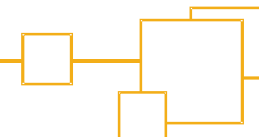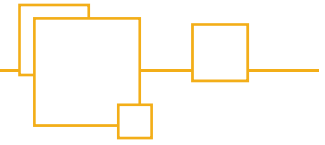# Managing Security and Access Control of SOA Services

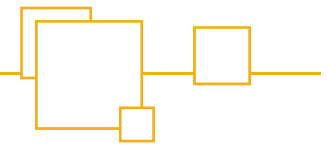- Michal Opatřil
- Junior solution architect

# Agenda

- SOA Services World Wide Adaptation
- SOA Services needs IAM
- SOA Services versus traditional Web Access
- Security and Architecture Mistakes
- Customer requirements
- CA SOA Security Manager as SOA solution
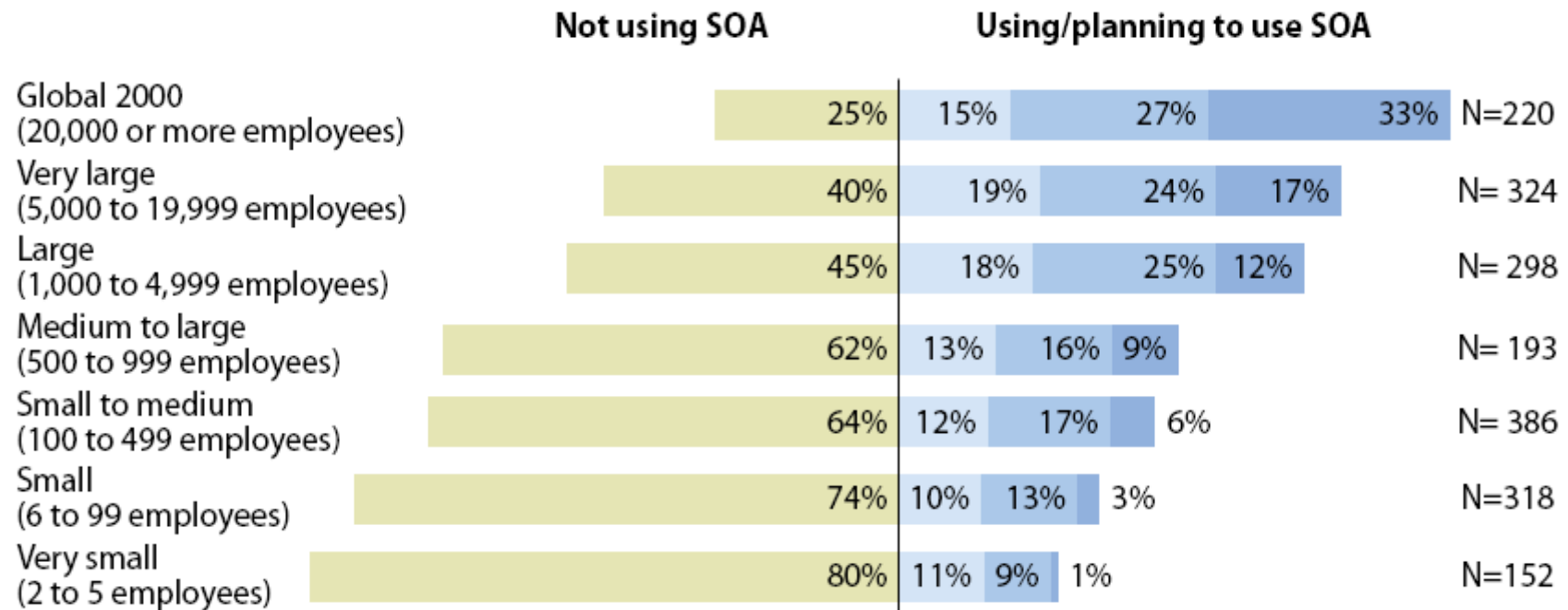- Practical Architecture

**Corinex Group**

# Services Adoption is Expanding

## Enterprise SOA Penetration Reaches 75% in Global 2000 Firms

"Which of the following best describes your firm's approach to,
or use of, service-oriented architecture (SOA)?"

