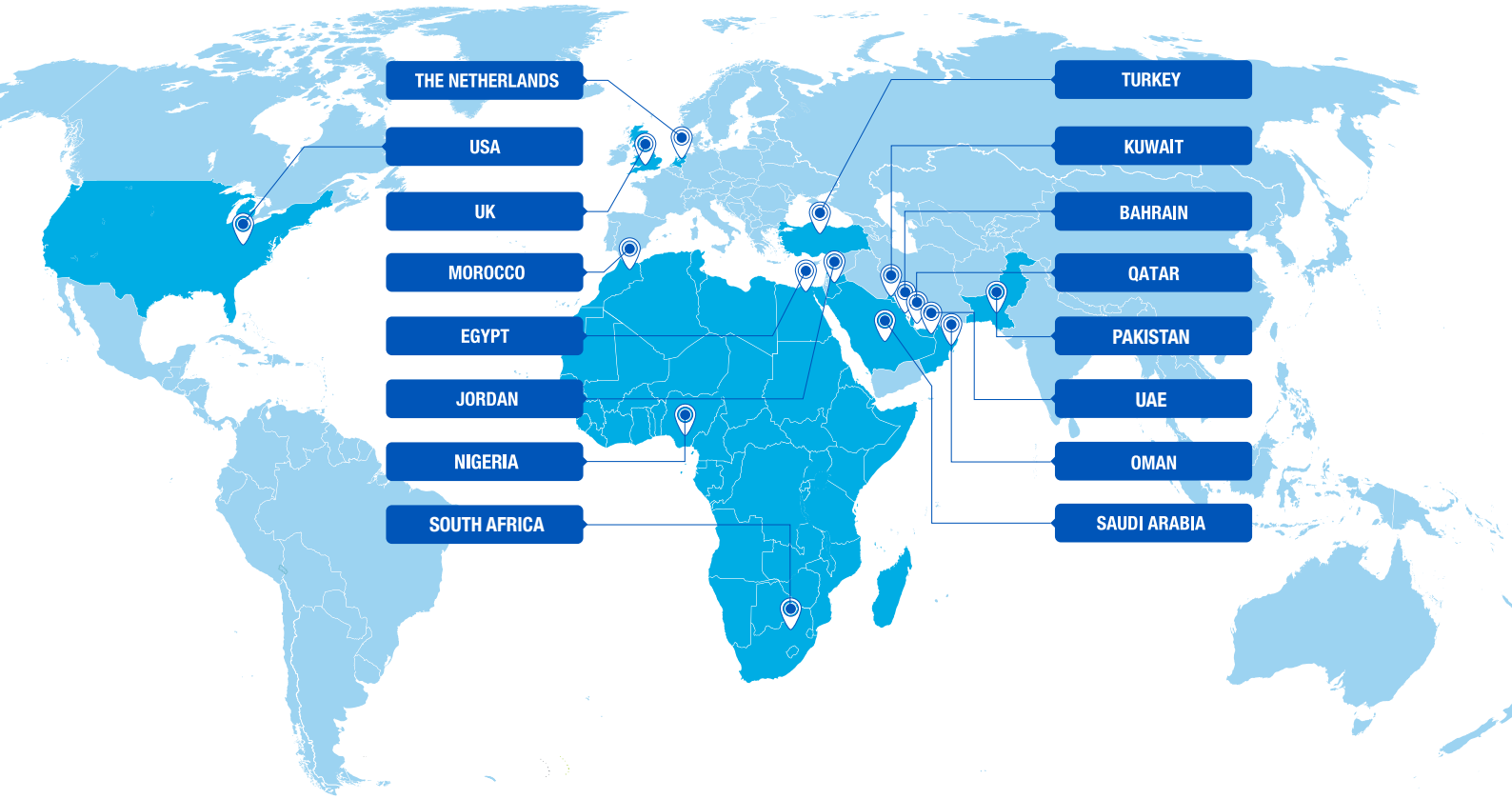

STARLINK
TRUSTED SECURITY ADVISOR
TRUE VALUE-ADDED
IT DISTRIBUTOR
ACCELERATE
AT THE SPEED OF STARLINK

About Us



Who We Are

StarLink is acclaimed as the largest and fastest growing "True" Value-Added IT Security Distributor across the Middle East, Turkey and Africa regions with on-the-ground presence in 16 countries.

With its innovative Security Framework and Vertical Security Trend Matrix StarLink is also recognized as a "Trusted Security Advisor" to over 2200 enterprise and government customers that use one or more of StarLink's best-of-breed and market-leading technologies, sold through our Channel network of over 1100 Partners.

The StarLink Solutions Lifecycle helps Channel Partners differentiate offerings, and assists customers to identify key risks and define priorities for addressing IT Security gaps relating to compliance and next-generation threat protection.

Overview

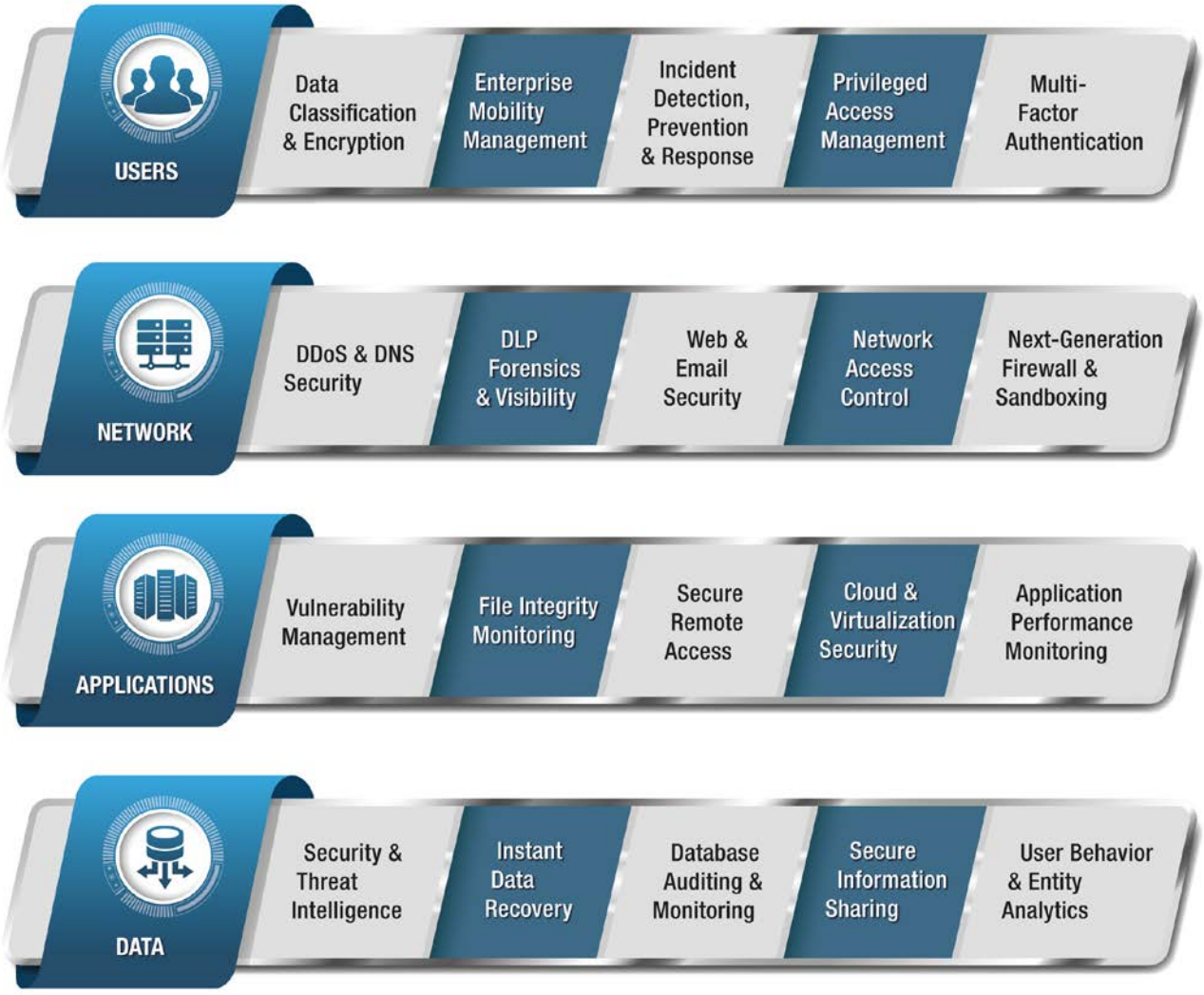
StarLink Vertical Security Trend Matrix

In recent years we have seen many changes in IT security. In an attempt to keep up with new and increasing threats to enterprise and government entities, traditional approaches to IT Security have limited impact. Organizations are dedicating more resources to IT Security and risk but attacks and vulnerabilities are increasing in frequency and sophistication.

The StarLink Vertical Security Trend Matrix provides Security leaders in the key verticals of Government, Telco, Oil & Gas and Banking, insight into how the latest IT Security trends cater to their respective industries, in order to address today's compliance and next-generation threat protection requirements.

The top 5 IT Security trends are namely, Behavioral Analytics, Internet of Things, Cloud, Mobile and Incident Response.

Overview



StarLink Security Framework

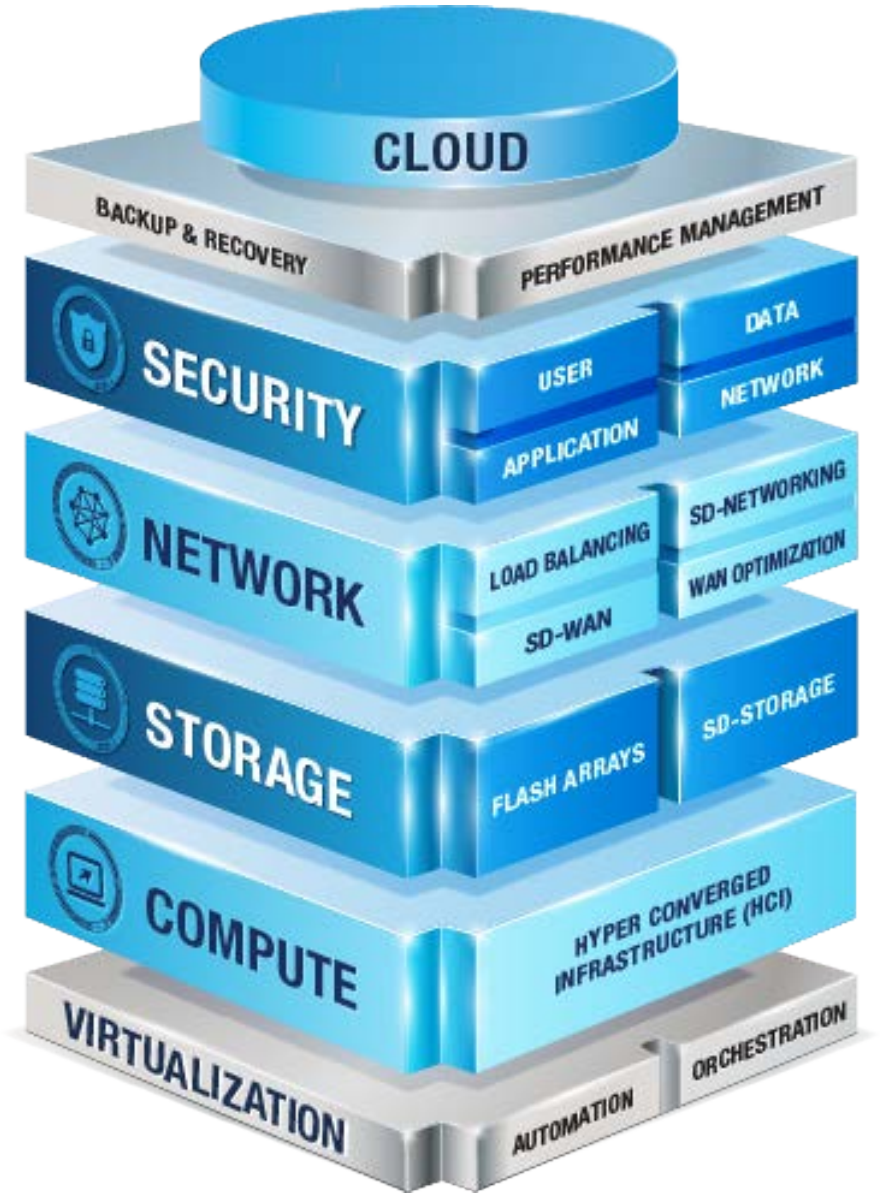
IT Security is a fragmented market, proliferated with many point products that are designed to address specific risks, and which may meet targeted compliance goals, but these solutions typically fail to provide a comprehensive, integrated picture of the threat landscape.

