

Mediafon Technology specializes in development and provision of IT/TELCO products and services. Our product portfolio includes not only IT and VoIP solutions and services but also artificial intelligence appliance and advanced digital signature solutions. We also built future IT technologies in our R&D center.

Mediafon TELCO SOLUTION provides fraud prevention services helps operators to secure revenue from international interconnect, while detecting and stopping all existing ByPass scenarios currently used by fraudsters.

Mediafon Carrier Services is the market leader in the Baltic States for voice traffic transit services and an alternative operator in Lithuania that provides wholesale fixed line and mobile services for national and international operators.

PROPOSED SERVICES

Address: Rue Turkie, Imm Jaeim Sahloul, 4054 – Sousse – Tunisia
Web: http://ste-smart-it.com
Email: contact@ste-smart-it.com
Fix: +216 73 368 940