Not pursuing and have no
immediate plans to do so

Will pursue
within 12 months

We use selectively, without a clear
strategy

We use with an enterprise-level
strategy for and commitment to SOA

**Not using SOA**      **Using/planning to use SOA**

| | Not using SOA | Will pursue | We use selectively | Enterprise-level | |
|---|---|---|---|---|---|
| Global 2000 (20,000 or more employees) | 25% | 15% | 27% | 33% | N=220 |
| Very large (5,000 to 19,999 employees) | 40% | 19% | 24% | 17% | N= 324 |
| Large (1,000 to 4,999 employees) | 45% | 18% | 25% | 12% | N= 298 |
| Medium to large (500 to 999 employees) | 62% | 13% | 16% | 9% | N= 193 |
| Small to medium (100 to 499 employees) | 64% | 12% | 17% | 6% | N= 386 |
| Small (6 to 99 employees) | 74% | 10% | 13% | 3% | N=318 |
| Very small (2 to 5 employees) | 80% | 11% | 9% | 1% | N=152 |

(percentages may not total 100 because of rounding)

Base: decision-makers at North American and European enterprises and SMBs

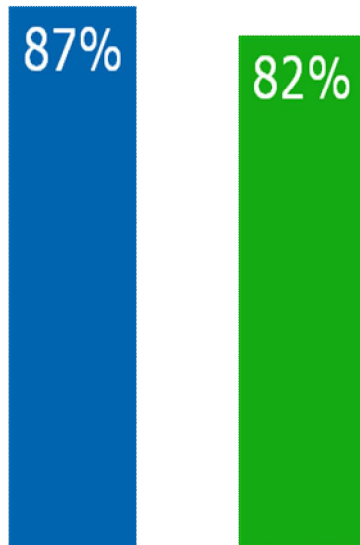Source: "SOA Is Far From Dead - But It Should Be Buried", Forrester Research, Inc., May 2009.

Corinex Group

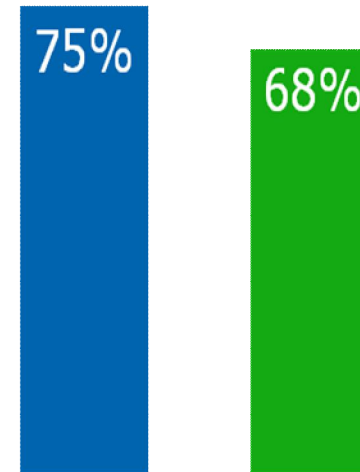# Organizations Have both Internal and External Services
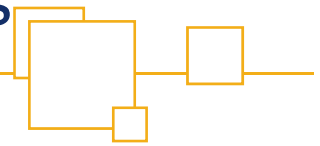
## INTERNALLY FACING