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.

To successfully deliver security capable of addressing today's risks, organizations need to take a holistic approach to IT Security. The StarLink Security Framework provides a strategic approach that cuts through the clutter and is designed to simplify risk management and ensure that all critical controls for effective enterprise IT Security are in place.

StarLink delivers real value to customers and partners with its vendor-agnostic and technology-centric Security Framework. Decision-makers can quickly and easily visualize multiple security domains to help understand, prioritize and mitigate risk. The innovative defense-in-depth Security Framework helps customers define their strategic objectives, top-down. Customers are able to comprehensively achieve their IT security vision, from the User to the Network to the Application and finally to the Data.

Overview



SDDC Technology Architecture

The software-defined data center (SDDC) is now a key focus area for most organizations. The shift in the datacenter paradigm is about reducing costs and providing service agility. To maximize data center ROI, key Security factors needs to be fundamentally considered including lateral movement of malware, network security virtualization, orchestration, people and process.

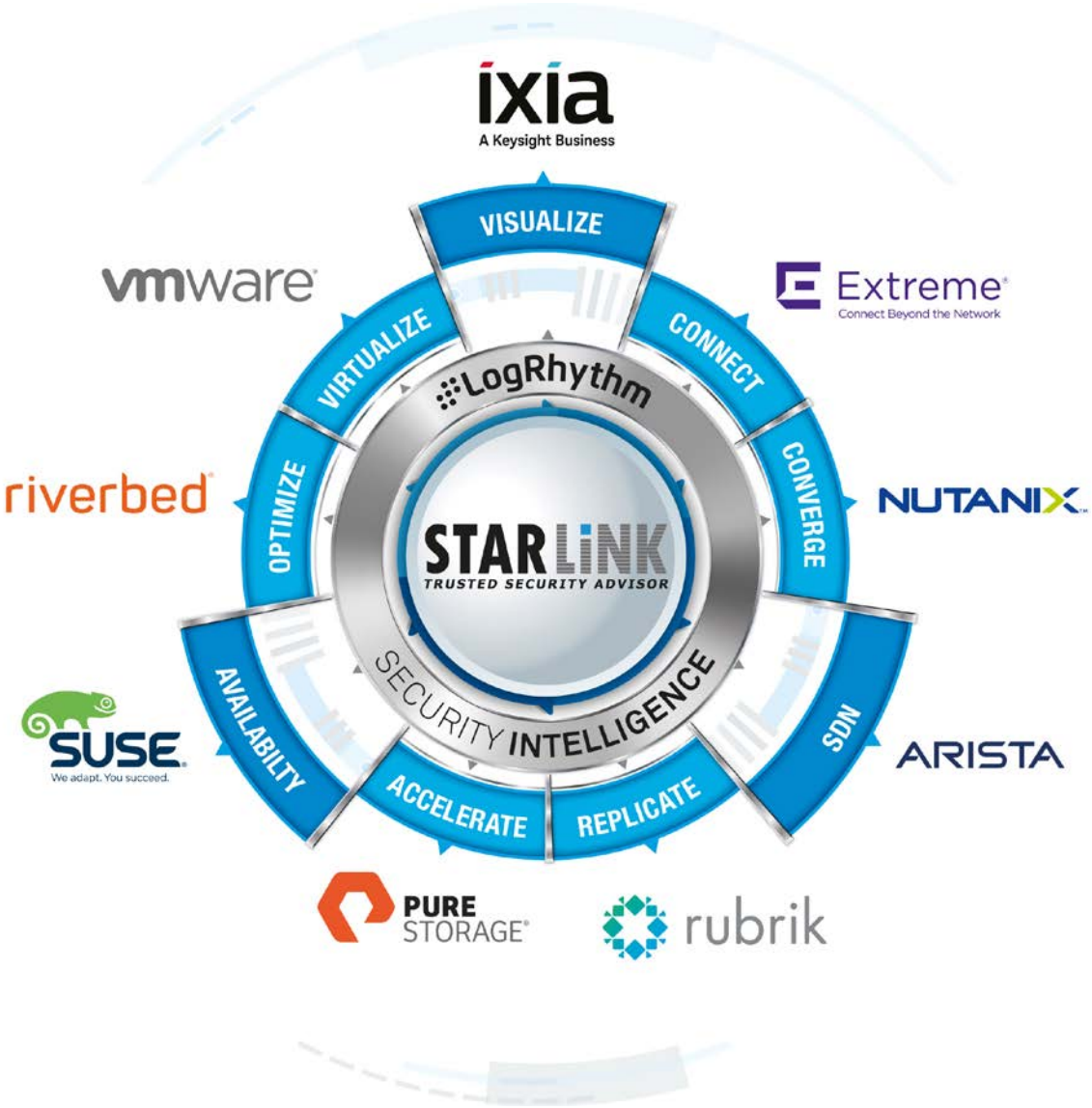
Simultaneously, with the surge in cyber threats including DDoS, against the cloud and IoT, as well as, ransomware leading to disruptions in IT and OT networks, plus mobile attacks and vulnerabilities on the rise, customers will be increasingly looking at automation and machine learning.

StarLink Solutions Lifecycle

IT security challenges can no longer be addressed by point products. Such products typically fail to provide a comprehensive, integrated picture of the threat landscape, each returning its own results but missing the opportunity to put results into context, falling short of enterprise-wide insights, and increasing the complexity of managing the IT security platform. At the root of the problem is the fact that most point solutions operate in silos; they typically do not integrate with other products in the security infrastructure. It becomes difficult for the security team to see through the noise and understand where real threats and real vulnerabilities are hidden.

An integrated approach requires capabilities to achieve compliance, as well as, to monitor for and prevent attacks on the network, on the endpoint and across other IT assets. Detected security concerns must be investigated quickly with tools that can integrate context from across the environment with the passing of security information, alerts and policies between security domains. Once this analysis is complete, security gaps can be bridged, and ongoing protection can be implemented. This methodology allows for faster, more effective identification and mitigation of potential security threats, as well as, helps in identification of behavior anomalies, risk prioritization, and increased visibility and control.

StarLink's portfolio has evolved into a uniquely integrated Solutions Lifecycle consisting of Datacenter & Cloud, Data Governance, Risk Analytics, Threat Protection, Secure Mobility, Incident Response, and Operational Intelligence. Each of these solutions comprise of vendors' core competencies, and feed into each other giving customers the ability to quickly understand their IT Security gaps, and set priorities accordingly, starting from achieving effective application performance and traffic visibility, to implementing critical controls, to verification of those controls, to zero-day malware protection, to sensitive data consumption, to remediation of next-generation threats, and then back around again, while centrally consolidating visibility of all machine data to generate valuable insights.



Datacenter & Cloud

Is my Sensitive Data optimized?

Increasing Datacenter & Cloud performance and accelerating delivery, positively impacts storage, network and application environments, enabling the rapid detection of issues while securing sensitive data to minimize risk and ensure business continuity. Furthermore automation of network services for cloud and virtualization allows for enforcement of security policies, as well as, configuration and change management.

Finally, more devices are now connecting to more data from more sources, which creates network blind spots and have become a costly and risk-filled challenge. It is therefore critical to deploy a highly scalable visibility and secure DNS architecture that enables the elimination of current blind spots, while providing resilience and control to sensitive data without added complexity.

Network Visibility, Tap & Packet Broker

ixia
A Keysight Business

ixiacom.com

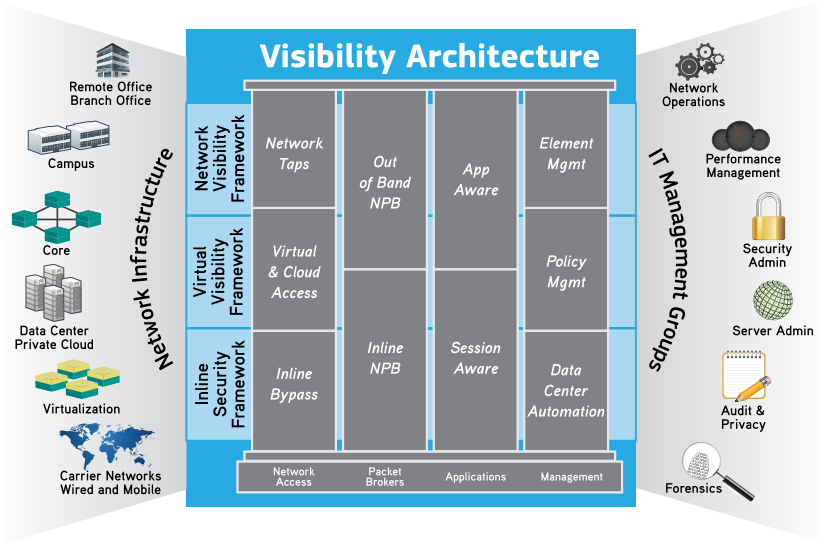
Ixia is a leading provider of network performance solutions that enable organizations to achieve optimized application and service delivery. Ixia's network lifecycle solutions enable customers to assess and validate the scale, performance and security of network infrastructure, devices and services, including resiliency testing and validation with real-world application traffic and attack simulation, and deliver end-to-end visibility across physical and virtual networks by providing access to data from any point in the network.

The Ixia Visibility Architecture

More mobile devices are now connecting to more data from more sources. IT challenges are complicated by increasingly high customer expectations for always-on access and immediate application response. This complexity creates network "blind spots" where latent errors germinate and pre-attack activity lurks. Stressed-out monitoring systems make it hard, if not impossible, to keep up with traffic and filter data "noise" at a rate that they were not designed to handle. Network blind spots have become a costly and risk-filled challenge for network operators.

The answer to these challenges is a highly scalable visibility architecture that enables the elimination of network "blind spots", while providing resilience and control without added complexity.

The Ixia Visibility Architecture is built on the industry's most comprehensive network visibility product portfolio and includes network access solutions, network packet brokers, application and session visibility solutions, and an integrated management platform.



Enterprise Networking Solutions

Extreme®
Connect Beyond the Network

extremenetworks.com

Extreme Networks is a software-and-service-led solutions company that provides advanced networking technology and platforms to solve today's tough networking challenges, reducing opex and driving IT efficiency. Extreme Networks' integrated solutions address the entire end-to-end wired and wireless network, including policy and compliance, network data analytics gathering to improve business outcomes, and performance. Extreme Networks is headquartered in San Jose, CA with more than 14,000 customers in over 80 countries, and has one of the highest Net Promoter Scores in the industry.

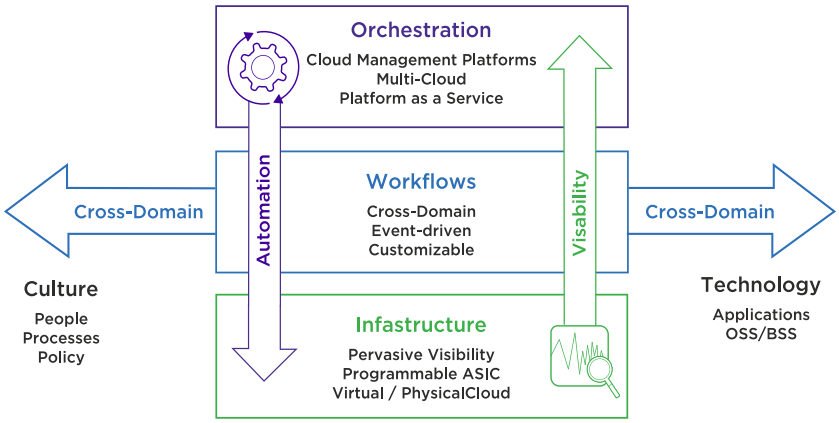


Figure 1: Digital transformation requires organizational agility across all domains.

Turnkey Hyperconvergence Infrastructure

NUTANIX

nutanix.com

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.

Modern Enterprise Datacenter

STORAGE + COMPUTE + VIRTUALIZATION

EXTENSIBLE | VM-CENTRIC
100% SOFTWARE-DEFINED

- 60 minutes — Fast Deployment
- Predictable Performance
- Scale-out One Node at a Time
- X 1 — One Platform to Manage
- 40-60% Lower TCO

Software Driven Cloud Networking

ARISTA

arista.com

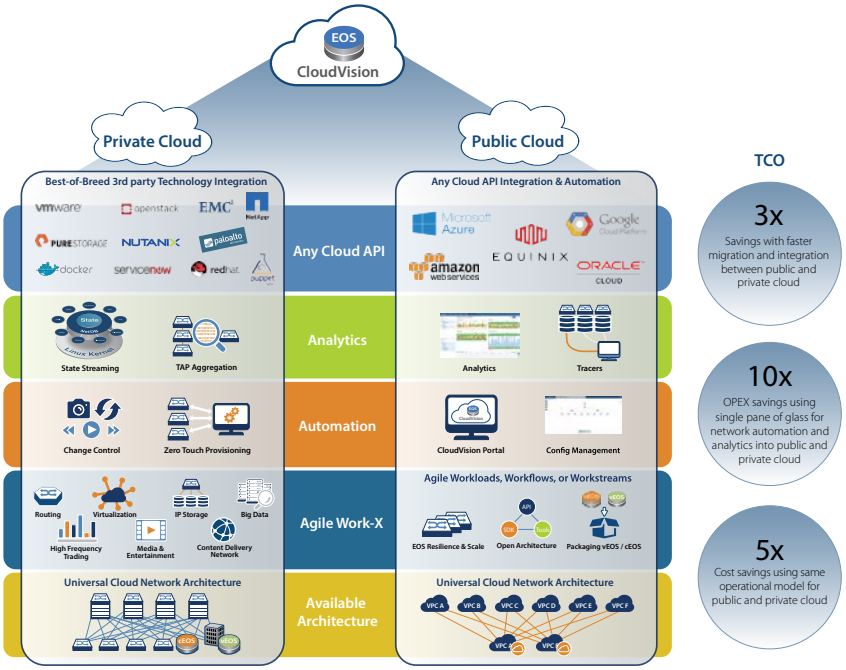
Arista Networks was founded to pioneer and deliver software driven cloud networking solutions for large data centre, high performance computing and cloud computing environments. Arista's switching and routing platforms have been designed in a number of form factors, port density and speeds for varying use cases.

Arista has built a revolutionary network operating system, Arista EOS® (Extensible Operating System), which is open, standards based and built on a stable, Linux core.

EOS provides a platform for customers to automate their IT workflows, while integrating with third parties to implement solutions in multi-vendor networks. EOS also enables customers to gain improved visibility, faster problem isolation and resolution, and greater visibility of network performance across physical and virtual networks.

Arista's platforms extend beyond the Data Centre, into Wide-Area, Service Provider and Campus environments. Customers include market leaders in Cloud, Service Provider, Content Delivery, Financial Services, Broadcasting and High Performance Computing globally.

UNIVERSAL CLOUD NETWORK AND ECOSYSTEM



Cloud Data Management

rubrik.com

Rubrik's Cloud Data Management platform democratizes public cloud for all enterprises by delivering a modern solution to recover, manage, and secure all data, regardless of location. The power within an enterprise to scale organically and respond to shifting business needs depends on instantaneous access, efficient data delivery, and intelligent data management across the entire organization. Rubrik eliminates the barriers to data mobility, providing mission critical functions needed to drive business agility, cost effectiveness, and performance as enterprises shift workloads to the cloud.

Rubrik Cloud Data Management is a single, software fabric that manages all data in the cloud, at the edge, or on-premises for many use cases including backup, disaster recovery, archival, compliance, analytics, and copy data management.

HOW IT WORKS

Data Management

The "brain" that handles the cradle-to-grave data lifecycle management for all your data (VMs, physical Linux servers, physical SQL databases, NAS) from ingest to retirement. Orchestrate versioned data, ensure data integrity, and apply content-aware global deduplication and compression. Use a single interface to manage all data sources across private and public clouds.

Atlas File System

A cloud-scale file system built from scratch to manage versioned data at scale. Atlas uses a hybrid flash and hard disk architecture to maximize I/O throughput, erasure coding for fault tolerance and data efficiency, and zero-byte cloning for application test and development without incurring additional storage penalty. Simply add nodes to increase storage capacity and I/O performance.

Distributed Task Framework

Assign and execute tasks across the cluster at scale in a fault tolerant and efficient manner. An intelligent task framework, designed to be masterless, divvies up tasks across cluster nodes based on data location and resource availability to deliver performance without compromising fault tolerance.

Enterprise Flash Storage Solutions

purestorage.com

Pure Storage helps companies push the boundaries of what's possible. The company's all-flash based technology, combined with its customer-friendly business model, drives business and IT transformation with Smart Storage that is effortless, efficient and evergreen. Pure Storage offers two flagship products: FlashArray//M, optimized for structured workloads, and FlashBlade, ideal for unstructured data. With Pure's industry leading Satmetrix-certified NPS score of 83.5, Pure customers are some of the happiest in the world, and includes organizations of all sizes, across an ever-expanding range of industries.

EFFORTLESS

Storage that just works

Pure Storage all-flash starts with unwavering reliability. FlashArray//M has proven 99.9999% availability over its first year of shipments – inclusive of upgrades and maintenance. That means your data is always-on, always-fast, and always-secure. One hour install is plug-n-play simple with an array that practically manages itself. And //M is cloud-connected, with unrivalled predictive support, and powerful analytics and protection.

EFFICIENT

Storage that does more

FlashArray//M lets you run lean with proven 5:1 average data reduction across the FlashArray install base – that's 2x better than the competition. Consolidate all your workloads safely with consistent mixed workload performance even through failures and upgrades, and get all your data services built-in and without performance penalty. Integrate and automate everything, seamlessly.

EVERGREEN

Storage that gets better with age

Get storage that behaves like SaaS and the cloud. Deploy it once and keep expanding and improving performance, capacity, density and/or features for 10 years or more – without downtime, performance impact, or data migrations. With the Evergreen™ Storage business model, you'll never re-buy a TB you already own.

Cloud Computing & Storage

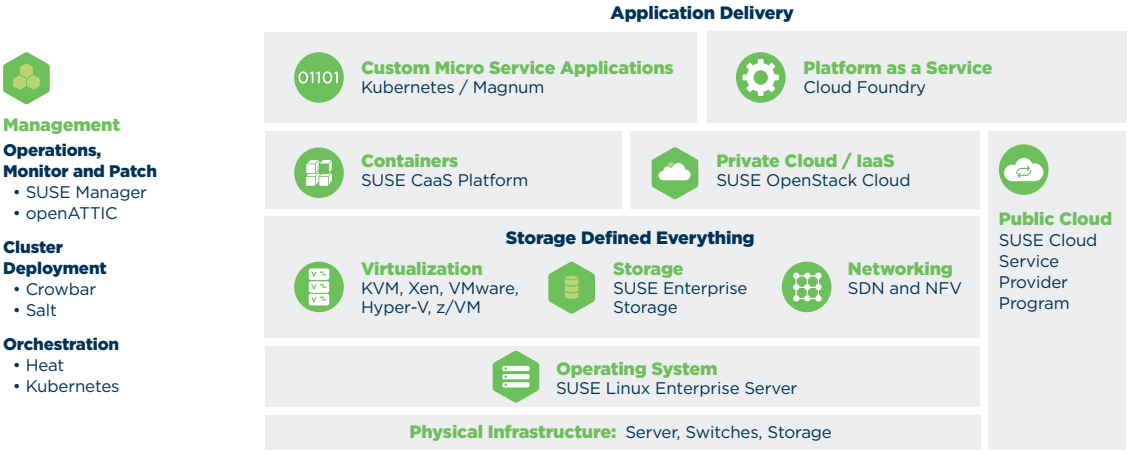
SUSE
We adapt. You succeed.

suse.com

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 20 years of engineering excellence, exceptional service and an unrivalled 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

An Open, Flexible Infrastructure Approach



WAN Optimization & Application Performance Platform

riverbed

riverbed.com

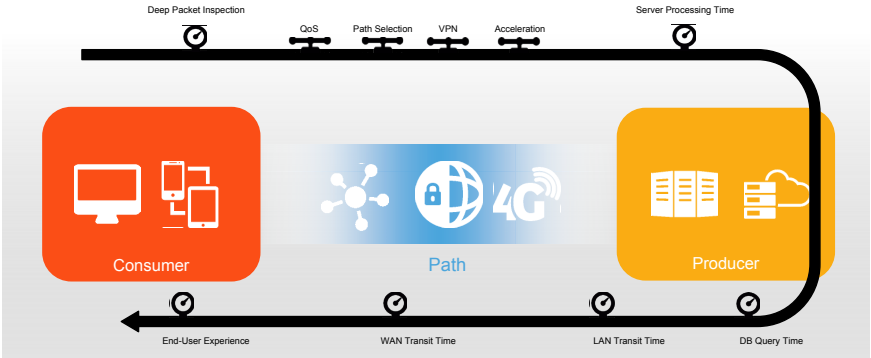
Riverbed Technology is the leader in Application Performance Infrastructure, delivering the most complete platform for location independent computing. Enterprise organizations rely on applications to power their businesses; therefore, Riverbed technology ensures the proper levels of performance namely through SteelHead, SteelCentral and SteelFusion which ensures WAN optimization, APM/NPM and the branch-in-a-box concept respectively.

SteelHead is the industry's #1 optimization solution for accelerated delivery of all applications across the hybrid enterprise. It also provides better visibility into application and network performance and the end user experience plus control through an application-aware approach to hybrid networking and path selection based on centralized, business intent-based policies for what you want to achieve – as a business.

SteelCentral drastically reduces the time and effort required to develop, deploy, and ensure application performance. Riverbed performance management and centralized management is the only end-to-end solution that combines user experience, application, and network visibility to detect and resolve issues before end users notice.

SteelFusion is the first and only hyper-converged infrastructure for branch IT, enables 100% consolidation of branch data and servers from remote sites into data centers, delivering complete data security and centralized data protection, without compromising on any of the benefits of running branch services locally for your users. SteelFusion eliminates the need for physical servers, storage and backup infrastructure at branch locations, creates the ability to instantly provision and recover branch services, and provides full visibility and superior performance of on-premises and cloud-based applications, leading to dramatic increases in data security, business continuity, agility and operational efficiency.

End-to-End Visibility, Optimization, and Control



Network Virtualization Platform for the Software-Defined Data Center

vmware®

vmware.com

VMware NSX is the network virtualization platform for the Software-Defined Data Center.

NSX enables the creation of entire networks in software and embeds them in the hypervisor layer, abstracted from the underlying physical hardware. All network components can be provisioned in minutes, without the need to modify the application.