87% — Web Services
82% — SOA

## EXTERNALLY FACING



75% — Web Services
68% — SOA

1b./2b. Are any of the SOA/Web service implementation(s) at your organization internally facing — that is, meant to serve the application needs of your organization's employees?
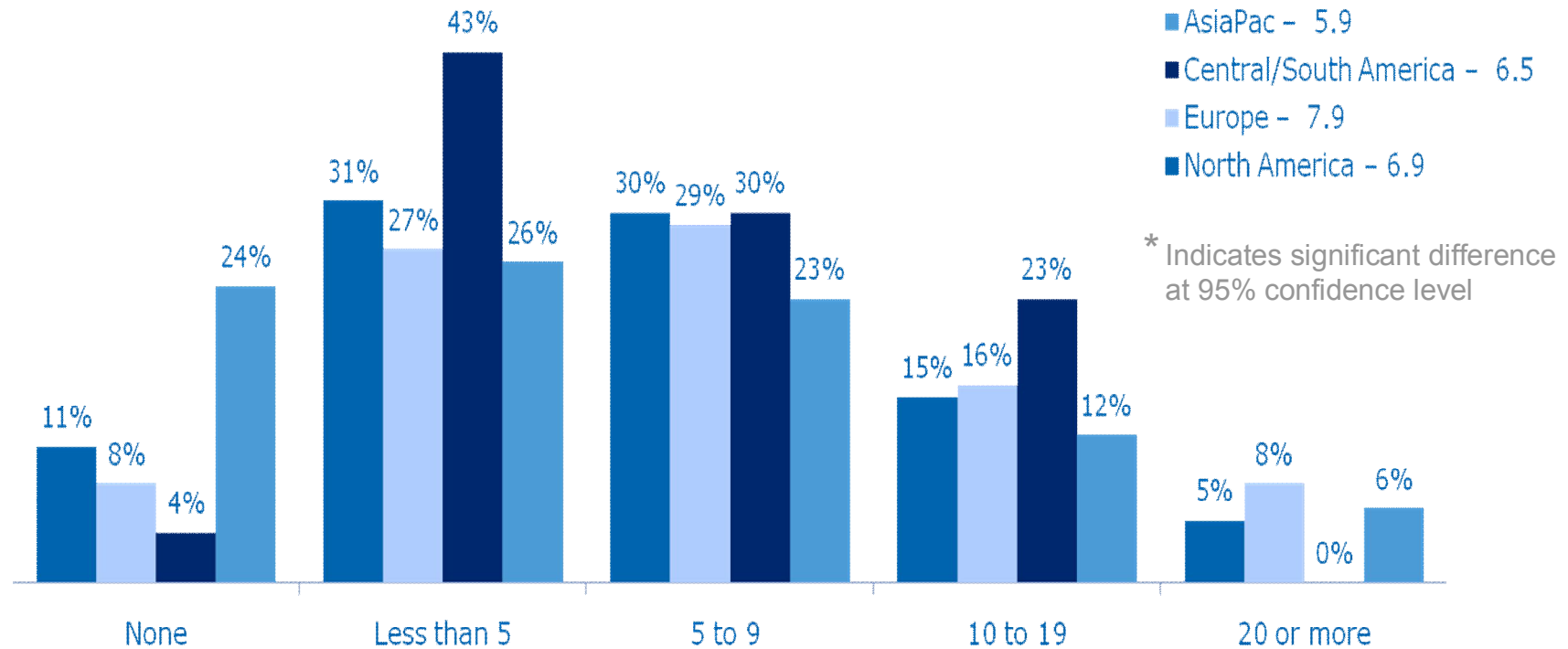
1c./2c. Are any of the SOA/Web service implementation(s) at your organization externally facing — that is, meant to serve the application needs of your organization's customers, partners, suppliers or other external stakeholders?

**Corinex Group**

# Web Services Are at Risk
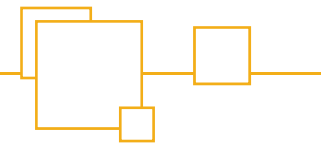
On average, SOA-based/Web services
IT executives are aware of 7 significant XML-targeted threats in
the past year



Legend:
- AsiaPac – 5.9
- Central/South America – 6.5
- Europe – 7.9
- North America – 6.9

\* Indicates significant difference at 95% confidence level

Chart data:

| Category | AsiaPac | Europe | Central/South America | North America |
|----------|---------|--------|----------------------|---------------|
| None | 11% | 8% | 4% | 24% |
| Less than 5 | 31% | 27% | 43% | 26% |
| 5 to 9 | 30% | 29% | 30% | 23% |
| 10 to 19 | 15% | 16% | 23% | 12% |
| 20 or more | 5% | 8% | 0% | 6% |

6b. In the past year, how many XML targeted threats or other malware attacks
have your SOA-based or Web services solutions experienced?