Security

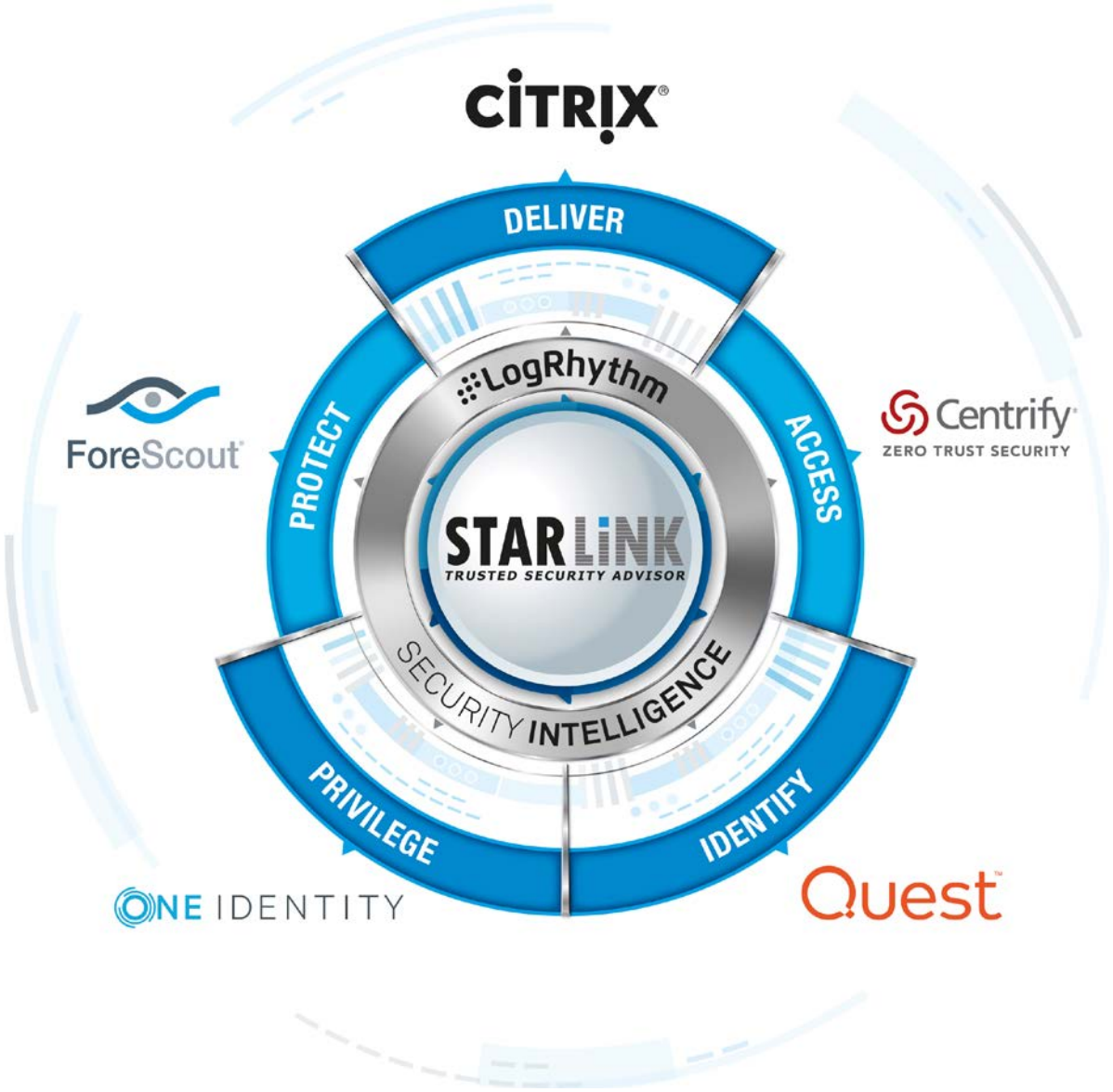
NSX embeds security functions right into the hypervisor. It delivers micro-segmentation and granular security to the individual workload, enabling a fundamentally more secure data center. Security policies travel with the workloads, independent of where workloads are in the network topology.

Automation

NSX lets you treat your physical network as a pool of transport capacity, with network and security services attached to workloads using a policy-driven approach. This automates networking operations and eliminates bottlenecks associated with hardware-based networks.

Application Continuity

NSX abstracts networking from the underlying hardware and attaches networking and security policies to their associated workloads. Applications and data can reside and be accessible anywhere. Move workloads from one data center to another, or deploy them into a hybrid cloud environment.



Access Control

Where is my Sensitive Data?

Access Control enables the organization to control access to sensitive data by understanding user privileges, securing privileged access and monitoring changes to directories, files, data repositories and databases, as well as, user activity. This in turn leads to alerts ensuring that sensitive data is only accessed by authorized users by providing comprehensive real-time visibility into all activities. Furthermore, classification mechanisms are put in place to guarantee that sensitive data cannot be leaked to unauthorized users. Finally the required processes and procedures to achieve continuous compliance are automated so that human error or risk of insider threats are minimized.

Secure Application and Data Delivery

citrix.com

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's 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.

Identity and Acccess Management

centrify.com

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 productivity through single sign-on, multi-factor authentication, mobile and Mac management, privileged access security and session monitoring. Centrify is trusted by over 5000 customers, including more than half of the Fortune 50.

WHAT WE DELIVER

Stronger Security + **Continuous Compliance** + **Enhanced User Productivity**

- Single sign-on
- Active directory bridging
- Privileged access security
- Multi-factor authentication
- Mac management
- Session monitoring
- Provisioning
- Enterprise mobility management
- Shared password management

IT & System Management, Network & Data Security

quest.com

Quest One-e-DMZ Security's Total Privileged Access Management (TPAM) Suite is a robust collection of integrated modular technologies designed specifically to meet the complex and growing compliance and security requirements associated with privileged identity management and privileged access control. The TPAM Suite provides organizations the flexibility to solve the critical issues associated with compliant privileged control in a modular fashion as needed on an integrated appliance.

The key modules that make up the TPAM Suite are:

Quest One Privileged Password Management: Secure storage, release control and change control of privileged passwords across a heterogeneous deployment of systems and applications is a requirement for all enterprises. Past internally developed solutions and procedures do not meet the needs driven by increased internal threats and compliance. The award winning capabilities of our Password Auto Repository (PAR) provides the enterprise class features, functions and scalability demanded by today's environment.

Quest One Privileged Password Management: Embedded, hard-coded accounts and passwords in scripts and applications are often overlooked back-door security vulnerabilities to the enter- prise. Through the robust CLI/API supported by PAR, hard-coded passwords can be replaced with a simple call script or program calls into PAR meeting the needs of application-to-application (A2A), application-to-database (A2DB) and application-to-system (A2S) requirements.

Quest One Privileged Session Management: From remote vendors to developer access to production or other privileged access requirements, the ability to control access, audit access, monitor access and record access is becoming more critical as companies converge internal resources and outsource. Our award winning TPAM suite provides full session management and controls including fine-grain resource access control, active session monitoring and full session recording in an unmatched size efficient format for future replay. Extensive session proxy types supported including: SSH, RDP, http/https, ICA, telnet, x5250, VNC and more.

Quest One Privileged Command Management: Enterprises today are being forced to do more with less resources. As a result, the need to provide restricted, controlled and delegated privileged access to internal resources is growing. The unique configurable privileged command capabilities provided through eGuardPost supports privileged access control down to the privileged command level. Not only are you able to control, record and monitor sessions - you can limit a users connection to a specific command for both Unix/Linux and Windows systems.

Privileged Access Management

oneidentity.com

Achieve complete, business-driven governance for identities, data and privileged access by marrying visibility and control with administration. Gain simplicity and affordability with a unified governance foundation that addresses the management, auditing and compliance needs that are prerequisites to strong governance.

Enhance your business performance with Identity Governance solutions that improve:

Enterprise Provisioning

Implement automated, codeless, business-driven provisioning of user identities and access privileges across the enterprise. Use a modeled approach and process orchestration to overcome the typical security and complexity limitations of traditional identity and access management frameworks.

Access Certification

Streamline the identity governance process of managing user identities, privileges and security across the enterprise, including application access, unstructured data and privileged accounts. Achieve all this by placing user management and access control into the hands of authorized business users.

Privileged Account Governance

Extend the governance advantages of unified policy, automated and business-driven attestation, enterprise provisioning, and access request and fulfillment to privileged accounts and administrator access. Simplify privileged governance with the ability to define roles and associated policies, access approval workflows and perform periodic attestation of privileged access.

Data Governance

Control, govern and grant access to one of your organization's most valuable assets - its data. Make it easier than ever by giving access control of sensitive data to business owners rather than IT.

You'll be able to ensure security and reduce the burden on your IT staff.

Network Security and Control

forescout.com

For Global 2000 enterprises and government organizations, ForeScout offers the unique ability to see devices the instant they connect to the network, control them and orchestrate information sharing among disparate security tools. Today, more than 2,000 customers rely on ForeScout.

Don't just connect the dots. Control them.

New devices join your network every hour. Unmanaged notebooks, smartphones and tablets. Internet of Things (IoT) devices of all shapes and sizes. Rogue endpoints. Servers. These devices significantly expand your attack surface yet are invisible to many security products. ForeScout can see them, control them and orchestrate system-wide response.

Transforming Security Through Visibility

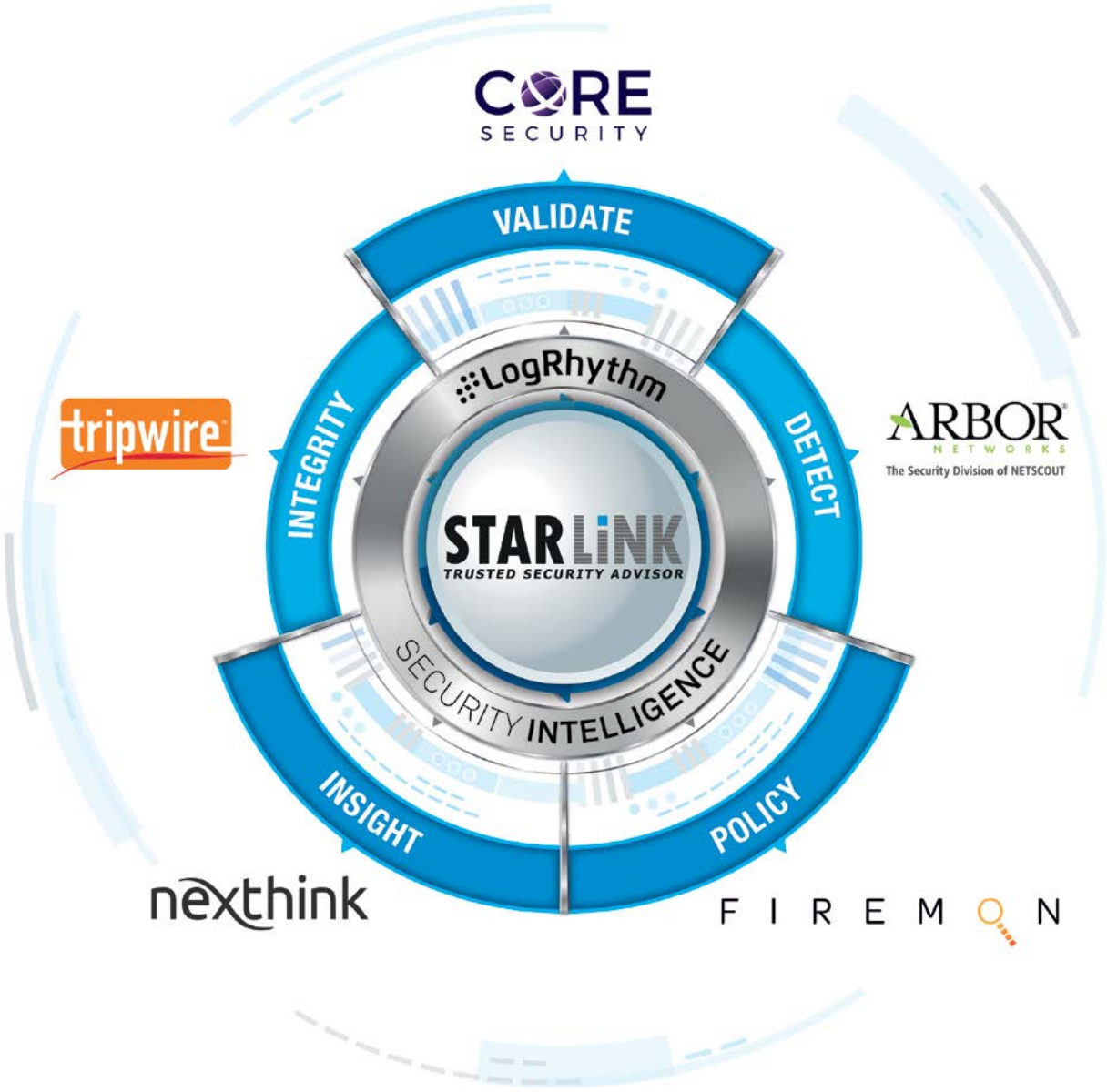
The unique capabilities of ForeScout can be summarized in three words:

See - The ForeScout CounterACT™ platform provides real-time visibility into IP-connected devices-managed and unmanaged, corporate and personal, wired and wireless. Because CounterACT™ doesn't require endpoint agents, it also discovers non-traditional IoT devices and personally owned BYOD devices. CounterACT™ identifies endpoints and applications; user, owner and operating system; configuration, software, patch state and the presence of security agents.

Control - CounterACT™ continuously scans the network and monitors the activity of every device. Unlike systems that simply flag violations and send an alert, CounterACT™ automates and enforces a comprehensive range of policy-based controls for network access, endpoint compliance and mobile device security.

Orchestrate - CounterACT™ integrates with more than 70 network and security. This ability to orchestrate information sharing and operation among security tools you already own allows you to:

- Share context and control intelligence across systems to enforce unified network security policy
- Reduce vulnerability windows by automating system-wide threat response
- Gain higher return on investment (ROI) from your existing security tools while saving time through workflow automation



Risk Mitigation

Is my sensitive data at risk?

Risk Mitigation ensures continuous monitoring of the entire corporate network and generates lists of vulnerabilities and deep risk metrics prioritized by importance for the IT Security decision maker. To ensure that the vulnerabilities are in fact relevant and do exist in context for the organization, it is then critical to automate the penetration testing of each of the vulnerabilities so that the list can be narrowed down to what is truly important to look at right away. It is also crucial to automatically produce a visual network topology map in order to understand how vulnerabilities at the network level, due to security configuration not being compliant in some areas of the network, can affect other areas of the network. This enables organizations to create threat models to proactively understand where threats can come from. Finally, many modern threats today, whether they be internal or external, can impact the entire network stack, and require effective traffic visibility and network forensics capabilities.

Vulnerability Aggregation, Penetration Testing & Validation

CORE SECURITY

coresecurity.com

Core Security is the leading provider of predictive security intelligence solutions for enterprises and government organizations. Built on the success of CORE Impact, the world's leading penetration testing tool, we help more than 1,400 customers worldwide proactively identify critical risks and match them to unique business objectives, operational processes and regulatory mandates. Core Security partners with a variety of complementary technology vendors to provide prebuilt integration and interoperability. Our patented, proven, award-winning enterprise solutions are backed by more than 15 years of applied expertise from CoreLabs, the company's innovative security research center.

Core Security : The Power of Thinking Ahead

As the leading provider of predictive security intelligence solutions, Core Security answers the call of organizations demanding a proactive approach to eliminating business risk. Our solutions empower customers to think ahead, take control of their security infrastructure and predict and prevent IT security threats.

Organizations have to predict security threats – not just react to them

Today, the majority of security spending is focused on solutions that take defensive or reactive approaches to threats. As a result, security teams are saddled with overwhelming amounts of disparate security data, tools that don't communicate and alerts that sound only after the damage has been done. Organizations that seek to survive and thrive must go on the offensive and predict and preempt threats before it's too late.

Core Insight Enterprise

- Enterprise-class predictive security intelligence platform
- Business risk identification, validation and prioritization
- Continuous threat simulation
- Continuous, proactive threat simulation
- Dashboard view of an organization's security risk profile
- Attack path discovery and remediation modeling

Core Impact Professional

- Automated, on-demand penetration testing
- Vulnerability validation from all leading scanners
- Multi-threat surface investigation
- Regulatory compliance verification

DDoS Attack Mitigation

ARBOR NETWORKS

The Security Division of NETSCOUT

arbornetworks.com

Arbor solutions provide multiple ways to identify and mitigate DDoS and other advanced targeted attacks. Arbor focuses on the network, identifying threats based on changes in traffic, proven counter-measures or threat intelligence from Arbor's research team (ASERT). Arbor also believes that workflow is key and our solutions are designed to help incident responders triage, investigate and block threats, better protecting the businesses in which they work.

Network Intelligence; Threat Detection and Mitigation; Incident Response and Security Forensics

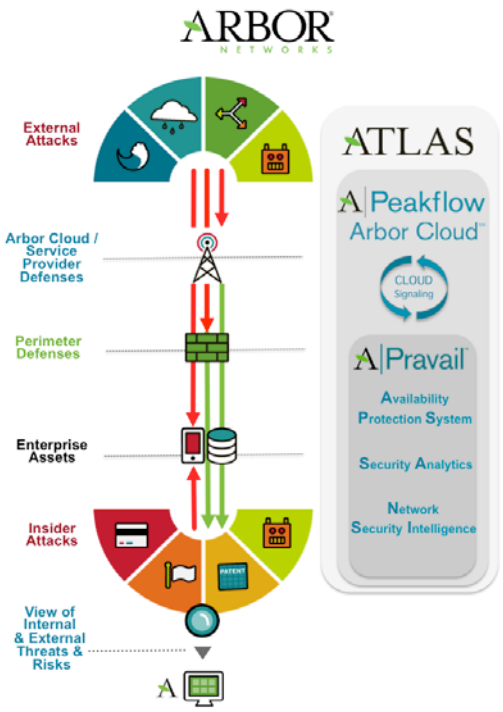
Arbor's Pravail® product portfolio has three areas of focus: protection from DDoS attacks; broad, cost-effective, scalable threat detection within the network perimeter; and, security analytics to reduce dwell time and improve the effectiveness of incident responders.

Unparalleled DDoS Protection and Network Visibility

As the leading network availability solution for the vast majority of global Internet service providers (ISPs) and many of the world's largest enterprises, Peakflow® offers proven DDoS protection and broad network visibility.

Multi-layered DDoS Protection – From the enterprise network to the Cloud

Arbor Cloud is powered by the world's leading experts in DDoS, using market leading DDoS protection technology. Whether your enterprise needs to maximize the availability of its network, services and applications-or you're a service provider seeking to launch or expand your managed DDoS protection service-Arbor offers a solution for you.



Enterprise Firewall Management

FIREMON

firemon.com

When you choose FireMon for network security policy management, you're getting 15 years of real-world cybersecurity problem-solving and the unique capabilities and services that come with that experience.

We take a holistic approach to security management that spans network security and operations to deliver on all four of Gartner's components in a Network Security Policy Management solution: security policy management, change management, risk and vulnerability analysis and application connectivity management.

Our solutions, whether the flagship Security Manager or the recently acquired Immediate Insight, work together to deliver unmatched visibility, integrations, automation and risk reduction.

With this approach, you gain a single source of truth for network security policy management that reduce complexity, inefficiencies and errors within your security infrastructure.

Solution Overview

1. Automation Of Manual Tasks

Streamline compliance auditing and validation processes by using automation to demonstrate that network access controls are in place at all times and are being tested frequently.

2. Dashboard-driven User Interface

Provides continuous management visibility into devices, complexity and compliance using web-based user interface that provides dashboard-driven, click-through reporting across the entire enterprise in a single pane of glass.

3. Unmatched In-depth Analysis

Provides conclusive, in-depth assessment of network security infrastructure using Elasticsearch that filters and slices global rule base using any combination of over 200 filter criteria, returning results in sub-seconds with the capacity to query thousands of devices at a time.

4. Unmatched Scalability

Security Manager distributes functions across multiple applications servers to perform simultaneous analysis and normalization across multiple platforms from multiple vendors, while splitting out reporting functions on a dedicated appliance.

5. Unmatched Data Retention

Security Manager stores every piece of data received indefinitely without any system performance degradation.

6. Deepest Visibility

Traffic Flow Analysis (TFA) features live traffic flow data and broader policy/rules search criteria, providing greater insight into the applications that are traversing a particular security rule.without any system performance degradation.

Endpoint Analytics & Management

nexthink

nexthink.com

Increase IT Efficiency

Supporting end-users and their multiple devices in today's hybrid environment means IT faces a relentless pace filled with change – both seen and unseen. Unlike data center tools which only monitor applications or the infrastructure, Nexthink's unique approach helps IT discover issues from the point of view of the end-user. Nexthink collects technical metrics from the endpoint related to the device, applications, connectivity and services being used, as well as direct feedback from the end-user to provide a new perspective into the end-user experience. With Nexthink, you will find and fix issues faster, deliver more reliable services, be more efficient and proactive resulting in more satisfied end-users.

Improve End-User Productivity

End-users care about fast devices, reliable apps and services that are always available. It matters to their productivity. By using real-time data collected on the endpoint and feedback from the end-user, Nexthink enables IT to: understand end-user experience in real-time, know when devices are slow, when users are having issues with an application or service, or are dissatisfied. With Nexthink, you can have a positive impact on end-user productivity by being more informed, more agile and more proactive.

Reduce Costs

IT is constantly under pressure to do more with less. Nexthink gathers comprehensive data about your endpoints, who is using them, how often they are being used and whether they are meeting the needs of the end-user. Nexthink also tracks information about how often services such as printing are used. Armed with this information, IT can quickly make data-driven decisions about how to effectively allocate IT budget, as well as identify areas where money is being wasted.

Vulnerability Management & Security Benchmarking

tripwire.com

Tripwire is the leading provider of Information Risk & Security Performance Management solutions to more than 6,500 businesses and government agencies worldwide. Tripwire solutions enable enterprises of all sizes to 1) automate compliance and reduce risk, and 2) measure and compare the performance of their IT security program with their own goals and industry peers.

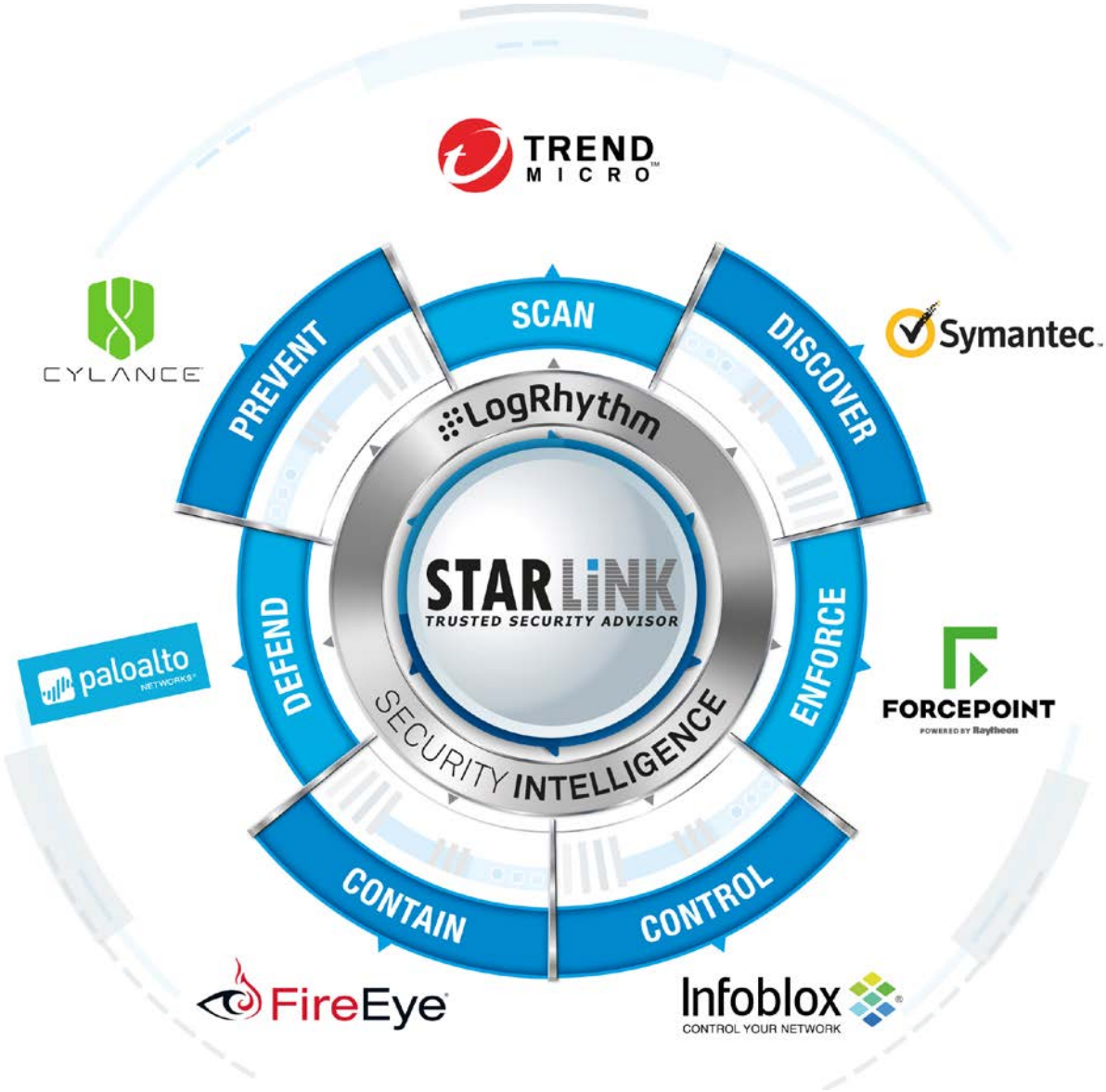
Tripwire delivers an integrated and open solution connecting Tripwire and third-party security products to leverage all available information to protect IT assets and high value data. Tripwire offers the industry's first security performance management application for CISOs - that gives CISOs a metrics language to communicate their company's security performance just like the CFO describes financial performance. From Vulnerability Management to agentless compliance policy auditing and file integrity monitoring,

Tripwire provides best-in-class products for reducing information risk and aligning security strategies with business initiatives. Tripwire delivers solutions for your business' security and compliance needs – regardless of size or industry.