**Corinex Group**

# Integration with IAM solution is critical

**Highly critical
32%**

**Not critical
7%**

**Somewhat
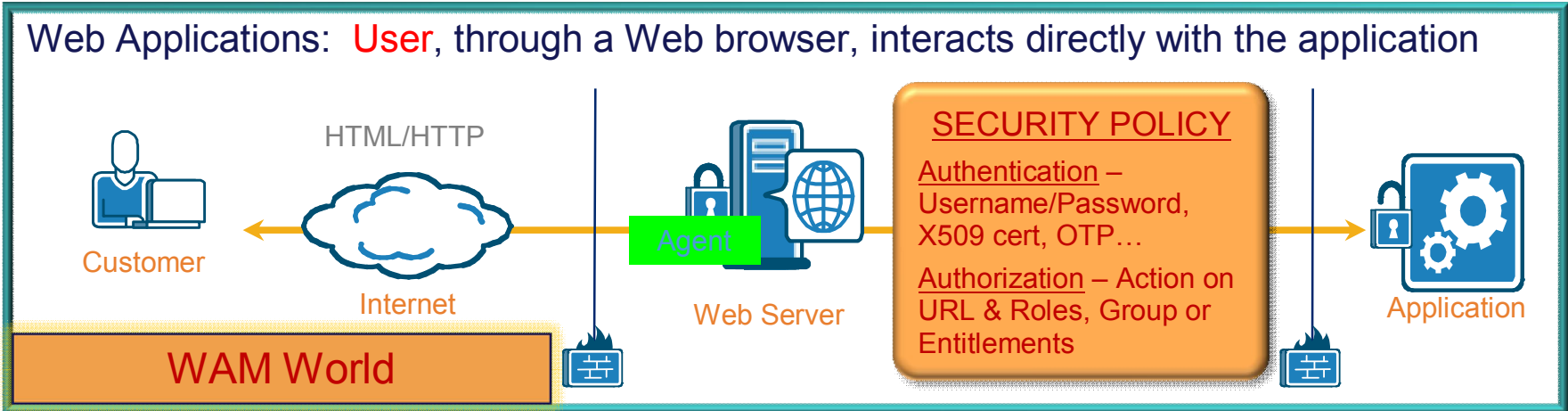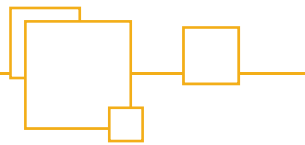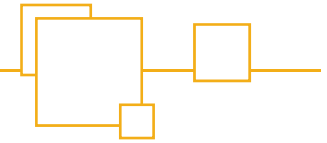critical
61%**
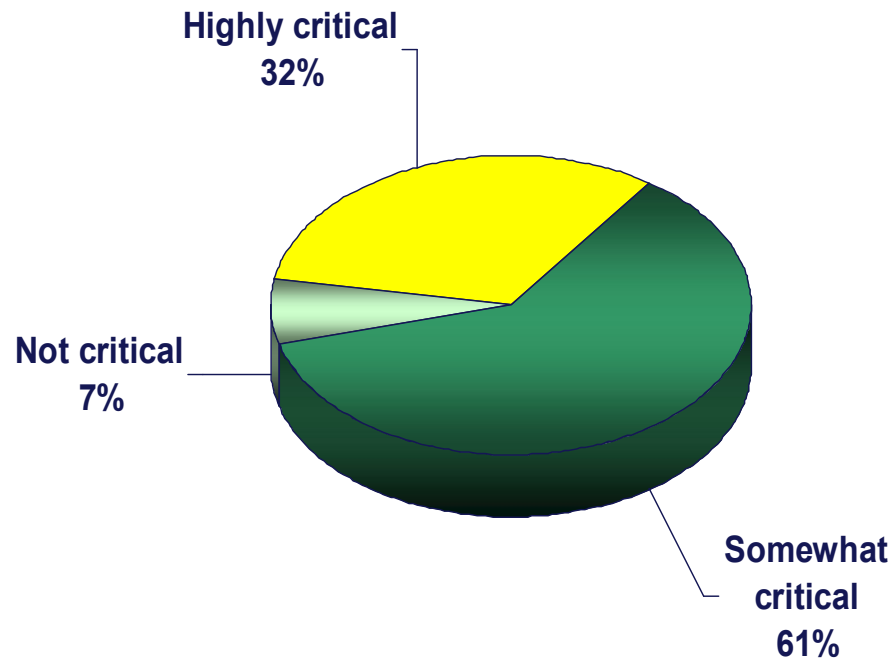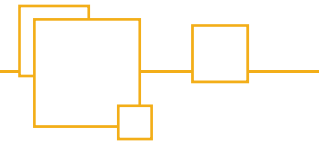
The vast majority of organizations believe integrating SOA-based/Web services security solutions with IAM is critical.