How Tripwire secures your organization:

- Configuration Policy Auditing shows compliance against internal or international policies/baselines and alerts on deviations
- Vulnerability Management prioritizes remediation of vulnerabilities across the entire technology stack
- File Integrity Monitoring warns on unauthorized changes
- Web Application Scanning finds flaws across your websites
- Security Performance Management consolidates and compares security metrics from your security solutions

Tripwire is headquartered in San Francisco, CA, with regional offices throughout the United States, London and Toronto.



Threat Protection

How can I protect my sensitive data?

Threat Protection provides visibility into all relevant network traffic coming in and going out of the organization. This ensures that protection mechanisms are applied only where attacks can happen by analyzing the required traffic, web, email, file etc., to determine whether the traffic contains signature-based or signature-less threats that attempt to do damage or communicate back to a command and control centers (CnCs) for data exfiltration, and to stop any such communication. Once malware does enter a corporate environment, it is crucial to gain security intelligence into where it attempts to travel within the corporate network and protect endpoints and the datacenter. Simultaneously, a platform needs to be in place to ensure that any unknown malware cannot execute on any IT-managed resource so as to avoid any adverse direct effects to the computing environment. Finally with effective and powerful authentication, encryption and key management, data is always safe even if it falls into the wrong hands.

Cloud & Virtualization Security

trendmicro.ae

As a global leader in IT security, Trend Micro develops innovative security solutions that make the world safe for businesses and consumers to exchange digital information. With over 25 years of security expertise, we're recognized as the market leader in server security, cloud security, and small business content security.

Trend Micro security fits the needs of our customers and partners. Our solutions protect end users on any device, optimize security for the modern data center, and secure networks against breaches from targeted attacks. We deliver top-ranked client-server, network, and cloud-based protection that stops new threats faster, detects breaches better, and protects data in physical, virtual, and cloud environments.

Our security is powered by Trend Micro™ Smart Protection Network™ global threat intelligence and is supported by over 1,200 security experts around the world.

For more than 25 years, Trend Micro has innovated constantly to keep our customers ahead of an ever-evolving IT threat landscape. It's how we got to be the world's largest pure-play security software provider and the global cloud security leader.

It's how we continue to set the pace for the IT security industry: by delivering simple, integrated solutions that elegantly solve your most pressing challenges.

Today, those challenges stem primarily from three trends that are sweeping the business landscape and reshaping IT infrastructures everywhere:

Consumerization: The explosion of endpoints is boosting productivity-but with users controlling multiple devices and using unsecured consumer applications such as DropBox™ at work, it's also forcing IT managers to re-think traditional perimeter defenses.

Cloud and Virtualization: The growing use of cloud-based and virtualized computing drives dramatic efficiency and operational gains-but if security strategies are not evolved to fit these environments, those benefits are not realized and security gaps are created.

Advanced Cyber Threats: Yesterday's viruses and malware are still lurking out there, requiring vigilant updating of traditional defenses-but the current explosion of advanced targeted attacks demands new, customized detection and response capabilities.

Trend Micro delivers smart, simple security that fits your infrastructure and defends your key assets as well as your bottom line, by letting you fully realize the business benefits of today's technology trends-while avoiding the costs of relying on security that can't keep up. For more information, please visit www.trendmicro.ae.

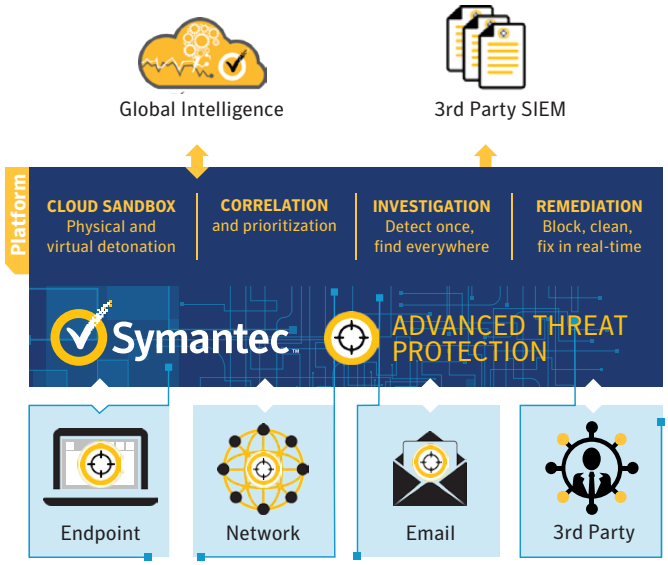
Network Forensics & Security Intelligence

symantec.com

A UNIFIED SOLUTION ACROSS CONTROL POINTS

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.



Web, Email, Data Security & DLP

forcepoint.com

Forcepoint brings fresh approach to safeguarding users, data and networks from insider and outsider threats.

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.

Insider Threat Detection

Forcepoint's new SureView® Insider Threat 8.0 gives customers an early warning system, automatically identifying the riskiest users within an organization, based on their behaviors as well as on information received from TRITON AP-DATA, Forcepoint's data loss prevention (DLP) solution. SureView Insider Threat gathers and provides rich context around user behaviors, including record and playback of user activities before, during and after risky behaviors.

Network Security

Delivering the most resilient and distributed next-generation firewall, Forcepoint's Stonesoft NGFW makes strong network security easy for highly distributed organizations. Now with Common Criteria certification, Stonesoft provides consistent visibility, responsiveness and policy enforcement across hundreds or thousands of locations with a single management console.

Cloud-based Protection of Office 365

With the move of enterprise applications to the cloud, data must be protected everywhere. The Forcepoint TRITON platform is now natively hosted in Microsoft Azure™, enforcing DLP for Microsoft Exchange Online in Office 365, directly from Microsoft's own cloud. Forcepoint's TRITON security solutions enforce consistent policy across the cloud, on premises and at endpoints, providing a unified, hybrid defense for distributed, highly-mobile organizations.

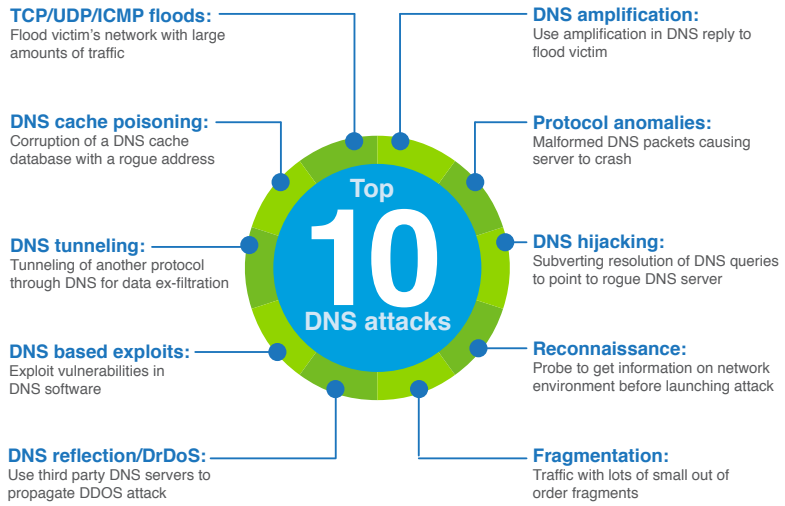
DNS, DHCP & IP Address Management

infoblox.com

Infoblox is the leader in Automated Network Control. Unlike traditional networks which are manual, fragile and vulnerable–Infoblox technologies make essential services of the modern network (such as DNS, DHCP and IP Address Management), automated, resilient and performing at their highest levels.

Infoblox revolutionized network services in 1999 when we delivered the first hardened DNS appliance, bringing a level of security and reliability network managers could not achieve previously. Infoblox has led the market ever since, and have the largest installed base of DNS, DHCP and IP address management (DDI) appliances.

PROTECTION AGAINST WIDEST RANGE OF DNS ATTACKS



Next Generation Malware, APT & Threat Protection

fireeye.com

Like water, cybercrime moves effortlessly around obstacles. Since governments and enterprises have implemented stronger policy and signature-based protections for regulated data and endpoints, sophisticated criminal organizations have changed their tactics, using different tools and targeting intellectual property and other networked assets.

Replacing mass-market malware, this next generation of threats is personalized and persistent. Threats are targeted, ever morphing, dynamic and zero-day. These carefully staged attacks look innocent as they walk by traditional firewall, IPS, anti-virus and Web gateways that rely on signatures and known patterns of misbehaviour. Once inside, malware phones home for instructions, which could be to steal data, infect other endpoints, allow reconnaissance, or lie dormant until the attacker is ready to strike.

FireEye is the leading provider of next-generation threat protection focused on combating advanced malware, zero-day and targeted APT attacks. FireEye's solutions supplement security defenses such as next generation and traditional Firewalls, IPS, AV and Web gateways, which can't stop advanced malware. These technologies leave significant security holes in the majority of corporate networks.

FireEye's Malware Protection Systems feature both in-bound and out-bound protection and a signature-less analysis engine that utilizes the most sophisticated virtual execution engine in the world to stop advanced threats that attack over Web and email. Our customers include enterprises and mid-sized companies across every industry as well as Federal agencies. Based in Milpitas, California, FireEye is backed by premier financial partners.

Today, security-conscious enterprises and Federal governments choose FireEye™ for industry leading protection against these next-generation threats. FireEye combats advanced malware, zero day and targeted APT attacks. FireEye's appliances supplement traditional and next-generation firewalls, IPS, AV and web gateways, adding integrated inbound and outbound protection against today's stealthy Web and email threats.

"Some IPS/IDS/NGFW vendors are no better at handling evasions today than they were when they released their original products."

Advanced Evasion Techniques: Weapon of Mass Destruction or Absolute Dud?, Bob Walder, Gartner, 2011

"With FireEye, we can now see and stop the attacks targeting our in-house and remote users. It has been an eye-opener for us to be able to determine with accuracy the threats that are passing through the firewall, URL gateway, IPS and antivirus." Director of Information and Data Security, Global 500 Financial Services firm.

Enterprise Security Platform

paloaltonetworks.com

Palo Alto Networks is leading a new era in cybersecurity by protecting thousands of enterprise, government and service provider networks from cyber threats.

Our game-changing security platform natively brings together all key network security functions, including a next-generation firewall, URL filtering, IDS/IPS and advanced threat protection. Because these functions are purposely built into the platform from the ground up, and they natively share important information across the respective disciplines, we ensure better security than legacy firewalls, UTMs, or point threat detection products.

The Palo Alto Networks platform can:

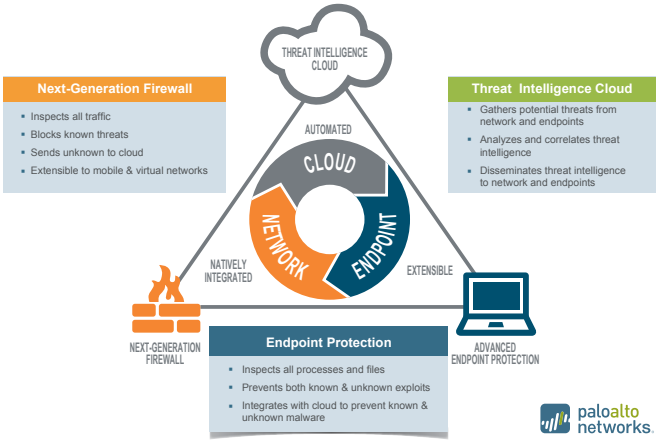
Eliminate gaping holes in an organization's security posture because it natively provides the right network security technologies and applies them in the right place in the network.