**Corinex Group**

# Securing Web Applications & SOA Services

## Web Applications: User, through a Web browser, interacts directly with the application

HTML/HTTP

Customer

Internet

Agent

Web Server

**SECURITY POLICY**

Authentication – Username/Password, X509 cert, OTP…

Authorization – Action on URL & Roles, Group or Entitlements

Application

**WAM World**

## SOA Services: Service/Application, often acting on behalf of the user, interacts with the Web service

XML/HTTP, FTP, JMS, MQ

XML/SOAP

Web Service Consumer

Internet

Gateways

XML Gateways

**SECURITY POLICY**

Authentication –

WS-Security Tokens (SAML, X509, uname), XML-DSig, XML-Enc

Authorization – Action on URI, XML Content, WS operations, Role, Group or Entitlements

Agent

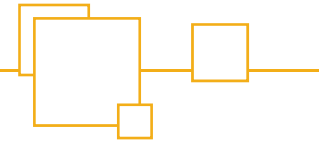Web Services

**SOA World**

*Corinex Group*

# Typical SOA/WS Security Mistakes

- **Architecting „Silos of Security"**
  - ■ Building security into each service
  - ■ Corollary – Leaving security to the application developers

- **Thinking that stopping threats/malware = effective security management**
  - ■ Corollary - Forgetting that "identity" matters with services
  - ■ Authentication, authorization, centralized auditing, SSO, federation, identity administration

- **Not understanding that Services have many layers/steps that need to be secured**
  - ■ Corollary – Thinking that guarding the "front door" is enough
  - ■ Corollary – Thinking that point-to-point (SSL) security is enough

**Corinex Group**

# Customer Requirements

- Centrally managed SOA services authentication
- Centrally managed SOA services authorization
- Authentication against specific application or more applications
- Securing heterogeneous applications
- Platform independent (.NET, JAVA, Microsoft, Linux/Unix)
- Support of various web servers (e.g. IIS, Apache)
- Support of various application servers (e.g. WebSphere, Weblogic, Jboss)
- Highly scalable and powerful solution
- Manage millions of identities

**Corinex Group**

# CA SOA Security Manager
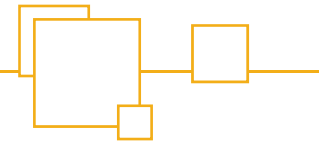
- **Content-based authentication**
  - ■ WS-Security – Username, X509, SAML (XML Encryption/Signing)
  - ■ XML Document Credentials Collector (DCC)
  - ■ XML Digital Signature
  - ■ SAML Session Ticket
- **Dynamic authorization policy model**
  - ■ Authorize based on XML variables in policy expressions
- **XML Threat prevention, routing, transformation, SLA monitoring**
- **Session synchronization**
  - ■ Enables single sign-on across multiple web services
- **Credential mapping**
  - ■ WS-Security header generation
  - ■ SAML Session ticket generation

**Corinex Group**

# SOA Managed Security Architecture
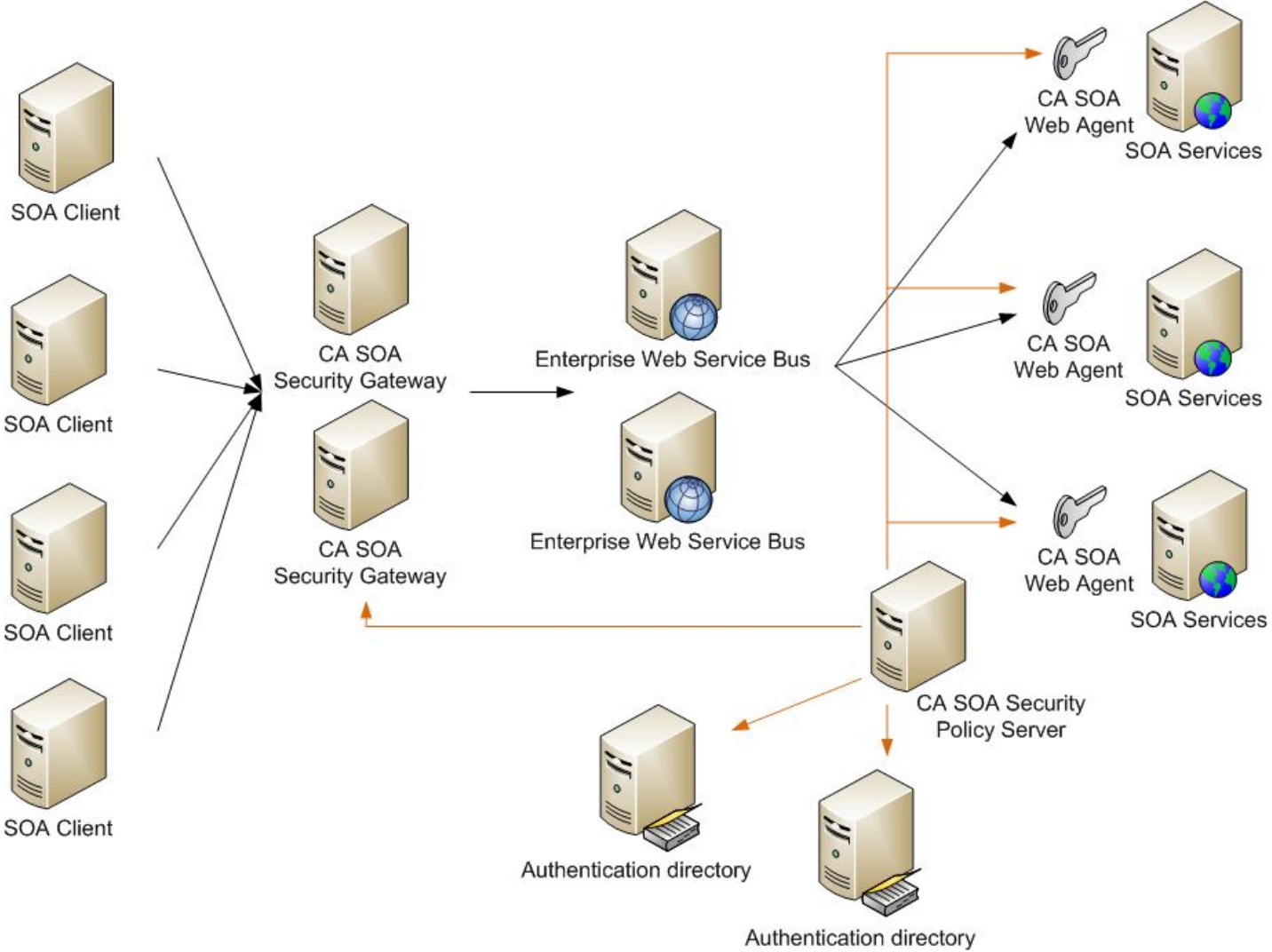
# Conclusion
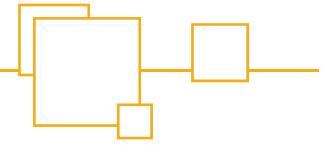
- End-to-End security for SOA infrastructure
- Multi-layer security
- Full integration with the IAM solution
- Various authentication schemas
- XML firewalling
- Centrally managed

**Corinex Group**