Safely enable applications and business operations because protection is based on a fine-grained visibility, correlation and control of what matters most in today's modern computing environments: applications, users and content, not just ports and IP addresses.

Eliminate the age-old compromise between security posture and business performance that organizations have faced for years because it is natively architected to operate in modern networks with new technology initiatives such as cloud computing, software-defined datacenters and mobility in mind.

With our platform, organizations can safely enable the use of all applications critical to running their business, maintain complete visibility and control, confidently pursue new technology initiatives and protect the organization from the most basic to sophisticated cyber-attacks - known and unknown.

Enterprise Security Platform



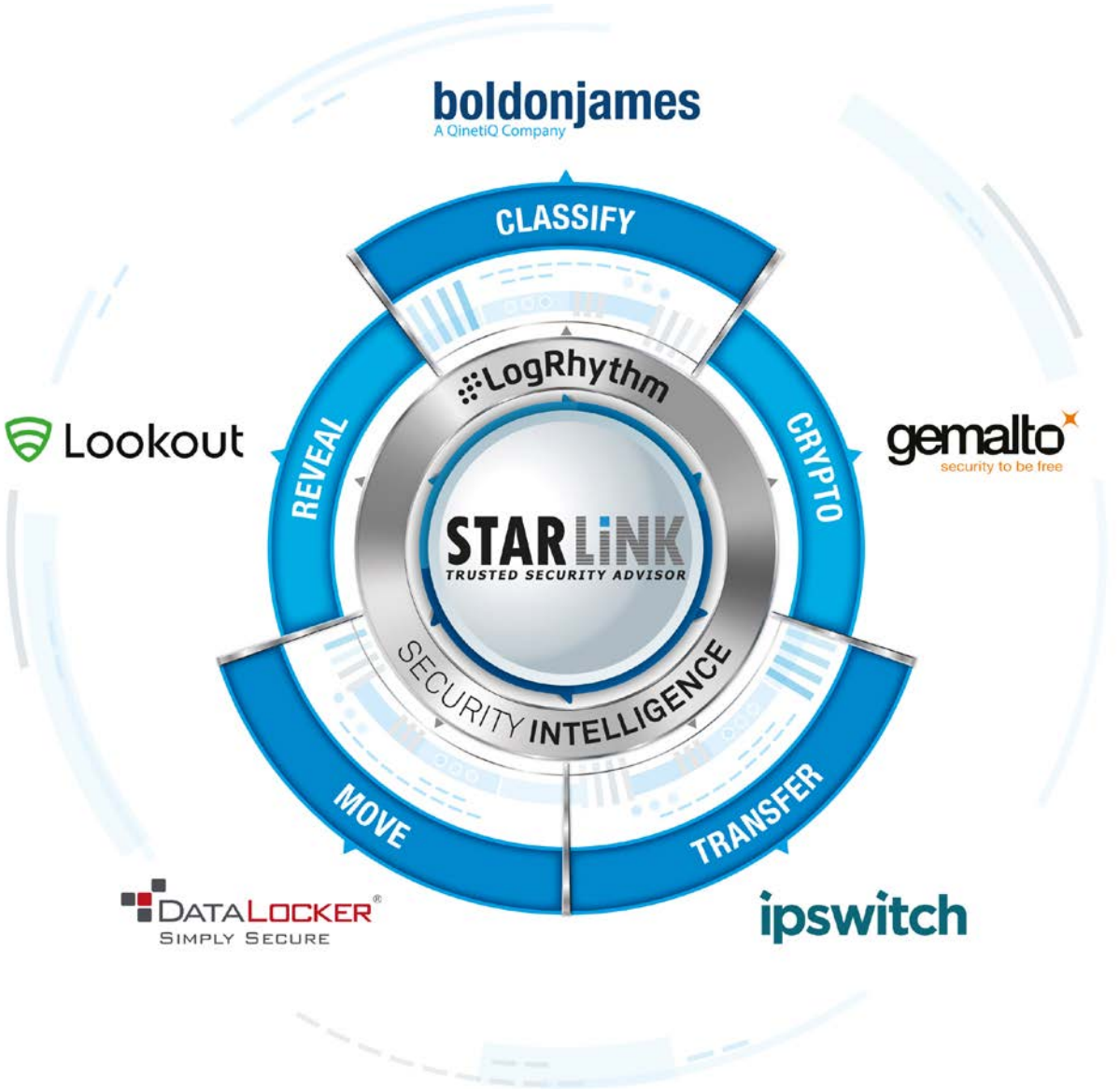
Advanced Threat Prevention based on Artificial Intelligence

CYLANCE
cylance.com

Cylance® Consulting has one goal in mind – securing our clients as quickly as possible and maintaining a higher level of security via prevention using AI technology. Our team is comprised of industry-leading experts in the most advanced technologies. No one in the industry can bring more depth of services and expertise than Cylance PERIOD.

SMARTER SECURITY FASTER SERVICES

- Industrial Control Systems
- Internet of Things / Embedded Systems
- Red Team Services
- ThreatZERO™
- Incident Response & Compromise Assessments
- Training



Secure Mobility

How do I share my sensitive data?

Secure Mobility enables collaboration of sensitive data by putting platforms into place to ensure that managing mobile devices, sharing of files and distributing content is done securely, both internal, as well as, external to an organization, so that data cannot be maliciously or mistakenly leaked. It is even possible to control from which location inside an organization that a user can access sensitive data. Secure file sharing can seamlessly automate secure site-to-site and user-to-site transfers, as well as, use email to securely send and receive large attachments without restrictions. Finally sensitive data needs to be available today to the mission-critical workforce, 24x7 online, as well as offline. So portability being critical, trusted users can securely transport data, and even their entire workspace environment, on hardware-encrypted portable storage, with comprehensive management of this media.

User-Centric Data Classification

boldonjames
A QinetiQ Company

boldonjames.com

Boldon James Classifier empowers users, who create and handle data, to easily assign value to it in the form of visual and metadata labels. This is a key step in determining how the data is managed, protected and shared and fundamental to any organization's data security and management strategy. Critically, involving users in the classification process helps to foster a strong security culture that takes ownership for protecting sensitive data. Recently the company launched their latest product – Mac Classifier – becoming the first data classification vendor to extend capabilities to cover the Microsoft Office for Mac suite, including coverage for Outlook, Word, Excel and PowerPoint.

Key Benefits:

- Adds meaning to unstructured information
- Caters for legacy documents and files
- Automates routine classification tasks
- Improves quality of Data Governance
- Empowers Enterprise Search and e-Discovery
- Enhances Data Loss Prevention and Archiving

Multi-Factor Authentication, HSM's & Data Encryption

gemalto
security to be free

gemalto.com

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 digital identities, transactions, payments and data – from the edge to the core.

SafeNet delivers the breadth of solutions that enable security teams to centrally employ defense-in-depth strategies-and ultimately make sure encryption yields true security. If access controls are lacking, the efficacy of encryption can be compromised. If cryptographic keys are vulnerable, so is encrypted data.

To truly protect sensitive data, organizations must follow encryption best practices as well as establish a strong Crypto Foundation - an approach that incorporates crypto processing and acceleration, key storage, key management, and crypto resource management.

Along with a comprehensive set of encryption platforms, SafeNet delivers the robust access controls and key management capabilities that enable organizations to practically, cost effectively, and comprehensively leverage encryption to address their security objectives.

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.

Secure Managed File Transfer & Large-File Email Bypass

ipswitch.com

MOVEit Managed File Transfer: Today's businesses share more information electronically than ever before between their business partners, customers, and employees. Ipswitch's MOVEit Managed File Transfer (MFT) System is the best way to reliably move that information in a timely, controlled, and secure manner to improve business productivity, meet SLAs and compliance requirements, and gain visibility and control of file movement.

MOVEit File Transfer: MOVEit File Transfer server is the reliable and secure hub that IT needs to transfer the organization's business files. With its broad protocol support, MOVEit File Transfer server connects with any system, server or client. Using the latest security technologies, it protects files both in transit and at rest. And as part of the MOVEit Managed File Transfer System, MOVEit File Transfer gives IT the visibility and control they need to confidently meet SLAs and compliance requirements.

MOVEit Central: MOVEit Central enables you to easily automate your file-based workflows. MOVEit Central provides a simple but powerful user interface for defining business workflows that's easy enough for anyone on your IT team to use because no scripting is required. The heart of MOVEit Central is a reliable workflow engine that ensures the predictable, secure delivery of your business files. Plus, a powerful centralized console ensures you'll have visibility and control over all file movements. That is why hundreds of companies, including many in healthcare and finance have turned to MOVEit Central to automate their file-based workflows and confidently meet their SLAs and compliance requirements.

MOVEit Mobile: IT departments want to give users the ability to transfer work files using their mobile devices while keeping the enterprise security they rely on with MOVEit. They want to allow users to upload and download files from either iOS or Android phones and tablets. Most importantly, they want to extend the secure, compliant, file-based processes to people when they are mobile. MOVEit Mobile enables mobile workers to reliably and productively participate in file-based business process workflows, while providing IT the security, visibility and control required to confidently run their business and meet compliance requirements.

MOVEit Ad Hoc: To get their work done employees are circumventing IT by turning to new, web-based consumer services to send and receive files, creating control, visibility, and security challenges for the business. MOVEit Ad Hoc Transfer offers employees and businesses a better alternative.

For employees, MOVEit Ad Hoc Transfer enables easy transfer of files of any size using a familiar interface: either Microsoft Outlook or a web browser. For IT, MOVEit Ad Hoc Transfer provides the comfort of knowing sensitive business files are being sent and received through a secure, enterprise-class Managed File Transfer system. Plus, the system relieves your email and storage systems from the burden of transferring and storing large files.

Data Encryption Solutions

datalocker.com

DataLocker is an innovative provider of encryption solutions. The company was founded in 2007 and has offices in the U.S. (headquarters), U.K., and Korea.

- Secure By Design: DataLocker products secure sensitive data using military-grade 256-bit encryption. With a wide range of products, DataLocker offers both hardware based external storage and software based cloud storage encryption options. Hardware based products do not require software or drivers to manage, encrypt or decrypt data.
- Compliance Driven: DataLocker technology makes it simple to ensure compliance with some of the strictest governmental regulations. Most DataLocker products are FIPS 140-2 validated, issued by the National Institute of Standards and Technology (NIST). FIPS validated DataLocker products are a cost-effective way to comply with HIPAA, SOX, DHS Initiatives, NRC, GLB and any other directive that requires data encryption.
- Proven Protection: DataLocker is trusted by governments, military and enterprises around the world. Other industries, including legal, financial and healthcare, use DataLocker products to secure, store, and transfer confidential data. To request a sample contact sales@datalocker.com.

DataLocker products combine superior convenience and usability with state of the art security. DataLocker is "Simply Secure."

Mobile Endpoint Security

lookout.com

Many organizations are now embracing the use of smartphones and tablets to increase productivity in the workplace. However, this era of mobility introduces new risks to enterprise data. Lookout Mobile Endpoint Security enables secure mobility by providing comprehensive risk management across iOS and Android devices to protect against app, network, and device-based threats while providing visibility and control over data leakage.

Productivity without compromise

We empower your organization to fully adopt secure mobility across personal and corporate owned devices without compromising productivity, employee privacy, or user experience

Data leakage control

Lookout allows you to set policies against non-compliant mobile apps that pose a data leakage risk

Threat protection

Lookout protects your organization from mobile threats across apps, network, and device

Proven risk reduction

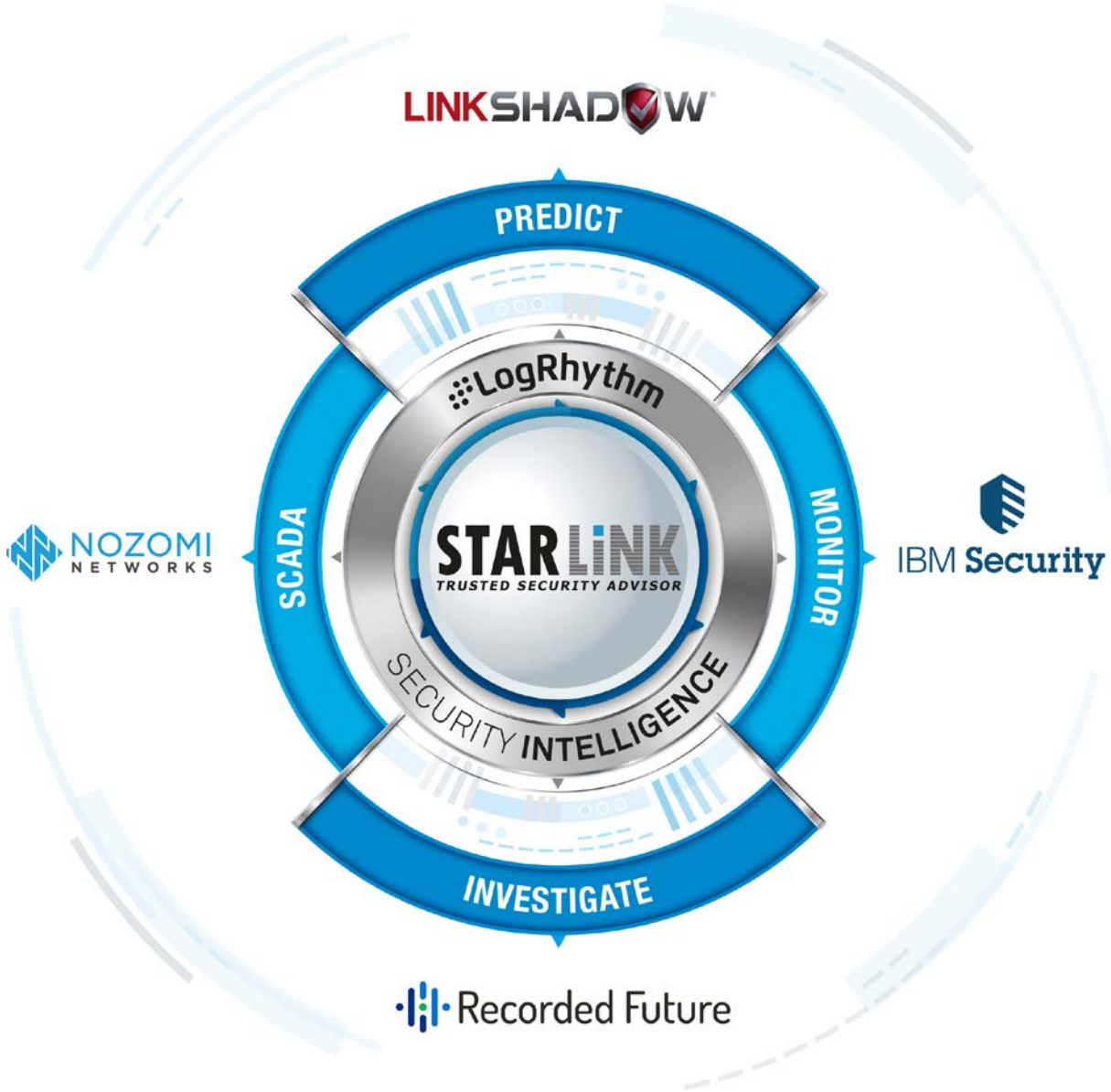
Forward-thinking organizations have achieved measurable risk reduction with Lookout Mobile Endpoint Security

Low TCO

Integrates with your existing EMM solution to seamlessly deploy the Lookout app, with a 95% self-remediation rate to limit helpdesk tickets

Respects user privacy

Lookout collects the minimum amount of personal information to protect both personally owned and corporate-owned devices



Incident Response

Has my sensitive data been breached?

Incident Response involves the monitoring and detection of security events, and the execution of proper remediation. Breaches can be mitigated with real-time, dynamic threat protection across the different stages of the kill chain. To be prepared to respond to modern malware in real-time and disrupt adversary behavior, sandboxing, endpoint detection, and threat intelligence are critical to identify and block cyber threats. Simultaneously self-learning intelligence of network nodes and users, as well as, behavioral analytics on endpoints, enable the validation of emerging zero-day threats that bypass other security controls, by correlating this information in order to identify outliers that indicate in-progress attacks. Finally, effective investigation and analysis of intrusions gives organizations the ability to pinpoint the root cause, the scope of the breach, the data loss, and the steps required to contain the breach, and enhance the adaptive threat response process to achieve automation.

The Next-generation Cybersecurity Analytics

LINKSHADOW

linkshadow.com

LinkShadow is designed to manage threats in real-time with attacker behavioral analysis which is meant for organizations that are looking to enhance their defenses against advanced cyber-attacks, zero-day malware and ransomware, while simultaneously gaining rapid insight into the effectiveness of their existing security investments.

AttackScape Viewer

TrafficSense Visualizer

ThreatScore Quadrant

Identity Intelligence

Asset AutoDiscovery

BlockCount Ratio

Integrated Security Solution

IBM Security

ibm.com/security

IBM integrated security intelligence protects businesses around the world.

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.

From infrastructure, data and application protection to cloud and managed security services, IBM has the expertise to help safeguard your company's critical assets. We protect some of the most sophisticated networks in the world, and employ some of the best minds in the business.

Identify - Build a secure enterprise with increased visibility

Risk Management and Compliance Services help you evaluate your existing security practices-including payment card industry (PCI) security, identity and IT regulatory compliance needs and gaps- against your business requirements and objectives. Our skilled security specialists provide recommendations to help you make more informed decisions about allocating your resources to better manage security risks and compliance. We can deliver a wide range of capabilities-from security program development, to regulatory and standards compliance, to security education and training.

Protect - Arm yourself to prevent attacks before they start

IBM identity and access management services target virtually every aspect of identity and access management across your enterprise, including user provisioning, web access management, enterprise single sign-on, multi-factor authentication, and user activity compliance. We offer a range of service options - from migration to consulting to fully managed services - that leverage IBM's leading security tools, technologies, and expertise. Our security specialists work with you to address your individual needs and provide the solutions that best match your business and security objectives.

Respond - Stop attacks in their tracks and mitigate exposure

IBM's Cybersecurity Assessment and Response services are designed to help you prepare for and more rapidly respond to an ever-growing variety of security threats. Our seasoned consultants deliver cybersecurity assessments, planning and response services, with proven expertise from mainframe to mobile.

Real-time Threat Intelligence

Recorded Future

recordedfuture.com

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 open Web to give you unmatched insight into emerging threats. Recorded Future helps protect four of the top five companies in the world.

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

Why Recorded Future

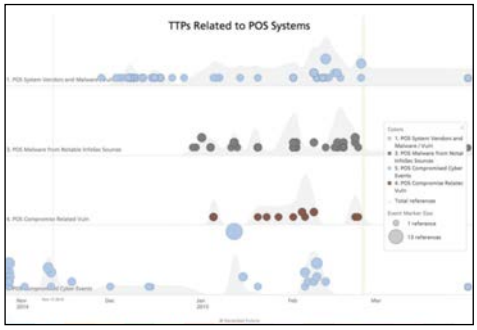
Faster Analysis:
Spend less time collecting data and supercharge your analytic capacity.

Cut the Middleman:
Direct access to billions of data points from the open, deep and dark Web for superior context.

Real-Time Monitoring:
Alerts to direct threats. Share live reports. Enrich your SIEM.

Relevant Intel:
Tailored to your environment, technology infrastructure, and corporate profile.

"Recorded Future gives us incredible context and insight into potential threats."
Dave Ockwell-Jenner, Sr. Manager, Security Threat & Operational Risk Mgmt., SITA



A timeline view enables analysts to visualize emerging trends for proactive security.

Real-time Visibility for Industrial Control Networks

NOZOMI NETWORKS

nozominetworks.com

Nozomi Networks has been delivering innovative 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.

Having gained traction and experience with large industrial enterprises, the company is now poised for growth. It is increasing its product development as well as its sales and marketing efforts to address the opportunity that exists in the emerging operational technology (OT) security market.

Total Visibility, Smart Detection, Accelerated Response

LogRhythm
The Security Intelligence Company

logrhythm.com

LogRhythm, a leader in security intelligence and analytics, empowers organizations around the globe to rapidly detect, respond to and neutralize damaging cyber threats. The company's patented award-winning platform uniquely unifies next-generation SIEM, log management, network and endpoint monitoring, and advanced security analytics. In addition to protecting customers from the risks associated with cyber threats, LogRhythm provides unparalleled compliance automation and assurance, and enhanced IT intelligence.

LogRhythm is consistently recognized as a market leader. The company has been positioned as a Leader in Gartner's SIEM Magic Quadrant report for five consecutive years, named a 'Champion' in Info-Tech Research Group's 2014-15 SIEM Vendor Landscape report, received SC Labs 'Recommended' 5-Star rating for SIEM and UTM for 2016 and earned Frost & Sullivan's 2015 Global Security Information and Event Management (SIEM) Enabling Technology Leadership Award.

LogRhythm's security intelligence and analytics platform enables organizations to detect, prioritize and neutralize cyber threats that penetrate the perimeter or originate from within.

Detect, prioritize and neutralize cyber threats that penetrate the perimeter or originate from within with;

- Next-Gen SIEM - Unified platform for advanced detection & response
- Security Analytics - Holistic threat analytics & compliance automation
- Log Management - Centralized visibility into all log and machine data, at any scale
- Network Forensics - Real-time deep packet analytics and full capture
- Endpoint Monitoring - Real-time user, file application and system behavior monitoring

2200+ Customers in the META

StarLink's strong base of customers includes leading financial institutions, the largest telecommunications and energy companies, as well as, high-profile government organizations. StarLink helps these organizations achieve and sustain compliance and optimally manage risks through full policy, procedure and controls lifecycle management. StarLink's solution offerings are now installed in more than 1000 data centers in the region, including 50 of the top regional banks, 15 of the region's top Telcos, 100 of region's top energy companies and 200 government entities. Our customers trust StarLink to secure their critical enterprise data and safeguard access to sensitive data in the most demanding datacenter environments by monitoring, securing and auditing privileged user access to provide 100% visibility on all activities.

Customer Testimonials:

Saudi Hollandi Bank Implements e-DMZ Security to Manage Privileged Users' Password and Monitor Remote Access Activities

"We chose the Password Auto Repository (PAR) and eGuardPost (eGP) from e-DMZ Security because it was uniquely designed to solve enterprise security and compliance issues associated with the management and control of shared privileged passwords such as root and administrator. The issue of Privileged Password Management and the unique features of PAR contribute directly to many specific PCI requirements," said Ali Alotaibi, IT Security Manager, Saudi Hollandi Bank.

National Bank of Kuwait Implements Guardium to Prevent Unauthorized Database Changes by "Super Users"

"We chose Guardium because they have become the 'gold standard' for database security and monitoring," said Tamer Gamali, Chief Information Security Officer (CISO), National Bank of Kuwait. "We needed tighter internal controls over our critical Oracle and Microsoft SQL Server-based Financial Systems. We considered solutions based on native database auditing, but Guardium gives us automated, real-time security alerts along with full visibility into all transactions without impacting database performance. It also provides a scalable, cross-DBMS audit architecture for handling the massive amounts of transactions in our large-scale heterogeneous data centers."

Abu Dhabi Commercial Bank Implements Guardium to Strengthen Database Controls

"We were seeking a unified, cross-DBMS solution that delivers granular, real-time controls without the complexity, overhead and risk of native DBMS-resident auditing, and Guardium fulfilled all our requirements. Our goal is to ensure that critical information is stored securely through the adoption of best-of-breed technologies." said Steve Dulvin, Head of IT Security at Abu Dhabi Commercial Bank.

Customer Success Services

Customer Success Services

Customers implementing IT Security technologies depend on expert technical services and support professionals that understand the challenges being addressed and the business impact, and then provide action in a timely manner to achieve successful deployments.

StarLink Customer Success Services comprises of a highly skilled team of IT Security Consultants offering remote and onsite advanced technical services to customers via Channel Partners.

In order to ensure continued customer success, SCS also offers a centralized approach to provide simplified and preventive IT sustenance post project closure.

The SCS portfolio includes Security Consulting Services, 24x7 Technical Support, Certified Training Services, Managed Security Services, Security Outsourcing Engineering.